UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

Magistrsko delo

Virtualna ekonomija v igrah in kriptovalute

(Virtual economy in games and cryptocurrencies)

Ime in priimek: Gašper Moderc
Študijski program: Računalništvo in informatika, 2. stopnja
Mentor: izr. prof. dr. Jernej Vičič
Somentor: asist. Aleksandar Tošić

Koper, junij 2020

Ključna dokumentacijska informacija

Ime in PRIIMEK: Gašper MODERC

Naslov magistrskega dela: Virtualna ekonomija v igrah in kriptovalute

Kraj: Koper

Leto: 2020

Število listov: 104 Število slik: 41 Število tabel: 5

Število referenc: 60 Število prilog: 3 Število strani prilog: 3

Mentor: izr. prof. dr. Jernej Vičič

Somentor: asist. Aleksandar Tošić

UDK: 004.738.5:336.74(043.2)

Ključne besede: Virutalna ekonomija, kriptovaluta, blockchain, razvoj iger

Izvleček: V magistrskem delu je opisana realizacija sistema za vzpostavitev virtualne ekonomije znotraj igre s pomočjo digitalnih kovancev. Uporabljene tehnologije so bile: igralni pogon Unity 3D in tehnologija Enjin, ki temelji na tehnologiji veriženja blokov *Ethereum*. Magistrsko delo se začne z zgodovino razvoja blockchain tehnologije. Nadaljuje se z izčrpnim opisom lastnosti tehnologije veriženja blokov. Podrobno je predstavljena tudi platforma Ethereum in koncept pametnih pogodb. Sledi zgodovina računalniških iger, njihovega izdelovanja ter povezav s tehnologijo blockchain. Predstavljena je tudi implementacija igre, ki je predmet raziskave, ter uporaba Ethereum dobrin znotraj igre. Na koncu je podana analiza rezultatov testiranja programa, ki je bila narejena po uspešnem testiranju.

Key words documentation

Name and SURNAME: Gašper MODERC

Title of the thesis: Virtual economy in games and cryptocurrencies

Place: Koper

Year: 2020

Number of pages: 104 Number of figures: 41 Number of tables: 5

Number of references: 60 Number of appendices: 3

Number of appendix pages: 3

Mentor: Assist. Prof. Jernej Vičič, PhD

Co-mentor: Assist. Aleksandar Tošić

UDK: 004.738.5:336.74(043.2)

Keywords: Virtual economy, cryptocurrency, blockchain, game development

Abstract: In the thesis we present an implementation of a tokenized in-game virtual economy based on blockchain technology. The implementation is based on the Unity game engine and the Enjin project based on the Ethereum blockchain. We begin by providing a historical view on blockchain technology which is continued by a detailed description of the inner workings of blockchains in general followed by a greater emphasis on Ethereum. We introduce a short history of computer games and their connection with blockchain technology. Our implementation is presented as a proof of concept which was used to perform experiments with groups of testers. To conclude, we present results from performed tests.

Kazalo vsebine

Kazalo preglednic

Kazalo slik

Kazalo prilog

Seznam kratic

DDoS	Distributed Denial-Of-Service (porazdeljeno onesposabljanje storitev)
ERC	Ethereum Request For Comment (Ethereum zahteva po komentarju)
DeFi	Decentralizing Finance (decentralizirani finančni sistem)
ETC	Ethereum Coin (kovanec Ethereum)
IoT	Internet Of Things (internet stvari)
SHA	Secure Hash Algorithms (varni zgoščevalni algoritmi)
P2P	Peer-To-Peer (omrežje enak z enakim)
UTXO	Unspent Transaction Output (neizkoriščeni izhodi transakcij)
PoW	Proof Of Work (dokaz o opravljenem delu)
PoS	Proof Of Stake (dokaz o zastavljenih sredstvih)
DPoS	Delegated Proof Of Stake (delegiran dokaz o zastavljenih sredstvih)
UI	User Interface (uporabniški vmesnik)
UX	User Experience (uporabniška izkušnja)
OS	Operating System (operacijski sistem)
RPC	Remote Procedure Call (klic oddaljene procedure)
SDK	Software Development Kit (programska oprema za pomoč pri razvoju)
UML	Unified Modeling Language (poenoteni jezik modeliranja)
GraphQL	Graph Query Language (jezik za poizvedbe na grafih)
JSON	JavaScript Object Notation (objektna notacija za JavaScript)
ENJ	Enjin Coin (kovanec Enjin)
FAMNIT	Fakulteta za matematiko, naravoslovje in informacijske tehnologije

Zahvala

Zahvaljujem se mentorju, dr. Jerneju Vičiču, in somentorju, mag. Aleksandru Tošiću, za pomoč pri izdelavi, moralni podpori in strokovnemu pregledu magistrskega dela. Zahvaljujem se tudi Fakulteti za matematiko, naravoslovje in informacijske tehnologije Koper za dovoljenje uporabe prostorov in računalniške opreme za izvedbo testiranj. Zahvaljujem se tudi vsem udeležencem testiranj, ki so končno izvedbo preizkusili in ocenili.

1 Uvod

Na trgu se pojavlja vedno več različnih iger za široko paleto različnih igralskih platform. Igre postajajo heterogene, vsaka z različnimi pravili in dobrinami, ki so trenutno vezane samo na eno igro. Dokaz za imetje neke dobrine imajo zgolj razvijalci igre, tako da je lastnina igralcev odvisna od poštenosti razvijalcev. V zadnjem času se pojavljajo decentralizirane tehnologije kot ena izmed rešitev takšnih težav. Te tehnologije omogočajo neregulirano izmenjavo dobrin med udeleženci, dokaz o lastništvu dobrin, ki ga ima vsak udeleženec, in možnosti za razvoj trgovanja med različnimi aplikacijami.

Povezave med igrami in decentraliziranimi tehnologijami so se začele pojavljati, a so redke. Decentralizacija v igrah lahko uporabniku omogoča:

1. neregulirano tržišče za izmenjavo dobrin;
2. izmenjava dobrin brez plačevanja dodatnih davkov;
3. večjo varnost nad dobrinami, saj so decentralizirana omrežja odporna na najrazličnejše napade;
4. enostavno izmenjavo dobrin preko poljubnih decentraliziranih menjalnic.

Po drugi strani se izdelovalci iger ob vpeljevanju decentraliziranih tehnologij srečujejo z velikimi težavami. Najpogostejše težave so:

1. pomanjkanje dokumentacije za tehnologije, saj so vse decentralizirane tehnologije mlade;
2. hitrostne, prostorske in funkcionalne omejitve, ki jih predstavlja decentralizirana tehnologija;
3. nezmožnost spreminjanja pogodb. Ko se pogodba enkrat sprejme in odda v sistem, je ni mogoče nikoli več popravljati, niti če se v njej zaznajo napake;
4. nezmožnost spreminjanja dobrin, ki jih uporabnik skozi igro pridobi – ko se dobrina zapiše, ostane za vedno nespremenjena.

V tem delu bo predstavljen specifičen primer vzpostavljanja sistema za izmenjavo dobrin med igralci določene igre. Obstajati mora taka igra, ki bo hkrati omogočala pridobivanje novih dobrin, uporabo le-teh v igri in tudi izmenjavo dobrin med igralci.

Vse dobrine, ki so pridobljene v igri, se zapišejo v verigo blokov, ki določa, komu pripada kakšna dobrina v igri. Za vsako dobrino, ki obstaja, je mogoče preveriti, kdo je njen lastnik. Podatki na verigi so javni, kar pomeni, da jih lahko vsi pregledajo. S tem lahko vsi uporabniki preverijo lastništvo dobrine nekega igralca, ki je predstavljen

z nekim identifikatorjem.

Izmenjava dobrin je mogoča brez uporabe takšnega sistema. Vsak igralec lahko naloži aplikacijo, ki prikazuje njegove dobrine v nekem sistemu. Take aplikacije imenujemo digitalne denarnice. Te lahko uporabnik poveže z računom in dostopa do vseh dobrin, ki so njegova last. Te dobrine lahko izmenjuje z ostalimi uporabniki, ki uporabljajo ta sistem. Izmenjava lahko poteka bodisi direktno preko digitalne denarnice, ko uporabnik pošlje nekaj dobrin drugemu uporabniku, bodisi preko obstoječih spletnih strani namenjenih izmenjavi decentraliziranih dobrin.

V splošnem delimo dobrine za igralce decentraliziranih iger na dve vrsti: medsebojno zamenljive in medsebojno nezamenljive. Razlika med tema dvema dobrinama je v tem, da če ima uporabnik več medsebojno zamenljivih dobrin, jih ne more med sabo razločiti. Primer takih dobrin so zlatniki v večini iger, saj je igralcu pomembna zgolj količina zlatnikov, ki jih zapravi. Nasprotno se da razločiti med čisto vsako medsebojno nezamenljivo dobrino, v igri pa imajo lahko različne funkcije in možnosti uporabe.

Sprva so se v igrah, temelječih na tehnologiji blockchain, pojavljale samo medsebojno zamenljive dobrine, saj takrat ni obstajal sistem, ki bi lahko ločil med temi dobrinami. Možnost razločevanja med njimi je omogočil standard ERC-1155, ki bo podrobneje opisan v razdelku 4 tega magistrskega dela. Uporabljen je bil tudi pri implementaciji medsebojno nezamenljivih dobrin v programu, izdelanem v okviru tega magistrskega dela.

Ideja tega programa je v tem, da skuša igralcem ponuditi poljubno število blockchain dobrin, ki jih lahko pridobijo v igri. Te dobrine lahko uporabniki prosto izmenjujejo med seboj in s tem polnijo zbirko virtualnih dobrin. Prikazano bo, kako je bilo to implementirano v programu s pomočjo platforme Enjin, ki temelji na blockchain tehnologiji Ethereum.

V prvi fazi je bila izvedena raziskava obstoječih tehnologij na tržišču, ki so namenjene izdelavi računalniških iger. V raziskavi so bile vključene platforme Enjin [15], Funfair [59], Decentraland [14] in Loom Network [38]. Izvlečkom raziskave in njeni analizi je namenjen razdelek 5, ki izčrpno primerja te tehnologije in njihovo ustreznost za izdelavo trgovine za izmenjavo dobrin med igrami.

Novi standardi in protokoli za tehnologije, ki temeljijo na platformi Ethereum, so omogočili možnost ustvarjanja unikatnih dobrin. Pomemben standard je bil ERC-721, ki bo podrobneje predstavljen v razdelku 4. Ta standard omogoča medsebojno razločevanje kovancev, iz česar sledi, da se da medsebojno razpoznavati tudi dobrine, ki jih ti kovanci predstavljajo. Ker ima vsak kovanec unikatno identifikacijo, lahko uporabnikom zagotovimo neponovljivost določenih dobrin. Neponovljivost lahko poveča povpraševanje po takih dobrinah in s tem narašča njihova vrednost – saj so unikatne v sistemu. S tem se odpre tudi možnost zbirateljstva v igrah, saj lahko igralci zbirajo dobrine predvsem za ustvarjanje lastne kolekcije in ne za uporabljanje dobrin v igri [24].

V tej implementaciji je bil prikazan tudi sistem za ustvarjanje unikatnih dobrin

in izmenjavo teh dobrin med igralci. Razvita je bila tudi delujoča povezava med instanco igre, strežnikom in verigo blokov, ki zagotavlja ustvarjanje poljubne količine medsebojno razločljivih dobrin. Delujoča različica te igre je bila testirana na javnem testiranju. Analiza testiranja in rezultati so predstavljeni v razdelku 7. Ta razdelek vsebuje tudi analizo izpolnjevanja zahtev igre, ki so predstavljeni v razdelku 6. V zaključku so podane morebitne nadgradnje sistema, ki bi ga lahko izboljšale in bodo preučene v nadaljnjem delu.

2 Zgodovina

V tem razdelku je opisan začetek ideje o tehnologiji blockchain. Najprej bodo prikazane težave, ki so spodbudile iskanje rešitve, nato bodo predstavljene kronološko urejene ovire pri implementaciji. Predstavljena bo najstarejša rešitev, ki je pogosto imenovana kot predhodnik današnje verige blokov, znana pod imenom Hash Cash. To je razvil Angleški znanstvenik Adam Black leta 1997 [5], [6]. Nato bo predstavljena tehnologija Bit gold, ki jo je razvil Ameriški znanstvenik Nicolas Szabo leta 1998 [56]. Nato bo predstavljena tehnologija Bit Cash, ki je usmerjena v nadzorovanje digitalne ekonomije. Nazadnje bo predstavljena slavna tehnologija Bitcoin, ki jo je razvila oseba pod psevdonimom Satoshi Nakamoto [50]. Omenjena tehnologija je na revolucionarni način rešila veliko problemov, ki so jih imele predhodne tehnologije.

2.1 Problematike trgovanja in spletnega bančništva

V tem podrazdelku so predstavljene problematike trgovanja in bančništva na spletu. To problematiko naj bi reševale različne tehnologije veriženja blokov. Problematike so obširne. Prej omenjena tehnologija Hash Cash je bila zasnovana za reševanje popolnoma drugačnega problema kot kasneje tehnologiji Bit Cash in Bitcoin. Hash Cash je ponujal rešitve za varovanje pred zlonamernimi napadi z namenom onesposobljenja storitev. Bit Cash in Bitcoin sta reševali probleme posrednikov pri elektronskem bančništvu, kupovanju itd.

Veliko držav je pred letom 1971 uporabljalo denar s podporo zlata. Tega leta je Ameriški predsednik Richard Nixon za boj proti inflaciji spremenil dolar iz prejšnjega sistema v fiat valuto [37]. Po tem dogodku denar ni bil več podprt z zlatom, ampak je imel vrednost samo zato, ker mu je bila vrednost pripisana iz strani oblasti. Ta sistem ni bil intuitiven in veliko ljudi ga je začelo zavračati, saj so menili, da je ta denar brez vrednosti. Dodaten pomislek je bila prevelika moč centralnih bank, ki so tiskale denar in mu pripisovale vrednost.

2.1.1 Napadi z namenom onesposobljenja storitev – DDoS in Hash Cash

Glavni razlog za nastanek tehnologije Hash Cash leta 1998 je bil porast DDoS (Distributed Denial of Service) napadov na spletne strani [6]. Pri tovrstnem napadu so lahko koordinirani napadalci poslali v kratkem času veliko zahtev na specifično spletno stran ali storitev. S tem so preobremenili strežnik do te mere, da je prišlo do prekinitve delovanja storitve. Zaradi hitrosti takratnih računalnikov je bilo mogoče poslati več kot tisoč zahtevkov v eni sekundi, če je bilo napadalcev več, se je lahko to število

pomnožilo s številom koordiniranih računalnikov. Ideja tehnologije Hash Cash je bila, da bi ob vsakem zahtevku za spletno storitev moral klient rešiti podano uganko, ki terja določeno procesorsko moč in s tem čas.

Tehnologija je dobila ime Hash Cash, ker so morali obiskovalci spletne strani reševati zgoščevalne probleme (ang. Hash). Spletna stran je obiskovalcu ponudila uganko, rešitev na to uganko je uporabniku ponudila ključ za uporabo nadaljnjih storitev. Uganko je reševala uporabnikova procesorska enota, ki je zmogla fiksno število operacij na sekundo. Uganka je bila sestavljena iz NP-težkega problema, ki ni enostavno in hitro rešljiv. Ker za take probleme ne obstaja dovolj hiter algoritem, je potrebno rešitev uganiti. Težavnost uganke je predstavljal delež pravilnih rešitev. Glede na povprečno procesorsko moč je s tem mogoče statistično izračunati, koliko časa bo procesor potreboval za rešitev uganke. Ko je procesor uganil eno izmed pravilnih rešitev, je bila ta poslana na strežnik in uporabnik je prislužil dostop do spletne strani – zato „Cash“ v imenu, kot plačilo za uporabo.

Tehnologija se je izkazala za učinkovito, saj je lahko poljubno povečala količino časa, ki jo je potreboval procesor za iskanje rešitve, da je uporabnik dobil dostop do spletne strani. Le-ta je lahko uporabniku nespremenjeno omogočala hiter dostop do spletne strani (v praksi skoraj neopazno povečanje/čakanje). Hkrati je tudi zavarovala spletno stran pred napadalci. Na primer, če storitev povprečno potrebuje 50 ms za ugibanje rešitve, povprečni uporabnik sploh ne opazi razlike v času nalaganja storitve. Hash Cash s tem zmanjša količino morebitnih napadalnih zahtevkov na 20 na sekundo ($1000ms/50ms = 20$) za vsak računalnik.

Hash Cash je naslednje leto navdušila pomembno inovacijo Bit gold, ki bo predstavljena v naslednjem razdelku.

2.1.2 Problem elektronskega bančništva in spletnega trgovanja z vmesnimi institucijami

Problem, ki ga je Nicolas Szabo rešil leta 1998, je bil problem vmesnih institucij v elektronskem bančništvu in v trgovanju po spletu. V kolikor obstaja centralna ustanova, ki ji je potrebno zaupati pri sklepanju trgovanja, je uporabnik odvisen od nje in njene stabilnosti. Problem se pojavi, ko hoče uporabnika ta institucija oškodovati, ko propade, ko jo kdo okrade itd. Tiste čase na spletu še ni obstajala rešitev, ki bi lahko ponujala trgovanje brez centralne institucije. Ta problem je poskušalo rešiti veliko ljudi.

Težave, ki so zavirale nastanek take tehnologije, so bile:

1. Obstoj in vzdrževanje kopije podatkov na vsakemu decentraliziranem vozlišču.
2. Kako zagotoviti, da se bodo vozlišča popolnoma strinjala med seboj glede na pravilnost kopije?
3. Kako sinhronizirati popravke v lokalnih kopijah?
4. Kako preprečiti problem dvojnega zapravljanja? To je primer, ko uporabnik zapravi isti kovanec večkrat, preden se trenutno stanje sinhronizira?

5. Kako zaupati ostalim uporabnikom v omrežju, da bodo posredovali resnične informacije?

Rešitev, ki bi rešila zgornje probleme, bi omogočala neposredni prenos vrednosti med dvema uporabnikoma po poljubnem komunikacijskem mediju. Takšna rešitev bi tvorila omrežje računalnikov, ki se vsi med seboj strinjajo o trenutnem stanju v omrežju in bilancah vsakega uporabnika. Ideja je, da ni potrebno zaupati vsakemu uporabniku v omrežju, temveč zgolj da se zaupa sistemu kot celoti. V primeru, da nekaj uporabnikov ni poštenih, se pojavljajo naslednja vprašanja:

1. Kako vedeti kdo ima koliko kovancev, komu zaupati o teh podatkih?
2. Kako preveriti ali je transakcija veljavna?
3. Kako preveriti problem dvojnega zapravljanja (ang. Double spending)?

Taki problemi so zavirali nastanek prve digitalne valute. Veliko teh problemov je rešila prva variacija z imenom Bit gold.

2.2 Bit gold

Bit gold, ki ga je razvil Nicolas Szazbo leta 1988, je rešil večino predhodno omenjenih, tedaj odprtih vprašanj [56]. Ta tehnologija je rešila veliko problemov, ki so bili opisani v podrazdelku o problemih elektronskega bančništva 2.1.2. Vseeno ni uspela rešiti problema o dvojnemu zapravljanju.

Nekateri mehanizmi, ki jih je uporabljal Hash Cash, so bili tudi del Bit golda. Uporabniki so pri tej tehnologiji morali reševati kriptografske uganke, ki so terjale veliko procesorskega časa, a tokrat na drugačen način. Ideja je bila, da se vse izvedene transakcije vpisujejo v velike bloke transakcij. Te bloke se kasneje zaklene in potrdi, ko nekdo iz omrežja uspe najti rešitev na kriptografsko uganko. Ta rešitev postane delček rešitve bodočega problema, saj je vsaka nadaljnja rešitev odvisna od rešitve prejšnjega bloka.

Z opisano tehnologijo je bilo mogoče rešiti problem o poznavanju količine dobrin, ki jih ima vsaka oseba v omrežju. To se je izračunalo tako, da se sešteje vhodne transakcije, ki predstavljajo prihodke, odšteje pa se izhodne transakcije iz podanega računa, ki predstavljajo stroške. Poleg tega je bilo mogoče uporabnikovo identiteto potrditi s pomočjo kriptografskih ključev, ki so podrobneje predstavljeni v podrazdelku 3.1. Največji problem Bit Gold-a je bil ta, da ni znal popolnoma rešiti problema dvojnega zapravljanja. To pomeni, da bi lahko nekdo, ki je pridobil kovanec, le-tega nakazal dvema različnima osebama in s tem podvojil imetje. Valuta, katero se lahko enostavno kopira, v praksi ni uporabna. V tistih časih je bil edini način za preprečevanje problema dvojnega zapravljanja zaupanje v centralno avtoriteto, da preverja legalnost vsake izmed transakcij. Nicolas Szabo kljub prizadevanjem za izdelavo digitalne valute, ki bi lahko obšla tako centralno ustanovo, z Bit goldom ni uspel uresničiti.

Prvi, ki mu je uspelo rešiti zadnje manjkajoče člene v verigi in je ustvaril prvo potencialno digitalno valuto, je bil Satoshi Nakamoto, ko je predstavil tehnologijo Bitcoin [50].

2.3 Bitcoin

Bitcoin je bil prvič predstavljen, ko je oseba pod psevdonimom Satoshi Nakamoto izdala tako imenovani „beli papir“ [50] o tej tehnologiji (ang. Bitcoin Whitepaper). Ta kratek članek je obrnil svet digitalnih valut na glavo, saj je bila v njemu predstavljena „enostavna“ rešitev kriptovalute, ki lahko obstaja in kroži brez kakršnega koli posredovanja centralne ustanove.

Kot dokaz, da je Bitcoin nastal, da bi se soočil s težavami, ki nastanejo ob centralizaciji moči centralnih bank, priča dešifrirana vsebina prvega Bitcoin bloka. Ta se namreč glasi: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks". Ta blok je Satoshi vstavil lastnoročno, saj ima skoraj vsaka veriga prvi blok (ang. Genesis block) ustvarjen ročno, na njega pa se kasneje pripnejo novi bloki.

Satoshi Nakamoto se je zgledoval po tehnologijah Hash cash in Bit Gold. Z Bitcoinom je predstavil rešitev problema dvojnega zapravljanja, ki je bil do tedaj nerešljiv. Predstavil je tudi rešitev za boj proti inflaciji z omejitvijo števila kovancev, ki lahko kadar koli obstajajo v sistemu, na približno 21 milijonov. Predstavil je tudi idejo za iniciativo uporabnikov do sodelovanja v rudarjenju preko sistema nagrad in ne-iniciative do napadanja sistema.

Bitcoin je rešil vse prej predstavljene težave za izključitev centralne ustanove iz izmenjavo kovancev med uporabniki. Predstavljal je tudi prvo potencialno digitalno valuto. Bitcoin je kmalu pridobil na priljubljenosti, zaradi obširne uporabe kriptografije pri implementaciji Bitcoina pa se je začelo uporabljati pojem kriptovaluta. Uporaba Bitcoina je uporabnikom omogočala popolno izključitev posredne osebe pri menjavi in nasploh potrebo po centralni instituciji, ki bi nadzirala transakcije, inflacijo itd. Tu se je začel pojavljati tudi izraz decentraliziran sistem za opis tehnologij veriženja blokov (ang. Blockchain).

Pri Satoshi Nakamotu je zanimivo, da njegova resnična identiteta dandanes ni popolnoma znana. Beli papir o Bitcoinu je bil namreč izdan pod psevdonimom, tako da so vsa ugibanja o njegovi resnični identiteti zgolj teorije. Ena od verjetnih teorij je tudi, da je Satoshi v resnici Nicolas Szabo – izumitelj Bit golda, ker naj bi edini imel dovolj znanja za ustvarjanje Bitcoina. A seveda je ta teorija enako verjetna kot vse ostale.

2.4 Ethereum

Med leti 2009 in 2014 se je razvijalo veliko novih rešitev, ki so imele namen poboljšati Bitcoin ali ponuditi dodatne funkcionalnosti za blockchain. Velik preskok je prinesla rešitev Ethereum, ki jo je predstavil ruski znanstvenik in programer Vitalik Buterin

leta 2015 [58]. Ethereum je predstavil veliko izboljšav za Bitcoin in dodal nove funkcionalnosti. Posebej pomemben za to magistrsko delo je, ker večina blockchain platform v tem raziskovalnem delu izhaja ravno iz Ethereuma.

Ethereum je predstavil funkcionalnost, ki je dandanes znana kot pametna pogodba. S pomočjo Ethereuma lahko programer z osnovnim znanjem naredi pametno pogodbo in pusti omrežju, da izvaja nadzor nad njenim izvajanjem [12]. Pametna pogodba se nahaja na blockhainu in se izvede ob določenem času ali intervalih. Vsaka izvedba pametne pogodbe stane nekaj dobrine, ki se imenuje GAS. Ta je v resnici manjša enota Ethereuma. Z nakazilom te dobrine se plača za procesorsko moč izvajanja pogodb. Cena izvajanja vsake pogodbe je po določenem ceniku odvisna od velikosti in kompleksnosti pogodbe.

Ethereum vsebuje popolni jezik po Turingu (ang. Turing complete language), kar pomeni, da je opisna moč enakovredna Turingovem stroju in s tem veliko ostalim programskim jezikom. Turingov stroj je matematični model, ki predstavlja mejo izračunljivosti današnjih računalnikov[33].

Ethereum prinaša tudi številne novosti, ki jih Bitcoin ni ponujal – tehnologijo Bitcoin, kot so na primer možnosti vpeljevanja psevdo-naključnih števil, vpeljavo trenutnih stanj računov uporabnikov, hitrejše bloke (10 sekund proti 10 minut – Bitcoin) ... Te spremembe so med drugimi navdušile svet izdelave računalniških iger, saj je uporabnikom privlačnih veliko teh novosti. Na primer vpeljava psevdo-naključnih števil lahko uporabnikom igre omogoča transparentni pregled nad poštenostjo programa. Omogoča tudi možnost razločevanja med različnimi kovanci v Ethereumu, izdelovalcu igre omogoča možnost, da preslika kovanec v določen izdelek v igri, na primer v meč v srednjeveški igri (ERC-20 [16]).

3 Lastnosti veriženja blokov

Namen tega razdelka je seznanjenje bralca s tehnologijami in tehnikami, ki so osnovni gradniki tehnologije veriženja blokov, in mu ponuditi hitro, a izčrpno razlago o le-teh. Sledi opis posrednih lastnosti, ki jih lahko izpeljemo s pomočjo opisanih tehnik. Po eksploziji interesa tako v tehnoloških kot raziskovalnih sferah, je prišlo do vrste variacij Bitcoin protokola. Veliko implementacij ima posebnosti, ki ciljno rešujejo specifičen problem. V magistrskem delu bo poudarek na dveh protokolih, ki sta najbolj razširjena in uporabljena – Bitcoin in Ethereum. Zadnji del tega razdelka zavzemajo aplikacije uporabe blockchaina v praksi.

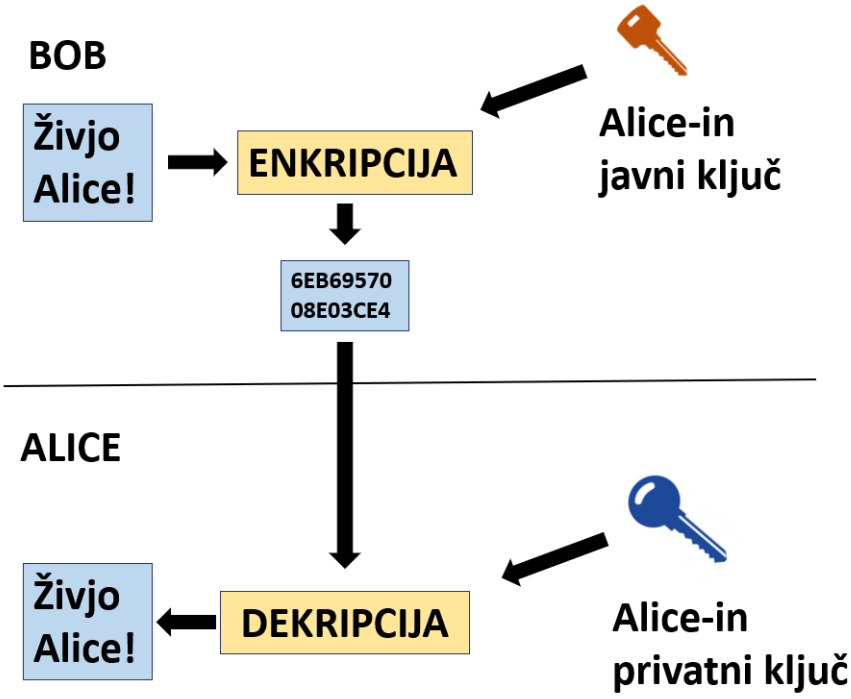
3.1 Asimetrična kriptografija

Asimetrična kriptografija igra pomembno vlogo v različnih disciplinah svetovnega spleta [55]. Uporabljena je pri identifikaciji uporabnikov, varni komunikaciji in zasebnosti za spletno trgovanje, transakcijah, podpisu pametnih pogodb in digitalnih dokumentov. S pospešenim razvojem svetovnega spleta dnevno pridobiva vse več uporabe.

Posebnost asimetrične kriptografije je to, da uporablja par ključev (p, k) za kodiranje. Ključ p predstavlja tako imenovani javni ključ in k zasebni ključ. Vsak uporabnik ustvari par ključev s pomočjo generatorja naključnih števil. Javni ključ uporabnik deli z vsemi udeleženci v omrežju, medtem ko zasebnega obdrži zase. Zasebni ključ je vedno znan zgolj eni osebi in je uporabljen za podpisovanje dokumentov. Zasebni ključ je matematično definiran s pomočjo funkcije f, ki preslika poljuben vhod x s pomočjo zasebnega ključa v nek izhod y, iz česar sledi $f(x, k) = y$. Vsi drugi udeleženci v omrežju lahko z uporabnikovim javnim ključem preverijo, ali je to sporočilo res podpisal on. Obstaja tudi taka funkcija g, za katero velja $g(y, p) = x$. Uporablja se lahko tudi obratni postopek, da neka oseba zakodira sporočilo z javnim ključem druge osebe, pošlje kodirano sporočilo tej osebi in ta oseba ga lahko prebere s pomočjo njenega zasebnega ključa. Na sliki 1 je prikaz enostaven primer takega delovanja asimetrične kriptografije.

Javni in zasebni ključ se pridobi z metodo, ki tvori naključna števila s pomočjo zelo velikih praštevil. Slednja sta ustvarjena na ta način zaradi matematične lastnosti, ki onemogoča praštevilom razcep na prafaktorje. Najboljši trenutno poznani napad za dešifrirati sporočila brez ustreznega zasebnega ključa je tako imenovani napad s surovo silo (ang. brute force attack). Ta napad se izvaja tako, da napadalec skuša uganiti ključ in zelo hitro preizkuša različne ključe. Verjetnost, da napadalec ustrezno ugane ključ, je minimalna, saj bi za dešifriranje enega sporočila z uporabo današnje opreme in varnosti v povprečju potreboval tudi več stoletij.

Slabost asimetrične kriptografije je v shranjevanju in varovanju zasebnega ključa.



Slika 1: Primer asimetrične kriptografije. V tem primeru je prikazan postopek pošiljanja sporočila med Bobom in Alice. Bob s pomočjo Alicinega javnega ključa zakodira sporočilo, Alice kasneje tega z njenim zasebnim ključem dekodira.

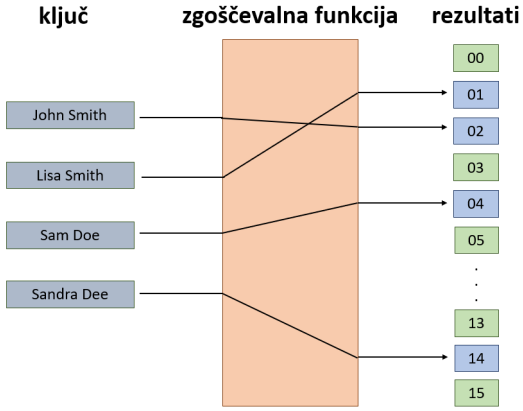
Uporabnik lahko ključ pozabi, izgubi ali postane tarča napada. Če dobi druga oseba dostop do zasebnega ključa, pridobi možnost podpisa dokumentov s tem ključem, kar mu omogoča izdajanje za drugo osebo. Uporabnik sam ustvari javni in zasebni ključ – javnega deli z javnostjo, medtem ko zasebnega obdrži zase.

Nujno potreben gradnik blockchaina je digitalni podpis, ki temelji na asimetrični kriptografiji. Oseba lahko namreč poljuben dokument podpiše s ključem in ga ne zakodira v celoti, temveč mu doda na konec določeno število bitov, ki predstavljajo njen podpis. Na ta način lahko vsi preberejo ta dokument. Vsi z javnim ključem te osebe lahko tudi preverijo ali je bil podpis res njen. Ker se da s pomočjo zgoščevalnih funkcij (ang. Hash funkcije, predstavljene so v podrazdelku 3.2) podpisati celoten dokument, se lahko zagotovi, da je mogoče preveriti, ali je bila pogodba med podpisovanjem in prenosom spremenjena [41].

3.2 Zgoščevalne funkcije

Zgoščevalne oz. razpršilne funkcije (ang. Hash functions) se uporabljajo v shranjevanju podatkov, verifikaciji podatkov, anonimizaciji gesel, podatkovnih bazah, digitalni forenziki itd. Za to delo so pomembne, ker so eden osnovnih gradnikov blockchaina. V osnovi delujejo tako, da vhod poljubne dolžine „zakodirajo“ v izhod fiksne dolžine. Primer preprostega delovanja zgoščevalne funkcije je na sliki 2.

Zgoščevalne funkcije delujejo na mnogo različnih načinov, a zagotoviti je potrebno določene lastnosti. Na primer: zgoščevalna funkcija mora biti vedno deterministična,



Slika 2: Preprost primer zgoščevalne funkcije. Vsako ime na levi strani se preko funkcije zakodira v število med 0 in 15.

kar pomeni, da v implementaciji ne sme uporabljati naključnih vrednosti. Delovanje zgoščevalne funkcije je enosmerno, kar pomeni, da če se z njo zakodira geslo, se ne da iz rezultata spet pridobiti ven besedo, ki je bila zakodirana. Sledi, da taka funkcija ni bijektivna preslikava, kar pomeni, da nima inverzne funkcije. To pomeni, da iz rezultata ne moremo nazaj izračunati prvotnega besedila.

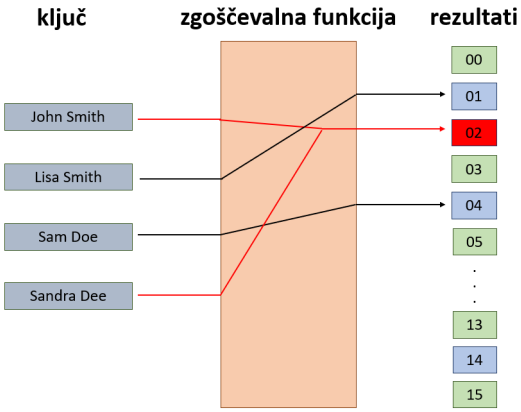
Denimo, da je $H(x)$ *dobra* zgoščevalna funkcija in x geslo. Potem je $y = H(x)$ končen niz, ki enolično določa geslo. Pri danem y ni mogoče ugotoviti x. Ta mehanizem je običajno uporabljen pri spletni avtentikaciji uporabnikov, saj lahko za uporabnika, ki predstavi y, sklepamo, da pozna tudi x.

