Studentska iskaznica u lancu

Marinčić, Juraj

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Sveučilišni studij

STUDENTSKA ISKAZNICA U LANCU

Završni rad

Juraj Marinčić

Osijek, 2022.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

Obrazac Z1P - Obrazac za ocjenu završnog rada na preddiplomskom sveučilišnom studiju

Osijek, 19.09.2022.

Odboru za završne i diplomske ispite

Prijedlog ocjene završnog rada na preddiplomskom sveučilišnom studiju

Ime i prezime Pristupnika:	Juraj Marinčić
Studij, smjer:	Preddiplomski sveučilišni studij Računarstvo
Mat. br. Pristupnika, godina upisa:	R 4395, 22.07.2019.
OIB Pristupnika:	09087835449
Mentor:	Izv. prof. dr. sc. Mirko Köhler
Sumentor:	Miljenko Švarcmajer, mag. ing. comp.
Sumentor iz tvrtke:	
Naslov završnog rada:	Studentska iskaznica u lancu
Znanstvena grana rada:	**Informacijski sustavi (zn. polje računarstvo)**
Zadatak završnog rad:	Zauzeto za Juraj Marinčić. Zadatak završnog rada je istražiti i ponuditi rješenja za vođenje studentskih iskaznica (iksica) pomoću blockchain tehnologije. Potrebno je navesti sve aktivnosti u kojima se koristi studenska iskaznica i napraviti model kako ih spremiti u lanac. Usporediti postojeće blockchainove i ponuditi najbolje rješenje. Navesti prednosti i nedostatke ovakvog sustava.
Prijedlog ocjene završnog rada:	Dobar (3)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 2 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 1 bod/boda Jasnoća pismenog izražavanja: 2 bod/boda Razina samostalnosti: 2 razina
Datum prijedloga ocjene od strane mentora:	19.09.2022.
Datum potvrde ocjene od strane Odbora:	21.09.2022.

Potvrda mentora o predaji konačne verzije rada:	Mentor elektronički potpisao predaju konačne verzije.
	Datum:

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O ORIGINALNOSTI RADA

Osijek, 30.09.2022.

Ime i prezime studenta:	Juraj Marinčić
Studij:	Preddiplomski sveučilišni studij Računarstvo
Mat. br. studenta, godina upisa:	R 4395, 22.07.2019.
Turnitin podudaranje [%]:	3

Ovom izjavom izjavljujem da je rad pod nazivom**: Studentska iskaznica u lancu**

izrađen pod vodstvom mentora Izv. prof. dr. sc. Mirko Köhler

i sumentora Miljenko Švarcmajer, mag. ing. comp.

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

SADRŽAJ

1. UVOD

U današnje vrijeme, pojmovi kriptovalute i *blockchain* se mogu čuti sve češće te je njihova primjena u svakodnevnom životu sve raširenija. Suprotno mišljenju velikog dijela populacije, kriptovalute se mogu koristiti za plaćanje fizičkih dobara konverzijom kriptovalute te plaćanjem fiat valutom ili direktnim plaćanjem kriptovalutama. Cilj rada je predstaviti hipotetski model studentske iskaznice implementirane pomoću tehnologije ulančavanja. Budući da se model još uvijek ne može realizirati, u cilju je prikazati pretpostavku predviđenog načina rada te odabrati najekonomičniji lanac/valutu za potrebe studentske iskaznice. Kroz rad je pojašnjena trenutna situacija plaćanja kriptovalutama te razlika između direktnog i indirektnog plaćanja istima. Također je objašnjena, na primjeru hardver novčanika, tehnologija prijenosa kriptovaluta na hladni novčanik te potencijalna primjena sličnog principa na zadani problem. Većina lanaca ima svoj *native* token/valutu tj. token stvoren isključivo za potrebe tog lanca/ekosustava. Zbog lake promjenjivosti cijena tih tokena pojašnjeno je što su to stabilne valute, njihove specifičnosti te zašto je i koja valuta optimalan izbor za rješenje. U daljnjem je opisana općenita struktura lanca i njegovi varirajući načini rada, kako bi se dao uvid u to zašto su određeni lanci bolji od drugih u specifičnim situacijama te kako bi se lakše ostvario izbor „idealnog“ lanca. Zatim je pregledom najpopularnijih i najkorištenijih lanaca izabrano najefikasnije rješenje od ponuđenih s obzirom na način rada i specifikacije. Naposlijetku je predložena ideja fizičke implementacije rješenja te “idealno“ rješenje u smislu odabira optimalnog lanca i valute.

1.1. Zadatak završnog rada

Zadatak završnog rada je istražiti i ponuditi rješenja za vođenje studentskih iskaznica (iksica) pomoću tehnologije ulančavanja. Potrebno je navesti aktivnosti u kojima se koristi studenska iskaznica i napraviti model kako ih spremiti u lanac. Usporediti postojeće lance i ponuditi najbolje rješenje. Navesti prednosti i nedostatke ovakvog sustava.

2. PREGLED PODRUČJA

Plaćanje kriptovalutama u svakodnevnom životu omogućeno je pomoću dva rješenja. Plaćati se može debitnim karticama gdje mjenjačnice otkupljuju kriptovalute te isplaćuju iznos na karticu u fiat valuti. Druga mogućnost je direktno plaćanje kriptovalutama gdje se traženi iznos šalje na adresu primatelja pomoću QR *(engl. QR- Quick response)* koda. Direktna relacija između kriptovaluta i kartica još nije omogućena jer je to trenutno nedovoljno istraženo i ne pronalazi traženi interes kod ulagača. Najbliža poveznica su hladni novčanici kao što su „Ledger“ i „Trezor“ gdje se valute uspješno pohranjuju na hardver. Unatoč tome, neka sveučilišta i znanstvene ustanove koriste tehnologiju ulančavanja kako bi studentima dodijelili digitalne certifikate o završenom stupnju obrazovanja [1].

2.1. Kartično poslovanje

Kartično poslovanje kriptovalutama se trenutno odvija indirektno te je nemoguće smjestiti valutu na karticu koja nije nikako povezana s lancem gdje se sama valuta nalazi. Globalno popularne mjenjačnice kao što su Binance i Crypto.com obilaze taj problem te izdaju vlastite debitne kartice [2] [3] u suradnji s Visom. Konverzija se odvija na način da se valute prodaju mjenjačnici te se na račun isplati fiat vrijednost u vrijednosti prodane valute koja se nadalje može, a i ne mora, ovisno o korisniku proslijediti na karticu. Te kartice se mogu koristiti na većini prodajnih mjesta i bankomata, ali još uvijek nisu 100% globalno prihvaćene.

2.2. Direktno plaćanje kriptovalutama

Direktno plaćanje kriptovalutama odvija se pomoću QR koda gdje je korisniku potreban uređaj koji podržava kripto novčanik te može očitavati QR kodove. Proces se odvija na taj način gdje vršitelj usluge QR kodu unaprijed dodijeli novčanu vrijednost te taj isti kod korisnik skenira. Nakon skeniranja, iz novčanika se uzima iznos valute kojom se plaća ekvivalentan cijeni upisanoj u QR kod. Najpoznatiji sustav ovakvog plaćanja je Binance Pay [4] kojeg je napravila najpoznatija i najkorištenija kripto mjenjačnica Binance. Sustav funkcionira pomoću QR koda, kako je i opisano, a broji 30 milijuna korisnika što je skoro 0.4% ljudske populacije. Brojke ovakve magnitude govore kako bi se globalna prilagodba kriptovalutama te i sama ideja studentske iskaznice na lancu mogla ostvariti u bližoj budućnosti.