Pri zgoščevalnih funkcijah je pomembna enakomerna porazdelitev začetnih vhodov čez vse mogoče izhode. Na primer veljavna zgoščevalna funkcija lahko zakodira vse znake v izhod „1“, a taka funkcija v praksi ne bi bila uporabna. Ta lastnost je zelo pomembna, ker če sta $H(x) = Y$ in $H(z) = Y$, pri čemer $x! = z$, se dva različna podatka preslikata v enak izhod, kar se imenuje kolizija. Preprost primer kolizije je opisan na sliki 3. Do kolizij pogosto prihaja, ker je pri zgoščevalnih funkcijah omejen izhodni prostor, saj je potrebno vnaprej določiti, koliko različnih izhodov obstaja. Obseg vhodov ni omejen, saj ni omejena niti dolžina vhoda. Sledi, da vedno obstaja neskončno mnogo kolizij. Te je potrebno minimizirati.

3.2.1 SHA–256 zgoščevalna funkcija

SHA–256 je zgoščevalna funkcija, ki jo uporablja Bitcoin.[2]. To zgoščevalno funkcijo je razvila Ameriška agencija NSA [29]. V njej se uporabljajo izhodne besede, sestavljene iz 32 bajtov. Ker je vsak bajt sestavljen iz 8 bitov, ki lahko zavzemajo bodisi vrednost 0 ali 1, je število vseh mogočih kombinacij $2^{256} = 10^{77}$. Teoretično je verjetnost kolizije v tako velikem razponu mogočih izhodov skoraj nemogoča.

Ta zvrst zgoščevalnih funkcij je v času pisanja (januar, 2020) veljala za eno najbolj odpornih na napade. V zadnjem času so v uporabo prišle tudi naprednejše zgoščevalne funkcije, na primer družina SHA–3 funkcij.



Slika 3: Preprost primer kolizije pri zgoščevalni funkciji. Dve imeni na levi strani („John Smith“ in „Sandra Dee“) sta se zapisali v enak izhod „02“.

Obstaja veliko vrst napadov na SHA zgoščevalne funkcije, a v praksi ni znan noben, ki bi bil dovolj zanesljiv, da bi bil vreden časovne zahtevnosti in potrebne procesorske moči. Primer mogočega napada bi bil na primer „Collision attack“, kjer skušajo napadalci doseči kolizijo – primer tega je opisan na sliki 3. Če se sistem sproži samo ko dobi za izhod specifičen izhod SHA funkcije, lahko z iskanjem kolizije sprožimo tak sistem. Če je potrebno ponarediti dokument z digitalnim podpisom, je skoraj nemogoče najti kolizijo tako, da se popravi zgolj del besedila (zlonamerno) in se hkrati s tem zadene pravilno kolizijo. Poudariti je potrebno, da je pri 10^{77} mogočih izhodov potrebno v povprečju približno 10^{38} poskusov za doseg kolizije. S trenutno procesorsko močjo to vzame več let.

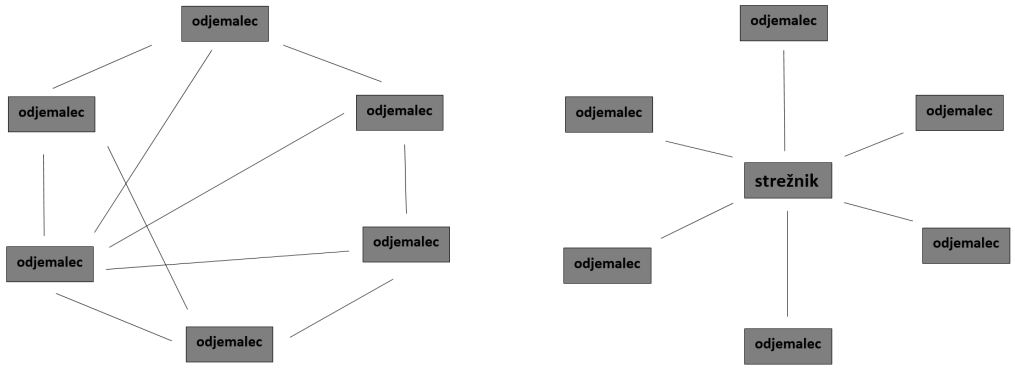
3.3 Omrežje P2P

Pomembno vlogo v blockchain igrah predstavlja omrežje enak-z-enakim (ang. peer-to-peer network). Glavni namen blockchaina je sporazumevanje uporabnikov brez prisotnosti centralne avtoritete [51], ki jo predstavlja ravno P2P omrežje. Preprost primer P2P omrežja proti omrežju odjemalec–strežnik je prikazan na sliki 4.

V primeru na sliki 4b je razvidno, da so vsi odjemalci neposredno odvisni od centralnega strežnika. V primeru, da strežnik iz neznanega razloga preneha z delovanjem, preneha teči tudi komunikacija med posameznimi odjemalci. Prav tako ima strežnik dostop do vseh informacij v omrežju, saj poteka celotna komunikacija čez njega. To sta bila dva razloga za osredotočenje razvoja blockchaina in uporabo omrežja iz slike 4a.

Pojem „omrežje“ je potrebno v tem kontekstu razumeti kot abstraktni pojem, saj je v kontekstu blockchaina razumljen kot interakcija uporabnikov med sabo s transakcijami preko centralne ustanove – na primer banke, ki za usluge seveda zahteva provizijo. P2P omrežju lahko rečemo „decentralizirano“ omrežje, ker nima nobenega strežnika ali centralne enote.

Če omrežje sestavlja skupek uporabnikov, ki želijo med seboj izvajati transakcije, je



(a) P2P omrežja (b) Omrežje odjemalec–strežnik

Slika 4: Razlike v strukturi omrežij med enakovrednimi odjemalci in med arhitekturo odjemalec–strežnik. Na levi so odjemalci povezani med seboj na naključen način. Na desni so vsi odjemalci povezani zgolj s strežnikom.

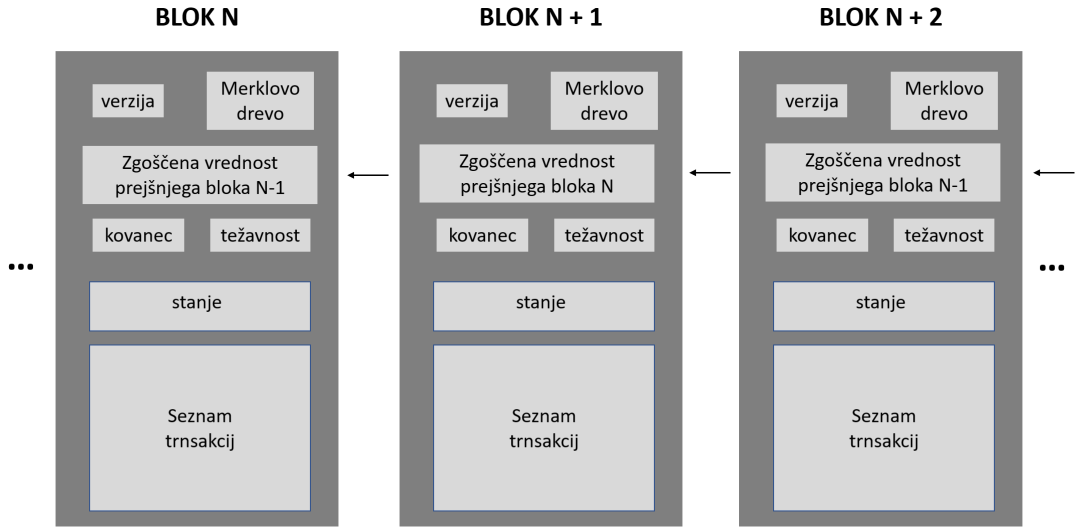
interakcija v omrežju odjemalec–strežnik zelo enostavna. V tem primeru se zgolj zaupa centralnemu strežniku, da preveri vsako transakcijo in jo bodisi potrdi bodisi zavrne. V kolikor ta ustanova deluje v korist uporabnikov, omrežje deluje brez težav. Če se odloči ta ustanova krasti ali goljufati, je ne more nihče ustaviti in kaznovati. V P2P omrežju je komunikacija težavnejša, ker ni centralne ustanove, ki bi lahko usklajevala stanja posameznih vozlišč. Postavlja pa se vprašanje: Kako v takem omrežju doseči dogovor med enakovrednimi, a drugačnimi vozlišči? To je eden izmed problemov, ki jih rešuje blockchain.

3.4 Blok in transakcije

Najbolj osnovna enota v verigi blokov je blok. Blockchain je v bistvu porazdeljena, decentralizirana in pogosto javna veriga blokov [57]. Vsebina blokov se zelo razlikuje med posameznimi implementacijami blockchaina. Primer bloka, ki je zelo soroden Ethereumu, je predstavljen v primeru na sliki 5.

Najbolj pomembna vsebina bloka je seznam transakcij, ki opisujejo spremembo sistema od predhodnega bloka. V njem so zapisane vse transakcije, ki so bile odobrene in s tem veljavne. Strogo pravilo veriženja blokov je to, da če transakcije ni v seznamu transakcij v bloku, potem se ta transakcija sploh ni zgodila. Transakcija je nakazilo sredstev iz enega računa na drugi račun. Kako se shranjuje trenutna bilanca vsakega računa, je odvisno od uporabljenega modela. Seveda je transakcija odobrena le, če je dokazano, da ima pošiljatelj v lasti omenjena sredstva. To se pogosto dokazuje z zasebnim ključem.

Blok vedno vsebuje referenco na prejšnji blok, najpogosteje na rezultat razpršilne funkcije (hash) prejšnjega bloka. Zaradi te odvisnosti je blok odvisen od predhodnika. Če bi se spremenilo kar koli v tem bloku, se potem spremeni njegov hash in s tem se v procesu ustvarjanja novega bloka ugotovi, da je nekaj narobe. S tem postane nemogoče delati na tej verigi, saj bodo napako zaznala vsa vozlišča in bodo to verigo zavrgla. Da velikost bloka ne naraste prehitro, vsebuje blok tudi koren Merkelovega drevesa. S tem dosežemo, da se lahko pri starejših blokih večji del podatkov izpusti in se ohrani le



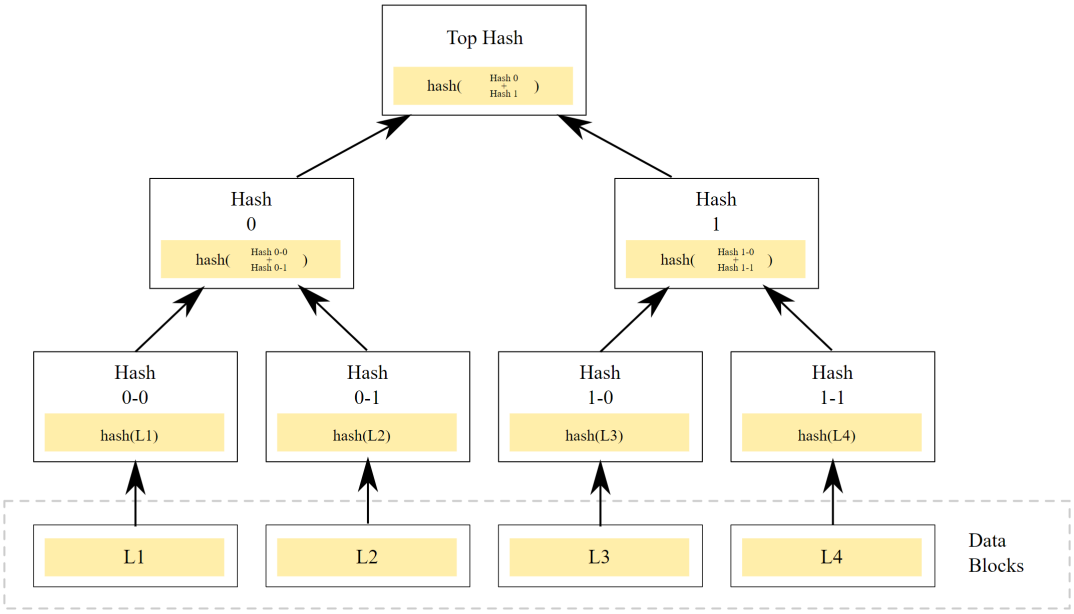
Slika 5: Preprost primer treh zaporednih blokov v verigi blokov. Vsak blok se navezuje na prejšnjega in vsebuje glavo, list transakcij in dodatne podatke.

ključne dele – koren in Merklovo drevo. Preprost primer delovanja Merklovega drevesa je prikazan na sliki 6. Zaradi drevesne strukture in rekurzivnega računanja hashov po drevesu navzgor se ohranja lastnost, da če se spremeni vsaj eden izmed podatkovnih blokov v drevesu, se zamenja tudi hash v korenu. Pravilnost hasha je enostavno mogoče preveriti s ponovnim izračunom hashov po drevesu navzgor.

Navadno blok vsebuje tudi podatke, ki so namenjeni rudarjenju blokov, kot so na primer „magično število“ (ang. Nonce) in težavnost bloka. Te komponente variirajo od implementacije do implementacije blockchaina v odvisnosti od želene hitrosti nastajanja novih blokov. Na primer Bitcoin ima čas bloka med 10 in 15 minut, medtem ko Ethereum med 10 in 15 sekund. Poleg tega lahko blok vsebuje tudi trenutna stanja ali spremembo v stanjih od zadnjega bloka, na primer pri Ethereumu. Prednost tega je enostavnejša raba in hitrejši dostop do trenutnega stanja. Seveda se v novih blokih pojavijo zgolj tista stanja, ki so bila spremenjena v zadnjem bloku. Ko je potrebno preveriti trenutno stanje nekega uporabnika, je potreben rekurziven sprehod po verigi od konca proti začetku, vse dokler ni najdena prva instanca spremembe stanja izbranega uporabnika. Ta model porabi veliko več prostora za shranjevanje, saj je potrebno vsa stanja opisovati ob vsaki spremembi. Na primer pri Bitcoinu ni trenutnih stanj, temveč so v vsakem bloku opisana samo ”nakazila”ene denarnice drugi denarnici in je potreben za izračun stanja sprehod po celotni verigi. Ta pristop je prostorsko varčen, saj je v vsak blok potrebno zapisati veliko manj podatkov.

3.5 Knjiga transakcij

V porazdeljenih sistemih je potrebno doseči dogovor o tem, kdo lahko izvaja določene transakcije, da se lahko potrdi njihovo veljavnost. Ker v tej strukturi ne obstaja nobena centralna enota, ki bi imela celotno tabelo vseh sodelujočih uporabnikov in njihovega trenutnega stanja, je potrebno implementirati podobno, a decentralizirano rešitev. To pomeni, da bi vsi uporabniki imeli kopijo in možnost branja te datoteke [46], [47]. Po-



Slika 6: Preprost primer Merklovega drevesa. Na sliki je razvidno, kako so štirje podatkovni bloki, označeni z L1 do L4, povezani v binarno drevo. Najnižji bloki vsebujejo zgolj hash podatkovnega bloka. Ostali bloki vsebujejo rezultat hash funkcije hashov otrok.

javi se vprašanje, kako narediti dovolj dober sistem, ki zagotavlja, da imajo vsi ves čas enako kopijo take datoteke? V resnici je potrebno na tem mestu zadostiti izreku CAP [25], ki pravi, da bi tako omrežje moralo zagotavljati:

- Konsistentnost – vsak poskus branja datoteke mora vrniti bodisi najbolj aktualno verzijo datoteke bodisi napako.
- Razpoložljivost – vsak zahtevek dobi odgovor. Za ta odgovor ni nujno, da je najbolj aktualen. Zahtevek nikakor ne sme vrniti napake.
- Toleranco deljivosti – sistem lahko deluje ne glede na to, da se izgubi nekaj zahtevkov zaradi časa potovanja sporočil med omrežji, ali pa ti prispejo na cilj z zamudo.

Rešitev je uporaba knjige transakcij (ang. Ledger) ali celo porazdeljene knjige transakcij (ang. Distributed ledger).
Bitcoin deluje na tehnologiji neporabljenih transakcij (ang. UTXO). Pri tem modelu ima vsaka denarnica vhodne in izhodne transakcije, ki opisujejo prejete in zapravljene Bitcoine. Bitcoin tako nima trenutnih „stanj“, da bi bilo razvidno, kdo ima v danem trenutku koliko kovancev, temveč je potrebno to prešteti glede na vhodne in izhodne transakcije iz danega računa. Pri Ethereumu je to veliko lažje, ker je bil uveden sistem stanj v njegovo implementacijo. To pomeni, da se za vsakogar v sistemu ve, koliko dane valute ima v izbranem trenutku. Slaba stran stanj je, da se zaradi tega celotna veriga močno poveča, ker je potrebno hraniti veliko več podatkov. Ko se posodobi nov blok v verigi, se „prepiše“ zadnje stanje tako, da se posodobi z vsemi novostmi, ki so se v

času izdelave tega bloka izvedle. Novosti so na primer transakcije in izvedbe pametnih pogodb, ki spremenijo trenutno stanje uporabnika. Tako ima vsak uporabnik datoteko stanj, ki se posodobi vsakič, ko se ustvari nov blok. Če pride nov odjemalec v sistem, mora izračunati stanja za vsakega uporabnika vse od začetka verige (po spremembah za vsak blok), da preveri, ali je celotna veriga do sedaj ustrezna. V primeru, da veriga ni veljavna, se na njej ne izplača delati, saj bi jo druga vozlišča zavrnila.

3.6 Konsenzi

Konsenzi so zelo pomembni postopki v porazdeljenem računanju za skupno soglašanje o rešitvi problema. Ker je v porazdeljenem sistemu veliko enakovrednih računalnikov, morajo vsi doseči skupen dogovor o tem, ali je transakcija veljavna ali ne. Za to rešitev obstaja veliko različnih konsenzov, vsaka blockchain implementacija pa uporablja enega ali več njih za določitev stanja verige.

Dober algoritem za konsenz mora zagotoviti, da v primeru konfliktnih stanj na deterministično in pravilen način odloči stanje, ki je pravilno. Kako pride do te odločitve, je stvar implementacije posameznega konsenza. Do dogovora med stanji o izbranem stanju mora priti v končnem času, zaželeno je tudi, da je taka odločitev čim bolj hitra. Zelo pomembno je tudi preprosto dejstvo, da če se vsi procesi strinjajo nad določeno transakcijo, da se tudi celotno omrežje odloči to transakcijo sprejeti.

Da je lahko nek konsenz lahko "dober", mora imeti naslednje lastnosti [4]:

- Biti mora odporen na napake in varen pred različnimi napadi. Na primer prenesti mora, če vozlišča zapustijo sistem in če poskusijo goljufati.
- Imeti mora dokončnost odločitev. To pomeni, da ko se neka odločitev potrdi, mora ostati potrjena in se ne sme spreminjati.
- Odločitve in spremembe morajo biti hitro sinhronizirane čez celotno omrežje. Upoštevati je potrebno tudi, da se lahko sporočila v omrežju izgubijo, tako da mora konsenz upoštevati možnost izgubljenih sporočil.
- Ne sme biti energijsko preveč potraten, saj lahko zahtevne kalkulacije in reševanje kriptografskih ugank na več milijonih vozlišč hkrati porabijo ogromno energije.

V tem podrazdelku je poudarek predvsem na uporabi konsenzov v blockchainu, čeprav imajo konsenzi veliko drugih področij uporabe. Predstavljeni so konsenzi PoW, PoS in DPoS.

3.6.1 Proof of work – PoW

Dokaz o opravljenem delom (ang. Proof of work) je najstarejši konsenz, ki se uporablja v blockchainu. Ta konsenz so predlagali leta 1993 [23]. V blockchain implementaciji se je prvič pojavil pri Bitcoinu. Ideja PoW je, da mora biti za vsak blok narejenega dovolj dela, da se ta blok sprejme. Tisti blok, ki ima dokazanega največ dela na njemu,

je brezkompromisno sprejet kot resnični blok. Količino dela, vloženega v blok, se dokazuje z dolžino verige, ki jo ima blok pod seboj, v primeru spremenljive težavnosti je upoštevana tudi težavnost blokov v verigi, ne zgolj njena dolžina. Na primer, če je veljavni blok na 10. mestu v verigi in izbran uporabnik trenutno uporablja blok z dolžino verige 9 in se zave obstoja bloka z daljšo verigo, nemudoma zavrže ta blok in začne delati na bloku z daljšo verigo.

Problem tega konsenza je v tem, da porabi ogromno količino električne energije in procesorske moči za izračun novega bloka. Prednost je v tem, da deluje na načelu en-procesor-en-glas. Iz tega sledi, da več procesorjev kot ima oseba v lasti, več verjetnosti je, da bo ustvarila nov blok. Tako dosežemo dejstvo, da več moči kot vsakdo vloži za podpiranje blockchain omrežja, večje možnosti ima za izplačilo. Uporabniki posledično tekmujejo med sabo, kdo bo prvi rešil uganko, saj je zanjo nagrajen.

3.6.2 Proof of stake – PoS

Naslednji zelo poznan konsenz je dokaz o zastavljenem deležu (ang. Proof of stake). Ta konsenz je bil predlagan kot izboljšava prejšnjega PoW konsenza tako, da porabi veliko manj energije [32]. Za primerjavo je ocenjeno, da se za rudarjenje (vzdrževanje) Bitcoina s PoW konsenzom porabi toliko električne energije, kot jo porabi celotna Češka republika (2018) [13]. Nasprotni članki trdijo, da situacija le ni tako kritična, saj je vsaj 74,1 % energije, porabljene v rudarjenju Bitcoina, obnovljive [27].

Pri PoS konsenzu lahko vsako sodelujoče vozlišče zastavi nekaj valute, da bi lahko potrjevalo bloke. Več valute kot neko vozlišče zastavi, večja je verjetnost, da bo pridobilo pravico za potrjevanje. Ideja pa je ravno v tem, da s tem, ko dobi pravico, je zastavilo veliko valute. Vso to valuto pa izgubi, če se ugotovi, da je lagalo pri potrjevanju transakcij. V primeru, da se ugotovi poštenost vozlišča, le-to dobi denarno nagrado. Iz tega razloga naj bi iniciativa za laganje obratno sorazmerno padala s količino zastavljenih sredstev. Pristnost delovanja vozlišča, ki potrjuje bloke, pa preverja celotno omrežje, ki lahko tudi ugotovi, ali je bil na novo narejeni blok res pravilno zgrajen.

Ker pri PoS ni potrebna tako velika količina računanja kriptografskih ugank, je porabljene energije veliko manj. V čisti obliki ima PoS veliko kritik, večinoma takih, ki se navezujejo na razdvajanje verige (ang. Fork chain). PoS sistem na začetku ni imel predvidenih nobenih posledic za kršitelje, ki se hočejo okoristiti z razdvajanjem verig. Na primer Ethereum je zelo veliko časa obljubljal prehod iz PoW na PoS, a težavnost odprave napak pri razdvajanju verige je prehod na nov konsenz naredila neprivlačen [9]. Rešitev za prehod na PoS so našli v Casper standardu, ki je prinesel posledice za razdvajanje verig. Predstavljena sta bila dva protokola, in sicer Casper CBC in Casper FFG. Ta protokol je predvidel rešitev pri razdvajanju verig v tem, da se določi nekaj blokov, kjer bo celotna veriga preverjala, ali je na teh blokih prišlo do razdvajanja ali ne. V primeru, da pride do razdvajanja, izgubi trenutni predstavnik te verige vse, kar je zastavil za potrjevanje.

3.6.3 DPoS

DPoS je zelo zanimiva implementacija konsenza, ki v bistvu pooseblja realne volitve. Razvit je bil kot nadgradnja konsenza PoS z dodatnimi prednostmi. Ideja tega konsenza je obljubljala zelo veliko povečanje skalabilnosti konsenzov PoW in PoS.

DPoS deluje tako, da uporabniki v sistemu glasujejo za druge uporabnike, da jih zagovarjajo, podobno kot volitve strank v resničnem svetu. Uporabniki lahko delajo dobra dela v omrežju in zaradi tega jih drugi uporabniki volijo na tak način, da jim nakazujejo določeno vsoto kovancev (zaradi tega v imenu PoS – dokaz s stavo). Vedno, ko se kreira nov blok, se ovrednoti celotno lestvico vozlišč po številu glasov. Glede na to se izbere prvo delegacijo vozlišč, ki bodo izbirale in potrjevale transakcije za naslednji blok. Verjetnost, da bo vozlišče izbrano za potrjevanje bloka, je sorazmerno z odstotkom glasov, ki jih je prejelo.

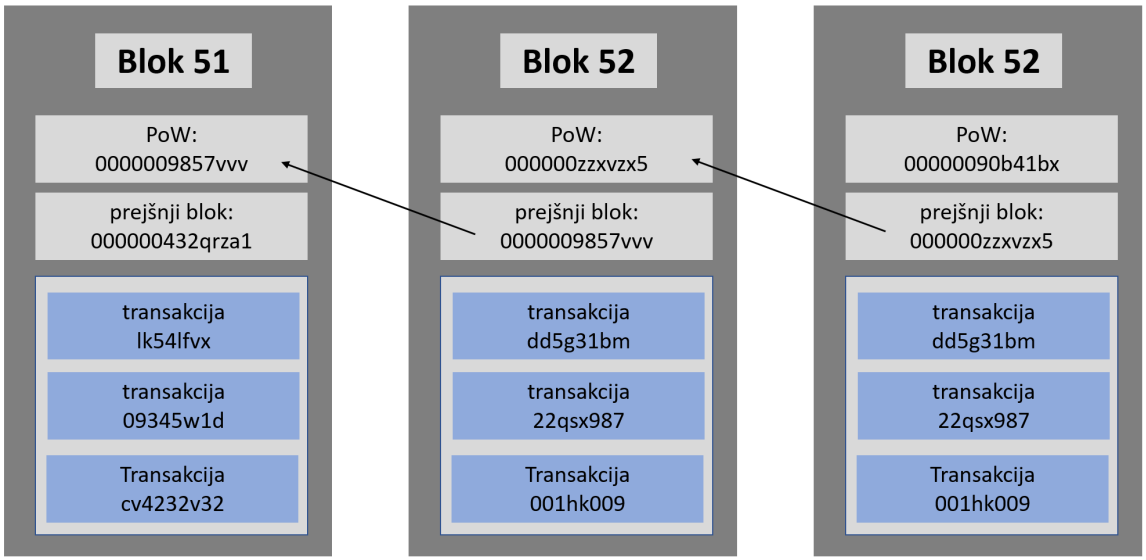
DPoS ima veliko kritik na delovanje. Na primer dejstvo, da mora obstajati resnični interes uporabnikov v omrežju, da skušajo pozitivno učinkovati na omrežje. Prav tako je nevarno, če se zlonamerni ljudje združijo in z dvotretjinsko večino preglasijo dobre akterje v omrežju in s tem vrinejo v verigo popravljeni blok. Ta nevarnost omogoča DPoS sistemom, da so veliko hitrejši. To izhaja iz tega, da je veliko hitreje sprejeti konsenz za odločitev pri manjšem številu delegatov. DPoS je manj decentraliziran od ostalih blockchain implementacij, saj je zgolj končno mnogo delegatov, ki sodelujejo pri sprejemanju odločitev.

3.7 Rudarjenje

Rudarjenje (ang. Mining) je dejavnost, ki povezuje celotni blockchain s PoW konsenzom [1]. Kot je bilo omenjeno v prejšnjih razdelkih, rudarji rešujejo zelo težke kriptografske uganke. Za te uganke je značilno, da jih ni mogoče nikakor algoritmično izračunati, temveč je potrebno ugibanje. V resnici rudarji dodajajo v glavo vsakega bloka naključno število toliko časa, dokler izhod SHA–256 zgoščevalne funkcije celotnega bloka ne vrne rešitve z določenim številom vodilnih ničel (težavnost).

Težavnost uganke ni stalna. V primeru, da bi težavnost ostala konstantna skozi čas, bi se s številom rudarjev v omrežju seveda spreminjal tudi povprečni čas rešitve uganke, s tem se spremeni število blokov, proizvedenih v danem časovnem intervalu. Na primer pri Bitcoinu je želja, da bi se v povprečju kreiral nov blok vsakih 10–15 minut. Težavnost uganke je potrebno prilagajati glede na trenutno število rudarjev v omrežju. Pri Bitcoinu se posodobi težavnost uganke približno vsakih 2016 blokov, kar je približno vsakih 14 dni.

Uporabnost rudarjenja je predvsem v tem, da se s povezovanjem blokov v verigo skuša preprečiti spreminjanje starih blokov. Kot je prikazano na primeru na sliki 7 je vsak blok odvisen tudi od hash-a prejšnjega bloka. Če se spremeni določen blok v verigi, se seveda pokvari tudi naslednji blok v njej, ta pokvari naslednji blok, vse dokler se ne pokvarijo vsi bloki naprej od spremenjenega. Z veriženjem se zaklene veriga, da ji ni mogoče spreminjati preteklosti [20].



Slika 7: Preprost primer povezovanja blokov v blockchain-u. Vsak blok vsebuje hash prejšnjega bloka. Tako se kreira veriga blokov v pravem pomenu besede.

Vstavljanje nepravilnih transakcij v nov blok je prav tako skoraj nemogoče. Vstavitev nelegalne transakcije, kjer bi zlonamerna oseba hotela pripisati sebi transakcijo druge osebe, ni mogoča brez poznavanja zasebnega ključa pripadajočem javnem ključu. Ostane le možnost, da se skuša "izbrisati"blok s storjeno transakcijo. V tem primeru zlonamerna oseba najprej zapravi določeno količino kovancev, jih zamenja za na primer fizično dobrino in s to zapusti trgovino. Med tem skuša napadalec ustvariti nov blok brez te transakcije. Nova veriga mora biti daljša, da bi jo druga vozlišča sprejela in s tem zavrnila verigo z narejeno transakcijo. Tudi to je mogoče le, če se poleg tega tudi reši trenutno uganko. Trenutna varnost deluje tako, da je potrebno po nakupu nečesa z Bitcoinom počakati toliko časa, da se transakcija potrdi, najpogosteje da se za njo potrdijo dva do štirje bloki. Za uspešno spremembo transakcije bi bilo potrebno nakazati vsoto kovancev izbrani denarnici, nato počakati dva do štiri bloke, zamenjati blok v sprejeto transakcijo in končno v krajšem času kot ostalo omrežje najti naslednji blok. S tem poskusi pa prepričati omrežje, da je spremenjena veriga najdaljša in s tem pravilna. To je matematično in statistično gledano skoraj nemogoče po verjetnosti, saj verjetnost, da bo kdo prvi razrešil uganko večkrat zapored, zelo hitro pada proti nič.

Iniciativa rudarjenja je v tem, da ob vsaki pravilni razrešitvi uganke dobi tisti, ki je uganko rešil prvi, določeno vsoto kovancev. Namreč vsak blok vsebuje na začetku prazno transakcijo, ki jo lahko rešitelj pripiše sebi in s tem poveča imetje. Rudarjenje je iz tega pogleda zgolj tekmovanje, kdo bo prvi razrešil uganko in s tem pridobil denarno nagrado.

3.8 Izpeljane lastnosti

Zaradi vseh zgoraj omenjanih lastnosti je mogoče zaključiti, da je veriga blokov nespremenljiva. To pomeni, da podatki verige ne morejo biti spremenjeni, ko so dovolj

globoko. V primeru Bitcoina je bilo v prejšnjih razdelkih opisano, kako rudarjenje preprečuje spreminjanje potrjenih blokov, ostale implementacije, ki uporabljajo drugačne metode konsenzov, pa dosežejo nespremenljivost na drugačne načine. Vsekakor je nespremenljivost glavna lastnost, ki jo mora konsenz zagotavljati, da je sploh uporaben za implementacijo v blockchainu.

Blochchain ponuja tudi možnost transparentnosti kode, kar je pogosto zelo pomembno. Posebej v rešitvah, ki ponujajo funkcije, povezane s pametnimi pogodbami – recimo Ethereum. Uporabniki imajo v takih primerih blockchaina možnost vpogleda v kodo delovanja in kodo pogodb, kar jim omogoča preverjanje delovanja in poštenosti implementacije.

Večina blockchain implementacij ponuja tudi določeno stopnjo anonimnosti, saj so transakcije v blokih lahko zakodirane ali samo predstavljene s ključi uporabnikov. Anonimnost deluje vse dokler ni dan ključ pripisan določeni osebi. Slaba stran je to, da se lahko za vsak ključ izpiše točno zgodovino vseh transakcij, ki jih je lastnik tega ključa opravil. Tako je anonimnost dosežena zgolj do neke mere.

Zelo pomembna lastnost je tudi decentralizacija. Ta ključna lastnost vsakega blockchaina ponuja delovanje celotnega omrežja brez kakršne koli centralne ustanove, kar naredi omrežje neodvisno. Velika stopnja decentralizacije preprečuje tudi združevanje rudarjev v skupnosti, ki bi lahko skupaj dosegli večino v omrežju. To velja, če so rudarji dovolj porazdeljeni po svetu in s tem tvorijo dovolj decentralizirano omrežje. To poveča varnost sistema in ga obvaruje pred večinskimi napadi.

Kot posledica decentralizacije in nespremenljivosti se pojavi lastnost varnosti imetja določenega uporabnika. Ker ni mogoče njegovega imetja ukrasti s spreminjanjem blokov in niti preko centralne entitete, ki bi lahko uporabniku odstranila imetje, je njegove imetje v tem omrežju varno. Poleg tega je dokaz o njegovem imetju shranjen na več tisoč ali celo milijon različnih napravah po celem svetu, tako da je z predložitvijo njegovega ključa zelo lahko dokazati lastništvo.

3.9 Aplikacije uporabe

V tem podrazdelku so prikazane najpogostejše uporabe blockchaina. Najbolj pomembna aplikacija je kriptovaluta, saj blockchain omogoča ustvarjanje digitalnih kovancev in izvajanje transakcij med njimi. Ostale predstavljene aplikacije so: pametne pogodbe, dobavne verige in video igre.

3.9.1 Pametne pogodbe

Blockchain implementacije, kot so recimo Ethereum, omogočajo zapis in izvajanje pametnih pogodb med uporabniki [17]. V tem primeru vse sodelujoče osebe v pogodbi podpišejo digitalni dogovor, ki je lahko vezan tudi na zunanje dejavnike, a se izvaja brez človekove interakcije. Primer pametne pogodbe je, da uporabnik A kupi 10 kovancev od uporabnika B, če je tisti dan padal sneg. V tem primeru se določi zaupljivo stran, ki ima informacije o snegu. Pogodba se izvrši vsak dan in če je prejšnji dan

padal sneg, se pogodba na blockchainu potrdi iz strani vozlišč, ki ob kreaciji in potrjevanju novega bloka te pogodbene podrobnosti preverijo. Več o pametnih pogodbah je opisano v razdelku 4.

3.9.2 Dobavne verige

S pomočjo blockchaina se je nadgradilo obstoječe dobavne verige. Te so skupki pogodb in dogovorov o tem, kako se bo dobavljalo potrebne surovine v tovarne preko veliko različnih dobaviteljev. S pomočjo blockchaina je mogoče zgraditi celotno omrežje sodelujočih dobaviteljev in uporabnikov preko pametnih pogodb in plačevanja kar v izbrani kriptovaluti – vse to brez človeškega posrednika [39]. Največja prednost takega sistema je, da ni potrebno nobeni sodelujoči strani v pogodbi zaupati ostalim sodelujočim, ampak zgolj zaupati v skupno omrežje, ki pogodbe potrjuje. Obstajajo dobavne verige, ki temeljijo kar na Bitcoinu – recimo proizvajalec avtomobilov Tomcar, rudarska industrija BHP Billiton, draguljarska industrija De Beers za sledenje draguljem ...

3.9.3 Video igre

Za video igre je zelo velik korak predstavljala vpeljava blockchaina v digitalne platforme. Blockchain namreč uporabnikom omogoča transparentni vpogled v kodo – in s tem v poštenost programa, zavarovanje digitalne lastnine in tudi med-platformno sodelovanje [40]. Blockchain implementacija Ethereum omogoča tudi razpoznavanje različnih digitalnih kovancev med seboj, kar lahko izdelovalci iger izkoristijo kot pretvorbo kovancev v digitalne dobrine. Na primer kovanec 123 v določeni igri predstavlja srednjeveški meč, če ta kovanec uporabnik prenese do druge igre, mu lahko tam predstavlja drugo dobrino – na primer avtomobil. S tem se lahko ustvari digitalno

4 Pametne pogodbe in Ethereum

Razvoj pametnih pogodb se je razvil nedolgo za tem, ko se je prvič pojavil Bitcoin [22]. Pametna pogodba je v osnovi digitalni sporazum med dvema osebama, ki ga morata oba podpisati z digitalnima podpisoma. Nato blockchain sproži to pogodbo ob specifičnih trenutkih. Veljaven primer take pogodbe je, da se vsak dan nakaže določena vsota denarne enote iz imetja osebe A osebi B, kot je na primer vračilo izposojenega denarja.

Čeprav obstajajo pametne pogodbe, ki delujejo na Bitcoinu, ta ni najbolj primeren za izvajanje pametnih pogodb. Namreč Bitcoinu manjka zelo pomembna lastnost – popolni jezik po Turingu [26]. To v praksi pomeni, da se z njim ne da implementirati poljubne pogodbe. Rešitev za to pomanjkljivost je predstavil Ethereum, ki v implementaciji vključuje skoraj popoln jezik po Turingu [43]. Ta omogoča izdelavo skoraj poljubne pametne pogodbe.

Na primer pri Ethereumu se lahko izvede določena pogodba ob vsaki izdelavi novega bloka, če so pogoji za njeno izvajanje izpolnjeni. Pogodba je lahko poljubno dolga, a daljša kot je, več stane njeno izvajanje – ta strošek se pojavlja vse dokler so izpolnjeni ostali pogoji za uresničevanje pogodbe.

4.1 Osnovno o pametnih pogodbah

Pri Ethereumu so pametne pogodbe zelo razvite, saj predstavljajo enega njegovih pomembnih fokusov. Ethereum pogodbe tako omogočajo na primer [21]:

1. izvajanje pogodbe zgolj, ko se strinja določen odstotek ljudi;
2. interakcijo sporazumov med različnimi ljudmi;
3. naključno izvajanje v pogodbi;
4. podporo drugim pogodbam.

Zelo pomembna točka je, da imajo pogodbe možnost interakcije med seboj. Na primer pogodba A se lahko vedno sklicuje na pogodbo B ter zažene celotno kodo te druge pogodbe. Recimo pogodba B vsebuje kodo za določanje psevdonaključnih števil glede na trenutno situacijo, recimo hash zadnjega bloka. Pogodba A lahko uporabi naključno število pogodbe B v izvajanju. To deluje podobno kot uporaba knjižnic v programskih jezikih.

Ker se pogodbe zavedajo obstoja drugih pogodb, je mogoče ustvariti tudi mrežo z znano velikostjo. V tej mreži se pogodba izvede zgolj, če se določen odstotek ostalih pogodb strinja z izvajanjem. Na primer: pogodba A se odloča, ali se bo izvedla in

upošteva mnenje pogodb B, C in D. Te pogodbe imajo lahko v implementaciji zapisano kodo, v kakšnih primerih se bodo strinjale s pogodbo A in v kakšnih ne. Na primer: pogodba B se lahko strinja s pogodbo A, če ji ponudi vsaj 10 Ethereum kovancev, če je danes sončni dan in če je bila včeraj sreda. Na ta način se lahko ustvari celotno omrežje glasovanja.

4.2 Ethereum standardi

Ethereum je uvedel tudi veliko tehničnih standardov, ki jih lahko pogodbe vsebujejo. Ti standardi drugim pogodbam zagotavljajo, da se lahko sklicujejo na to pogodbo z dogovorjenim komunikacijskim protokolom, če določena pogodba vsebuje tak standard. To deluje podobno kot protokoli v računalniških omrežjih.

Kratica za Ethereum standarde je ERC (ang. Ethereum request for comments), kar poudarja dejstvo, da so standardi javni in odprti, tako da jih lahko javnost pred izdajo oceni, poišče napake in predlaga spremembe. Vsak standard mora biti javno potrjen, preden lahko izide v uporabo. Da se tak standard uvede, mora seveda obstajati potreba po njem.

4.2.1 ERC-20

Za to delo je najbolj pomemben standard ERC-20, ki ga je predlagal Fabian Vogelsteller leta 2015 [60]. Točna implementacija tega standarda je opisana v algoritmu 1. Priljubljenost standarda je lahko dokazana s tem, da je leta 2019 standard presegel 200.000 ustvarjenih kovancev na Ethereum omrežju [48]. Številka v zadnjih letih strogo narašča, predvsem zaradi hitrega naraščaja priljubljenosti iger, temelječih na blockchainu.

Algoritem 1 Struktura vmesnika ERC-20

```
function totalSupply() public view returns (uint256);
function balanceOf(address who) public view returns (uint256);
function transfer(address to, uint256 value) public returns (bool);

function allowance(address owner, address spender) public view returns (uint256);
function transferFrom(address from, address to, uint256 value) public returns (bool);
function approve(address spender, uint256 value) public returns (bool);

event Transfer(address indexed from, address indexed to, uint256 value);
event Approval(address indexed owner, address indexed spender, uint256 value);
```

ERC-20 opisuje načine, kako se lahko izdela nove kovance na Ethereum omrežju in kako se jih lahko menjuje (pošilja) med uporabniki. Opisuje zgolj šest osnovnih funkcij, ki jih mora pametna pogodba vsebovati, da lahko interaktira z ostalimi pametnimi

pogodbami s poljubnimi Ethereum kovanci. Teh šest funkcij omogoča fleksibilnost za nadaljnji razvoj in hkrati vzdržuje trdne temelje za vse pogodbe, ki želijo komunicirati med seboj. ERC-20 je mišljen zgolj kot denarno sredstvo, zato razlikovanje med posameznimi kovanci ni niti potrebno niti zaželeno.

4.2.2 ERC-721

Ker ERC-20 ni znal razločevati med različnimi kovanci, se je kmalu pojavila ideja o nadgradnji s standardom, ki bi imel to lastnost razpoznave. Tako je nastal standard ERC-721, ki je nadgrajeval standard ERC-20 in mu dodal več novih funkcionalnosti [52]. Natančna implementacija tega standarda je opisana v algoritmu 2. Najpomembnejši doprinos tega standarda je bila uvedba medsebojno nezamenljivih kovancev (ang. non-fungible). Za navadne porabe kriptovalute to ni potrebno, saj je načeloma en Bitcoin enakovreden vsem ostalim, podobno kot tudi pri realnih denarnih valutah, na primer evrih in dolarjih. Bistvo ERC-721 standarda je to, da lahko en kovanec predstavlja točno določeno digitalno dobrino in se vsi uporabniki v omrežju strinjajo, kaj ta kovanec predstavlja. Na primer kovanec 123 lahko predstavlja digitalnega psa, ki se razlikuje od kovanca 125, ki predstavlja mačko. Pod prejšnjim ERC-20 standardom bi oba predstavljala en kovanec – denarno enoto.

Algoritem 2 Struktura vmesnika ERC-721

```
event Transfer(address indexed _from, address indexed _to, uint256 _tokenId);
event Approval(address indexed _owner, address indexed _approved, uint256 _tokenId);
event ApprovalForAll(address indexed _owner, address indexed _operator, bool _approved);

function balanceOf(address _owner) public view returns (uint256 _balance);
function ownerOf(uint256 _tokenId) public view returns (address _owner);
function exists(uint256 _tokenId) public view returns (bool _exists);

function approve(address _to, uint256 _tokenId) public;
function getApproved(uint256 _tokenId) public view returns (address _operator);

function setApprovalForAll(address _operator, bool _approved) public;
function isApprovedForAll(address _owner, address _operator) public view returns (bool);

function transferFrom(address _from, address _to, uint256 _tokenId) public;
function safeTransferFrom(address _from, address _to, uint256 _tokenId) public;
function safeTransferFrom(address _from, address _to, uint256 _tokenId, bytes _data) public;
```

Zelo pomembna lastnost je tudi ta, da se lahko v standardu ERC-721 določi, koliko kovancev lahko obstaja, ki predstavljajo „enako“ digitalno dobrino. Na primer, določi se lahko, da bodo kadar koli obstajali največ trije kovanci, ki bodo predstavljali

mačko. Ti kovanci lahko bodisi obstajajo od samega začetka bodisi se izdelajo pozneje – v danem trenutku lahko obstaja nič, ena, dve ali tri mačke. To sedaj nakazuje, da je v bistvu vsak kovanec v ERC-721 standardu unikaten in se ga da razlikovati od vseh drugih kovancev, čeprav jih lahko več predstavlja enako digitalno dobrino [8].

Sploh v nastanku računalniških iger je zelo pomembno, da vsebujejo pogodbe v igrah vsaj ERC-721 standard, da se lahko predstavlja različne digitalne stvari v igri z Ethereum kovanci. Prva digitalna igra, ki je uporabljala ERC-721 standard, je bila CryptoKitties, ki je izšla 20. septembra 2017 [7]. Kmalu za izidom te igre in strmim povečanjem priljubljenosti se je povečalo tudi povpraševanje po specifičnih Ethereum standardih. Sledil je nastanek ERC-1155 standarda, ki je dodatno razširil standard ERC-721.

Zelo pomembno je dejstvo, da ERC standardi ne določajo natančne implementacije menjave kovancev med pogodbami in uporabniki, temveč da zgolj delujejo kot vmesnik, ki opišejo strukturo pogovora pogodb med seboj. Čeprav lahko Ethereum implementacija podpira različne standarde – recimo ER–721 – še ne pomeni, da je implementacija te pogodbe dobra, temveč zgolj da vsebuje vse potrebne funkcije za uporabo ERC-721 vmesnika. Iz tega razloga je potrebno pred vsako interakcijo s pogodbo, bazirano na ERC standardu, preveriti tudi njeno implementacijo.

4.3 Aplikacije pametnih pogodb

V tem razdelku bodo opisane različne implementacije in aplikacije uporabe pametnih pogodb Ethereruma v praksi. Ethereum je med novejšimi blockchain implementacijami in se ne uporablja v tako veliko sistemih kot na primer Blockchain, a sta njegova fleksibilnost in obseg delovanja večja, zato tudi priljubljenost Ethereuma in pametnih pogodb zelo hitro narašča.

Potrebno je omeniti, da lahko pametne pogodbe obstajajo na glavni Ethereum verigi in uporabljajo kot sredstvo osnovno Ethereum kriptovaluto ETH, ali pa obstajajo na stranski verigi. Obstoj na stranski verigi omogoča implementacijo novih pogodb, ki imajo določeno strukturo in so specializirane za reševanje točno določenih problemov. Take pogodbe pogosto vsebujejo tudi unikatne kriptovalute, ki so pogoste odvisne od ETC-ja.

4.3.1 DeFi

Zelo zanimiva aplikacija Ethereum pametnih pogodb je DeFi (ang. Decentralised Finance). DeFi je gibanje, ki ga soustvarjajo skupine razvijalcev in projektov, ki razvijajo interoperabilne protkole na podorčju financ. Njena posebnost je to, da deluje popolnoma decentralizirano, brez centralne ustanove, ki bi omejevala vključevanje novih orodij in nadzorovala interakcijo med uporabniki z platformo. DeFi ponuja tudi nekatere hibridne rešitve, ki niso povsem decentralizirane, saj se nekaterih problemov ne izplača decentralizirati [11].

Cilj gibanja DeFi je, da bi lahko vključevala najrazličnejše finančne rešitve, kot so na primer bančništvo, varčevalni računi, zavarovalnice itd. Osnovna ideologija sloni na ideji odprtih finančnih sistemov, ki bi se jih lahko posluževali tudi tisti, ki sedaj nimajo dostopa do finančnih inštrumentov. Prvi uspešen projekt je MakerDAO. Gre za popolnoma decentralizirano avtonomno organizacijo, ki s pomočjo pametnih pogodb omogoča deležnikom samo-uravnavanje, ki s pomočjo običajnih tržnih tokov ponudbe in povpraševanja ohranjajo stabilnost vrednosti žetona DAI na točno 1$ in tistim ki zagotavljajo likvidnost izplačujejo obresti. Kovanec dai, ki sledi vrednosti dolarja je mogoče integrirati v ostale protokole. To je pomemben korak, saj služi kot most med tradicionalnimi in digitalnimi valutami. V kratkem so so v defi ekosistem prišli ostali projekti ki ponujajo storitve kreditov, zavarovanja, trgovanja z obveznicami, varčevanja, pokojninskih skladov, avtomatiziranih skladih, itd. Bistvena prednost vseh protokolov je, da pravil ni mogoče spreminjati, da so pravila in pogoji jasna zagotovljeno obvezujoča hkrati pa je lastnik ves čas v popolni kontroli svoje lastnine. Ker gre v večini primerov gre zgolj za skupek pametnih pogodb je strošek sistema zgolj razvoj in vzdrževanje. Na ta način je posojilo dai na makerDAO doseglo stabilno obrestno mero zaokroženih 10% na leto, kar je veliko višje kot tradicionalno bančništvo in trenutno ekosistem zajema 789.3M dolarjev.

V primeru, da bi se veliko orodij vključilo v DeFi, bi lahko vse elektronske transakcije delovale na enak način, z enakimi protokoli. Tako bi omogočili decentralizirano komunikacijo med vsemi pametnimi pogodbami. Pri DeFi sploh ni pomembno, kakšna so ta orodja in strani, ki hočejo sodelovati v omrežju, pomembno je zgolj, da imajo implementiran skupni vmesnik. Tako so omogočene spletne finance brez omejitev na določene bančne kartice in spletne strani za transakcije.

Dodatna zelo uporabna lastnost je to, da je celotno omrežje zelo enostavno avtomatizirati, saj vsa orodja delujejo preko Ethereum pametnih pogodb. Transakcije in izvajanje pametnih pogodb postanejo skoraj instantne. Dodatna zelo uporabna lastnost je, da je izgradnja takih orodij in uporaba DeFi-ja zelo enostavna, saj deluje na preprostih Ethereum pametnih pogodbah in je zelo enostaven za uporabnike [35].

4.3.2 Dobavna veriga

Zelo potencialno področje za uporabo pametnih pogodb Ethereuma je dobavna veriga. Implementacija Bitcoina v dobavnih verigah je bila opisana v tem podrazdelku 3.9.2, Ethereum pametne pogodbe omogočajo več dodatnih možnosti. Ker Ethereum pametne pogodbe vsebujejo skoraj popoln jezik po Turingu, lahko z njim opišemo skoraj poljuben program v pogodbah za opis želenega delovanja dobavnih verig. Zelo uporabna lastnost je tudi, da se lahko pogodbe sklicujejo na druge pogodbe in s tem ustvarijo nekakšno digitalno verigo pogodb.

Na primer v podjetju Daitan sloni celotna avtomobilska proizvodnja na čistih Ethereum pametnih pogodbah [42]. Kot zelo uporabna lastnost se je zopet pokazala možnost sklicevanja na druge pametne pogodbe. Izkazalo se je, da to zelo skrajša čas razvijanja nove rešitve in tudi zanesljivost delovanja. S skrajšanim časom razvijanja se zmanjša tudi cena projekta, kar naredi Ethereum pametne pogodbe zelo privlačne za uporabo.

4.3.3 Internet stvari

Internet stvari (ang. Internet of things – IoT) je skupek naprav, ki so med sabo povezane, lahko sodelujejo med sabo in opravljajo specifično delo [49]. Ocena za leto 2017 je bila, da je na svetu 8,4 milijarde takšnih naprav, kar je več kot je bilo na svetu ljudi. Do leta 2030 pričakujejo tudi do 500 milijard takih pametnih naprav [53].

Zaradi hitro naraščajočega števila in tesne medsebojne povezanosti je ključnega pomena tako hitrost kot učinkovitost medsebojnega komuniciranja. Odvisnost od centralne avtoritete ni zaželena, tako zaradi odvisnosti od nje v slučaju padca delovanja naprave, kot tudi zaradi morebitne preobremenjenosti take naprave s številom IoT naprav. Skalabilnost celotnega sistema je namreč v omrežju odjemalec–strežnik odvisna od zmožnosti centralne naprave.

Logična rešitev za prejšnji problem je decentralizacija teh naprav od centralne naprave in uvedba konsenza za komunikacijo med napravami. Potrebni tip konsenza je popolnoma odvisen od primera uporabe teh naprav. Za veliko problemov so se izkazale zelo uporabne pametne pogodbe. Te namreč omogočajo zelo hitro komunikacijo med napravami, saj se pogodbe lahko izvajajo s hitrostjo procesiranja posamezne naprave. Dodatna zanimiva lastnost je tudi možnost uvedbe kriptovalute za transakcije med napravami. Stvari lahko pridejo tako daleč, da lahko določena naprava potrebuje za delovanje elektriko in to vsak dan kupi od druge naprave preko pametne pogodbe s transakcijo kriptovalute. Naprave se lahko tako povežejo v celotno omrežje, ki je teoretično lahko poljubno veliko. V tem omrežju komunikacija teče vse dokler se znajo naprave zanesljivo pogovarjati med seboj – uporabljajo iste ali podobne komunikacijske protokole.

4.3.4 Računalniške igre

Tudi v računalniških igrah je uporaba pametnih pogodb v zadnjem času zelo narasla. Privedla je celo do tega, da so se začele pojavljati različne platforme za ponujanje ustvarjenih pametnih pogodb uporabnikom. Programer, ki želi uporabljati Ethereum v novi igri, lahko zgolj uporabi obstoječo platformo in ima na ta način že vključene delujoče pametne pogodbe. Primeri takih Ethereum platform za igre so opisani v razdelku 5. Nato programer z ustreznimi klici v programskem okolju zgolj aktivira posamezne dele pametne pogodbe in uporablja Ethereum pametne pogodbe v igri z minimalnim poznavanjem ozadja Ethereuma.

Platforme za računalniške igre se nahajajo zelo visoko na lestvici najbolj uporabljenih blockchain implementacij. Na primer platforma Enjin, ki je ena najbolj uporabljenih nasploh, je v času pisanja tega dela na 80. mestu najbolj vredne blockchain implementacije s kar 60 milijoni dolarjev. Igre, ki temeljijo na Enjinu, igra kar 20 milijonov različnih uporabnikov.

Pametne pogodbe so v računalniških igrah zanimive predvsem za izvajanje transakcij med igralci in za uvajanje novonastalih kovancev v obtok. Potencial se prikazuje tudi v povezani digitalni ekonomiji med različnimi igrami. Potencialen primer je izmenjava kovancev med vsemi igrami, ki trenutno obstajajo, a takšna rešitev trenutno še ne obstaja.

5 Računalniške igre in blockchain

V tem razdelku so predstavljene izbrane razvijajoče se igralske platforme, ki uporabljajo blockchain. Namen tega razdelka je bralca seznaniti z najnovejšimi platformami in pristopi ter predstaviti njihove prednosti in slabosti. Predstavljen je tudi postopek izbire najbolj primerne blockchain platforme za to magistrsko delo. Analizirane so različne metrike, na podlagi katerih bo bila utemeljena končna izbira platforme.

5.1 Igralni pogoni

Igralni pogon je programsko okolje, ki omogoča razvijalcem hitrejši razvoj iger in tudi ponovno uporabnost komponent posameznih iger za izdelavo novih iger [36].

V tem podrazdelku je najprej predstavljena zgodovina igralnih pogonov, ki bralca seznani z začetkom razvoja igralnih pogonov skozi čas. V drugem delu so opisane njihove glavne funkcije. Na koncu je predstavljen izbran igralni pogon, ki je bil uporabljen za izdelavo tega dela – Unity 3D.

5.1.1 Zgodovina igralnih pogonov

Računalniške igre se vse od začetka niso razvijale samostojno, temveč je njihov razvoj spremljal tudi igralni pogon (ang. game engine). Sprva je vsaka igra vsebovala ločen igralni pogon, ki je služil razvoju igre, vpeljevanju novih funkcionalnosti in dolgotrajnemu vzdrževanju [19]. Tako sta se igra in njen igralni pogon razvijala vzporedno, saj so spremembe enega neposredno vplivale na spremembe drugega.

Po letu 1990 so se začeli razvijati prvi neodvisni igralni pogoni, ki niso bili več vezani na eno igro, temveč so nudili možnost razvijanja in vzdrževanja več različnih, a medsebojno sorodnih iger. Fokus igralnih pogonov je bil v tistih časih ozek, saj je omogočal ponovno uporabo zgolj posameznih komponent. Uporabljal se je večinoma za nadgrajevanje igre in vzdrževanje iger ter izdelavo nadaljevanj serije neke igre.

Tretja faza razvoja je prinesla popolnoma neodvisne igralne pogone širokega spektra. Ti igralni pogoni so omogočali izdelavo skoraj poljubne igralne igre in so se obdržali v uporabi vse do danes. Primera takih igralih pogonov sta Unity 3D in Unreal Engine, ki sta danes med najbolj priljubljenimi pogoni.

Večina teh igralnih pogonov je dandanes na voljo širši javnosti brezplačno. Obstajajo tudi plačljive nadgradnje licence za dodatne funkcionalnosti, podporo pri uporabi in svetovanje iz strani proizvajalca. Za izdelavo predstavljene igre je bila uporabljena brezplačna verzija programa Unity 3D, saj omogoča vso funkcionalnost v brezplačni verziji in je enostaven za uporabo.

5.1.2 Funkcije igralnih pogonov

Razlog za uporabo igralnih pogonov za izdelavo računalniške igre je predvsem v zmanjšani količini dela in večji zanesljivosti delovanja. Z uporabo ustreznega igralnega pogona se lahko uporabi prej raziskane in optimalne algoritme. Razvijalec se lahko tako ukvarja s programerskimi področji na veliko višjem nivoju, kot bi bilo to drugače potrebno. Zmanjšana količina potrebnega časa neposredno vodi tudi do cenejšega razvoja, vzdrževanja in tudi manjše potrebne ekipe za razvoj programske opreme. Najpomembnejša orodja, ki jih lahko ponujajo igralni pogoni, so (L. Bishop et al., P Paul et al.) [36], [44]:

1. pogon za fizikalne zakonitosti;
2. grafični pogon;
3. pogon za umetno inteligenco;
4. pogon za skripte – skriptni jeziki;
5. pogon za zvok.

Ta orodja lahko drastično zmanjšajo čas razvoja, saj vsebujejo široko uporabljene algoritme in izčrpno testirane rešitve, ki se hitro posodabljajo ob najdenih napakah. Na primer pogon za fizikalne zakonitosti ima zmožnost simulacije fizikalnih zakonov v digitalnem svetu sam po sebi. V primeru, da razvijalec ustvari kroglo v digitalnem svetu in ji nastavi težo, bo nanjo vplivala gravitacija, krogla se bo odbijala od tal glede na njeno elastičnost in bo zakrivala sončne žarke. V nasprotnem primeru bi moral vse to novi razvijalec implementirati sam. Z uporabo igralnega pogona ima razvijalec za uporabo pripravljen celoten spekter fizikalnih zakonov. Seveda, če hoče razvijalec prilagoditi fizikalne zakone, na primer na zakone drugih planetov, more popraviti delovanje programa v fizikalnem pogonu.

5.1.3 Igralni pogon Unity 3D

Za to delo je bil izbran pogon Unity 3D. Ta pogon omogoča enostavno izdelavo računalniških iger na več kot 25 različnih platformah, podpira izdelavo 2D iger, 3D iger in iger v virtualni resničnosti [3]. Igro je mogoče izdelati tako, da deluje skoraj brez spremembe na poljubno mnogo različnih platformah, tako da se spremeni zgolj uporabniški vmesnik (ang. User interface/user experience – UI/UX), za optimizacijo na izbrano platformo.

Unity 3D je bil prvič predstavljen leta 2005 za podporo izdelovanja računalniških iger na operacijskem sistemu MAC OS. Z leti je pridobil možnost razvijanja tudi za druge računalniške platforme, na primer Windows, Android, Linux, Samsung TV itd. Unity podpira v splošnem tri različne programske jezike: C#, JavaScript in Boo. Vsi ti trije programski jeziki se med izvajanjem prevedejo v C++ jezik za hitrejše in optimizirano delovanje.

Ta igralni pogon vsebuje vse funkcionalnosti in orodja, ki so bile opisane v razdelku 5.1.2. Uporaba teh orodij je večinoma na visokem nivoju, da se razvijalcu ni potrebno

spuščati v implementacijo, ter zgolj spreminja parametre. Na primer za spreminjanje gravitacije ima parameter, kjer določi trenutno gravitacijo – privzeta gravitacijska moč je nastavljena na zemeljsko. Omogoča tudi enostavno delo z animacijami, zvokom, umetno inteligenco in grafičnim pogonom.

5.2 Uporaba blockchaina za podporo ekonomije v igrah

Pomembno vprašanje za uporabo blockchaina v igrah je: "Na kakšen način implementirati blockchain v to specifično igro?"Na tem mestu obstajata dve različni možnosti:

1. integracija v igralni pogon;
2. uporaba zunanjega blockchaina.

Prva možnost se je izkazala za praktično, saj če blockchain omogoča uporabo v igralnem pogonu, se lahko pravilnost delovanja preverja skoraj instantno. Dodatno lahko ponuja celo interakcijo z vmesnikom te platforme na visokem nivoju, da se razvijalcu ni potrebno spuščati v implementacijo blockchaina.

Druga možnost je uporaba oddaljenih funkcij (ang. RPC – Remote Procedure Call) blockchaina. Tako se čas razvijanja podaljša, večja je tudi možnost za napake, ker mora biti razvijalec popolnoma seznanjen z delovanjem blockchaina. Prav tako je potem razvijalec tudi vezan na morebitne popravke v primeru sprememb v delovanju uporabljene blockchain implementacije. Dobra lastnost te možnosti je, da se lahko razvijalec poveže do izbrane platforme preko poljubnega vmesnika, ki je lahko bodisi igralni pogon bodisi kaj drugega. Tako lahko tudi nadgrajuje vmesnik po lastnih željah in potrebah.

V tem razdelku so opisane različne implementacije blockchaina, ki so narejene specifično za razvoj in implementacijo v računalniških igrah. Pri vseh implementacijah so opisani razlogi za uporabo, prednosti in slabosti. V podrazdelku 5.3.6 bo opisana končna izbrana kombinacija, ki je bila izbrana za to delo, in razlogi za to odločitev.

5.2.1 Enjin

V zadnjem času je ena hitro razvijajočih se blockchain platform Enjin. Ta platforma je bila ustvarjena leta 2009, a je doživela prvi preboj z ustvarjanjem prve kripto valute leta 2017 [15]. Enjin temelji na Ethereumu, na katerem temelji tudi večina ostalih platform, ki so vsebovane v tej analizi.

Vizija Enjina je, da omogoči razvijalcem enostaven razvoj računalniških iger, s čim manj predznanja. Na tak način se lahko vsakdo s programerskim predznanjem vključi v igro Enjin in se enostavno poveže na blockchain verigo, v tem primeru Ethereum.

Fokus Enjina je na igralnem pogonu Unity 3D, saj nudi Enjin popolno integracijo v tem igralnem pogonu. Uporabljati se ga da tudi v drugih igralnih pogonih, a je celotna optimizacija vmesnika mišljena predvsem ozko za Unity 3D. Na primer, če razvijalec uporablja igralni pogon Unity 3D, je Enjin lahko ena boljših možnosti, če le niso razvijalčeve zahteve preveč specifične. V primeru da razvijalec uporablja drugi igralni pogon, obstajajo bolj specializirane alternative.

5.2.1.1 Uporaba platforme Enjin

Za uporabo platforme Enjin razvijalec najprej pripravi igralni pogon Unity 3D in v njem postavi osnove igre. Ko je ogrodje igre postavljeno, doda še vmesnik Enjin SDK, ki skrbi za pravilno komunikacijo Unity 3D in platforme Enjin. Integracija teh dveh sistemov je samodejna, saj za vse poskrbita sami. Uporabnik ima na voljo kratek tečaj uporabe in tudi primere klicev oddaljenih funkcij, ki jih bo potreboval za izdelavo in razvoj računalniške igre.

Ko ima uporabnik nameščen vmesnik Enjin SDK v Unity 3D igralnem pogonu, lahko vsakemu igralcu te igre ustvari nov Enjin račun in digitalno denarnico, ki služi prikazu dobrin, ki jih igralec poseduje na blockchainu. Fokus Enjina je ravno v omogočanju izmenjave dobrin med igralci, ustvarjanje novih dobrin za razvijalce in omejevanje različnih dobrin. Na primer, če razvijalec ustvari novo dobrino, lahko označi v Enjin pogodbi, da jih bo vedno ustvarjenih največ 50. Tako imajo uporabniki te igre zagotovilo, da ima s petimi takšnimi kovanci vedno vsaj desetino vseh kovancev, ki bodo kadar koli obstajali v tej igri. Ravno to daje občutek vrednosti vsaki digitalni dobrini igralca.

5.2.2 Decentraland

Decentraland je zanimiva platforma, ki se je razvila leta 2017 [14]. Decentraland uporabniku omogoča kupovanje omejene količine virtualnih posestev na Ethereum omrežju, njihovo spreminjanje, urejanje in tudi monetizacijo.

Kot pove ime Decentraland je glavni fokus platforme na decentraliziranih virtualnih posestvih. To v praksi pomeni, da ni centralne ustanove, ki bi nadzorovala lastništvo posestva in nadzor mogoče izrabila. S tem zavaruje tudi pred propadom take ustanove, saj bi v tem primeru vsi uporabniki izgubili vsa posestva. Decentralizacija celotnega sistema omogoča tudi neposredno kupovanje, prodajo in nadzor nad uporabnikovim delom posestva.

Unikatna razlika med Decentralandom in ostalimi platformami je predvsem v tem, da tu ni neposrednih dobrin, temveč je vse predstavljeno preko vmesnika, ki ga predstavljajo virtualna posestva.

5.2.2.1 Uporaba platforme Decentraland

Postopek uporabe blockchaina je pri Decentralandu drugačen kot pri ostalih platformah. Celoten sistem se deli v dve dobrini: „Mano“ in posestva (ang. Land). Če želi uporabnik imeti digitalno posestvo v Decentralandu, jo mora kupiti preko njihove

trgovine z dobrino imenovano „Mana“. Ta dobrina je v resnici kriptovaluta, ki stoji za Decentralandom. Razvijalec mora najprej kupiti ustrezno količino „Mane“ preko poljubne spletne menjalnice, nato pa v Decentraland trgovini kupiti izbrano posestvo.

Na teh posestvih lahko razvijalec počne skoraj kar koli. Primarna funkcija je, da ustvarja nove dobrine na teh posestvih in igra igro. Na primer igralec lahko promovira kakšno drugo igro na posestvih, posestvo lahko po različnih postopkih monetizira, lahko prodaja delčke posestev naprej drugim uporabnikom itd. Možnosti za upravljanje posestev so široke, saj decentraliziran sistem ni za to predstavil nobenih omejitev.

Če se razvijalec odloči uporabiti Decentraland v računalniški igri, mora najprej ustvariti posestvo na njihovi matični mreži ter na njem ustvariti določene objekte, ki predstavljajo objekte v njegovi igri. Pravico do teh objektov uporabnik kasneje prodaja v igri. Ideja je inovativna, a predstavlja tudi nekaj ovir. Uporabnik mora biti namreč za preverjanje lastništva objekta in za pregled možnosti interakcije s tem objektom prijavljen tudi v Decentraland, ne zgolj v igro razvijalca, kar predstavlja dodatno delo.

5.2.3 Loom Network

Loom Network je relativno nova platforma, ki je prišla v uporabo v začetku leta 2018. Glavna ideja Loom Networka je, da bi razvijalcu omogočil hiter in enostaven razvoj računalniških iger.

Ta platforma ponuja vrsto različnih vodičev, kjer se lahko manj izkušeni razvijalec najprej spozna s blockchainom, nato z Ethereumom, nazadnje tudi z Loom Networkom. Ideja je v tem, da lahko uporabnik samo z osnovnim znanjem računalništva postavi prvo računalniško igro z blockchainom. Loom Network omogoča tudi naprednim razvijalcem razvijanje zahtevnejših projektov in skokovito nadgradnjo znanja.

Velik poudarek ima na Ethereum stranskih verigah, kar omogoča veliko skalabilnost glede števila obdelanih transakcij in s tem podpirajočega števila igralcev.

5.2.3.1 Uporaba platforme Loom Network

Celotna interakcija razvijalca s platformo Loom Network poteka preko njihovega Loom SDK-ja. (ang. SDK – Software development kit). Ta vmesnik poskrbi za spreminjanje funkcijskih klicev razvijalca v njihove preslikave na Loom omrežju. Na primer, če želi razvijalec napisati funkcijo za pošiljanje kovancev med uporabniki, ne napiše celotne blockchain kode, temveč zgolj uporablja klice Loom SDK-ja. Loom SDK nato poskrbi za ustrezne pretvorbe v nižje nivojske funkcije, ki ustrezno opisujejo dogajanje na blockchainu.

Loom SDK je neodvisen od platforme in igralnega pogona, kar pomeni, da lahko v splošnem razvijalec z njim interaktira iz poljubnega programa. Najpogosteje preko klicanja oddaljenih RPC procedur. To omogoča možnost integracije v poljuben uporabnikov izdelek, kar omogoča fleksibilnost te platforme.