2.3. Hladni novčanici

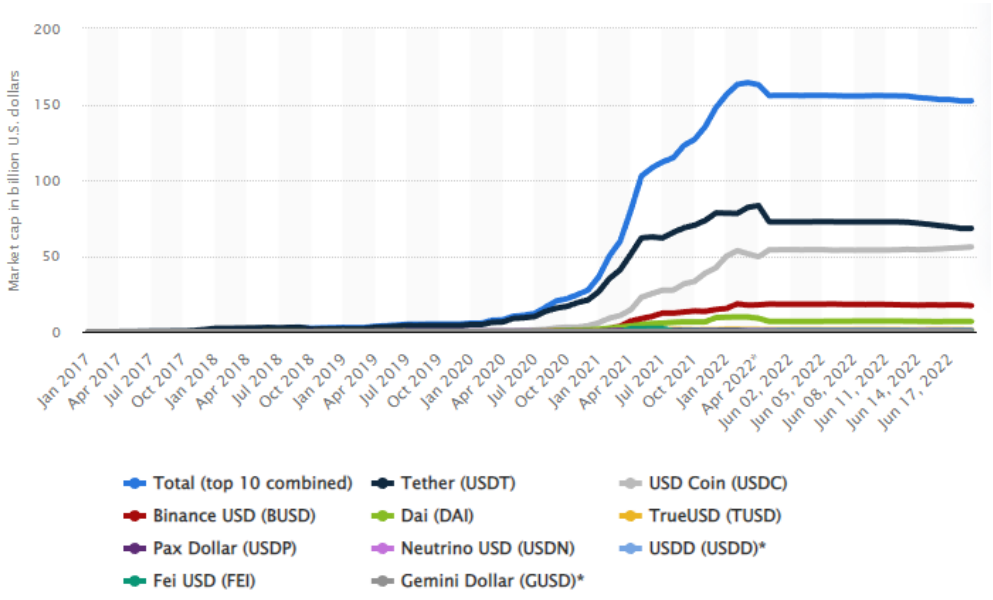
Hladni novčanici su uređaji koji pružaju najefikasniju moguću zaštitu sredstvima korisnika. Istovremeno mogu pohranjivati valute s više različitih lanaca što bi se u idealnoj situaciji trebalo očekivati i od predviđene studentske iskaznice. Sigurnost sredstava je iznimno važna za realizaciju rješenja. U slučaju slabije zaštite će sredstva koja se dijele kao subvencije te samim time i sredstva te države ili zajednice biti ugrožena i izložena hakerskim napadima. Slično kreditnim karticama, ključevima za auto i USB-ovima (*engl. USB– Universal serial bus*), u novčaniku se nalazi sklopovska pločica, mikrokontroler te sigurnosni modul gdje se nalazi tajni ključ. [5] Kriptovalute se zapravo ne nalaze u novčaniku nego ostaju na lancu, a novčanik služi sa pohranjivanje korisnikovog tajnog ključa kojim pristupa valutama. Sam novčanik nikad ne dolazi u doticaj s internetom te je imun na *malware* i *cyber* napade. Kada korisnik vrši transakciju on zapravo potpisuje posebnu poruku gdje potvrđuje da je on zaista vlasnik tog ključa što je nemoguće učiniti bez pristupa hladnom novčaniku. Osim u prethodno navedenom, sigurnost hladnog novčanika se očituje i u tome što je i sam novčanik dodatno zaštićen PIN-om *(engl. PIN- Personal identification number)* ili tajnim ključem, a u slučaju krađe ili gubitka novčanika, korisnik još uvijek može otključati svoja sredstva sa zaporkom koja se inače sastoji od 12 ili 24 nasumičnih riječi. [6] Tvrtka „Radar Relay“ je 2018. godine razvila softver koji omogućuje direktan prijenos sredstava s jednog hladnog novčanika na drugi. To dovodi do pitanja može li ta tehnologija evoluirati do toga da se s hladnog novčanika sredstva mogu prebacivati putem nečeg primjenjivog kao što su QR kodovi. Trenutni standardizirani hladni novčanici imaju USB nastavak te se moraju spojiti s uređajem tim putem kako bi se transakcije mogle vršiti. Budući da su današnji mobilni uređaji sposobni očitavati QR kodove pomoću kamera tehnološki pothvat implementacije navedenog u hladni novčanik ne bi trebao biti nemoguć pothvat. No problem leži u tome što trenutni novčanici pohranjuju samo privatni ključ, a ne same valute. Upravljanje valutama se odvija tek kada je novčanik povezan s uređajem što bi potpuno isključilo opciju QR koda prije nego što se riješi problem direktne pohrane valuta na novčanik ili u ovom slučaju iskaznice.

Sl. 2.1. Ledger Nano X, [7]

Iako su kompaktni i portabilni, građom odstupaju od normiranog oblika sredstava za plaćanje kao što su kreditne ili studentske kartice te se prilagodba takvom fizičkom obliku teško može očekivati u bližoj budućnosti. „Ledger Nano X“ je za sada estetski najprihvatljiviji kandidat te relativno blizu dizajna kojem se teži u slučaju studentske iskaznice. Sam uređaj je kompaktan te modernim izgledom može izazvati raširenu prilagodbu te biti socijalno prihvaćeniji unatoč normiranom izgledu današnjih iskaznica.