Za uporabnika je enostavna tudi interakcija s programom, ki vključuje Loom Network, saj se uporabnik prisotnosti Loom SDK-ja sploh ne zaveda. Najpogosteje misli, da je v interakciji z glavnim programom, najpogosteje z igro. To omogoča manj zahtevnim uporabnikom enostavno uporabniško izkušnjo. Zahtevnejši uporabniki, ki jih zanima dogajanje v ozadju, pa lahko vidijo uporabo decentralizacije dobrin v blockchainu.

5.2.4 FunFair

FunFair je platforma, ki je prvič prišla v uporabo konec leta 2017 in doživela večji razvoj leta 2018. Kot je opisano v njihovi beli knjigi [59], je vizija te platforme predvsem omogočiti razvijalcem narediti hitre, poštene in decentralizirane igre.

Fokus podjetja je na igrah za spletne igralnice – kazinoje. Platformo se lahko uporabi tudi v ostalih igrah in implementira v igralnih pogonih. Transparentnost platforme omogoča igralcem vpogled v kodo, kar pomeni, da imajo možnost vpogleda v poštenost igre. Ta pomembna lastnost je privlačna v spletnih igralnicah, saj je pomembna želja igralcev to, da zaupajo denar zgolj poštenim igram.

Pri digitalnih računalniških igrah, ki so pogosto kompleksnejše in večje od iger v spletnih igralnicah, transparentnost kode ni vedno glavnega pomena. Pri takih igrah včasih igra vlogo tudi konkurenčna prednost, saj želi podjetje programske rešitve skriti pred konkurenco. Zato ne more vedno uporabiti transparentnih pogodb in delov kode.

5.2.4.1 Uporaba platforme FunFair

Uporaba te platforme je za razvijalce težja od ostalih, saj ne ponuja nobenega vmesnika in tudi ne integracije igralnim pogonom. Primanjkljaj vodičev (ang. tutorial), kjer bi se lahko začetniški razvijalec naučil uporabe platforme, te najbrž tudi odvrne od uporabe te platforme.

Specializacija za spletne igralnice lahko odvrne tudi veliko ljubiteljev običajnih iger, ki bi radi vključili eno izmed blockchain platform v računalniške igre. Integracija te platforme je zahtevna, saj so klici funkcij omejeni na potrebe spletnih igralnic in je potrebno preurediti obstoječo kodo novim klicem oddaljenih procedur.

Za izdelavo iger, namenjenih spletnim igralnicam, je FunFair celovita rešitev pri implementaciji blockchaina. Enostavnost dokazovanja poštenosti je v tem področju velikega pomena. Transparentnost kode je tudi prijazna do potencialnih razvijalcev, saj se lahko začetni razvijalci enostavno naučijo pisanja kode in rokovanja s sistemom FunFair na obstoječih transparentnih sistemih. Hitrost platforme in enostavnost uporabe za končnega uporabnika, ki največkrat sploh ne ve, da uporablja to platformo, omogoča enostavno uporabniško izkušnjo.

5.3 Analiza blockchain platform

V tem podrazdelku so najprej predstavljene objektivne primerjave med posameznimi pomembnimi atributi za preučevane blockchain platforme. Točke analize so izbrane iz vidika ciljev za to magistrsko delo. Na koncu bodo predstavljeni tudi subjektivni zaključki te analize, ki bodo služili predvsem izboru ustrezne platforme za nadaljnje delo.

5.3.1 Podpora standardu ERC-721

Pomembne dodatne možnosti za igre, narejene na blockchain platformah, predstavlja standard ERC-721. Ta standard omogoča in opisuje, kako se lahko naredi medsebojno nezamenljive kovance tako, da se jih da jasno razločiti med sabo [24]. Ker je ena najbolj pomembnih zahtev nadaljnjega dela vsebovanje unikatnih dobrin, kar ponuja ERC-721 standard, je to pomembna točka za analizo.

Platforme Enjin, Decentraland in Loom imajo vgrajeno podporo za ERC-721 standard, Loom in Enjin imata tudi podporo za specifične standarde, ki standard ERC-721 nadgrajujejo. Enjin vsebuje nadgradnjo protokola ERC-1155 in Loom Network vsebuje nadgradnjo ERC-1178. Platforma FunFair ne nudi podpore za noben ERC-721 standard ali enakovredni standard. Rezultati so prikazani v tabeli 1.

Tabela 1: Primerjava platform glede na podporo ERC-721 standarda.

Platforma:	Podpora ERC-721
Enjin	Da, podpira tudi ERC-1155
Decentraland	Da
Loom Network	Da, podpira tudi ERC-1178
Funfair	Ne

5.3.2 Ethereum Plazma

Vse pogosteje se pojavlja vprašanje, kako narediti platforme, ki temeljijo na Ethereumu, vzdržljive, prilagodljive uporabniku in tudi skalabilne [31]. Ker s časom postaja komunikacija z Ethereum verigo zasičena in je transakcij vedno več, se je pojavila rešitev, da bi se ustvarilo dodatno verigo. Ta veriga bi bila pripeta na glavno Ethereum verigo in bi z njo komunicirala zgolj, ko je to potrebno. S tem bi se rešilo problem prilagajanja verige potrebam uporabnika in preobremenjenosti glavne verige. Te verige imenujemo stranske verige. Zaradi zgolj občasne komunikacije stranske verige z glavno verigo postane tudi komunikacijsko breme manjše, s tem se poveča količina prometa, ki lahko vzporedno teče čez glavno verigo, kar poveča skalabilnost glavne verige. Ogrodje, ki vsebuje stranske verige na Ethereumu se imenuje „Ethereum Plasma“.

Po analizi se je izkazalo, da prav vse preučevane platforme nudijo usluge preko plazemskih stranskih verig. Ta metrika je bila za končno analizo neuporabna, a je pokazala, da vse izbrane blockchain platforme v tem pogledu zadoščajo osnovnim potrebam. Rezultati so prikazani v tabeli 2.

Tabela 2: Primerjava platform glede na podporo Ethereum Plasm.

Platforma:	Podpora Ethereum Plasm
Enjin	Da
Decentraland	Da
Loom Network	Da
Funfair	Da

5.3.3 Možnost integracije z igralnim pogonom

Kot je bilo omenjeno v podrazdelku 5.1.2, je zaželena funkcija uporabljene blockchain platforme za nadaljnje delo možnost integracije te platforme z izbranim igralnim pogonom. Vsak program, ki hoče komunicirati z blockchainom, potrebuje vmesnik. Tega lahko razvije bodisi razvijalec sam bodisi ga ponudi ponudnik blockchain platforme. Prednost obstoja takega vmesnika je v tem, da razvijalcu ni potrebno skrbeti za razvoj vmesnika, temveč bo za to poskrbel ponudnik. S prihodom novih verzij se namreč včasih zgodi, da sistem ne deluje več enako kot prej, temu pogosto sledijo sinhronizacijske težave. Te je pomembno rešiti v najkrajšem mogočem času, da ne bi prišlo do napak v delovanju programa in računalniške igre. V primeru, da uporabnik uporablja uradno verzijo takega vmesnika, postane možnost nastanka takih težav občutno manjša.

Analiza vseh teh platform je pokazala, da je edina blockchain platforma, ki trenutno ponuja integracijo SDK-ja z igralnim pogonom, Enjin. Ta ponuja integracijo ravno z igralnim pogonom Unity 3D, ki je trenutno eden najbolj uporabljanih igralnih pogonov [30]. Rezultati so prikazani v tabeli 3.

Tabela 3: Primerjava platform glede na možnost integracije z igralnim pogonom.

Platforma:	Možnost integracije z igralnim pogonom
Enjin	Da (Unity)
Decentraland	Ne
Loom Network	Ne
Funfair	Ne

5.3.4 Uspešnost kripto valute

V času raziskave v okviru tega magistrskega dela je bila najbolj uspešna blockchain platforma Enjin, ki je zasedala 60. mesto na lestvici [10]. Nižje je bila uvrščena platforma Decentraland s približno 90. mestom. Blizu je bila tudi platforma Loom Network s 100. mestom. Zadnja je bila platforma FunFair s 130. mestom.

Najbolj vredna platforma v ameriških dolarjih je bila Enjin s 120 milijoni ameriških dolarjev, sledila sta Decentraland in Loom Network z dobrimi 60 milijoni in na zadnjem mestu je bila FunFair z relativno nizkimi 41 milijoni. Rezultati te analize so predstavljeni v tabeli 4.

Tabela 4: Primerjava platform glede na vrednost platform in trenutno mesto najbolj vrednih blockchain implementacij.

Platforma:	Vrednost platforme v ameriških dolarjih	Trenutno mesto
Enjin	120.000.000	<60
Decentraland	64.000.000	<90
Loom Network	62.000.000	<100
Funfair	41.000.000	<130

5.3.5 Zaključek analize

Tabela 5: V končni primerjavi je razvidno, da integracijo z igralnim pogonom ponuja zgolj platforma Enjin, ki ima tudi največji tržni delež. Vse tehnologije razen Funfair vsebujejo integracijo ogrodja Ethereum Plasm.

Platforma:	ERC-721	Plasm	Igralni pogon	Vrednost	mesto
Enjin	Da – ERC-1155	Da	Da (Unity)	120.000.000	<60
Decentraland	Da	Da	Ne	64.000.000	<90
Loom Network	Da – ERC-1178	Da	Ne	62.000.000	<100
Funfair	Ne	Da	Ne	41.000.000	<130

Izkazalo se je, da je najboljša platforma za nadaljnje delo Enjin, saj podpira vse zastavljene zahteve za razvoj nadaljnjega projekta, kot je prikazano v tabeli 5. Ta zaključek je rezultat specifičnih zahtev tega dela. V primeru, da ima razvijalec drugačne zahteve, se seveda celotni zaključki analize razvrednotijo.

Na drugem mestu sta bili platformi Decentraland in Loom Network, ki jima manjka zgolj integracija v igralni pogon. Integracija je v tem delu prednost, včasih je lahko tudi slabost, najpogosteje, če želi razvijalec imeti igro neodvisno od platforme. Na primer, če bi Unity prenehal s podporo, bi bilo platformo Enjin veliko težje uporabljati, uporaba ostalih treh platform se ne bi spremenila.

Na zadnjem mestu je pristala platforma FunFair, saj je njen poudarek izven razvoja računalniških iger in je osredotočen na spletne igralnice. Iz tega razloga tehnologija ne ponuja vsebovanosti standarda ERC-721, ki je za to delo pomemben.

5.3.6 Končna izbira: Unity 3D in Enjin

Celotno nadaljnje delo je bilo nato izvedeno v kombinaciji igralnega pogona Unity 3D in platforme Enjin. Ta kombinacija omogoča hiter razvoj preko Enjin SDK, ki poskrbi, da so funkcije pravilno pretvorjene v klice oddaljenih RPC procedur za interakcijo z blockchainom. S tem se občutno zmanjša možnost napak. Enjin SDK se razvija skupaj z Unity 3D, tako da z izidom nove verzije Unity pridobi tudi Enjin novo verzijo, posebej prirejeno za zadnje popravke v Unity 3D. Poleg hitrejšega razvoja to omogoča tudi lažje in cenejše vzdrževanje sistema, saj ima vzdrževalec na voljo celotno Enjin

dokumentacijo poleg običajne dokumentacije izdelka.

Enjin SDK tako interaktira posredno do Enjin stranke verige, ki neposredno interaktira z Ethereum verigo. Na ta način je mogoče združevati (ang. batching) transakcije na kar dveh nivojih. S tem je mogoče učinkovito povečati število mogočih transakcij. Ti dve tehnologiji skupaj praktično omogočajo izgradnjo skoraj poljubnega izdelka računalniške igre in zraven ponujata tudi možnost prikrojevanja blockchain potrebam igre.

6 Implementacija

V tam razdelku je implementacija razdeljena na dve ločeni komponenti. Pri obeh komponentah gre za uporabo blockchaina v razvoju računalniških iger. V obeh primerih je uporabljena kombinacija igralnega pogona Unity 3D in platforme Enjin.

Pri prvi komponenti je opisan postopek izdelave in tudi končni izdelek implementacije vmesnika za izmenjavo kart med igralci. Izdelava tega sistema je generična, kar omogoča vključitev v poljubno igro, ne glede na to, kakšne karte obstajajo. Sistem je mogoče uporabljati celo za drugačne dobrine, ki niso karte, vendar imajo podobne lastnosti. To komponento je mogoče uporabiti za vse unikatne dobrine, ki delujejo na sistemu blockchain.

Pri drugi komponenti je opisan postopek izdelave specifičnih dobrin v igri. Te dobrine so v igri predstavljene kot karte, ki jih lahko igralci zbirajo in prosto izmenjujejo med sabo. Vsaka karta da igralcu boljše zmožnosti v igri, tako da je igralec spodbujen k zbiranju takih kart. Ker so vse karte medsebojno nezamenljive, je bila želja ustvariti popolnoma unikatne karte, da v sistemu nikoli ne obstajata hkrati dve enaki karti. Da lahko tak sistem funkcionira, mora podpirati naključno izdelavo kart. Število teh kart ne sme biti omejeno, saj bi jih lahko zmanjkalo. Delujoč primer, ki zadovoljuje te pogoje, je opisan v podrazdelku 6.2.

6.1 Izdelava vmesnika za menjavo kart med igralci

Prvi cilj sistema je ponudba možnosti zamenjevanja dobrin med igralci. V tem vmesniku mora imeti uporabnik možnost pregleda nad trenutnimi dobrinami in njihovo količino ter podrobnostmi. Te lahko ponudi drugim igralcem z ustvarjanjem nove ponudbe. Na primer: uporabnik lahko naredi ponudbo za prodajo karte za 20 Enjin kovancev. Drugi igralci imajo možnost brskanja po ponudbah in sprejetja ponudb. Ponudbo sprejmejo tako, da s klikom za sprejetje zamenjajo znesek, ki ga je ponudnik določil, za dobrino, ki jo je ponudnik ponudil. Sistem mora nato poskrbeti za zamenjavo, da dobi vsak igralec dobrino, ki jo je kupil.

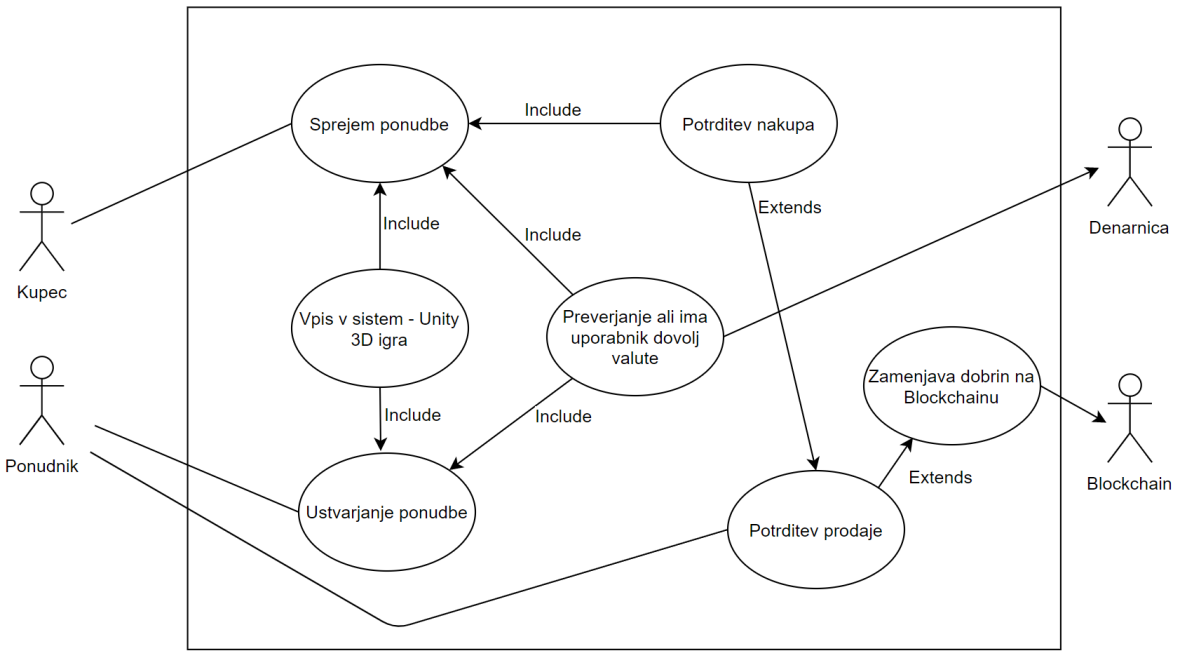
Izdelan je vmesnik s funkcionalnim sistemom za izpeljavo zamenjave. Uporabnik lahko vse dobrine vidi v igri, prav tako lahko pregleda dobrine tudi v digitalni denarnici, ki prikazuje vse njegove dobrine na blockchainu. Privzeta digitalna denarnica za ta sistem je Enjin Wallet. Sistem za izmenjavo trenutno ne poskrbi za atomarno izmenjavo, tako da ni popolnoma odporen na goljufije. Obstaja možnost nadgradnje sistema z močnejšimi varnostnimi mehanizmi, recimo uvajanje posrednika za izmenjavo ali uporabo vgrajene funkcije za atomarne zamenjave v Enjin SDK, ki trenutno ne deluje v polnem obsegu.

6.1.1 Analiza, metodologija in načrtovanje sistema

V tem podrazdelku bodo predstavljene vse faze izdelave sistema. Najprej je predstavljena analiza in načrtovanje, konča se s fazo implementacije. V fazi analize problema je predstavljena študija izvedljivosti in zahteve projekta. Predstavljene bodo tudi prednosti izbrane metodologije – iterativnega razvoja (ang. iterative design). Na koncu je predstavljen postopek modeliranja sistema z diagrami UML (ang. Unified Modelling Language diagrams). Ti opisujejo sestavo končnega sistema iz abstraktnega vidika in služijo kot opora za izdelavo in vzdrževanje sistema [18].

6.1.1.1 Analiza sistema

Cilj sistema je izmenjava dobrin v računalniški igri, ki je narejena v igralnem pogonu Unity 3D. Ker Unity nima vgrajenega blockchain vmesnika, je bil uporabljen vmesnik Enjin SDK. Poleg tega je potrebno, da vsako izmenjavo, ki jo zahteva Unity 3D, zaradi dodatne varnosti potrdimo tudi na digitalni denarnici uporabnika. V primeru, da želi oseba A izmenjati dobrine z osebo B, mora najprej oseba B izdelati ponudbo, nato oseba A to ponudbo sprejme v igri in dobi na denarnico zahtevek za potrditev izmenjave. Če se odloči za sprejem, pritisne gumb za potrditev, nakar denarnica zahteva geslo ali prstni odtis za overjanje. Nato prejme zahtevek za potrditev oseba B, ki mora ravno tako sprejeti ponudbo v denarnici. Ko obe osebi potrdita, se zgodi izmenjava dobrin na blockchainu kot transakcija. Ko se imetje v denarnici naslednjič osveži, je menjava dobrin vidna, saj denarnica bere podatke iz blockchaina. Ko uporabnik spremeni imetje dobrin v računalniški igri, mora vedno biti sinhroniziran tudi prikaz stanja iz blockchaina v igro.



Slika 8: Primer UML diagrama za prikaz primera uporabe sistema menjevanja dobrin med dvema uporabnikoma računalniške igre.

Slika 8 prikazuje pričakovano delovanje sistema iz pogleda uporabnika. Obstajajo štiri akterji, ki sodelujejo pri eni izmenjavi dobrin. Uporabnika sistema, v tem kontekstu kupec in ponudnik, morata biti prijavljena v računalniški igri za izpeljavo izmenjave. Ponudnik ustvari ponudbo, ki jo kupec poišče med vsemi obstoječimi in jo nato sprejme. Seveda morata imeti oba akterja potrebne dobrine za ustvarjanje in sprejetje ponudbe. To je preverjeno v njunih digitalnih denarnicah, ki preverjajo trenutno stanje uporabnikov na blockchainu. Če denarnici potrdita, da imata oba akterja dovolj dobrin za izpeljavo dogovorjene izmenjave, se prenese potrditev nakupa do kupca, ki ima možnost ponudbo bodisi sprejeti bodisi zavrniti. Če jo kupec sprejme, dobi gumb za potrditev ponudnik, ki lahko ponudbo zopet potrdi ali zavrne. Pri pravilnemu postopku ponudnik prodajo potrdi in sistem pride v fazo izmenjave dobrin na blockchainu. To seveda zahteva zapis izmenjave v nov blok in potrditev transakcije, zato potrebujemo tudi zunanjega akterja – blockchain, ki poskrbi za pravilno izpeljavo izmenjave.

6.1.1.2 Metodologija izdelave

Izbrana je bila različica iterativne metodologije izdelave, ki meji na generacijo prototipov (ang. Prototype development). Izbor iterativne faze zgodaj v projektu lahko privede do nižjih cen razvoja in hkrati zagotavlja najboljšo mogočo končno rešitev [28]. Ideja je, da se tekom razvoja sistema uporabljajo iteracije in da se vsako fazo izdelave izvaja večkrat. Po koncu vsake iteracije se izvaja potrebno testiranje in preverjanje skladnosti s funkcijskimi in ne-funkcijskimi zahtevami. Faze se lahko poljubno mnogokrat ponovijo, saj se po vsaki fazi razumevanje končnega produkta izboljša. Po izdelavi je bilo ugotovljeno, da je bila ta metoda učinkovita, saj je bilo mogoče skozi razvoj projekta popraviti tudi določene funkcijske zahteve in jih prikrojiti boljšemu delovanju. Vsaki iteraciji skozi vse faze je sledil tudi končni prototip, ki je bil kasneje testiran in preverjen ali zadovoljuje vse (ne)-funkcijske zahteve.

6.1.1.3 Funkcijske specifikacije

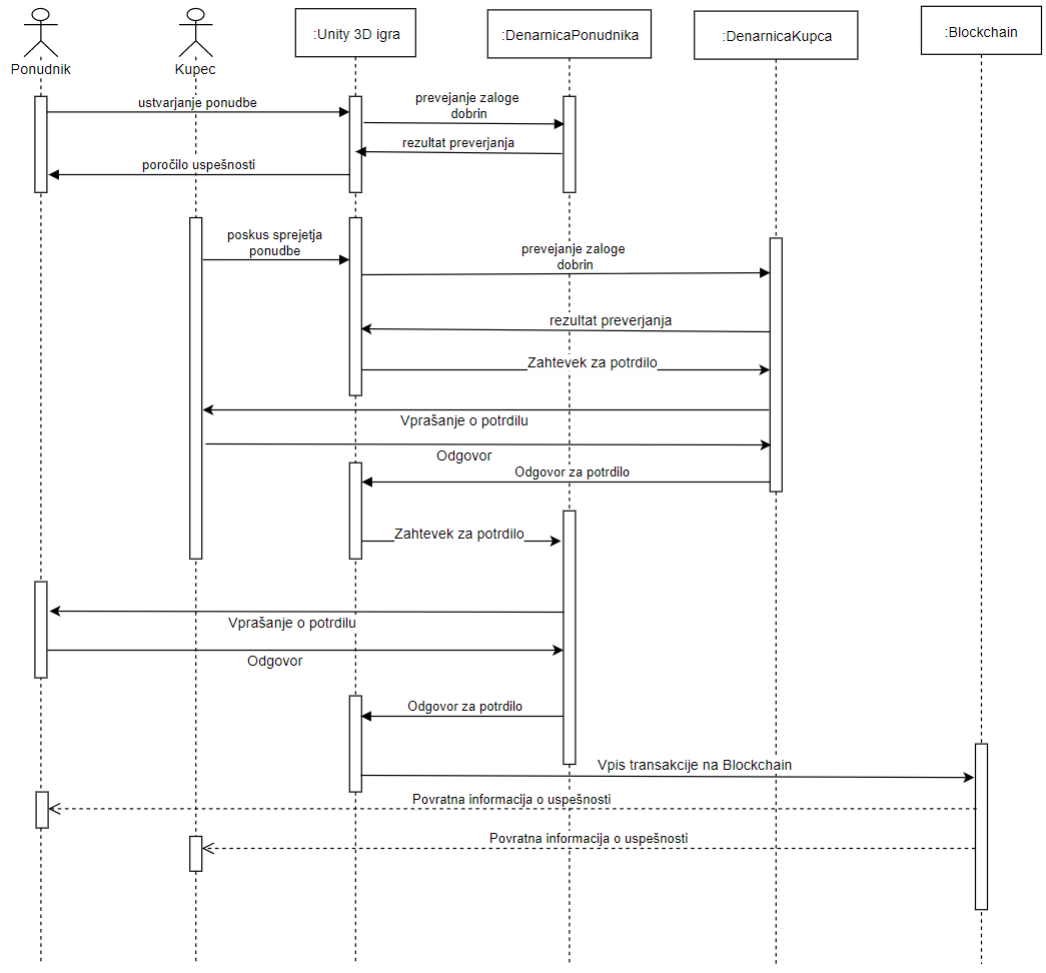
Funkcijske specifikacije opisujejo vse potrebne funkcije končnega sistema. Najprej se funkcijske specifikacije določi v fazi analize in načrtovanja, med razvojem izdelka se v vsaki iteraciji preverja zadovoljevanje teh zahtev. Če določena zahteva ni izpolnjena, se bodisi v novi iteraciji skuša v sistem vključiti tudi to funkcijo bodisi se pregleda ali je ta funkcija res potrebna. Včasih se lahko namreč zgodi, da so lahko funkcijske zahteve nasprotujoče ali so celo medsebojno neskladne. Funkcijske specifikacije za ta sistem so sledeče:

1. možnost preverjanja identifikacije uporabnika;
2. možnost ustvarjanja novih ponudb za ponudnika;
3. možnost iskanja po ponudbah;
4. možnost sprejemanja ponudb za kupca;
5. možnost preverjanja količine dobrin v denarnicah;

6. potrjevanje ponudb za kupca v denarnici;
7. potrjevanje ponudb za ponudnika v denarnici;
8. izmenjava ponudb med denarnicami;
9. prikaz uspešne izmenjave v Unity 3D.

6.1.1.4 Načrtovanje sistema in modeliranje

V tem podrazdelku je prikazan potek načrtovanja in modeliranja. Za modeliranje so bili uporabljeni standardni in široko uporabljeni UML diagrami, na primer sekvenčni diagram, ki opiše celotni proces delovanja sistema s poudarkom na kronološkem zaporedju dogodkov [54]. Sekvenčni diagram tega sistema je predstavljen na sliki 9.



Slika 9: Primer UML sekvenčnega diagrama za kronološke izmenjave sporočil med akterji: Ponudnik, kupec, Unity igra, denarnica ponudnika, denarnica kupca in veriga blokov za proces izmenjave kart v sistemu.

V sistemu se proces izmenjave kart začne z ponudnikom, ki ustvari ponudbo. Ponudnik namreč komunicira z igro, narejeno v igralnem pogonu Unity 3D, izbere dobrino, ki jo želi prodati, ter določi njeno ceno. Nato s potrditvenim gumbom pošlje zahtevek

v igro za izdelavo ponudbe. Za preverjanje, ali ima uporabnik dovolj dobrin, mora biti poslana prošnja na denarnico. Denarnica to preveri na blockchainu in vrne odgovor, ki bodisi omogoči v igri ponudniku ustvarjanje nove ponudbe bodisi ponudba propade in se sploh ne ustvari na strežniku.

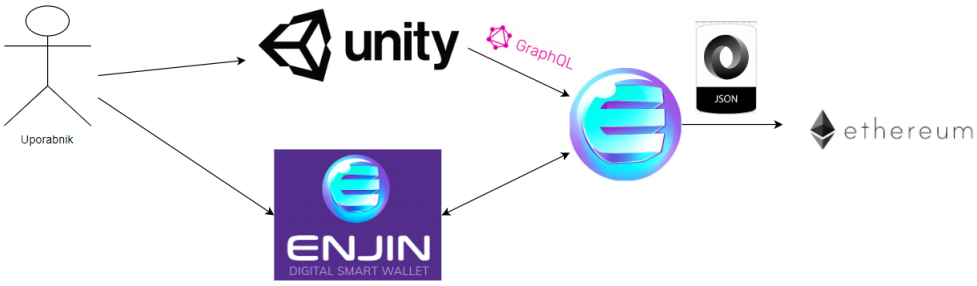
Kupec ima možnost brskanja po ponudbah in ko najde dobrino, ki jo želi kupiti, pritisne na gumb za nakup. To privede do tega, da mora igra zopet preveriti, ali ima igralec dovolj surovin za izdelavo te ponudbe. Če jih nima, se ponudba ne sprejme in izmenjava ne steče, temveč vrne kupcu napako s prikaznim sporočilom, da sprejetje ponudbe ni mogoče. V nasprotnem primeru se pošlje denarnici kupca prošnjo za izpeljavo transakcije. Igralec mora nato preko digitalne denarnice ponudbo sprejeti ali jo zavrniti. Če jo zavrne, se proces ustavi in igra izpiše napako – nakup ni uspel. V nasprotnem primeru igra pošlje zahtevek po potrdilu denarnici ponudnika, ki lahko zopet bodisi zavrne bodisi sprejme potrdilo. V primeru, da ponudnik zahtevek sprejme, igra sproži akcijo na blockchain, ki potrdi transakcijo in o uspešnem rezultatu obvesti oba uporabnika.

6.1.2 Enjin SDK in Enjin denarnica

Enjin SDK je vmesnik, ki ga lahko razvijalec namesti v Unity 3D igralni pogon za lažjo komunikacijo z Enjin stransko verigo. Enjin SDK je na voljo v trgovini za nadgradnje Unity-ja (ang. Unity Asset store). Namestitev tega vmesnika je hitra in brezplačna. Z namestitvijo dobi razvijalec kratek tečaj o uporabi in popolno dokumentacijo vseh funkcijskih klicev, ki so na voljo. Glavni namen Enjin SDK-ja je, da na enostaven način predstavi razvijalcu možnosti platforme Enjin. Razvijalec lahko z uporabo te knjižnice uporabi vse Enjin funkcije v kodi in kodo poljubno prilagodi. Enjin SDK uporablja jezika GraphQL in JSON za izmenjavo sporočil z Unity stransko verigo in glavno Ethereum verigo.

Za preverjanje funkcionalnosti sistema in shranjevanje uporabnikovih dobrin je potrebno imeti tudi digitalno denarnico. Za izdelavo tega sistema in preverjanje njegovega delovanja je bila izbrana denarnica Enjin, saj ima posebej prilagojen uporabniški vmesnik za Enjin dobrine. V splošnem lahko uporabnik izbere poljubno denarnico za uporabo ob računalniški igri. Digitalna denarnica služi pregledu vseh kovancev, ki jih ima vsak uporabnik v danem trenutku. V kolikor so ti kovanci medsebojno nezamenljivi, uporabnika pogosto zanima tudi, kaj predstavlja ta kovanec v igri. To je razlog za uporabo Enjin denarnice za testiranje, saj ima možnost prikazovanja virtualnega pomena dobrine, ki jo predstavlja določen Enjin kovanec.

Na sliki 10 je prikazana komunikacija igralca s komponentami, ki so bile predstavljene. Računalniška igra je razvita v igralnem pogonu Unity 3D, zato uporabnik neposredno komunicira z Unity 3D programom. Uporabnik ima prav tako nameščeno poljubno denarnico, a bo v fazi testiranja predpostavljeno, da uporablja denarnico Enjin Wallet. Tako Unity 3D kot Enjin Wallet komunicirata z Enjin omrežjem. Unity uporablja za komunikacijo z Enjin omrežjem Enjin SDK. Komunikacija med Enjin SDK in Enjin omrežjem poteka preko GraphQL. Zahtevki, ki so bili poslani na Enjin omrežje, nadaljujejo v obliki protokola JSON do Ethereum blockchain verige, kjer bo-



Slika 10: Prikaz končne arhitekture sistema. Slika prikazuje komponente, ki so v interakciji z uporabnikom. Prikazani so tudi protokoli, ki skrbijo za prenos podatkov med temi komponentami.

disi preverjajo trenutno stanje uporabnikov, ali zapišejo nove transakcije za potrjevanje izmenjave dobrin.

6.1.3 Končna implementacija

V tem razdelku bo opisan končni sistem za izpeljavo izmenjave kart. Podane bodo slike primera vmesnika, ki skrbi za pravilno izbiro kart in potrjevanju izmenjave. Slike so zajete v igralnem pogonu Unity 3D in v programu Enjin Wallet. Za lažjo predstavo o delovanju sistema so opisani tudi kratki primeri uporabe,.

Slika 11: Primer prikaza ponudb treh različnih igralcev. Na sliki so tri različne ponudbe, vsaka vsebuje ime ponudnika, opis karte in njeno ceno v zlatnikih

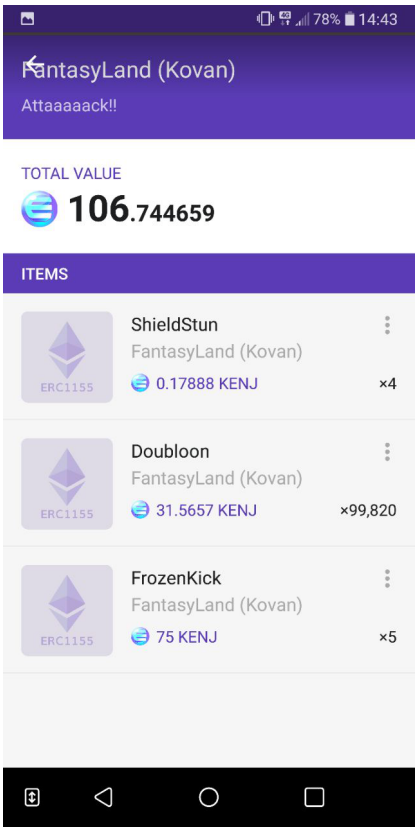
Na sliki 11 je razviden pogled na uporabniški vmesnik za pregled vseh trenutno obstoječih ponudb. Na desni zgoraj se nahaja gumb za filtriranje, kjer je mogoče karte filtrirati preko različnih filtrov, na primer cene. Levo spodaj je prikaz trenutnega stanja bilance v denarnici. Ta spremenljivka je prebrana neposredno iz denarnice uporabnika

in omogoča sistemu preverjanje ponudb, ki jih lahko uporabnik sprejme. Seveda se izvede dodatno preverjanje aktualnosti te spremenljivke pred vsakim nakupom in prodajo. Na sredini vmesnika so razporejene ponudbe. Vsaka ponudba vsebuje ime ponudnika, opis dobrine, ki jo prodaja ponudnik, in njeno ceno v zlatnikih. Te ponudbe so prebrane iz strežnika, ki vsebuje vse trenutno obstoječe ponudbe. V kolikor se uporabnik odloči za nakup dobrine, pritisne na gumb „Buy item“ v polju z informacijami o tej dobrini. V spodnjem desnem kotu ima uporabnik možnost narediti novo ponudbo s klikom na gumb „Make new offer“.