2.4. Stabilne valute

Stabilne su valute one kriptovalute kojima je svrha i cilj održavati 1:1 vrijednost prema određenoj fiat valuti ili u iznimnijim slučajevima sredstvima kao što je zlato i slično. One su idealan odabir za vršenje direktnih transakcija zbog marginalnih oscilacija u cijeni. Omjer 1:1 je nešto čemu sve stabilne valute teže i u pravilu bi ga trebale održavati, ali to nije uvijek istina te sama održivost ovisi i o vrsti stabilne valute te čime je podržana. Stabilne valute čine otprilike 20% cijelog kripto tržišnog udjela te su neizostavan dio trenutnog i budućeg poslovanja kriptovalutama. Osim toga što čine velik udio cijelog tržišta, sama vrijednost u dolarima se povećala s dvadeset milijuna dolara u siječnju 2017. do sto pedeset milijardi dolara u srpnju 2022. što je prikazano na slici 2.2. gdje se vidi rast pojedinih valuta od kojih su četiri najveće fiat-podržane, a peta kripto-podržana.



Sl. 2.2. Tržišni udio stabilnih valuta od siječnja 2017. do srpnja 2022., [8]

2.4.1. Fiat-podržane stabilne valute

Fiat-podržane stabilne valute su najčešće podržane u zalihama gotovine, obveznicama ili blagajničkim zapisima kao što je slučaj s USD Coinom (USDC) (eng. USD- United States dollar). Ovaj tip stabilnih valuta je najrašireniji te zauzima najveći tržišni udio. Predstavljaju, trenutno, najsigurniju opciju pohranjivanja kriptovaluta u stabilne valute što se iskazalo u gotovo nikakvim oscilacijama u cijenu najvećih valuta kao što su Tether (USDT), USD Coin (USDC) i Binance USD (BUSD). Na slikama 2.3., 2.4. i 2.5. su prikazani grafovi kretanja cijene od začetka tih valuta pa do današnjeg doba. Može se iščitati kako je najveću negativnu oscilaciju osjetio Tether spustivši se do 0.9136 dolara u jednom trenutku što je 8.864% odstupanja od ciljane vrijednosti nasuprot valutama Binance USD i USD Coin koje su u najgorem slučaju osjetile 3% odstupanja. Unatoč ovim brojkama koje bi u implementaciji sustava plaćanja stvarale problem, Tether je uspješno stabilizirao valutu u roku od par tjedana, a BUSD i USDC u dva i jedan dan. Također je bitno naglasiti da su se BUSD i USDC susreli s tim problemom nedavnije 2020., a Tether 2017. kada su kriptovalute općenito bile nestabilnije i ne toliko utjecajne. No unatoč prijašnjim odskakanjima iz grafova se može zaključiti da su se sve tri valute nakon određeno vremena stabilizirale te sad već u konstanti od par godina broje maksimalne oscilacije u promilima ili u najgorem slučaju u desetinama postotka.

Sl. 2.3. Graf kretanja cijene USDC od rujna 2018. do rujna 2022., [9]

Sl. 2.4. Graf kretanja cijene BUSD od rujna 2019. do rujna 2022., [9]

Sl. 2.5. Graf kretanja cijene USDT od 2015. do rujna 2022., [9]

2.4.2. Kripto-podržane stabilne valute

Kripto-podržanim stabilnim valutama se cijena podržava drugim kripto valutama te se stabilizira prodajom istih kako bi se cijena obnovila ili zamjenom tih kriptovaluta za ekvivalent u stabilnoj valuti koja se podržava. Može se raditi o jednoj valuti kao što je naprimjer Bitcoin, a mogu biti podržane i s više raznih valuta. Najpoznatija ovakva valuta je Dai te predstavlja jedinu potencijalnu kripto-podržanu valutu za implementaciju rješenja s obzirom na tržišni udio, sigurnost i oscilacije u cijeni. Ona za kupnju zahtjeva polog od kriptovaluta u većoj vrijednosti nego što se vraća u Dai tokenu kako bi se spriječila novčana nepokrivenost u slučaju pada vrijednosti tih valuta. U suprotnom slučaju položene se valute mogu podići natrag za istu vrijednost u Dai tokenu. Iz grafa na slici 2.6. se da iščitati da je Dai postigao najveću negativnu oscilaciju odstupanjem od 3.52% početkom 2020. no krajem 2021. se događa još jedna „veća“ oscilacija od 1.22%. Iako se valuta u oba slučaja stabilizirala nakon jednog dana promjenjivost kripto tržišta je velika te je sama podrška istima upitna.

Sl. 2.6. Graf kretanja cijene DAI od studenog 2019. do rujna 2022., [9]

2.4.3. Stabilne valute podržane sredstvima

Stabilne valute podržane sredstvima mogu biti podržane ekvivalentom vrijednošću u dragocjenim metalima kao što su srebro i zlato, nafti, dijamantima ili nečemu kao što su nekretnine. Unatoč svim opcijama najkorištenija i najpoznatija stabilna valuta podržana sredstvom je PAX (*Pax standard token)* Gold koji ekvivalent svoje cijene mjeri prema cijeni zlata. Vidljivo na slici 2.7. njegova vrijednost u dolarima se mjeri u tisućama te bi ta valuta svakako bila nepogodna za rješavanje problema nečega kao što je studentska prehrana na državnoj razini s obzirom na oscilacije od čak 50%. Ostale stabilne valute podržane sredstvima su jako male, nesigurne ili pokrivene previše nepouzdanim sredstvima te ih se ni ne razmatra za ozbiljne kandidate.

Sl. 2.7. Graf kretanja cijene PAXG od lipnja 2019. do rujna 2022., [9]

2.4.4. Algoritmičke stabilne valute

Algoritmičke stabilne valute su podržane algoritmom koji „upravlja“ cijenom valute. Stabilizacija valute se u većini algoritama odvija na taj način da se u slučaju povećanja vrijednosti iznad ciljane, ukupan broj tokena smanji, a u slučaju pada vrijednosti poveća. Ovakve stabilne valute su izrazito nesigurne naspram ostalih tipova jer nisu pokrivene rezervama fiat valute te su izložene napadima putem tržišne manipulacije. Na slici 2.8. je prikazan graf cijene najpoznatije, a u prošlosti i najjače algoritmičke stabilne valute po tržišnom udjelu. Nekadašnja joj je vrijednost tržišne kapitulacije težila skoro deset milijardi dolara, a danas se srozala na niskih četiristo milijuna. U najnižem odstupanju vrijednost joj je bila čak manje od jednog centa naspram ciljane vrijednosti od jednog dolara. Algoritmičke valute nipošto ne dolaze u obzir za implementaciju rješenja zbog sklonosti prevelikim oscilacijama u cijeni i podložnosti potpunom krahu i tržišnoj manipulaciji cijene.

Sl. 2.8. Graf kretanja cijene UST od studenog 2020. do rujna 2022., [9]

2.4.5. Optimalni odabir stabilne valute

Optimalna valuta za traženo rješenje bi morala biti prvenstveno stabilna, sigurna te imati mogućnost vršiti transakcije na poznatijim to jest pouzdanijim lancima. S obzirom na već objašnjeno, najbolji izbor bi bila jedna od fiat-podržanih valuta uz svu sigurnost koju pružaju te minimalne oscilacije. Kripto-podržane stabilne valute bi bile drugi izbor pošto su se pokazale sigurnijim i preciznijim od preostala dva tipa. Unatoč tome sklonost promjeni kripto tržišta se ne smije izostaviti prilikom odabira te su one još uvijek nedovoljno sigurne da bi se iskoristile za naše rješenje. Ostala dva tipa ne dolaze u obzir zbog nezadovoljavajuće konstante u cijeni, a u slučaju algoritmičkih valuta zbog izloženosti tržišnoj manipulaciji te općenito ogromnim odskakanjima od ciljane vrijednosti. Od navedene tri najpoznatije tj. USDT, USDC i BUSD najbolji izbor predstavlja USDC zbog najmanjih oscilacija, raširenoj uporabi preko više različitih lanaca te najveća sigurnost i transparentnost o porijeklu imovine kojom je valuta podržana.