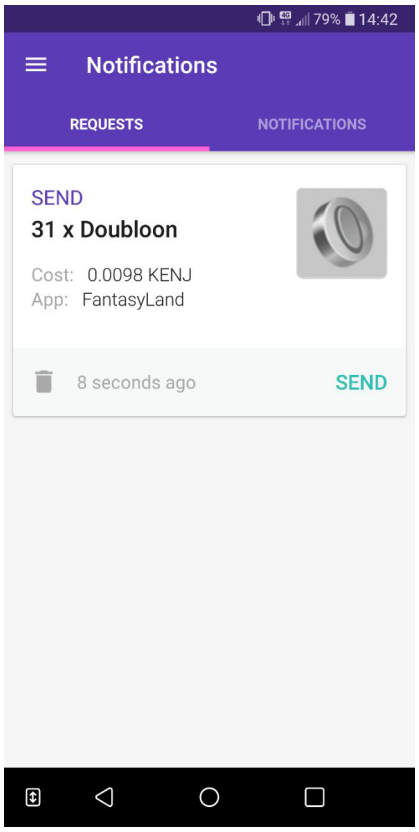
Slika 12: Primer prikaza možnosti pri izdelavi nove ponudbe. Uporabnik izbere karto, ki jo želi ponuditi, in izpolni polje o želeni ceni za to karto.

Na sliki 12 je razviden meni uporabnika za izdelavo nove ponudbe. V drsnem okencu ima ponudnik na voljo vse dobrine v denarnici. S klikom na poljubno karto se ta dobrina prebarva v sivo, kar pomeni, da je trenutno izbrana za izmenjavo. V kolikor ima uporabnik veliko dobrin, ima možnost filtriranja dobrin s klikom na gumb „Select filters“. Ko se odloči za karto, ki jo hoče ponuditi, mora določiti ceno za ponujeno dobrino v zlatnikih. Z vpisom cene v okence se shrani njegova želena cena. Zadnji korak je pritisk na gumb „Confirm“ za potrjevanje ponudbe ali gumb „Cancel“ za preklic procesa izdelave ponudbe.

Na sliki 13a je prikazan primer vsebine denarnice izbranega uporabnika. Uporabnik ima vedno možnost pregleda kovancev v denarnici. V denarnici lahko vidi tudi virtualni pomen teh kovancev. Na sliki ima uporabnik v denarnici 99.820 dobrin z imenom Doubloon, ki predstavljajo denarno valuto v računalniški igri. V denarnici ima tudi 4 dobrine z imenom »ShieldStun« in 5 dobrin z imenom »FrozenKick«. Vsaka dobrina vsebuje tudi opis in njeno vrednost v Enjin kovancih. Vrednost v ENJ je prikazana, ker se lahko vsako dobrino spremeni nazaj v Enjin kovance. Proces za pridobivanje Enjin kovancev iz ustvarjenih dobrin se imenuje taljenje (ang. Melting).



(a) Primer vsebine denarnice na telefonu.



(b) Zahtevek potrditve na telefonu.

Slika 13: Primera uporabniškega vmesnika v denarnici. Na levi sliki je prikazana vsebina testne denarnice s kovanci, ki jih poseduje uporabnik. Na desni sliki je primer zahtevka za potrditev transakcije za pošiljanje valute v zameno za dobrino.

Na sliki 13b je prikazan primer zahtevka za sprejetje kupčije v igri. Uporabnik lahko izbira med gumbom za potrditev in gumbom za zavrnitev ponudbe. Videti je tudi mogoče, da uporabnika kupčija stane 31 Doubloonov. Vsaka transakcija ima tudi ceno za izvedbo. V tem primeru je cena 0,0098 ENJ kovancev.

6.2 Evolucijski razvoj kart

V tem razdelku bo prikazana implementacija evolucijskega razvoja kart v igri. Zahteve za implementacijo so bile naslednje:

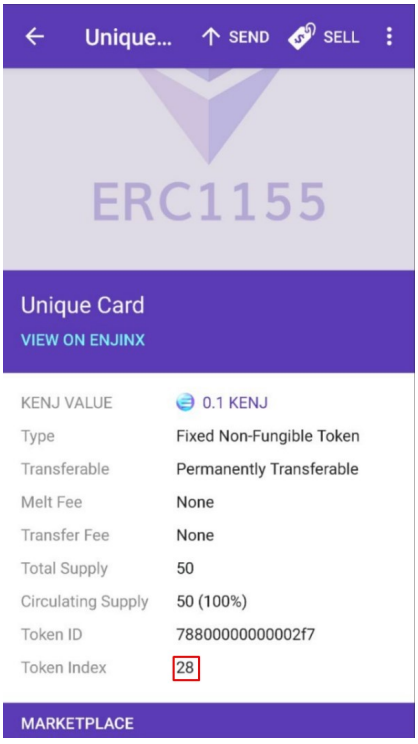
1. Vsaka karta v igri mora biti edinstvena, kar pomeni, da ne moreta dva uporabnika imeti enake karte.
2. Karte ni mogoče predstaviti kot objekt na strežniku in na blockchainu, zato je potrebno karto predstaviti kot besedo (ang. string).
3. Igra mora znati pretvoriti besedo v karto v kratkem času
4. Kart ne sme nikoli zmanjkati

5. Skozi čas morajo na novo pridobljene karte postati močnejše

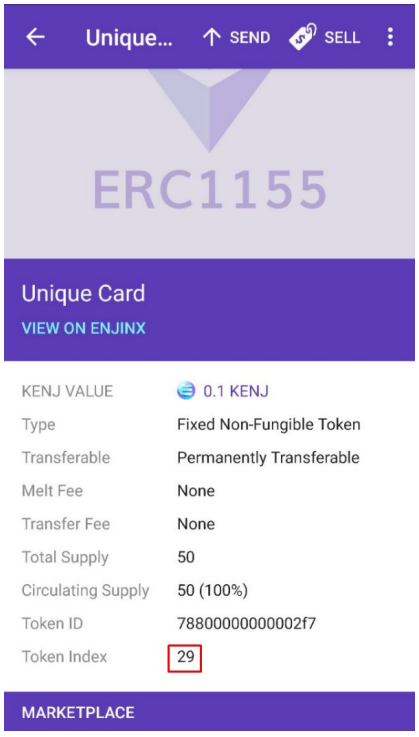
6.2.1 Predstavitev kart na blockchainu

Enjin vmesnik omogoča ustvarjanje medsebojno zamenljivih dobrin in medsebojno nezamenljivih dobrin. Razlika med njimi je ta, da če je neka dobrina medsebojno nezamenljiva, se da razlikovati med instancami te dobrine, medtem ko se med medsebojno zamenljivimi dobrinami ne da razlikovati. Najenostavnejši primer so zlatniki v igrah, ki so navadno predstavljeni kot medsebojno zamenljive dobrine, saj ni pomemben lastnik zlatnika, temveč zgolj to, koliko zlatnikov ima neka oseba v igri. Medsebojno nezamenljive dobrine je mogoče ločiti med sabo preko njihovega indeksa na blockchainu, ki opisuje zaporedno številko njene izdelave.

Za predstavitev kart na blockchainu je bila ustvarjena množica medsebojno nezamenljivih dobrin, ki so dobivale zaporedne številke med časom njihove izdelave. Najprej je potrebno ustvariti model dobrin, ki se ga opiše kot skupek lastnosti, na primer ime modela, cena za trgovanje, njegova vrednost v Enjin kovancih itd. Ko je model ustvarjen, se lahko ustvarja instance tega modela. Posamezne instance so na blockchainu skoraj popolnoma enakovredne. Razlikujejo se samo v indeksu, ki predstavlja zaporedno številko izdelave tega kovanca, kot je tudi razvidno na sliki 14.



(a) Primer dobrine z zaporedno številko 28.



(b) Primer dobrine z zaporedno številko 29.

Slika 14: Prikaz modela dobrin za izdelavo instanc kart. Instanca na levi ima zaporedno številko 28, instanca na desni 29. To je edina razlika med tema dvema dobrinama.

Nove instance se tako ustvari v času delovanja programa, ko uporabnik izpolni zahtevo za pridobitev nove karte. V tem trenutku se mora na blockchainu samodejno kreirati nov kovanec iz obstoječega modela, biti mora indeksiran in dodeljen v lastništvo tega uporabnika.

Ob kreaciji modela instanc je potrebno kot parameter podati tudi maksimalno število dobrin, ki bodo kadar koli obstajale v sistemu. Za zadostitev funkcionalne zahteve iz začetka razdelka, tj. da kart ne sme nikoli zmanjkati, je potrebno zagotoviti, da jih je lahko kar vedno več. Zato je potrebno izbrati tudi opcijo, da se lahko maksimalno število kart kadar koli poveča. Ta možnost je navadno manj zaželena, ker uporabnikom ne nudi varnosti, da njihova dobrina zaseda konstanten delež celotne ponudbe dobrin.

6.2.2 Predstavitev kart s semenom

Ker karta ne more biti shranjena na blockchainu kot abstraktni objekt, mora obstajati v igri neka bijektivna preslikava, ki lahko preslika predstavitev karte v njen dejanski objekt v igri. Predstavitev karte je lahko bodisi beseda (ang. string) bodisi število (ang. integer). Funkcija tako sprejme kot parameter predstavitev karte in vrne objekt, ki to karto predstavlja. Zaradi bijektivnosti funkcije je mogoče sestaviti tudi obratno funkcijo, tako da za vsak objekt izračuna pripadajočo predstavitev te karte.

Izbrana je bila predstavitev karte z besedo, ki je sestavljena zgolj iz številk, kar omogoča lepe lastnosti pri predstavitvi karte in intuitivnostjo delovanja funkcije. Prav tako ta predstavitev nima težav z dolžino – številom znakov, saj so lahko besede v Unity skoraj poljubno dolge. Predstavitev karte je v nadaljevanju omenjena kot seme karte.

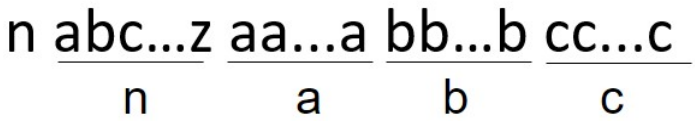
Seme je sestavljeno iz naslednjih komponent:

1. števila n, ki pove, iz koliko komponent je sestavljen ključ;
2. n števil, ki opisujejo velikosti naslednjih komponent;
3. n komponent variabilnih velikosti, ki opisujejo posamezno moč posamezne kategorije.

6.2.2.1 Predstavitev delovanja semena karte in pripadajoče funkcije

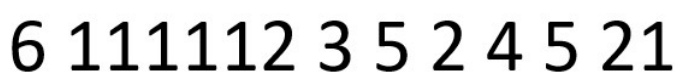
Na sliki 15 je prikazan splošen primer semena. Ta ima najprej parameter n, ki ponazarja število komponent, ki jih to seme določa. Sledi n komponent, ki so označene z $a, b, c, ..., d$. Vsaka od teh sedaj ponazarja število števk, ki bodo opisovale posamezno komponento. To je pomembno, da se lahko prihrani veliko prostora pri dolžini semena. V igri je parameter n statičen, saj imajo vse karte enako število komponent, v splošnem pa bi lahko variiral.

Na sliki 16 je prikazan primer sestave semena. V splošnem med številkami ni presledkov – ti so bili dodani za lažje razumevanje bralca. Seme na sliki je sestavljeno iz šest komponent, kar predstavlja prvo število. Sledijo opisi dolžin kategorij, ki so vsi enaki 1, zgolj zadnji je 2. To pomeni, da preostanek semena beremo po temu ključu.



Slika 15: Prikaz splošne sestave semena. Vse črke so predstavljene iz 1 ali več številk v desetiškem zapisu.

Moči semena so: 3, 5, 2, 4, 5, 21.



Slika 16: Prikaz primera sestave semena. To seme vsebuje šest komponent, pet jih je dolžine ena in ena kategorija je dolžine dve.

Kategorije v semenu v igri predstavljajo naslednje:

1. Razred lika, ki mu je namenjena karta s tem semenom – v trenutni iteraciji nastopajo razredi: Bojevnik, lokostrelec, čarovnik.
2. Variacija karte tega lika – vsak lik ima šest kart različnih variacij. Vsaka variacija ima enako ime ampak različne parametre
3. 3 do n predstavljajo parametre trenutne variacije karte.

Vsaka variacija karte ima opisane lastnosti, kako je karta poboljšana s točkami v posameznih kategorijah. Na sliki 17 so prikazane tri karte, ki so last igralca v igri. Vse tri karte pripadajo liku čarovnika in vse tri so iz iste variacije, a imajo točke drugače razporejene po kategorijah. Kot je razvidno imajo vse tri karte enako ime in oznako napada, saj pripadajo isti variaciji. Razlikujejo se zgolj v parametrih po besedi "Attack", "Ember: Burn"itd.

Slika 17: Prikaz primera treh kart istega razreda – čarovnika z isto variacijo karte, a drugače razporejenimi točkami po kategorijah.

Ker morajo biti karte v igri približno enako močne, je bilo potrebno tudi uravnotežiti točke po kategorijah. Uporabljen je bil enostaven algoritem za dosego tega

cilja. Najprej se je določilo število kategorij za vsak lik in variacijo karte. Nato se je fiksno število točk prerazporedilo med te kategorije. V trenutni implementaciji se je razporedilo 20 točk med štiri kategorije. To se je naredilo tako, da se je ustvarilo vse kombinacije semen, ki so imele skupno 20 točk v štirih kategorijah. S tem se je doseglo, da so bile karte med seboj enako močne preko funkcije, ki je vsako kategorijo preslikala v efekt na karti.

6.2.2.2 Predstavitev evolucije semen skozi čas

Ker je število razredov v igri omejeno, prav tako je omejeno tudi število variacij vsake karte, je število kombinacij določenega števila točk med kategorijami končno mnogo. Število kombinacij kategorij se da enostavno izračunati nad številom porazdelitev n točk v k kategorij. Število vseh kombinacij se enostavno pridobi, če se množi število razredov in število variacij.

Da se zadosti potrebam, da je teh kart neskončno mnogo in da se njihova moč veča skozi čas, je potrebno zagotoviti neskončno mnogo kombinacij. To je bilo storjeno tako, da se je najprej naredilo vse mogoče porazdelitve fiksnega števila točk v izbrane kategorije, na primer 20 točk. Ko uporabniki čez čas kupujejo nove dobrine in odklepajo nove karte, prej ali slej zmanjka porazdelitev. Ko se to zgodi, se enostavno naredijo nove karte, tokrat z 10 % več točkami. V trenutnem primeru bi to pomenilo, da se razvrsti 22 točk med štiri kategorije. Novonastale karte so tako močnejše od prejšnjih, kar zadosti zahtevi po evoluciji v močnejše karte skozi čas. Ko zmanjka novih porazdelitev, program prav tako poviša mejo za 10 %, kar se ponavlja v neskončnost.

6.2.3 Shranjevanje vezi med blockchain indeksom in pripadajočim semenom

Ker so karte predstavljene na blockchain omrežju kot indeks karte po kronološkem nastajanju kart in v igri kot beseda iz številk, je potrebno nekje shraniti povezavo med vsemi kartami in pripadajočimi indeksi. Rešitev je tabela preslikav na vedno dostopnemu strežniku, ki vsebuje vsa semena in njihove pripadajoče blockchain indekse. Na sliki 18 je prikazan primer take tabele, ki je bila uporabljena na testiranju igre.

Vsakič, ko je potrebno povezati seme z blockchain indeksom ali obratno, je potreben dostop strežnika in tabele v njem. Za to delo je bila definirana funkcija, ki skrbi za pošiljanje velikega števila povpraševanj hkrati in sprejemanje velikega števila rezultatov – vrstic iz tabele hkrati. Na ta način se nekoliko razbremeni delovanje strežnika, saj ta dobi manj povpraševanj v določeni časovni frekvenci, s tem pa se zmanjša tudi število dostopov do baze.

Da bi se čim bolj zmanjšal čas obdelave uporabniške zahteve, se vsa semena izdela vnaprej in shrani na strežniku. Vsakič, ko zmanjka razpoložljivih semen, se naredijo nova in se jih shrani v posebnih tabelah. Semena se shrani v tabelo v naključnem vrstnem redu, tako da vsakič, ko uporabnik zaprosi strežnik za novo, prosto seme, se mu dodeli prvo seme, ki je na voljo, nato se le-tega izbriše iz tabele, da bo naslednji uporabnik dobil drugo seme.

seed ▾ 1	blockchainid
331050302	2
321040004	33
321020204	43
321010010	42
320060100	28
310050102	27
310020206	37
301060000	36
301010206	32
301000502	35
301000012	46
300000406	50
300000210	31

Slika 18: Prikaz primera tabele, ki vsebuje nekaj semen in pripadajoče blockchain indekse.

Vsakič, ko igralec pridobi novo karto v igri, se mora zgoditi naslednje:

1. izbrati je potrebno novo naključno seme, ki bo predstavljalo njegovo karto;
2. na blockchainu je potrebno ustvariti novo instanco karte iz trenutnega modela in shraniti njen blockchain indeks;
3. novo ustvarjeno instanco je potrebno zapisati v lastnino trenutnega uporabnika, kar je vidno v njegovi denarnici;
4. v tabelo je potrebno zapisati ključ, ki predstavlja vez med semenom in blockchain indeksom karte;
5. iz denarnice uporabnika je potrebno prebrati vse karte in jih prikazati v igri.

7 Analiza

V tem razdelku so opisana testiranja uporabnosti programske opreme, ki so bila izvajana na Fakulteti za naravoslovje, matematiko in informacijske tehnologije v Kopru. Izvedeni sta bili dve delavnici, prva 10. januarja 2020, druga 21. januarja 2020. Prvo testiranje je trajalo pet ur, na njem je bilo prisotnih sedem ljudi. Prisotnih je bilo šest moških in ena ženska, vsi so bili študenti. Drugo testiranje je trajalo štiri ure, na njem je bilo prisotnih 11 ljudi. Vsi prisotni so bili moškega spola. Devet udeležencev je bilo študentov, eden asistent in eden profesor. Delavnica je potekala v računalniški sobi na fakulteti, kjer je vsak sodelujoči dobil v uporabo računalnik z igro, uporabiti pa je moral tudi mobilni telefon za dostop do digitalne denarnice. Na voljo je bil tudi avtor igre, ki je poskrbel, da vse poteka v skladu z navodili in da je na voljo za vprašanja.

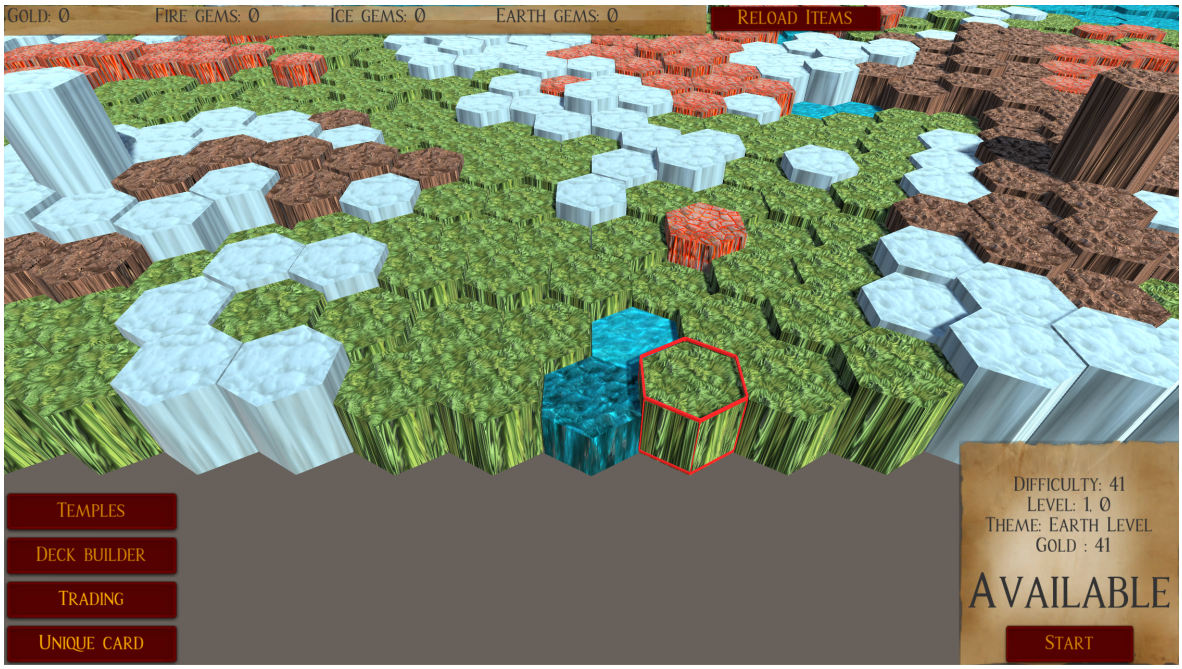
7.1 Metodologija in motivacija

Testiranje je zajemalo več kot samo interakcijo s sistemom za izmenjavo kart med igralci. Narejena je bila celotna igra, ki je omogočala igranje v neskončnost – nivoji so bili namreč narejeni naključno, s sčasoma povečujočo težavnostjo. Uporabniki so lahko izbirali, ali bodo igrali nivoje, ki so bili lažji za premagati, ampak so z zmago prinesli manj surovin, ali nivoje, ki so bili težji in so uporabnikom dali boljše nagrade. Na sliki 19 je prikazan zemljevid, kjer so lahko igralci izbirali nivoje za igranje.

Igra poteka tako, da ima vsak igralec tri različne like, ki jih lahko nadzira v virtualnem svetu. Vsak lik ima sprva štiri karte, ki definirajo njegove razpoložljive poteze. Te karte so razmeroma šibke. S tem ko premaguje različne nivoje, pridobi zlatnike. Z zlatniki lahko kupi nekoliko boljše karte, ki mu omogočajo lažje igranje in tudi več možnosti za odigrati potezo.

Obstajajo tudi veliko težji nivoji, ki zmago uporabnika nadgradijo s tako imenovanimi diamanti. Vsak težji nivo uporabnika nadgradi z natanko toliko diamanti, da jih lahko zamenja za eno veliko močnejšo karto. Te karte so unikatne karte, predstavljene s semenom, in so bile predstavljene v razdelku 6. Uporabnik jih lahko kupi s klikom na gumb "Unique Card", ki je prikazan na sliki 19. S klikom sproži transakcijo na blockchain, kjer se mu odštejejo diamanti, ki jih je zapravil. Nato v kolekcijo dobi novo, unikatno karto.

Pred igranjem igre je vsak uporabnik na pametni telefon namestil aplikacijo Enjin Wallet, ki mu je omogočala hiter in učinkovit pregled nad njegovimi dobrinami, ki so bile v tem primeru unikatne karte. Digitalna denarnica je služila tudi za potrjevanje transakcij iz smeri lastnika denarnice.



Slika 19: Prikaz zemljevida, kjer so igralci izbirali nivoje za igranje. Vsak heksagon predstavlja en nivo, ki ga mora uporabnik premagati. Uporabnik lahko premika pogled po zemljevidu v neskončnost. Težavnost nivoja se povečuje z višino heksagona in oddaljenostjo od izhodišča.

Prva interakcija uporabnikov z blockchainom je bila nakup edinstvenih kart. Druga interakcija je bila izmenjava teh kart med igralci. Ker je vsaka karta unikatna, bi bila izmenjava, delujoča po načelu karta-za-karto, neučinkovita. V tem primeru bi mogel prodajalec karte definirati karto, ki bi jo rad dobil v zameno za dobrino. S tem bi tudi natančno določil prejemnika, saj ima tako karto lahko zgolj ena oseba. Iz tega razloga je bila uvedena izmenjava po načelu karta-za-zlatnike.

Prodajalec je ustvaril ponudbo, kjer je ponudil karto v zameno za znesek zlatnikov, ki ga je sam prosto določil. Ko je bila ponudba ustvarjena, so se podatki o njej shranili na strežnik in vsi drugi igralci so lahko to ponudbo tudi videli. Ko se je nek igralec odločil za nakup, je pritisnil na gumb za potrditev nakupa, kar je poslalo prošnjo za sprejetje ponudbe v denarnico lastnika karte. Dodatno je bilo uvedeno tudi opozorilno okence, ki se je pojavilo na zaslonu prodajalca med njegovim igranjem igre in ga opozorilo na to, da mora sprejeti ponudbo v denarnici. Ko je ponudbo sprejel, so se prvemu igralci odšteli zlatniki in dobil je določeno karto, drugi igralec je nato dobil znesek zlatnikov.

Problem tega poteka je bil, da če je nek igralec sprejel več ponudb naenkrat in so bile te naknadno sprejete, je lahko zapravil več denarja, kot ga je imel, in je zato zapadel v dolg. Tega se je lahko enostavno rešil, če je prodal dovolj kart ali odigral dovolj iger, da je dolg odslužil. Shema ni najbolj primerna za resnično igranje, a ker so bila testiranja kratka, je bil namen uvedbe te sheme izboljšati uporabniško izkušnjo, saj so se jim zlatniki odšteli zgolj, če so karto dejansko kupili. V nasprotnem primeru bi se jim zlatniki odšteli takoj, ko so poslali ponudbo za karto, a če prodajalec karte

ponudbe ne bi sprejel dovolj hitro, bi ves ta čas ostal kupec brez karte in brez zlatnikov.

7.2 Opis izvedbe testiranja

Kot je bilo omenjeno, sta potekali dve testiranji v računalniški učilnici na fakulteti FAMNIT. Testiranje je bilo javno, povabljeni so bili tudi ljudje, ki so imeli predhodne izkušnje s programom, ostali so se s programom srečali prvič. Prav tako so na drugo testiranje bili povabljeni ljudje, ki so bili prisotni tudi na prvem testiranju, sodelovali pa so tudi novi ljudje, ki so bili prvič v stiku s programom.

Prvo testiranje je trajalo približno pet ur. Drugo testiranje je bilo nekoliko krajše in je potekalo štiri ure. Vsak uporabnik je dobil pripravljen računalnik z nameščeno igro. S pomočjo prisotnega pomočnika je naložil na telefon aplikacijo Enjin Wallet in jo povezal z njegovim računom v igri.

Medtem ko so uporabniki igrali igro, so se nekatere njihove dejavnosti shranjevale na strežnik z namenom obdelave teh podatkov za testiranje in analizo. Zabeležene so bile naslednje dejavnosti:

1. Zmaga nivoja, kjer so se zabeležili naslednji podatki: Težavnost nivoja, uporabnikov ID in trenutni čas.
2. Nakup unikatne karte iz blockchaina, kjer so bili zabeleženi: uporabnikov ID, čas nakupa in številka prejetega semena.
3. Izmenjava dobrin med dvema igralcema, kjer so bili zabeleženi: prodajalčev ID, kupčev ID, številka zamenjanega semena, cena karte v zlatnikih in čas izmenjave.

Uporabniki so bili prikazani zgolj z njihovim Enjin ID-jem, kar jim je omogočalo anonimnost.

Za dodatno motivacijo je bil prižgan tudi projektor v učilnici, ki je bil usmerjen na tablo, prikazoval je trenutne najboljše rezultate vseh igralcev in s tem lestvico najboljših. Metrika za najboljši rezultat je bila težavnost najtežjega nivoja, ki ga je vsak uporabnik premagal. S tem so igralci dobili iniciativo premagovanja vedno težjih nivojev, namesto da bi vsi igrali zgolj lažje nivoje.

Na prvem testiranju je bilo prisotnih sedem uporabnikov, ki so bili prisotni ves čas. Testiranje je potekalo z manjšimi težavami, saj izmenjava kart med igralci ni popolnoma delovala. Uporabniki tudi niso dobili sporočila na zaslonu, da jih čaka potrditev v denarnici in so zaradi tega lahko potrditev zamudili. Igra je imela tudi nekaj hroščev, ki so poslabšali uporabniško izkušnjo. Testiranje je tudi preseglo pričakovan nakup unikatnih kart, ki je bil omejen na 50 kart v testiranju.

Na drugem testiranju je bilo prisotnih 11 uporabnikov, ki so bili večinoma prisotni do konca, le dva sta predčasno odšla. Odpravljene so bile vse težave z izmenjavo dobrin med igralci, popravljeni so bili tudi vsi hrošči, ki so se pojavili na prvemu testiranju.

Poskrbljeno je bilo tudi, da se ne bo dosegel limit nakupa unikatnih kart, saj je bilo pripravljenih 10.000 kart. V primeru, da bi se limit kadar koli dosegel, bi program podvojil število obstoječih kart.

7.3 Rezultati testiranja

Na prvem testiranju potek izmenjave dobrin uporabnikom ni bil dovolj všeč, zaradi česar je trpelo število izmenjanih dobrin. V petih urah je prišlo samo do 10 izmenjav med igralci. Po izboljšani uporabniški izkušnji z obvestili na zaslonu, lažjim trgovanjem in popravljenimi hrošči, se je število izmenjav povečalo na 59 izmenjav med igralci. Zato v rezultatih prvega testiranja ne bodo omenjene izmenjave med igralci, temveč bo poudarek predvsem na ostalih dejavnikih. V drugem testiranju bodo raziskani vsi podatki.

7.3.1 Pregled in primerjava premaganih nivojev igralcev

V tem podrazdelku bo prikazana primerjava premaganih nivojev igralcev med obema testiranjema. Ugotoviti je potrebno, ali predhodne izkušnje vplivajo na količino zmag igralca ter na težavnost najtežjega nivoja, ki ga je igralec uspel premagati. Ker sta testiranji trajali približno isto časa, se lahko primerja tudi število zmag in najzahtevnejše premagane nivoje med testiranji.

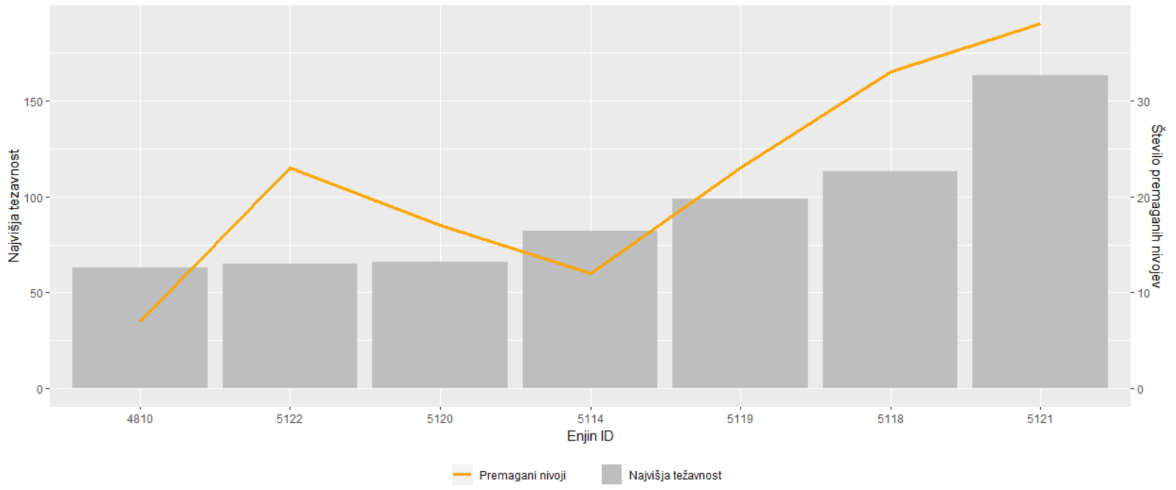
Pri vsakem grafu so podane tudi p-vrednosti korelacije neodvisnih spremenljivk po Pearsonovi [45] in Spearmanovi [34] metodi. Te vrednosti se uporabljajo za potrjevanje hipotez, ki slonijo na podobnosti med funkcijami. Če je p-vrednost manjša od 0,05, pomeni, da lahko z veliko stopnjo zaupanja trdimo, da spremenljivki nista povezani. S tem se da tudi meriti stopnjo povezanosti med spremenljivkama.

Ti dve metodi predpostavljata, da so uporabljene spremenljivke ordinalne, intervalne ali racionalne. Obe spremenljivki morata biti istega tipa in imeti enako obliko. Pearsonova metoda išče linearna razmerja med spremenljivkama, Spearmanova pa upošteva vsa monotona razmerja. Posledično je mogoče s Spearmanovo metodo najti razmerja, ki jih Pearsonova metoda ne najde.

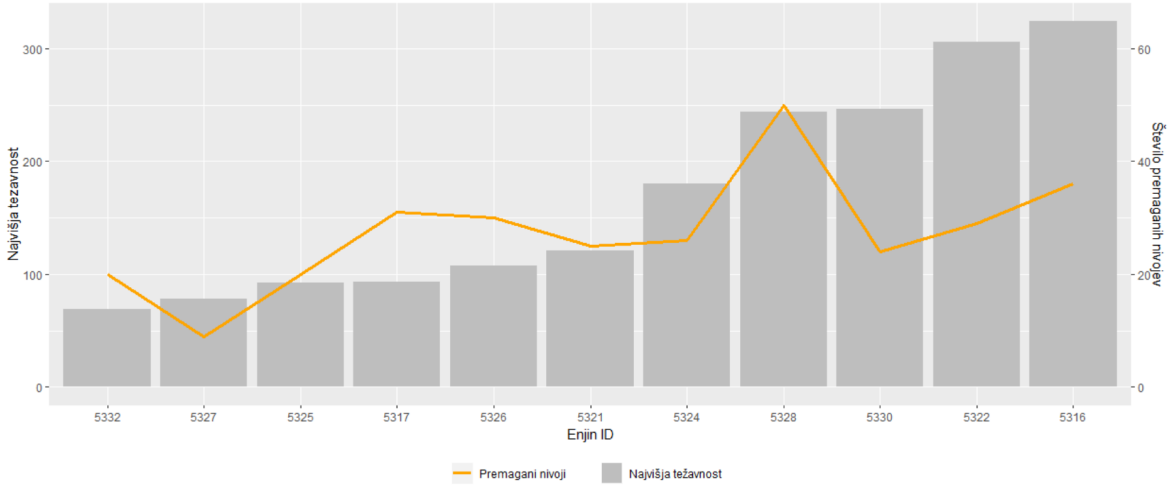
V nadaljevanju bosta bili ob vsakem grafu podani p-vrednost po Pearsonovi in Spearmanovi metodi. Označeni bosta bili s P za Pearsonovo in S za Spearmanovo p-vrednost.

Za analizo uspešnosti igralcev so uporabljene tri metrike:

1. količina zmag posameznega igralca;
2. skupni seštevek težavnosti vseh premaganih nivojev;
3. težavnost najzahtevnejšega nivoja, ki ga je premagal uporabnik.



(a) Premagani nivoji na prvem testiranju
(p-vrednost P: 0,01787, S: 0,02692)



(b) Premagani nivoji na drugem testiranju
(p-vrednost P: 0,06645, S: 0,04204)

Slika 20: Primerjava premaganih nivojev med prvim in drugim testiranjem. Višina stolpca je najvišja težavnost, ki jo je dosegel vsak uporabnik (z legendo na levi). Paličasti graf opisuje število premaganih nivojev (z legendo na desni).