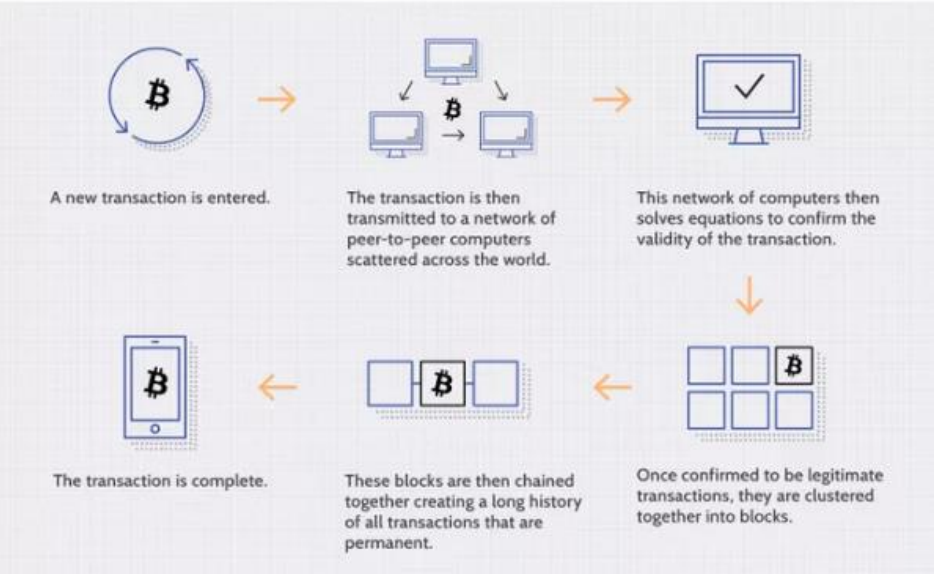
2.5. Studentski lanac

Tehnologija ulančavanja je dosegla izraženu popularnost tijekom proteklih godina te otvorila vrata za proširenje trenutnih tehnoloških i znanstvenih vidika. Samim time, prestižna sveučilišta kao što su MIT (*eng. MIT- Massachusetts Institute of Technology)*, Harvard, Oxford i Berkeley

nastoje konstantno aktualizirati svoje obrazovne programe, nude pohađanje kolegija vezanih za *blockchain* i Bitcoin. Američko sveučilište „Deloitte University“ održalo je natjecanje za *startup* tvrtke gdje je tvrtka koja je predložila ideju studentske iskaznice na lancu osvojila prvo mjesto. Sam model lanca i detaljnije specifikacije nisu objašnjene, no ono što se zna je da bi se implementacija iskaznice ostvarila pomoću mobilne aplikacije gdje bi student također imao vlastiti digitalni identitet[10]. Zasad još nijedno sveučilište nije razvilo svoj privatni lanac za vlastite potrebe. No s obzirom na kvalitetu sveučilišta koja su se osvrnula na te implementirala tehnologiju ulančavanja u svoje obrazovne programe, postoji mogućnost da će svako od tih sveučilišta imati vlastiti lanac u budućnosti.

3. OPĆENITA STRUKTURA LANCA I NAČIN RADA

Lanac, pojednostavljeno, funkcionira kao baza podataka, no za razliku od običnih baza informacije se umjesto u tablice, obrađuju i spremaju u blokove koji se dodaju jedan nakon drugoga i međusobno povezuju pokazivačima. Velik broj računala diljem svijeta obrađuju informacije ili rješavaju kompleksne jednadžbe potrebne za potvrdu transakcije. Blokovi se pune mnoštvom informacija o transakcijama te nakon što im se kapacitet popuni, linearno se nadograđuju na lanac i u informacije im se upisuje vrijeme spajanja s lancem. [11] Blokovi se ne mogu mijenjati ni premještati te lanac na taj način osigurava točnost pohranjenih informacija i kronologiju koja se ne može alterirati. Lanci u osnovi funkcioniraju na isti način no razlike u načinu rada mogu činiti velike razlike u tome kako prosječan korisnik doživljava korištenje što se na kraju i translatira u zadani problem. Cilj lanca je uspješno vršiti transakcije bez umiješanih posrednika i dodatnih potvrda koje se mogu krivotvoriti.



Sl. 3.1. Proces unosa i potvrde transakcije na lancu, [12]

3.1. Dokaz o radu (*Proof of work)*

Dokaz o radu mehanizam funkcionira na pogon računala diljem svijeta, takozvanih rudara, koji rješavaju kompleksne jednadžbe, zadatke i pogađaju nasumične brojeve kako bi potvrdili transakciju. Ovim načinom je osiguran integritet informacija, podataka i valuta koji se šalju