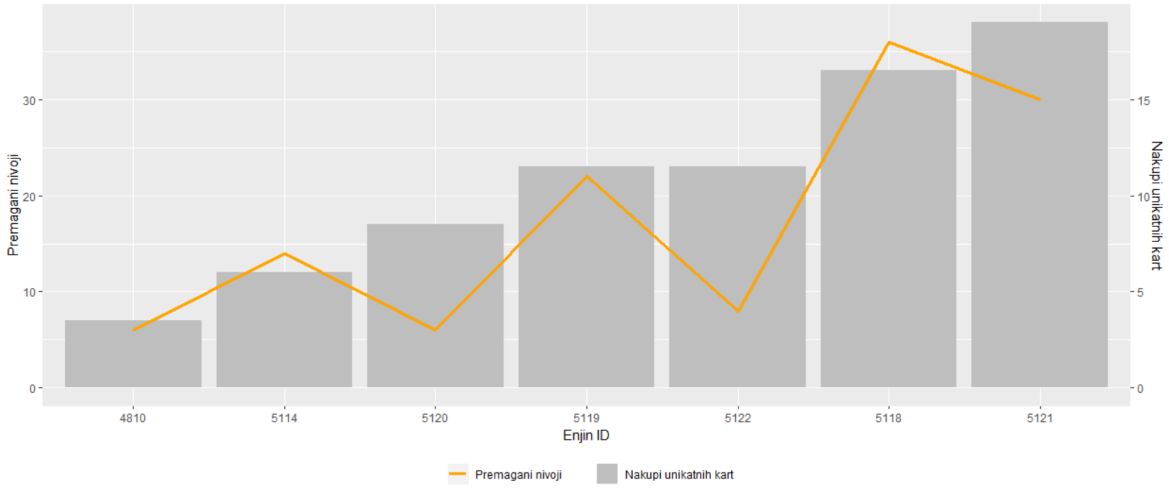
Iz slike 20 je razviden napredek igralcev igre na prvemu in drugemu testiranju. Na prvemu testiranju vidimo, da je bila maksimalna dosežena težavnost 160 in druga 110. Vsi ostali so dosegli manj kot težavnost 100. Število premaganih nivojev po večini narašča z najvišjo doseženo težavnostjo. Z izjemo dveh uporabnikov, se je večina uporabnikov držala trenda, da z več igrami sčasoma preidejo tudi na višje težavnosti. Izmed teh dveh uporabnikov je eden presenetil in premagal več težjih nivojev, kot se je zanj pričakovalo, drugi pa je večinoma premagoval samo nivoje z nizko težavnostjo.

Na drugem testiranju, ki se je izvajalo manj časa kot prvo, so igralci dosegali veliko boljše rezultate. Težavnost igre se ni spremenila, edina nova dejavnika sta bila delujoče testiranje in izkušnje nekaterih igralcev iz prvega testiranja. Vseeno je razlika občutna, saj je v drugem testiranju uspelo sedmim igralcem prekoračiti limit 100

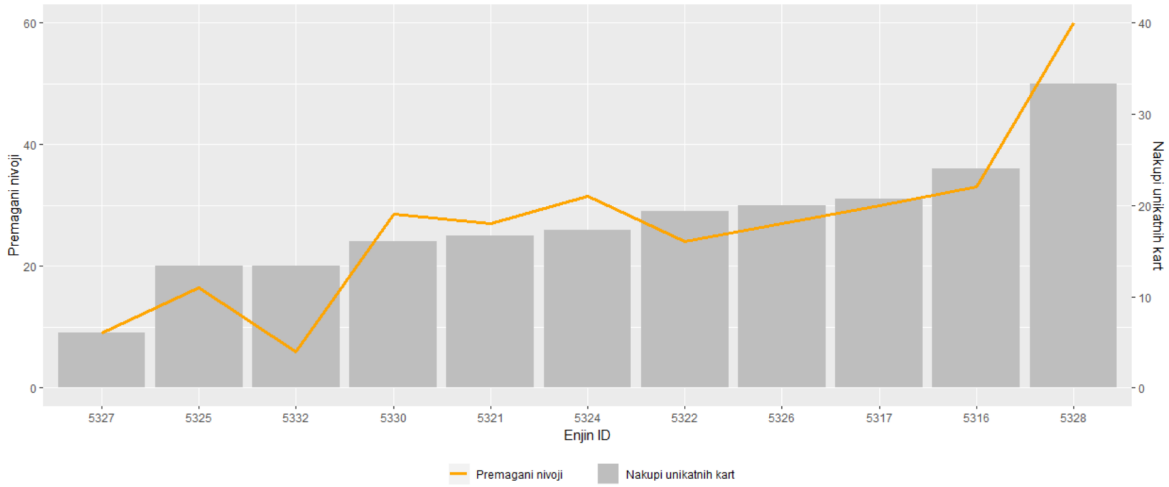
težavnosti, v primerjavi z dvema iz prvega testiranja. Petim od teh igralcev je uspelo izboljšati absolutni rekord prvega testiranja, dosegli so rezultate do 320 točk, kar je dvakratno izboljšanje prejšnjega rekorda. V drugem testiranju ni več opazno, da bi se s številom iger povečevala najvišja težavnost, ki jo je uporabnik dosegel. Zanimivo je, da je nekomu uspelo preigrati 15 iger več, kot vsem ostalim, in je po najvišji težavnosti zasedel komaj četrto mesto. V drugem testiranju se je korelacija med spremenljivkama zmanjšala. Po Spearmanovi metodi sta spremenljivki podobni in odvisni, medtem ko po Pearsonovi nista. To pomeni, da je korelacija veliko slabše izražena kot pri prvemu testiranju. Sklepati se da, da igralci v drugem testiranju niso več tako hitro napredovali po znanju igranja kot pri prvem, temveč se razlogi za boljše uspehe skrivajo drugje.

7.3.2 Primerjava doseženih točk igralcev s številom nakupov kart preko blockchaina

Kot je bilo omenjeno, če igralci premagajo težje nivoje na zemljevidu, pridobijo posebne diamante, ki služijo za nakup unikatnih kart preko blockchaina. Te karte so veliko močnejše od vseh ostalih kart, ki jih lahko igralci dobijo. Najprej je potrebno preučiti, če so bile te karte zadostna motivacija, da so igralci pogosteje igrali take nivoje (težje, z diamanti za nagrado), kot lažje, kjer so dobili za nagrado zgolj zlatnike.



(a) Nakupi kart na prvem testiranju
(p-vrednost P: 0,02212, S: 0,03075)



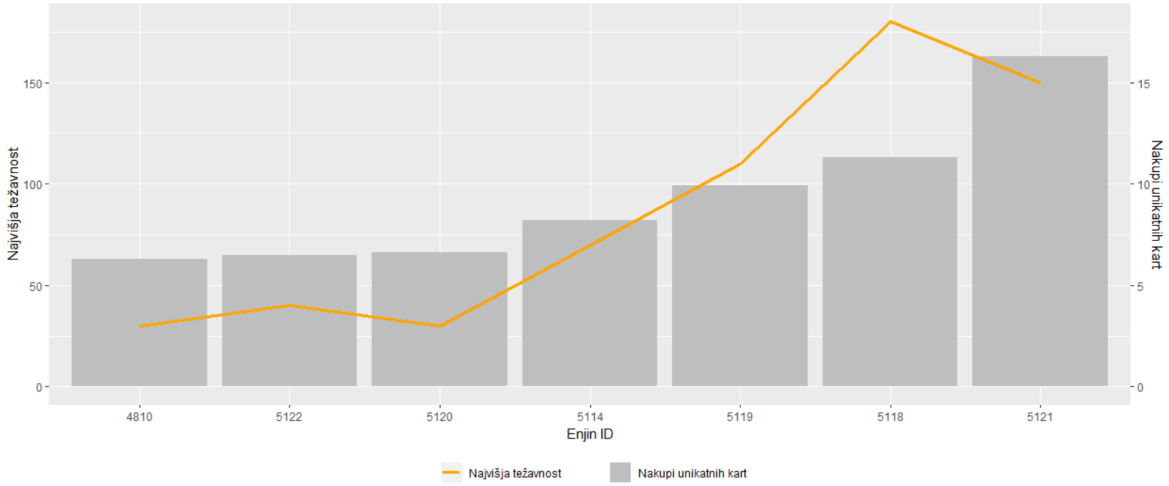
(b) Nakupi kart na drugem testiranju
(p-vrednost P: 0,00007, S: 0,00171)

Slika 21: Primerjava nakupa unikatnih kart glede na število premaganih nivojev. Višina stolpca predstavlja premagane nivoje vsakega izmed igralcev (z legendo na levi). Paličast graf predstavlja število nakupov unikatnih kart (z legendo na desni).

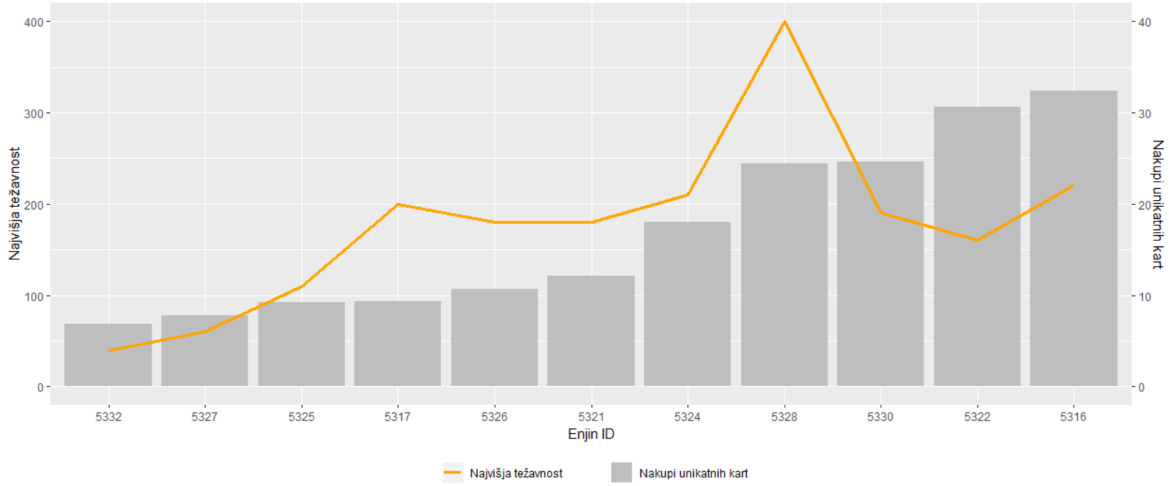
Na sliki 21 je predstavljena primerjava med razmerjem nakupov kart v igri glede na število nivojev, ki jih je uporabnik premagal. Razvidno je, da na prvem testiranju ni bilo veliko korelacije, iz česar lahko sklepamo, da igralci niso predhodno imeli občutka moči teh kart, ki jih lahko tako pridobijo z nakupom kart preko blockchaina. Na drugem testiranju vidimo, da so igralci skušali pridobiti čim več unikatnih kart. Razlika je kar očitna, saj je bilo v prvem testiranju skupno premaganih 153 nivojev. Izmed teh je bilo 61 težkih, kar pomeni, da je 40 % nivojev bilo težjih. Na drugem testiranju je bilo odigranih 300 iger, od teh je bilo 195 težkih. To pomeni, da je bilo 65 % nivojev težkih. Tako je razvidno, da so se na drugem testiranju igralci bolj zavedali moči teh kart. Vlogo je igralo tudi boljše trgovanje, saj je tudi prodaja teh kart prinesla zaslužek.

Razvidno je tudi, da z naraščanjem števila premaganih nivojev skoraj vzporedno

narašča tudi število nakupa unikatnih kart. Pri obeh grafih tudi korelacijska kvocienta potrdita, da sta funkciji medsebojno tesno povezani, s tem da na drugem testiranju veliko bolj kot pri prvem. Skupaj s prejšnjo ugotovitvijo lahko potrdimo, da so bili igralci dodatno motivirani k nakupu unikatnih kart v drugem testiranju – bodisi ker so se bolje zavedali njihove moči bodisi ker jim je trgovanje omogočilo dodatno vrednost.



(a) Nakupi kart na prvem testiranju
(p-vrednost P: 0,01658, S: 0,005621)



(b) Nakupi kart na drugem testiranju
(p-vrednost P: 0,07949, S: 0,02164)

Slika 22: Primerjava nakupa unikatnih kart glede na maksimalno doseženo težavnost. Višina stolpca predstavlja najvišjo doseženo težavnost vsakega izmed igralcev (z legendo na levi). Paličast graf predstavlja število nakupov unikatnih kart (z legendo na desni).

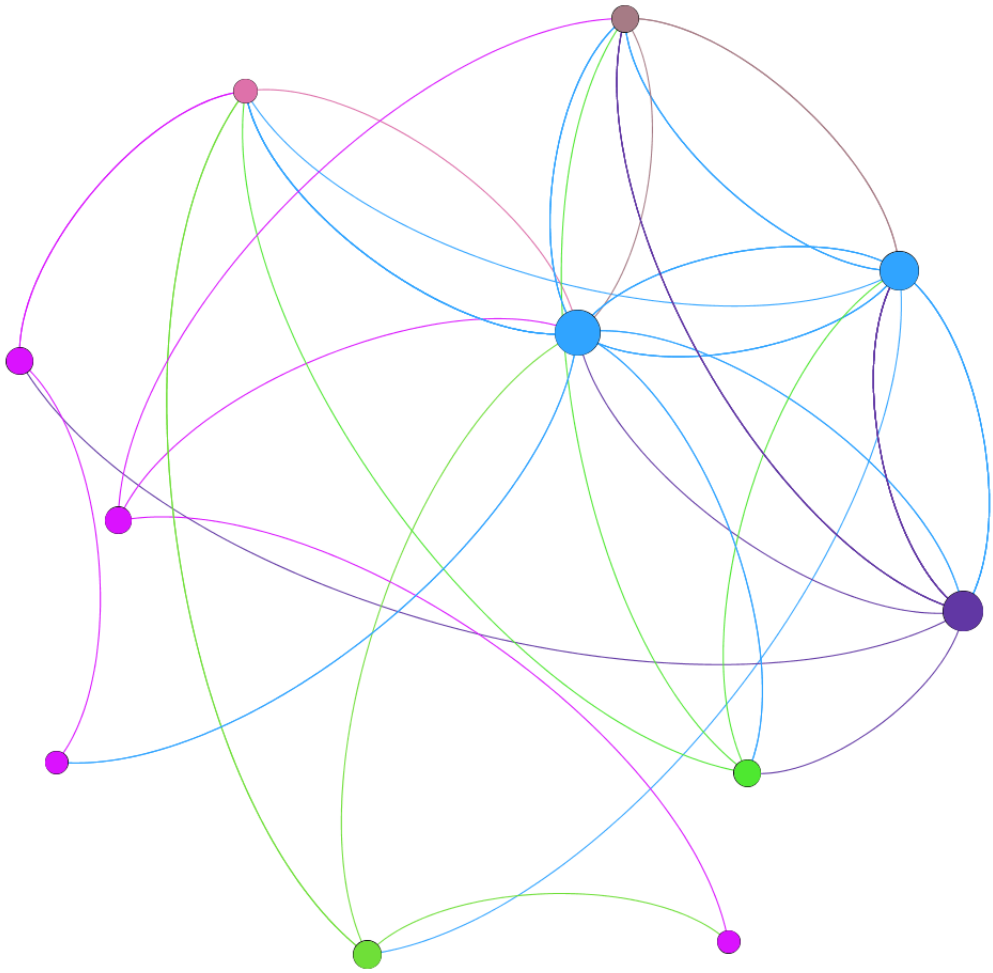
Na sliki 22 je obravnavano razmerje med nakupom unikatnih kart in maksimalno doseženo težavnostjo. Razvidno je, da je na prvem testiranju število nakupa unikatnih kart dobro ocenilo maksimalno težavnost, ki jo je premagal igralec. To je tudi potrjeno s korelacijskimi koeficienti, ki so pokazali, da sta spremenljivki v korelaciji po obeh

metodah. Izjema je zadnji igralec, ki je kupil nekaj manj kart od ostalih, a jih je znal dobro izkoristiti in je s tremi kartami manj dosegel najvišjo težavnost. Na tem mestu je potrebno seveda upoštevati tudi kakovost kart, ki jih dobi igralec, ne zgolj kvantiteto. Kakovost je odvisna od veliko dejavnikov, saj lahko dobljena karta sovpada z igralno strategijo igralca, lahko je boljša za njegove naključno zgrajene nivoje, ali ne.

Na drugem testiranju se je izkazalo, da je bila korelacija med številom nakupa kart in maksimalno doseženo težavnostjo veliko manjša, saj je zgolj Spearmanova metoda potrdila korelacijo. Prvi razlog za manjšo korelacijo je bil ta, da je večina igralcev na drugem testiranju igrala raje težje nivoje kot lahke, zato je bilo število unikatnih kart med igralci približno enako. Drugi razlog je bil, da je sedaj postalo pomembneje, da so igralci pametno trgovali karte med sabo, saj so tako prišli do najboljših kart za izbrano strategijo. Razvidno je, da sta dva igralca z relativno malo nakupljenimi kartami dosegla skoraj dvakrat toliko točk od ostalih.

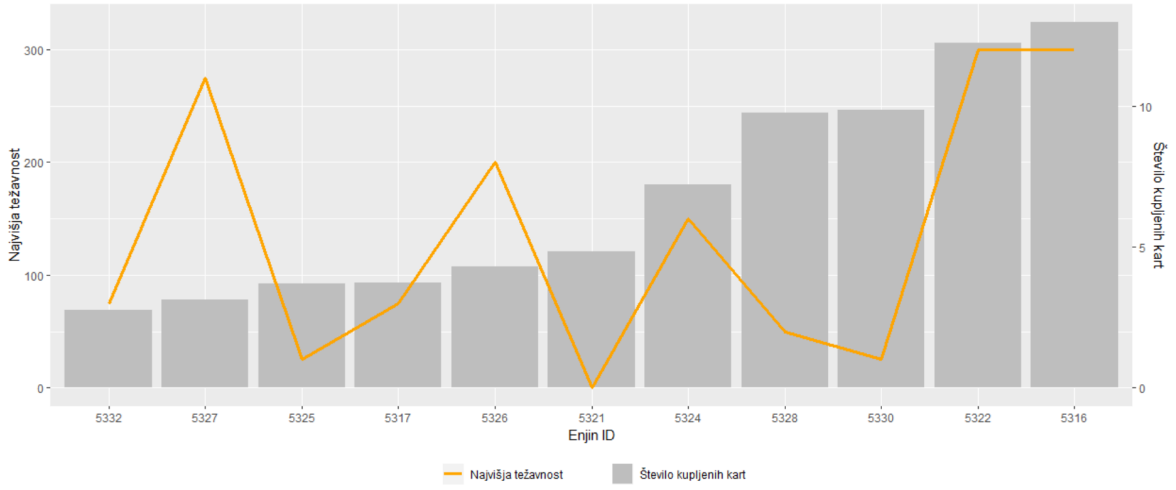
7.3.3 Pregled trgovanja igralcev

V tem podrazdelku bodo analizirane izmenjave dobrin igralcev med sabo. Preučevano bo zgolj drugo testiranje, kjer je bilo izmenjav veliko več kot v prvem. Izkazalo se je, da so vsi igralci izpeljali vsaj eno izmenjavo, tako da je varno sklepati, da so bili vsi seznanjeni s postopkom izmenjave dobrin. Preučevani bodo različni profili igralcev, glede na to, ali so se predvsem posvečali menjavam ali igranju.

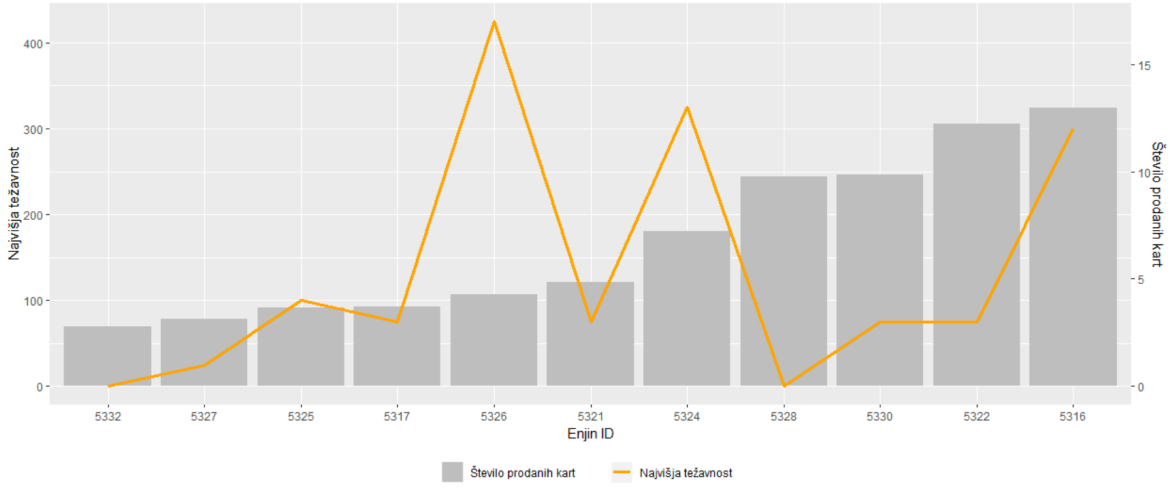


Slika 23: Prikaz izmenjave kart med igralci. Vsak igralec je predstavljen kot vozlišče v grafu. Velikost vozlišča predstavlja najvišjo težavnostjo nivoja, ki ga je premagal igralec. Povezave predstavljajo enosmerno pošiljanje dobrine, pobarvano z barvo lastnika karte, ki je začel izmenjavo.

Na sliki 23 so predstavljene vse izmenjave, ki so se zgodile v času testiranja. Vozlišča predstavljajo igralce, povezave pa izmenjave med njimi. Debelina povezave predstavlja število izmenjav, ki sta jih igralca opravila v neko smer. Iz grafa vidimo, da so bili igralci v trgovanju aktivni, saj so izmenjave tekle v veliko različnih smeri. Prav tako opazimo, da so igralci z velikim vozliščem imeli povečini tudi veliko povezav. Iz tega je mogoče z veliko verjetnostjo sklepati, da obstaja nekakšna povezanost med številom izmenjav, ki jih je opravil igralec, in najvišjo težavnostjo nivoja, ki jo je dosegel. Ta verjetnost bo podrobneje obravnavana v nadaljevanju razdelka.



(a) Nakupi kart v drugem testiranju
(p-vrednost P: 0,247, S: 0,4638)



(b) Prodaja kart v drugem testiranju
(p-vrednost P: 0,666, S: 0,385)

Slika 24: Primerjava nakupa in prodaje kart preko izmenjevalnega sistema glede na maksimalno doseženo težavnost. Višina stolpca predstavlja najvišjo doseženo težavnost vsakega izmed igralcev (z legendo na levi). Paličast graf predstavlja število nakupov unikatnih kart (na levi) in prodajo unikatnih kart (na desni). Legenda za število kart je na desni strani vsakega grafa.

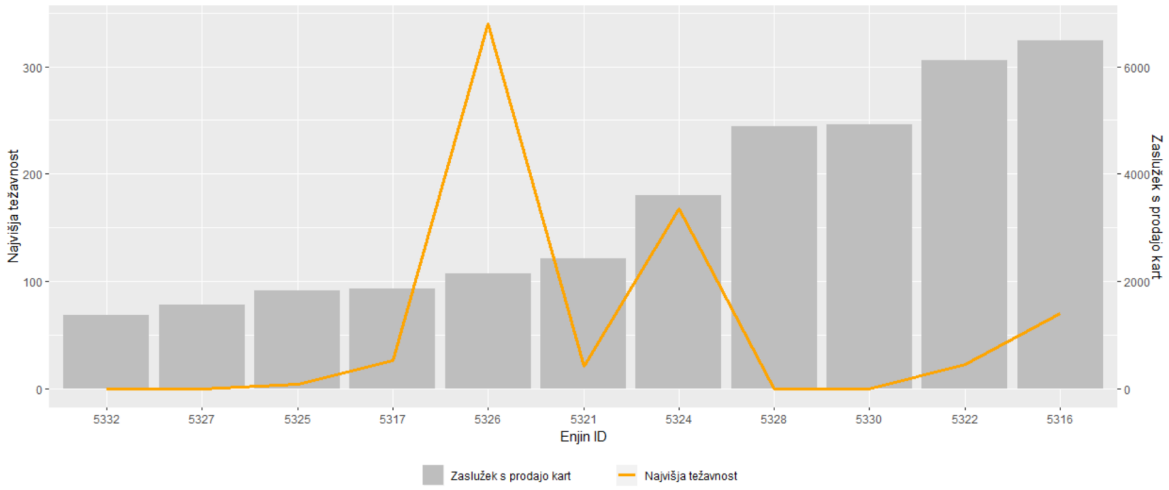
Na grafu 24 se vidi, da skupna količina prodanih in kupljenih kart ni povezana z najvišjo težavnostjo, ki so jo dosegli igralci, kar tudi potrdita korelacijska koeficienta. Po interni analizi je bilo ugotovljeno, da so se v testiranju oblikovale tudi posebne skupine igralcev, ki se pojavljajo pri igrah z odprto menjavo dobrin med igralci. Te skupine se ukvarjajo z ustvarjanjem dobička preko prekupčevanja kart, kjer je glavna ideja, da kupijo čim več kart po nizki ceni ter jih drago prodajo.

V desnem grafu vidimo, da so samo trije igralci prodali več kot štiri karte. Vsi izmed teh so prodali vsaj 12 kart. Iz tega je mogoče sklepati, da so začeli ustvarjati nekakšno ekonomijo z namenom zaslužka. Izmed teh treh igralcev je eden pretvoril

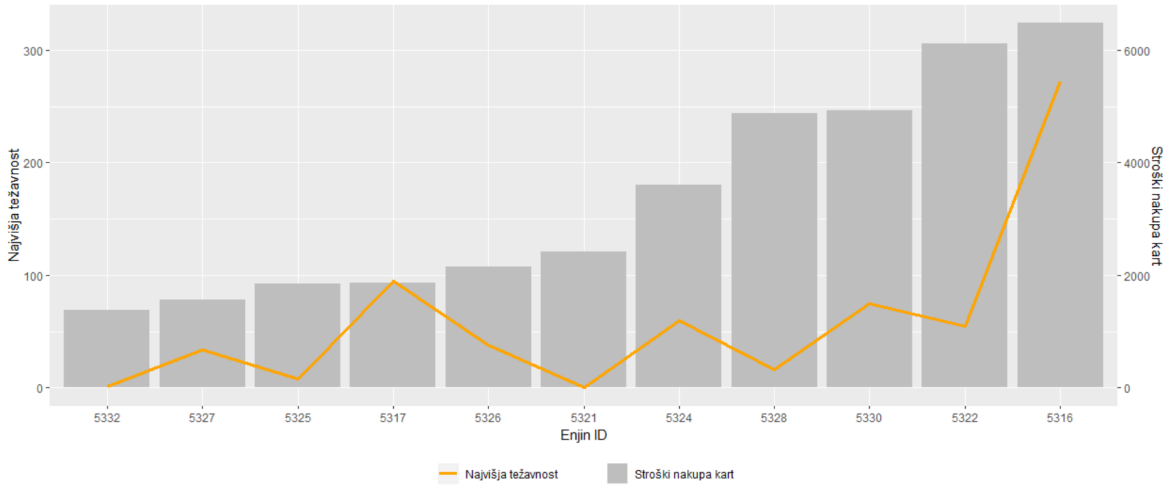
prislužen dobiček v tako močen kupček kart, da je z njim premagal tudi najtežji nivo na testiranju.

Iz levega grafa je razvidno, da sta oba igralca, ki sta presegla mejo 250 težavnosti, kupila veliko kart – celo največ izmed vseh na testiranju. Tudi naslednja uvrščena igralca sta kupila nekaj kart, čeprav relativno malo. To nakazuje, da je bilo potrebno za dosego najvišje uvrščenosti kupiti veliko kart za izpopolnitev kupčka. K temu je pripomogla izmenjava dobrin med igralci.

Razvidno je, da so tisti igralci, ki so izmenjali vsaj nekaj kart, dosegli veliko več točk, kot so jih dosegli na prvemu testiranju, kjer je bilo izmenjav med igralci relativno malo. Izmed najboljših štirih igralcev sta bila dva taka, ki sta se z igro srečala prvič, zato predhodne izkušnje iz prvega testiranja pri njima niso igrale vloge.



(a) Dobiček prodaje kart v drugem testiranju
(p-vrednost P: 0,7021, S: 0,3176)



(b) Stroški nakupa kart v drugem testiranju
(p-vrednost P: 0,05204, S: 0,08155)

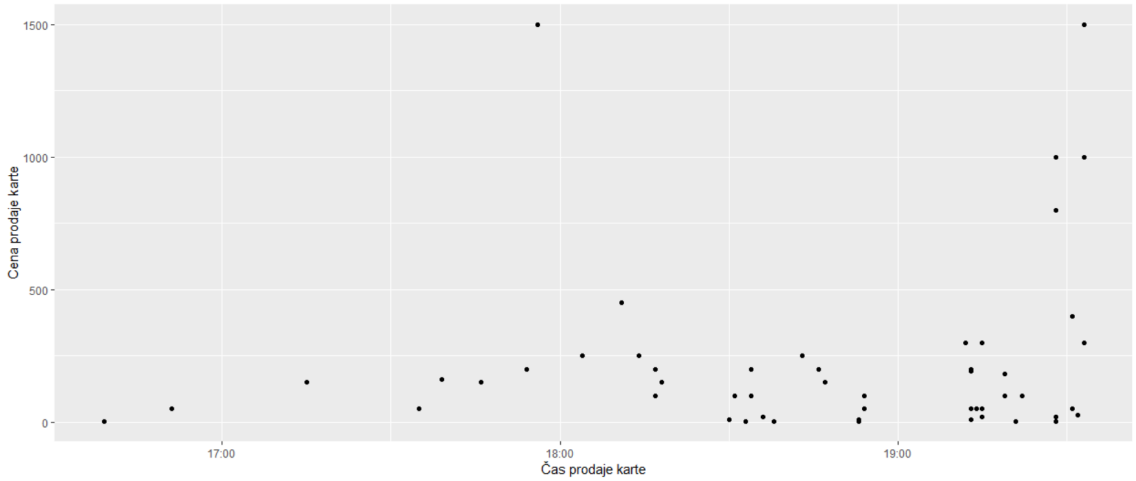
Slika 25: Primerjava dobička iz prodaje kart in stroškov nakupa kart preko izmenjevalnega sistema glede na maksimalno doseženo težavnost. Višina stolpca predstavlja najvišjo doseženo težavnost vsakega izmed igralcev (z legendo na levi). Paličast graf predstavlja dobiček iz prodaje unikatnih kart (na levi) in stroške nakupa unikatnih kart (na desni). Legenda za število kart je na desni strani vsakega grafa.

Iz slike 25 se poudarjeno vidi sklep, narejen iz prejšnjega odstavka. Zaslužek ni neposredno povezan z najvišje doseženo težavnostjo, a imajo igralci z veliko manjšo doseženo težavnostjo pogosto več zaslužka kot tisti, ki so dosegli višjo težavnost. Vidi se, da so se nekateri igralci, ki so dosegli nižjo težavnost, naredili dobiček z izmenjavo kart. Ker se da blockchain dobrine vedno menjati tudi za realen denar, se taki profili ljudi vedno pojavljajo.

Na drugem grafu je razvidno, da je nekoliko nestabilen tudi graf stroškov, a sta korelacijska koeficienta blizu pragu za korelacijo. V času testiranja, ki je trajalo samo 5 ur, se namreč ni popolnoma vzpostavila stabilna ekonomija. Ker igralci niso imeli

podatkov o ceni zadnje prodanih kart, so morali prodajno ceno zgolj ugibati. Prav tako so na drugi strani tudi kupci zgolj ugibali vrednost karte. Vseeno se vidi manjšo korelacijo med vsoto zlatnikov, porabljenih za nakup kart, in maksimalno doseženo težavnostjo. Vidi se, da so boljši igralci morali zapravljati za premagovanje najtežjih nivojev.

Iz grafa lahko opazimo, da so nekateri igralci z manj izdatki dobili pomembnejše karte kot drugi. Računati je potrebno tudi na to, da so nekateri igralci dobili boljše unikatne karte kot drugi, iz česar sledi, da so nekateri morali več kupovati za kompenzacijo razlike. Drugi so zgolj prodajali karte za najvišjo mogočo ceno. Videti je, da so morali najboljši igralci vsaj nekaj zapraviti za dosego najboljših položajev.



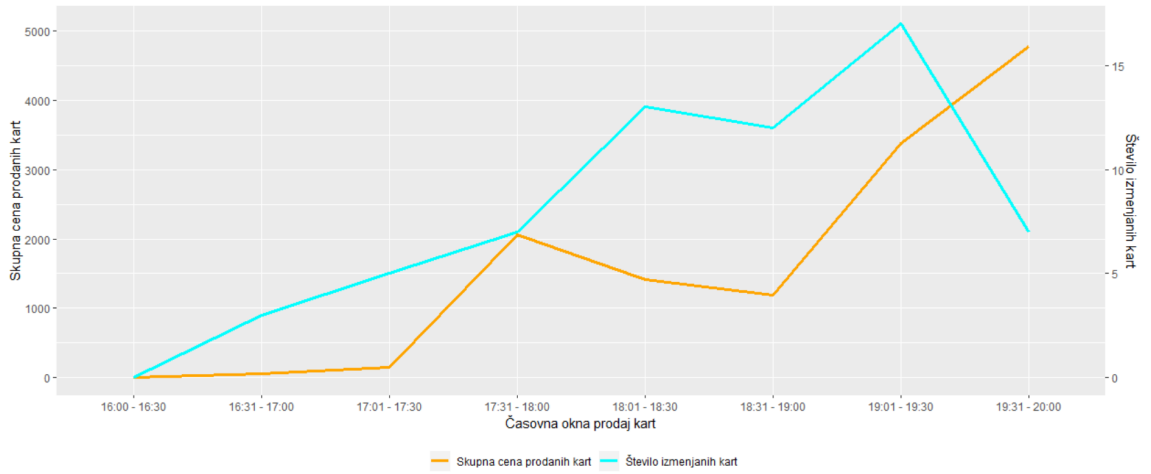
Slika 26: Prikaz cene prodaje kart v relaciji s časom. Na vodoravni osi so označeni časi prodaje kart. Točke na grafu prikazujejo ceno prodaje kart v določenem trenutku z legendo na levi.

Iz slike 26 je razvidno, da se je cena izmenjanih kart spreminjala skozi čas. Pomemben dogodek se je zgodil takoj na začetku testiranja, ko je bila pridobljena najboljša unikatna karta, kar jih je bilo moč dobiti. Prodala se je za 1500 zlatnikov, kar je bila tudi maksimalna cena skozi celotno testiranje.

Vidi se, da so cene kart poskočile takoj na začetku testiranja, ko so vsi igralci želeli pridobiti čim boljše karte, ki bi jim pomagale pri hitrem napredovanju. Nato je sledila faza konstantne prodaje, kjer so se manj vredne karte prodajale po relativno nizkih cenah. Tik pred koncem je sledila zadnja faza, kjer so vsi igralci skušali dobiti vse najboljše karte na tržišču, da bi dosegli čim višjo težavnost. Cene kart so tik pred koncem sunkovito poskočile, ker so igralcem pomagale pri premagovanju najtežjih nivojev.

Razvidne so tudi "prijateljske"izmenjave kart, kjer so se igralci med seboj dogovorili, da so izmenjali karte skoraj zastonj, z namenom, da nekomu pomagajo. Taki dogodki so se pojavljali ves čas. Izmenjave so stroškovno stale okoli simboličnih 10 zlatnikov.

Na grafu iz slike 27 so prikazani trendi cene prodaje kart po časovnih oknih ter število prodanih kart v vsakem časovnem oknu. Časovno okno je v tem primeru 30



Slika 27: Prikaz cene prodaje kart in število prodaje kart v relaciji s časom. Vodoravna os je razdeljena na časovna okna dolžine 30 minut. Točka na grafu prikazuje skupno ceno prodanih kart (z legendo na levi), v relaciji s skupnim število prodanih kart (z legendo na desni) v določenem časovnem oknu.

minut. Vidi se, da se v prvi uri testiranja ni zgodila nobena menjava, saj igralci niso uspeli premagati težjih nivojev, ki bi jim zagotovili njihovo prvo unikatno karto. V drugem in tretjem časovnem oknu se tudi ni zgodilo nič presenetljivega, saj se je zgodilo samo tri in pet izmenjav, ki so bile skupno vredne približno 200 zlatnikov.

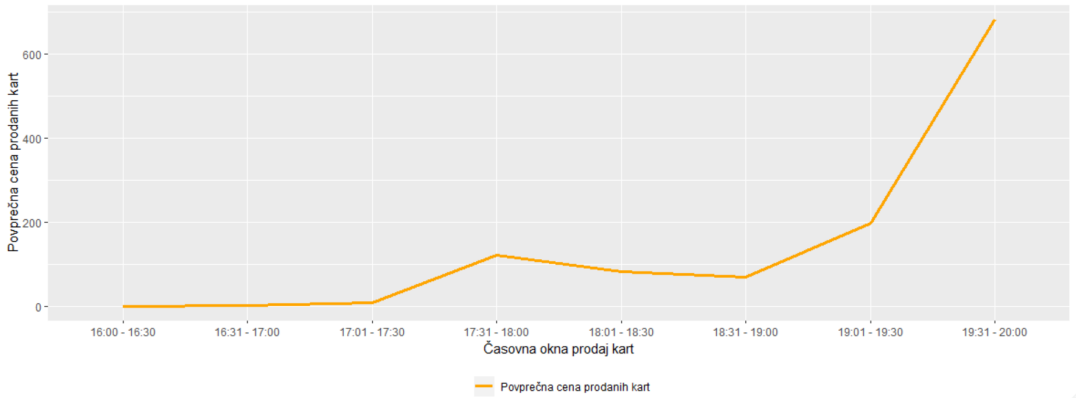
V četrtem časovnem oknu se je zgodila prva resna izmenjava, ko je nek igralec dobil tako imenovano "čisto"(ang. pure) karto. Taka karta ima vse sposobnosti usmerjene v zgolj eno dimenzijo, s čimer postane nadpovprečno močna. Take karte so statistično redke in jih je skoraj nemogoče dobiti. Ta karta se je kmalu prodala za 1500 zlatnikov, kar je razvidno v velikem skoku na grafu.

V naslednjih dveh oknih je število prodanih kart naraslo in skupna cena je padla. Najvišja cena karte je bila v teh oknih veliko nižja, s tem je padlo tudi povprečje cene kart. Tik pred koncem, v predzadnjem okencu, sta spet poskočila tako število izmenjanih kart kot tudi skupna cena.

V zadnjem oknu je nekaj igralcev zaključilo z igranjem, zato je število prodanih kart upadlo. Skupna vrednost izmenjav je celo presegla prejšnji maksimum z manj kot polovico izmenjav kot v prejšnjem oknu. Videti je, da so igralci cenili izmenjavo dobrin v zadnjem trenutku, saj so verjeli, da jim bodo te karte pomagale doseči višje nivoje.

Na sliki 28 je prikazana povprečna cena prodanih kart v vsakem časovnem oknu. Časovna okna so dolga 30 minut. Kot je bilo razvidno iz prejšnjega grafa na sliki 27 se v prvih treh časovnih oknih ni dogajalo nič zanimivega.

V četrtem oknu, ko se je prodala prva draga karta, je visoko dvignila povprečje prodanih kart. V naslednjih dveh oknih se je ekonomija spet stabilizirala na prejšnje stanje, tako da je povprečje nekoliko padalo, a bilo vseeno primerljivo s prejšnjim maksimumom.

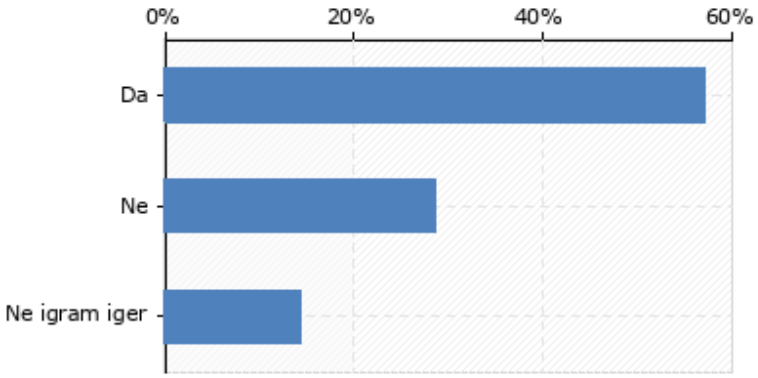


Slika 28: Prikaz povprečne cene prodaje kart v relaciji s časom. Vodoravna os je razdeljena na časovna okna dolžine 30 minut. Točka na grafu prikazuje povprečno ceno prodanih kart (z legendo na levi), v določenem časovnem oknu.

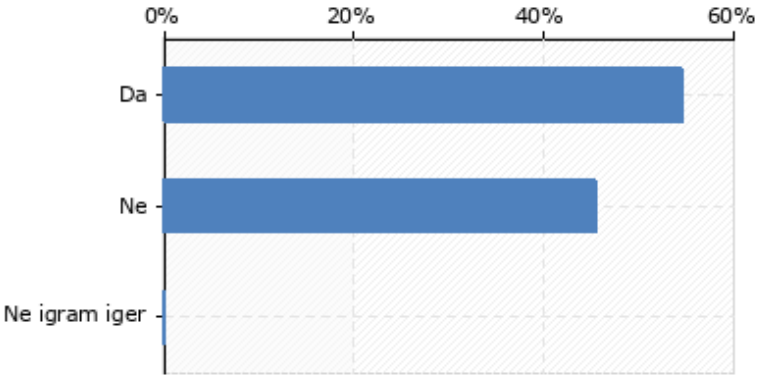
V zadnjih dveh okencih je začela povprečna cena kart skokovito naraščati in v zadnjem oknu je več kot potrojila prejšnji maksimum. Tudi ta graf prikaže pomembnost izmenjave dobrin pri igranj ter tudi prepričanje igralcev, da jim bodo boljše karte zagotovile višje mesto na lestvici najboljših.

7.3.4 Pregled rezultatov ankete

Po koncu vsakega izmed obeh testiranj so vsi udeleženci prejeli anketo, ki so jo izpolnili preko telefona. Anketo so na obeh testiranjih izpolnili vsi udeleženci, torej je prisotnost popolna. Anketa je na voljo za ogled v prilogah A, B in C. Prvo vprašanje v anketi je zgolj spraševalo po Enjin identiteti uporabnika, ki mu je bila dodeljena za testiranje, da se lahko odgovore ankete uteži s podatki iz testiranja. Na prvem testiranju je anketo rešilo sedem udeležencev (n = 7) in na drugem 11 (n = 11). Za vsako vprašanje bodo podani rezultati iz obeh anket hkrati, nato bo sledila obrazložitev rezultatov.



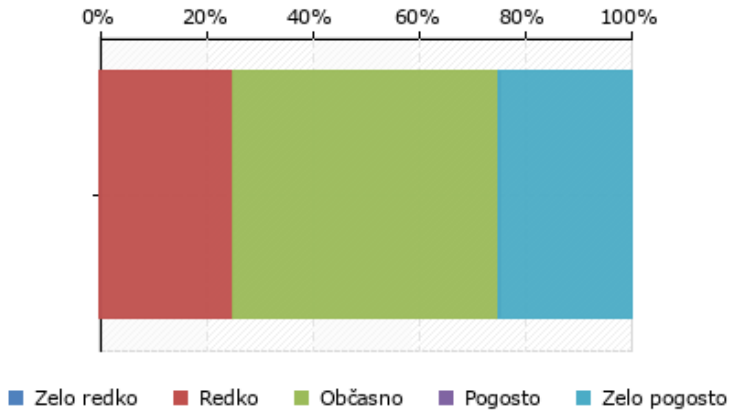
(a) Rezultati prvega testiranja (n = 7)



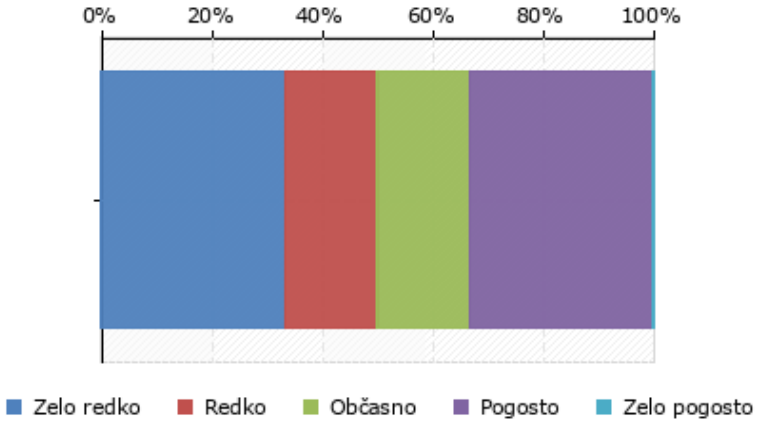
(b) Rezultati drugega testiranja (n = 11)

Slika 29: Ali igrate kakšno igro, v kateri je mogoče izmenjevati dobrine med igralci?

Rezultati prvega vprašanja so vidni na sliki 29. Na obeh testiranjih je večina ljudi povedala, da igra igre, ki vsebujejo izmenjavo dobrin med igralci. V obeh testiranjih je bilo takih udeležencev skoraj 60 %. V prvi anketi ena oseba ni bila prepričana ali igra take igre ali ne. Vprašanje je pokazalo, da je bila večina udeležencev na testiranju predhodno seznanjena z vsaj enim načinom izmenjave dobrin. Tako je mogoče sklepati, da lahko primerjajo sistem izmenjave z ostalimi.



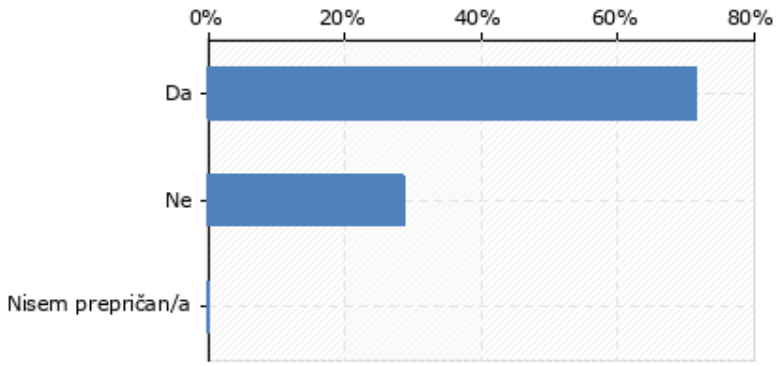
(a) Rezultati prvega testiranja (n = 4)



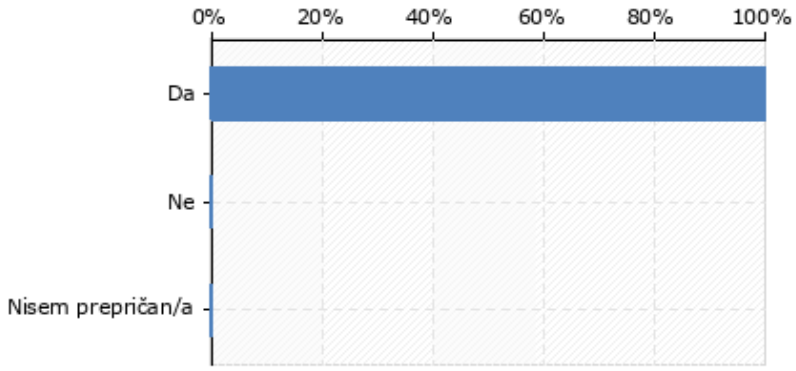
(b) Rezultati drugega testiranja (n = 6)

Slika 30: Kako pogosto menite, da izmenjujete dobrine v takih igrah?

Tretje vprašanje, ki je prikazano na sliki 30, se je nanašalo na pogostost izmenjevanja dobrin v igrah. Izkazalo se je, da imajo igralci izrazito mešane izkušnje z izmenjavo dobrin v teh igrah. Na prvem testiranju večina ljudi misli, da trguje zgolj občasno, ostali bodisi redko bodisi zelo pogosto. Na drugem testiranju so bili porazdeljeni skoraj enakomerno med opcijami zelo redko do pogosto. Različne igre seveda ponujajo različne načine testiranja, različne izkušnje in tudi izmenjava dobrin lahko v različnih igrah pomeni različne stvari. Igre lahko ponujajo zgolj izmenjavo kozmetičnih dobrin ali ponujajo izmenjavo vseh dobrin, kar jih ima igralec.



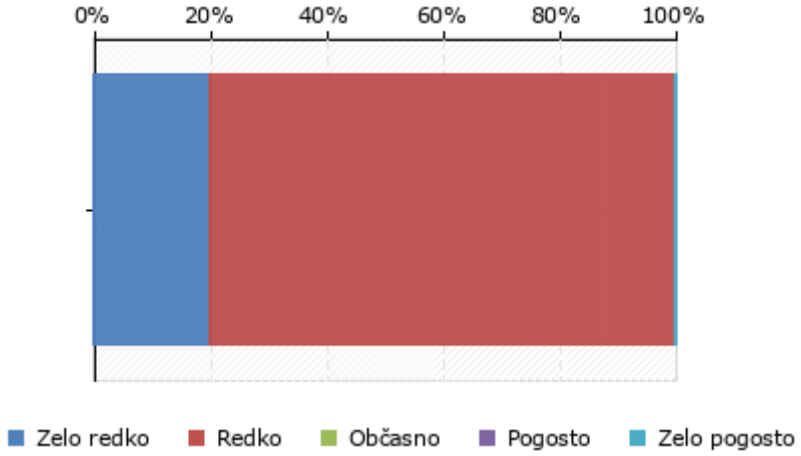
(a) Rezultati prvega testiranja (n = 7)



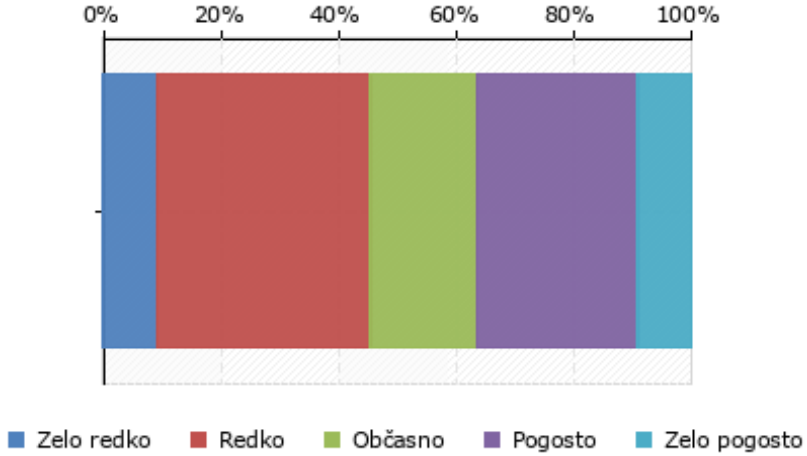
(b) Rezultati drugega testiranja (n = 11)

Slika 31: Ali ste uporabljali možnost izmenjave dobrin na tem testiranju?

Na sliki 31 so prikazani rezultati četrtega vprašanja. Rezultati za prvo testiranje so bili nekoliko slabši, saj skoraj 30 % udeležencev ni uporabljajo sistema za izmenjavo dobrin med igralci. Na srečo so bili rezultati na drugem sistemu spodbudni, saj so pokazali, da so na drugem testiranju čisto vsi uporabljali ta sistem. Očitno so izboljšave sistema preko mnenj testirancev iz prvega testiranja pripomogle k boljši uporabniški izkušnji tudi za vse ostale.



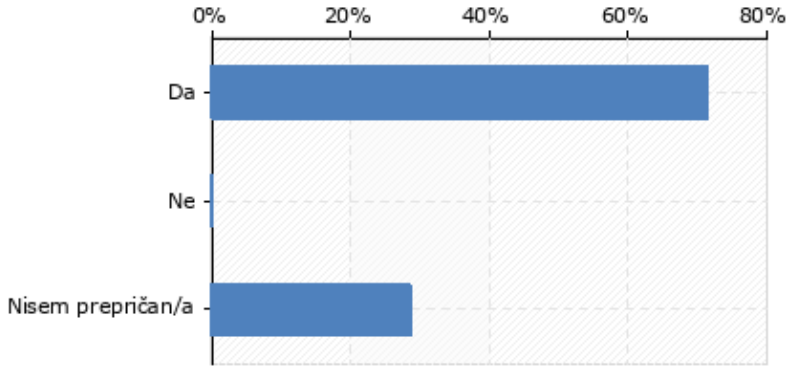
(a) Rezultati prvega testiranja (n = 5)



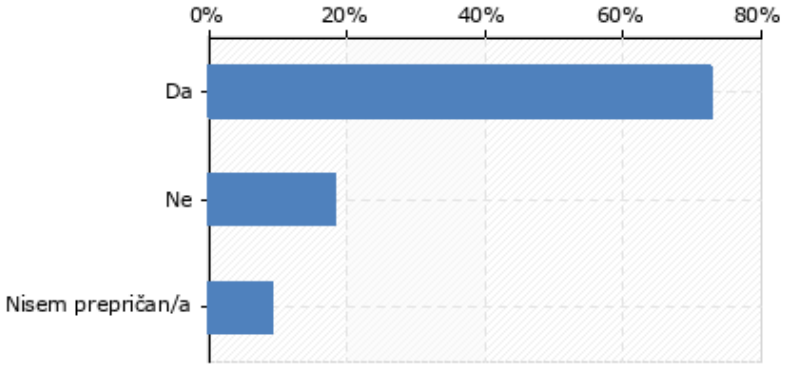
(b) Rezultati drugega testiranja (n = 11)

Slika 32: Kako pogosto menite, da ste izmenjevali dobrine na testiranju?

Podvprašanje 5 je bilo vidno samo anketirancem, ki so odgovorili na četrto vprašanje z "da"ali "ne vem". Razvidno je, da so rezultati prvega testiranja slabši, saj so imeli udeleženci, ki so medsebojno izmenjevali dobrine, bodisi občutek, da so to počeli redko, bodisi zelo redko. Na drugem testiranju se je uporabniška izkušnja toliko izboljšala, da je večina udeležencev mislila, da so trgovali vsaj občasno. Nekaj jih je imelo celo občutek, da so trgovali pogosto ali zelo pogosto, kar je izjemen napredek. Izmenjava dobrin med igralci je postala privlačnejša v drugi iteraciji.



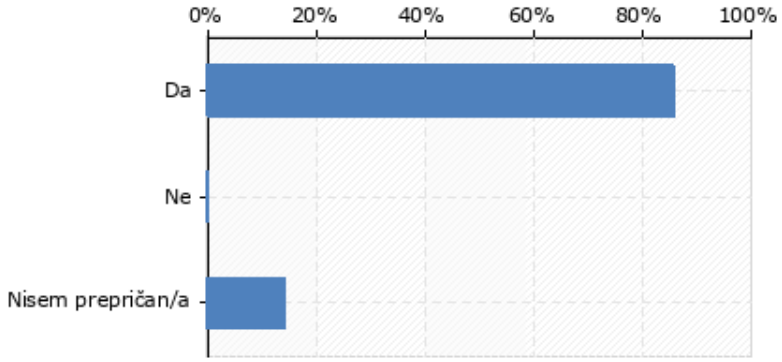
(a) Rezultati prvega testiranja (n = 7)



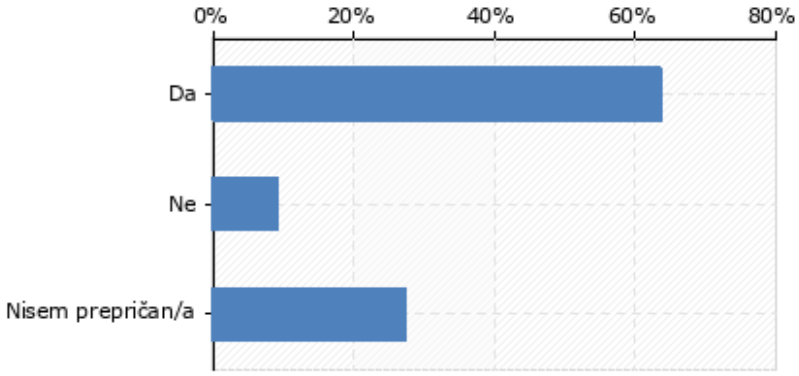
(b) Rezultati drugega testiranja (n = 11)

Slika 33: Ali ste seznanjeni s tehnologijo blockchain?

Vprašanje 6 je bilo preprosto, saj je spraševalo zgolj po tem, ali so uporabniki bili predhodno seznanjeni z blockchainom. Rezultati na sliki 33 prikazujejo, da jih nekaj ni bilo popolnoma prepričanih, v drugem testiranju pa zgolj dva nista bila seznanjena z blockchainom. Vedeti je potrebno, da so na testiranju večinoma sodelovali študenti fakultete FAMNIT, kjer je blockchain tudi del snovi, zato se pričakuje, da so bili s tem seznanjeni. Na drugem testiranju je bilo tudi nekaj zunanjih udeležencev, ki so za blockchain najbrž slišali prvič.



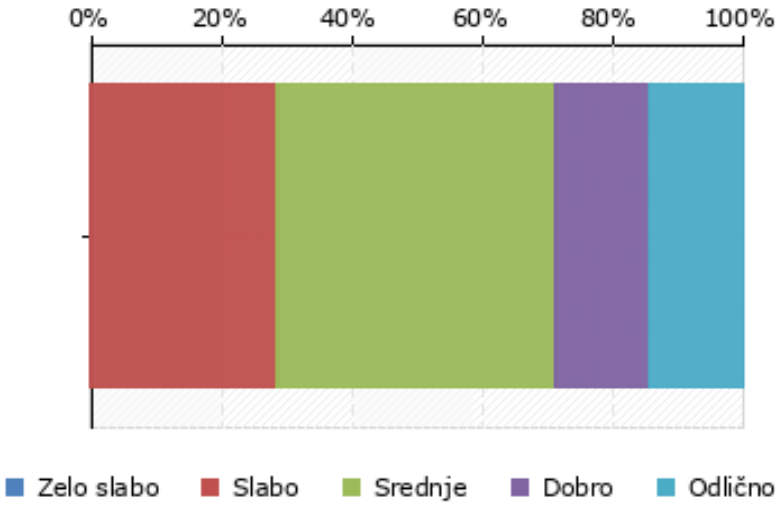
(a) Rezultati prvega testiranja (n = 7)



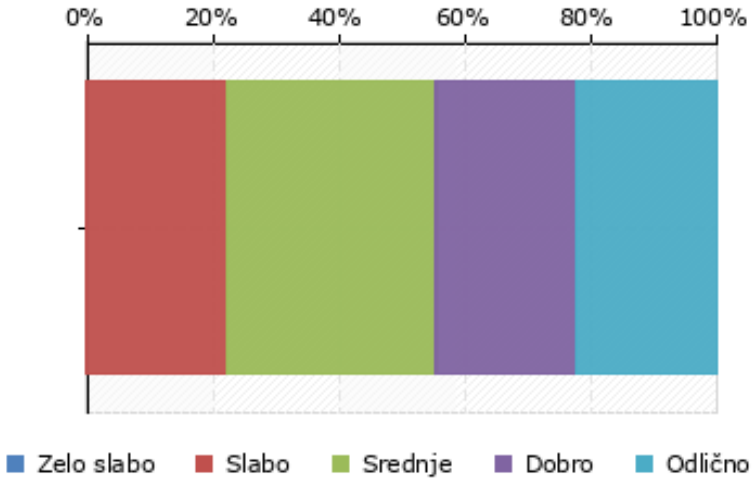
(b) Rezultati drugega testiranja (n = 11)

Slika 34: Izmenjava dobrin je na tem testiranju potekala preko tehnologije blockchain. Ali štejejo to tehnologijo kot bolj varno od do sedaj uporabljanih?

Naslednje vprašanje je spraševalo uporabnike po njihovem mnenju, ali gledajo na blockchain kot varnejšo tehnologijo od tistih, ki so do sedaj široko uporabljene v svetu igranja iger. Skozi to delo se je velikokrat omenilo prednosti blockchaina. Vprašanje je, ali so bili uporabniki s temi prednostnimi predhodno seznanjeni. Iz slike 34 je razvidno, da je na prvem testiranju več kot 80 % uporabnikov menilo, da je blockchain varnejši od ostalih rešitev. Vedeti je potrebno, da je večina teh ljudi obiskovala predavanja na to temo in je bila s prednostnimi vsaj enkrat do tedaj seznanjena. Na drugem testiranju je ena oseba menila, da blockchain ne prinaša izboljšane varnosti, kar tri osebe niso bile popolnoma prepričane. Sklepati je mogoče, da ljudje, ki se toliko ne ukvarjajo z računalništvom, niso vedno seznanjeni s blockchainom in ne poznajo njegovih prednosti.



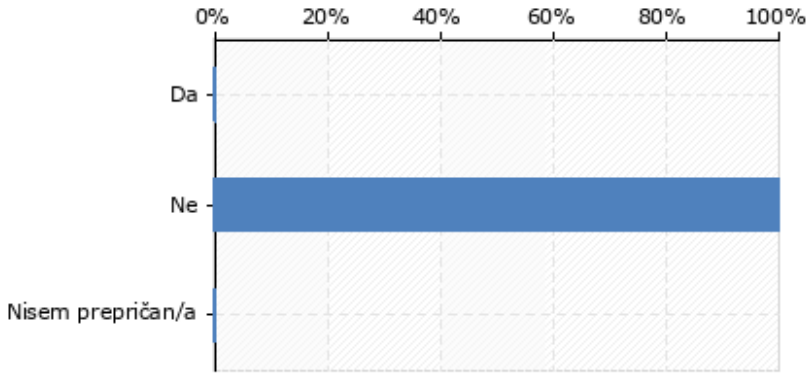
(a) Rezultati prvega testiranja (n = 7)



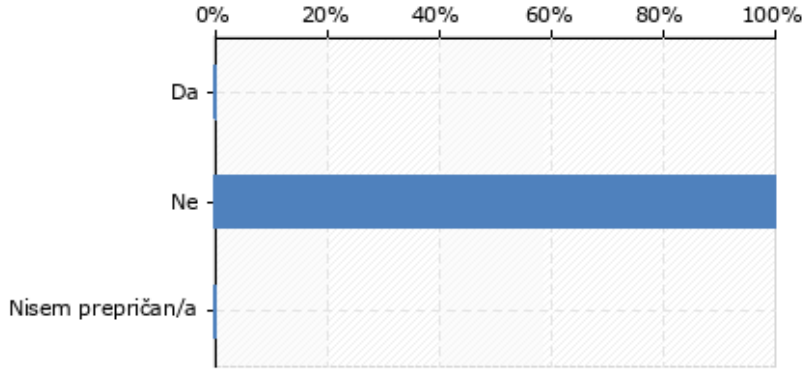
(b) Rezultati drugega testiranja (n = 9)

Slika 35: Kako dobro ste seznanjeni s pametnimi pogodbami?

Vsi uporabniki, ki so omenili, da so seznanjeni z blockchainom ali pa niso bili prepričani pri 6. vprašanju, so dobili vprašanje 8. Na sliki 35 lahko vidimo, da so vsi uporabniki, ki so seznanjeni z blockchainom, vsaj slabo seznanjeni tudi s pametnimi pogodbami. Na drugem testiranju je bilo več udeležencev, ki so bili odlično in dobro seznanjeni s temi pogodbami. Na prvem testiranju je bilo veliko udeležencev ali slabo seznanjeno ali srednje seznanjenih s pametnimi pogodbami. To je spodbuden dejavnik, ker pove, da znajo uporabniki dobro primerjati pametno pogodbo v tej igri s poznanimi pametnimi pogodbami.



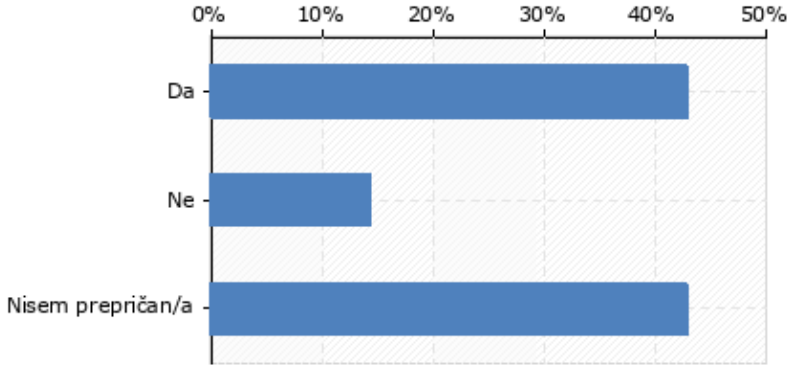
(a) Rezultati prvega testiranja (n = 7)



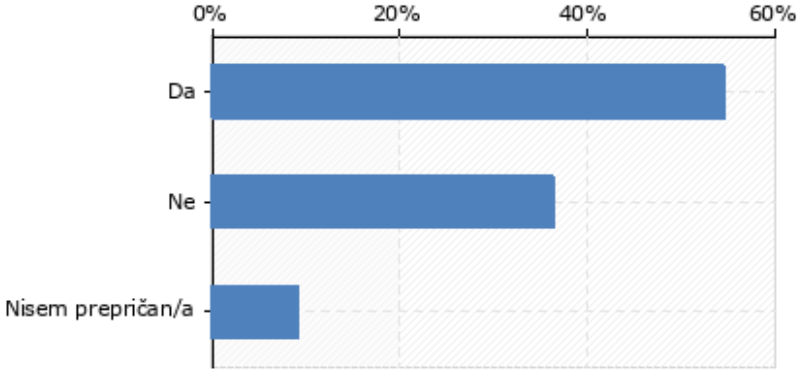
(b) Rezultati drugega testiranja (n = 9)

Slika 36: Ste že igrali igro, ki uporablja tehnologijo blockchain?

Vprašanje 9 na sliki 36 je pokazalo, da ni nihče od udeležencev igral igre, ki bi delovala preko blockchaina. Vedeti je potrebno, da so bile igre z blockchainom v času pisanja tega dela relativna redkost. Problemi za izdelavo teh iger so bili nekajkrat našteti v tem magistrskem delu, ki pa so bili očitno tako pogosti, da ni noben izmed udeležencev sploh poskusil igrati take igre. Pri tem se je treba spomniti, da jih je bilo kar nekaj zelo dobro seznanjenih z blockchainom. V nadaljevanju bomo videli, ali bi uporabniki bili pripravljeni igrati igro, temelječo na blockchainu, če bi delovala na tak način, kot deluje igra s testiranja.



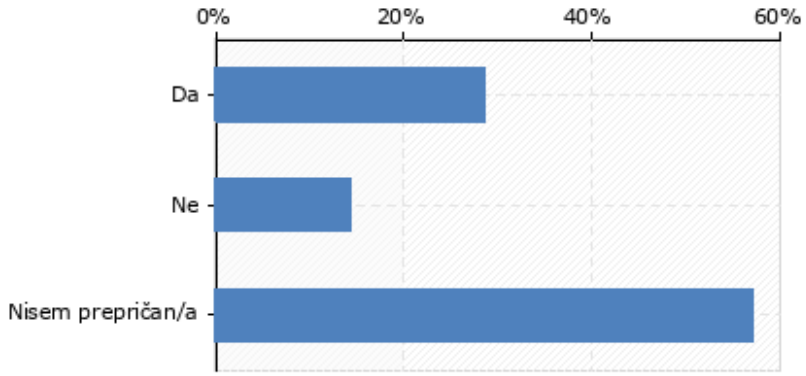
(a) Rezultati prvega testiranja (n = 7)



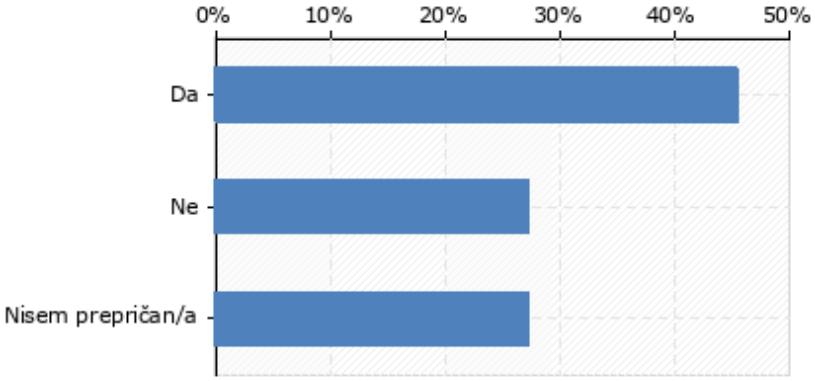
(b) Rezultati drugega testiranja (n = 11)

Slika 37: Ali ste opazili, da je bila izmenjava dobrin v igri na testiranju omogočena preko tehnologije blockchain?

Na tem mestu se začnejo vprašanja, ki zadevajo kakovost izdelave igre, uporabnikovo izkušnjo iz testiranja in kako dobro je bila implementirana izmenjava dobrin med igralci. Na sliki 37 je prikazano vprašanje, ali so uporabniki med testiranjem ugotovili, da je izmenjava dobrin delovala na blockchainu. Na prvem testiranju večina ljudi bodisi ni ugotovila bodisi ni bila prepričana. Trije uporabniki so to ugotovili, najverjetneje zaradi denarnice Enjin Wallet, ki so jo morali namestiti na telefon – denarnica je namenjena izključno za delovanje s kriptovalutami. Na drugemu testiranju so vsi, ki so bili na prvem testiranju, vedeli, kaj stoji za izmenjavo dobrin, saj so to izvedeli iz ankete, ki so jo rešili na prvem testiranju. Samo eden izmed novih uporabnikov je ugotovil, da se za izmenjavo dobrin uporablja blockchain, vsi ostali tega niso uvideli ali niso bili prepričani. Iz tega je mogoče sklepati, da je bilo maskiranje blockchaina v ozadju boljše na drugem testiranju, dodatno pa bi se to dalo izboljšati, če bi se uporabljala druga digitalna denarnica namesto Enjin Wallet za potrjevanje transakcij.



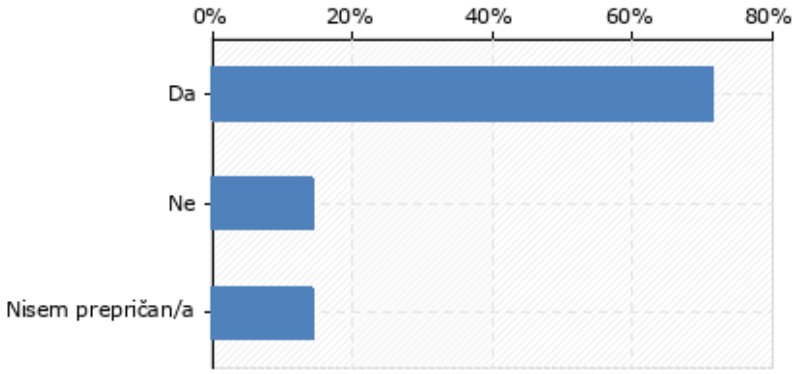
(a) Rezultati prvega testiranja (n = 7)



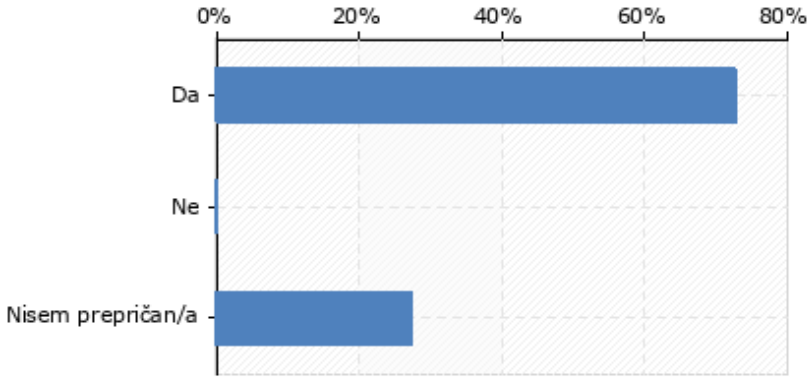
(b) Rezultati drugega testiranja (n = 11)

Slika 38: Ali je bila vaša izkušnja primerljiva z izkušnjami trgovanja pri drugih igrah?

Vprašanje 11 na sliki 38 je neposredno vprašalo po uporabniški izkušnji izmenjave dobrin iz testiranja – ki temelji na blockchainu. Blockchain prinaša kar nekaj slabosti v primerjavi z ostalimi poznanimi tehnologijami. Na prvem testiranju igralci niso bili preveč navdušeni z delovanjem blockchaina, saj sta samo dva vprašana podala mnenje, da se jim zdi izkušnja primerljiva. Vsi ostali bodisi niso bili prepričani, bodisi niso bili zadovoljni z blockchainom. Na drugem testiranju so bili rezultati optimistični, saj je skoraj polovica udeležencev menila, da je blockchain v trenutni fazi primerljiv z ostalimi tehnologijami. Skoraj 30 % udeležencev meni, da blockchain v trenutni fazi ni primerljiv, prav toliko jih ni popolnoma prepričanih. Drugo testiranje je tako dalo pobudo, da se mogoče da narediti izmenjavo dobrin na blockchainu celo tako dobro, kot to ponujajo manj varne tehnologije, ki imajo posledično hitrejše in bolj odzivne uporabniške vmesnike.



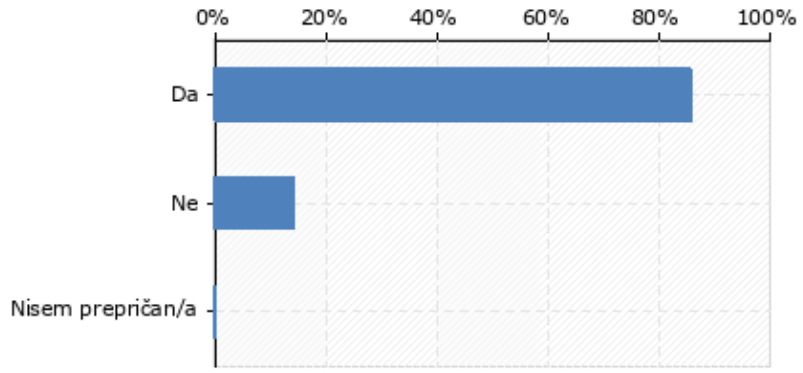
(a) Rezultati prvega testiranja (n = 7)



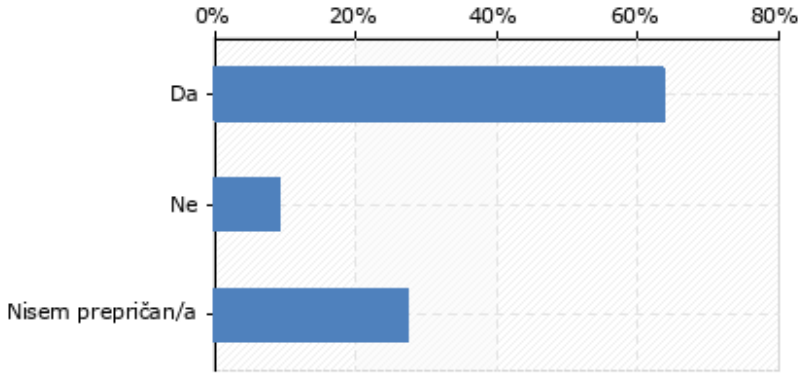
(b) Rezultati drugega testiranja (n = 11)

Slika 39: Ali menite, da dodatno potrjevanje na digitalni denarnici poveča varnost vaše digitalne lastnine?

Naslednje vprašanje je uporabnike spraševalo po njihovem mnenju ali lahko dodaten korak, ki ga morajo izvesti v digitalni denarnici pri izmenjavi dobrin, poveča varnost njihove digitalne lastnine. Rezultati na sliki 39 prikazujejo, da je na obeh testiranjih okoli 75 % vprašanih menilo, da ta korak izboljša njihovo varnost. Samo na prvem testiranju je ena oseba menila, da ta korak ne pripomore nič k povečavi varnosti njihove digitalne lastnine, vsi ostali niso bili prepričani. Iz tega se da sklepati, da če je uporabnik prisiljen zavarovati digitalne dobrine na telefonu z dodatnim geslom, ima občutek večje varnosti. To je tudi optimističen rezultat, saj pove, da so uporabniki odprti do ideje, da se lahko varnost njihove digitalne lastnine poveča. Videti je, da verjamejo, da brez tega koraka varnost njihovih dobrin ni popolna.



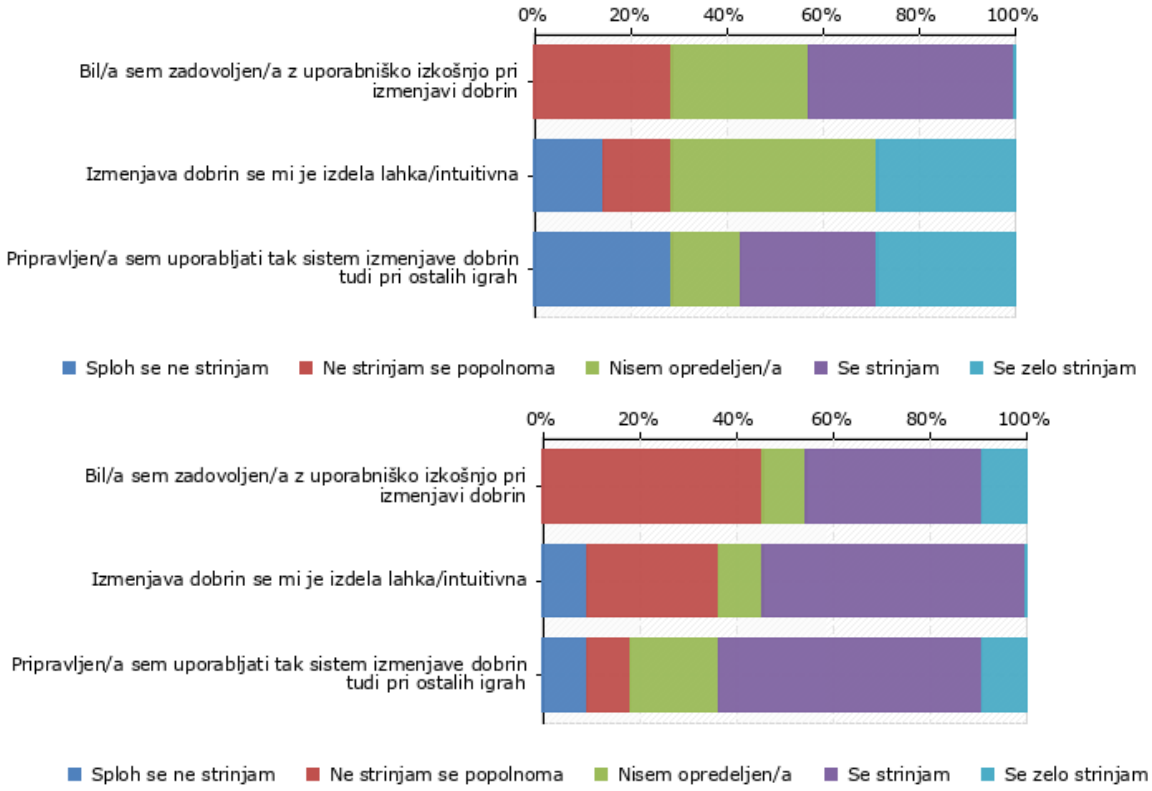
(a) Rezultati prvega testiranja (n = 7)



(b) Rezultati drugega testiranja (n = 11)

Slika 40: Ali bi bili pripravljeni opraviti korak potrjevanja na vaši denarnici, če bi bili prepričani, da to poveča varnost vaše digitalne lastnine?

Vprašanje, predstavljeno na sliki 40, prikazuje, ali bi bili uporabniki pripravljeni storiti dodatni korak potrjevanja v njihovi denarnici, če bi bili prepričani, da to poveča varnost njihovih dobrin. Kot je bilo razvidno iz prejšnjega vprašanja, je večina ljudi prepričana, da dodaten korak poveča njihovo varnost, zato je mogoče na to vprašanje gledati samo kot na potrditev, ali bi uporabniki bili pripravljeni narediti korak potrjevanja ali ne. Vidimo, da je bilo na prvem testiranju ta korak pripravljeno narediti več kot 80 % vprašanih, samo ena oseba ne bi bila pripravljena. Na drugem testiranju je bilo več kot 60 % vprašanih pripravljeno narediti tak korak, okoli 30 % ni bilo prepričanih, spet ena oseba tega koraka ne bi bila pripravljena narediti. Tudi ti rezultati so spodbudni, saj nakazujejo, da trenutna implementacija izmenjave dobrin navdušuje uporabnike in bi bili tak sistem pripravljeni uporabljati tudi pri ostalih igrah.



Slika 41: Rezultati vprašanja 14 in njegovih podvprašanj iz prve ankete (zgoraj) in iz druge ankete (spodaj)

Vprašanje 14, ki je sestavljeno iz treh podvprašanj, je predstavljeno na sliki 41. Razvidno je, da je bilo na obeh testiranjih približno 40 % ljudi zadovoljnih z uporabniško izkušnjo pri izmenjavi dobrin. Na prvem testiranju jih je bilo nekoliko več neopredeljenih, saj nekateri sploh niso uporabljali te funkcije, medtem ko so jo na drugem testiranju uporabljali vsi.

Drugo podvprašanje je veliko bolje prikazalo napredek pri iterativnem razvoju sistema za izmenjavo dobrin. Na prvem testiranju se je približno 30 % udeležencev strinjalo, da je izmenjava dobrin intuitivna. Na drugem testiranju se je s to trditvijo strinjalo skoraj 60 % vprašanih. Pri drugem testiranju se je zmanjšal tudi delež udeležencev, ki se sploh ni strinjal s trditvijo, da je trgovanje intuitivno.

Tretje podvprašanje je prikazalo optimistične rezultate, saj se je na prvem testiranju več kot 50 % udeležencev strinjalo s trditvijo, da bi takšen način izmenjevanja dobrin bilo pripravljeno uporabljati pri ostalih igrah, medtem ko 30 % udeležencev sploh ne bi bilo pripravljenih uporabljati takega sistema v ostalih igrah. Po drugem testiranju se je delež popolnoma nezadovoljnih ljudi zmanjšal iz 30 % na manj kot 10 %. Iz 50 % na 60 % se je povečalo tudi število udeležencev, ki so se strinjali s trditvijo, da bi bili pripravljeni uporabljati ta sistem pri ostalih igrah.

7.3.5 Analiza rezultatov

Iz ankete je bilo razvidno, da prvi sistem ni popolnoma navdušil uporabnikov, vendar je drugi sistem popravil veliko napak in je bil uporabnikom všečen. Uporabniki bi bili celo pripravljeni sodelovati s takim sistemom tudi pri ostalih igrah. Na tem mestu se je potrebno spomniti, da ta sistem omogoča veliko več varnosti od ostalih trenutno obstoječih sistemov, a ima nekaj pomembnih slabosti. Najtežje prehodna ovira je to, da mora sistem čakati med 5 in 15 sekund po vsaki transakciji, da se transakcija vpiše na blok in s tem blockchain potrdi transakcijo. Pri navadnih sistemih to seveda ni potrebno in lahko traja ta operacija manj kot sekundo. Uporabnikom ni nikoli všeč čakati 15 sekund pred praznim zaslonom, da dobijo novo dobrino, zato je potrebno ta proces ustrezno zamaskirati ali ponuditi uporabniku možnost, da v tem času v igri počne nekaj drugega.

Rezultati iz testiranja so pokazali, da lahko z omogočeno izmenjavo dobrin igralci izdelajo boljše kupčke in s tem pridejo tudi dlje v igri. Iz rezultatov je bilo razvidno, da je na prvem testiranju v petih urah uspelo samo dvema uporabnikoma preseči mejo 100 točk (najboljši uporabnik je imel na koncu 160 točk). Z omogočeno izmenjavo dobrin med igralci so uporabniki na drugem testiranju v zgolj štirih urah presegli mejo 300 točk (najboljši uporabnik je imel 320 točk, kar je dvakrat več kot prej). Na drugem testiranju je kar sedmim uporabnikom uspelo preseči mejo 100 točk. Iz tega je mogoče sklepati, da izmenjava dobrin dobro deluje na lažje in učinkovitejše igranje igre.

V rezultatih ni bila izpolnjena predpostavka, da bi uporabniki, ki so več trgovali, bili uspešnejši v igranju igre. Videti je bilo, da so najboljši igralci vsaj nekaj trgovali, a so bili večinoma zasedeni z igranjem igre in se niso toliko posvečali menjavi kart. Nekateri drugi igralci so se odločili posvečati pozornost izmenjavi kart namesto igranju igre in so s tem pridobili ogromno zlatnikov. Eden izmed uporabnikov je samo z izmenjavo kart zbral toliko zlatnikov kot dva najboljša igralca z igranjem igre skupaj. Videti je, da se v igri oblikujejo različne skupine igralcev, ki imajo različne cilje, četudi to niso tisti, ki so prikazani na lestvici najboljših. Seveda je pri igrah najbolj pomembno to, da se uporabniki zabavajo.

Pri rezultatih je potrebno znova poudariti, da je celoten blockchain v začetni, razvijajoči se fazi. Blockchain prinaša velik potencial, ki bi lahko prinesel revolucionarni napredek pri varnostni digitalne izmenjave dobrin, a trenutno prinaša preveč nepremostljivih ovir. Blockchain prinaša veliko varnost dobrin, neodvisnost od centralnih ustanov in regularnost tržišča. Po drugi strani je potrebno premostiti njegove slabosti, kot so počasnost transakcij, kjer lahko ena transakcija zahteva več 10 sekund za potrditev, nekoliko zahtevnejšo uporabo za navadnega uporabnika in nizko omejitev števila transakcij na časovno enoto. Orodja, ki so bila uporabljena v tem delu, so tudi nova, v času implementacije tega dela so bila stara komaj par mesecev. Vse to vpliva na uporabniško izkušnjo, tako da postane pomembno to, da prepričamo uporabnika, da sta dodatni čas in težavnost trgovanja vredna dodatne varnosti za njegovo digitalno lastnino. Cilj je seveda zgraditi tako dober vmesnik, da uporabnik sploh ne bi zaznal omejitev blockchaina, a trenutna najboljša orodja tega še ne omogočajo.

8 Zaključek

V tem magistrskem delu je bila prikazana zgodovina razvoja igralnih pogonov in blockchaina. Vse to je bralcu predstavilo trenutno stanje blockchaina in različnih blockchain platform. Predstavljene so bile njihove prednosti in omejitve. Poudarjene so bile razlike med trenutno najbolj uporabljanimi blockchain platformami.

Predstavljena je bila tudi igra, ki je bila izdelana v sklopu tega dela in omogoča izmenjavo digitalnih dobrin med igralci preko blockchaina. Ker ima blockchain veliko omejitev in nezaželenih lastnosti, je bilo prikazano, kako se skuša te nezaželene lastnosti skriti pred uporabnikom, da se mu omogoči čim bolj prijazno in intuitivno uporabniško izkušnjo.

Igralci te igre lahko dobrine med sabo neposredno izmenjujejo, brez kakršnih koli omejitev. Igra je bila v nekem smislu maska, ki je skrivala sistem izmenjave dobrin v ozadju. Igra je zamotila igralce in jim dala razlog, da morajo med sabo izmenjevati dobrine, da bodo lahko postali močnejši. S tem so igralci uporabljali sistem za izmenjavo dobrin in ga jemali kot nekaj intuitivnega, kot del igre. Vsaka interakcija s sistemom je bila zabeležena, kasneje pa analizirana ter predstavljena v razdelku 7.

Izvedeni sta bili dve javni testiranji na Fakulteti za matematiko, naravoslovje in informacijske tehnologije v Kopru. Na teh dveh testiranjih se je zbralo 7 in 11 udeležencev, ki so preizkušali sistem 4 do 5 ur. Na koncu so podali mnenje v obliki izpolnjevanja ankete. Anketa je bila analizirana skupaj s podatki o njihovi interakciji s sistemom.

Z analizo je bilo potrjeno, da so uporabniki dosegali boljše rezultate, če se je izvajalo izmenjevanje dobrin med igralci. Povečala se je tudi všečnost igranja igre. V anketi je bilo razvidno, da je bil sistem lahek in intuitiven za uporabo, a za ta sistem obstajajo tudi izboljšave. Veliko igralcev je dejalo, da so pripravljeni tudi v prihodnosti uporabljati ta sistem, kar pomeni, da ta sistem poleg povečanja varnosti ponuja tudi dovolj dobro uporabniško izkušnjo, da bi ga uporabniki uporabljali v ostalih igrah.

Skozi opis razvoja in implementacije programa in nato skozi pregled rezultatov anket in testiranja so bili predstavljeni problemi in omejitve tehnologije blockchain. Predstavljene probleme, na primer povečan čas transakcij, je potrebno v uporabniškem vmesniku skriti pred uporabnikom, da bi mu omogočili boljšo uporabniško izkušnjo. A ker je celotna tehnologija v zgodnji fazi razvoja, ni mogoče narediti vmesnika, ki bi deloval tako učinkovito in hitro kot ostale centralizirane tehnologije.

V nadaljevanju izvedenega dela bodo preučevane naslednje nadgradnje sistema:

1. Uporaba alternativ za digitalne Enjin denarnice, kjer ni potrebno sprotno potrjevanje v denarnici.

2. Asinhrono čakanje na rezultat iz blockchaina na strežniku namesto na instanci uporabnikove igre – preprečiti je potrebno, da bi se dobrine izgubile, če bi uporabnik zaprl igro.

3. Shranjevanje podatkov o uporabniku v oblaku, kar bi uporabniku omogočalo igranje preko več naprav in toleranco v primeru izbrisa igre iz naprave.

4. Omogočanje več različnih možnosti v igri medtem ko uporabniki čakajo na odgovor iz blockchaina.

5. Komunikacija sistema z blockchaina preko strežnika namesto iz instance igre za povečanje varnosti.

Poleg izboljšave izmenjave dobrin bo nadaljnje delo obsegalo tudi dokončanje igre. Izvedenih bo več javnih testiranj na fakulteti FAMNIT, kjer se bo iterativno spremljal napredek igre v relaciji z zadnjo verzijo, nove verzije pa se bodo popravljale in dopolnjevale skladno s predlogi uporabnikov, ki bodo sodelovali pri testiranjih.

Literatura in viri

[1] A. M. Antonopoulos. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, dec 2014.

[2] B. Asolo. What is sha-256 and how is it related to bitcoin? *MYCRYPTOPEDIA*, 11 2018.

[3] S. Axon. Unity at 10: For better—or worse—game development has never been easier. *ArsTechnica*, 09 2016.

[4] Z. Ayesh. Blockchain consensus algorithms: What are their properties? *Medium*, 05 2019.

[5] A. Back. Hash cash postage implementation. 05 1997.

[6] A. Back. Bitcoin: The cryptoanarchists' answer to cash. 09 2002.

[7] BitcoinWiki. Erc-721 examples. https://en.bitcoinwiki.org/wiki/ERC-721. Accessed: 28.1.2020.

[8] Brenn. Noobs guide to understanding erc-20 vs erc-721 tokens. 3 2018.

[9] V. Buterin. Slasher ghost, and other developments in proof of stake. 10 2014.

[10] CoinMarketCap. Coinmarketcap. https://coinmarketcap.com/currencies/enjincoin/. Accessed: 28.1.2020.

[11] B. Curran. What is defi? understanding the decentralized finance landscape. 10 2019.

[12] C. Dannen. *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners*. Apress, mar 2017.

[13] Digiconomist. Bitcoin energy consumption index. *Digiconomist*, 03 2020.

[14] Y. Jardi in M. Araoz E. Ordano, A. Meilich. A blockchain-based virtual world. *Decentraland*.

[15] Enjin. Enjin whitepaper. https://www.cryptoground.com/storage/files/1527489134_enjincoin_w
Accessed: 28.1.2020.

[16] W. Entriken. Eip, 08 2019.

[17] P. Franco. *Understanding Bitcoin: Cryptography, Engineering and Economics (The Wiley Finance Series)*. Wiley, nov 2014.

[18] B. Grady. *The Unified Modeling Language User Guide (2nd Edition)*. Addison-Wesley Professional, may 2005.

[19] J. Gregory. *Game Engine Architecture*. A K Peters/CRC Press, aug 2014.

[20] N. Hampton. Understanding the blockchain hype: Why much of it is nothing more than snake oil and spin. 09 2016.

[21] A. Hertig. How do ethereum smart contracts work, 2018.

[22] P. Stafford in H. Murphy. Has the blockchain hype finally peaked. *Financial Times*, 29, 2016.

[23] C. Dwork in M. Naor. *Pricing via Processing or Combatting Junk Mail*, page 139–147. Springer Berlin Heidelberg.

[24] Evans in M. Tonya. Cryptokitties, cryptography, and copyright. *AIPLA QUARTERLY JOURNAL*, 47(2):219, 2019.

[25] S. Gilbert in N. Lynch. Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. *Acm Sigact News*, 33(2):51–59, 2002.

[26] V. Buterin in ostali. Ethereum white paper: a next generation smart contract & decentralized application platform. *First version*, 53, 2014.

[27] C. Bendiksen in S. Gibbons. The bitcoin mining network: - trends, composition, average creation cost, electricity consumption & sources.

[28] M. Tremaine in T. Teorey. Cost/benefit analysis for incorporating human factors in the software lifecycle. *Commun. ACM*, 31:428–439, 04 1988.

[29] W. Penard in T. van Werkhoven. On the secure hash algorithm family. *Cryptography in Context*, pages 1–18, 2008.

[30] P. Mishra in U. Shrawankar. Comparison between famous game engines and eminent games. *International Journal of Interactive Multimedia & Artificial Intelligence*, 4(1), 2016.

[31] J. Poon in V. Buterin. Plasma: Scalable autonomous smart contra. *plasma.io*, 08 2017.

[32] U. Irfan. Bitcoin is an energy hog. where is all that electricity coming from? 6 2019.

[33] J. Obregon in J. Stubbendick J. Harm. Ethereum vs. bitcoin.

[34] A. Well in R. F. Lorch J. L. Myers. *Research design and statistical analysis*. Routledge, 2010.

[35] D. Kajpust. Is defi ethereums killer app? 10 2019.

[36] T. Whitted M. Finch in M. Shantz L. Bishop, D. Eberly. Designing a pc game engine. *IEEE Computer Graphics and Applications*, 18(1):46–53, 1998.

[37] P. Lewis. Nixon's economic policies return to haunt the gop. *New York Times*, 1976.

[38] Loom. Loom network. https://loomx.io/. Accessed: 28.1.2020.

[39] B. Marr. How blockchain will transform the supply chain and logistics industry. 03 2018.

[40] B. Marr. Enjin is creating a real-life ready player one, and it's powered by blockchain. 04 2019.

[41] A. J. Menezes. *Handbook of Applied Cryptography (Discrete Mathematics and Its Applications)*. CRC Press, dec 1996.

[42] M. R. Mergulhão. How to build a car manufacturing supply chain system using ethereum. 02 2019.

[43] M. Bartoletti in T. Cimoli N. Atzei. A survey of attacks on ethereum smart contracts. *IACR Cryptology ePrint archive*, 2016:1007, 2016.

[44] S. Goon in A. Bhattacharya P. P. Sarathi. History and comparative study of modern game engines. *International Journal of Advanced Computer and Mathematical Sciences*, 3:245–249, 2012.

[45] K. Pearson. Proceedings of the royal society of london-royal society (great britain)-google books. *Notes on regression and inheritance in the case of two parents*, pages 240–242, 1895.

[46] C. Mulligan A. Brown in B. Kewell R. Maull, P. Godsiff. Distributed ledger technology: Applications and implications. *Strategic Change*, 26(5):481–489, Sep 2017.

[47] S. Ray. Distributed ledger technology: Applications and implications. 02 2018.

[48] N. Reiff. What is erc-20 and what does it mean for ethereum? 6 2019.

[49] M. Rouse. Iot analytics guide: Understanding internet of things data.

[50] N. Satoshi. Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot, 2019.

[51] R. Schollmeier. A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. pages 101 – 102, 09 2001.

[52] D. Shirley. What is erc-721? http://erc721.org/. Accessed: 28.1.2020.

[53] Smartz. How blockchain and smart contracts can impact iot. 08 2018.

[54] UML Superstructure Specification. Omg unified modeling languagetm (omg uml), superstructure. *OMG Object Management Group*, 08 2011.

[55] W. Stallings. *Cryptography and Network Security: Principles and Practice (2nd Edition)*. Prentice Hall, jun 1998.

[56] N. Szabo. Bit gold. 12 2008.

[57] N. Szabo. Blockchains: The great chain of being sure about things. 10 2015.

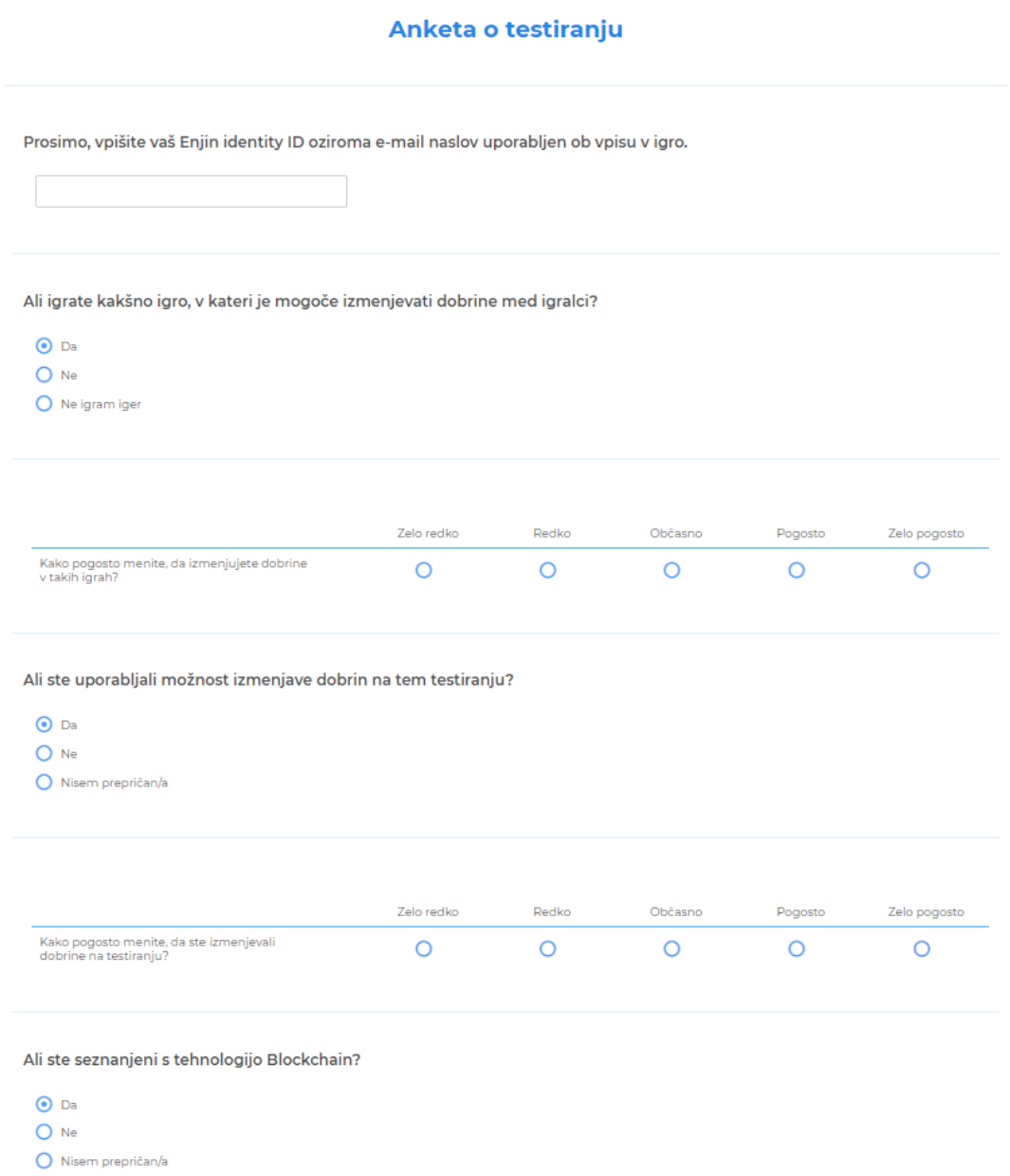
[58] D. Tapscott. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Portfolio, 05 2016.

[59] FunFair Technologies. Blockchain solutions for gaming: Commercial whitepaper v2.0 draft. *FunFairTechnologies*, 09 2018.

[60] F. Vogelsteller. Erc: Token standard. 11 2015.

Priloge

A Prva stran ankete



Anketa o testiranju

Prosimo, vpišite vaš Enjin identity ID oziroma e-mail naslov uporabljen ob vpisu v igro.

Ali igrate kakšno igro, v kateri je mogoče izmenjevati dobrine med igralci?

- Da
- Ne
- Ne igram iger

	Zelo redko	Redko	Občasno	Pogosto	Zelo pogosto
Kako pogosto menite, da izmenjujete dobrine v takih igrah?					

Ali ste uporabljali možnost izmenjave dobrin na tem testiranju?

- Da
- Ne
- Nisem prepričan/a

	Zelo redko	Redko	Občasno	Pogosto	Zelo pogosto
Kako pogosto menite, da ste izmenjevali dobrine na testiranju?					

Ali ste seznanjeni s tehnologijo Blockchain?

- Da
- Ne
- Nisem prepričan/a

B Druga stran ankete

Izmenjava dobrin je na tem testiranju potekala preko tehnologije Blockchain. Ali smatrate to tehnologijo kot bolj varno od do sedaj uporabljanih?

- Da
- Ne
- Nisem prepričan/a

	Zelo slabo	Slabo	Srednje	Dobro	Odlično
Kako dobro ste seznanjeni s pametnimi pogodbami?	○	○	○	○	○

Ste že igrali igro, ki uporablja tehnologijo Blockchain?

- Da
- Ne
- Nisem prepričan/a

Ali ste opazili, da je bila izmenjava dobrin v igri na testiranju omogočena preko tehnologije Blockchain?

- Da
- Ne
- Nisem prepričan/a

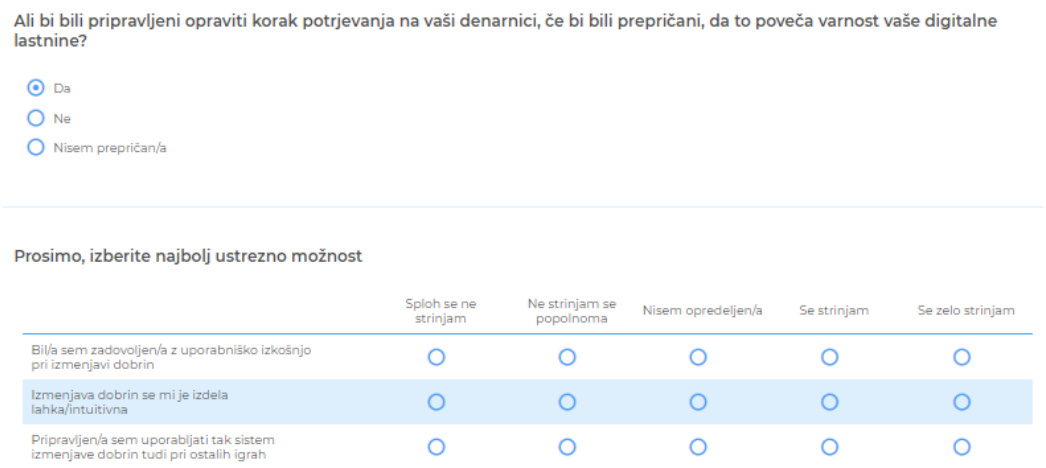
Ali je bila vaša izkušnja primerljiva z izkušnjami trgovanja pri drugih igrah?

- Da
- Ne
- Nisem prepričan/a

Ali menite, da dodatno potrjevanje na digitalni denarnici poveča varnost vaše digitalne lastnine?

- Da
- Ne
- Nisem prepričan/a

C Tretja stran ankete



Ali bi bili pripravljeni opraviti korak potrjevanja na vaši denarnici, če bi bili prepričani, da to poveča varnost vaše digitalne lastnine?

- (•) Da
- ( ) Ne
- ( ) Nisem prepričan/a

Prosimo, izberite najbolj ustrezno možnost

	Sploh se ne strinjam	Ne strinjam se popolnoma	Nisem opredeljen/a	Se strinjam	Se zelo strinjam
Bil/a sem zadovoljen/a z uporabniško izkošnjo pri izmenjavi dobrin	○	○	○	○	○
Izmenjava dobrin se mi je izdela lahka/intuitivna	○	○	○	○	○
Pripravljen/a sem uporabljati tak sistem izmenjave dobrin tudi pri ostalih igrah	○	○	○	○	○