putem transakcije. Lanci koji koriste ovaj mehanizam su također puno sigurniji od drugih s obzirom da se za napad na lanac ili izmjenu podataka treba posjedovati 51% svih računala koja trenutno rudare tj. potvrđuju transakcije. Bez obzira na sigurnost, očit problem nastaje pri prevelikim opterećenjima lanca gdje bi se za održavanje većeg broja transakcija morao koristiti veći broj računala ili uređaja za rudarenje te bi troškovi električne energije bili značajno veći te štetili i trenutnim zalihama energije u svijetu. *Proof of work* zasnovani lanci se također ne očituju brzinom kao lanci s drukčijim načinom rada i najčešće su skuplji po pitanju troškova transakcija naspram ostalih lanaca. Dvije najpoznatije valute Bitcoin i Etherum se temelje na *proof of work* načinu rada, ali Ethereum koji je podložniji modernizaciji i promjenama u bližoj budućnosti prelazi na *proof of stake* način rada što se svakako ne događa bezrazložno. [13]

3.2. Dokaz o pologu (*Proof of stake)*

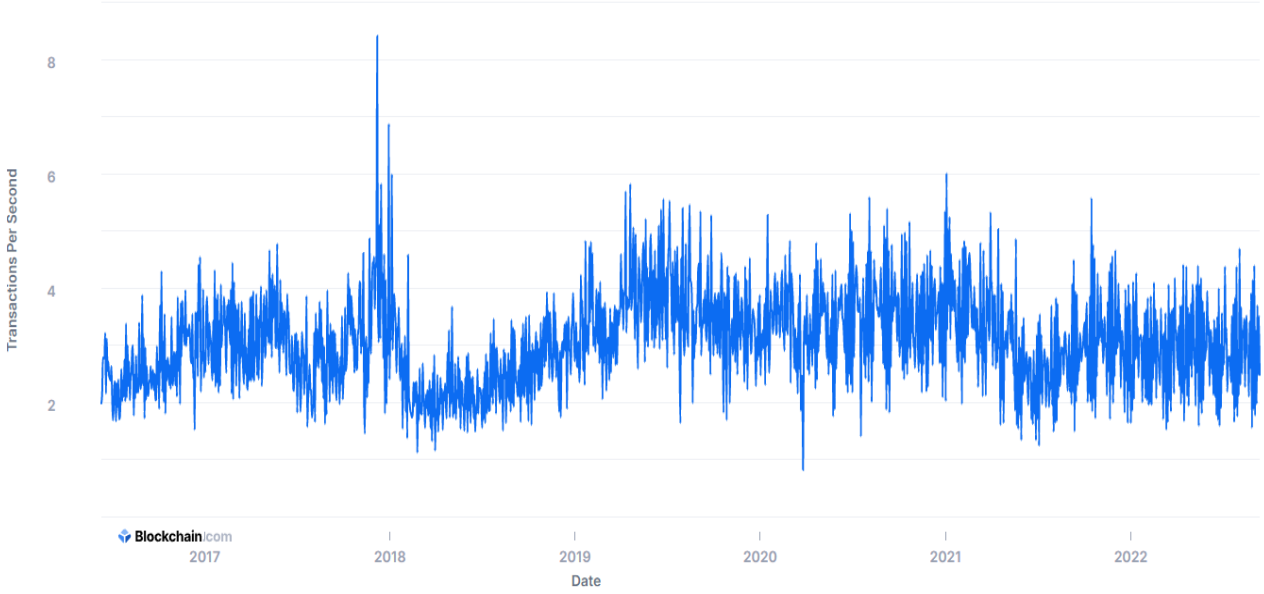
Dokaz o pologu, za razliku od ranije spomenutog mehanizma, ne zahtijeva napredan hardver niti izdašnu potrošnju energije. Lanci koji operiraju na ovaj način omogućuju sudjelovanje u autorizaciji transakcija i najmanjim sudionicima. Za postajanje *validatorom,* kako se to naziva u ovom načinu rada, potrebno je „zaključati“ određeni iznos tokena u *smart contractu* čiji kod predstavlja niz uputa za izvedbu transakcije ili tražene operacije kao što je zaključavanje tokena. *Validatori* su zauzvrat nagrađeni s dodatnim tokenima, istog tipa koji su i zaključali, a taj cijeli proces se naziva *staking*. Sudjelovanjem u *stakingu* se postaje *validatorom* te je moguće sudjelovati u potvrdi transakcija. S obzirom da se *validator* s najvećim brojem tokena uzima kao prioritet u potvrđivanju transakcije, manji ulagači mogu tvoriti *staking* bazene tj. grupe *validatora* te zajedničkim snagama autorizirati transakcije te naknadno pravedno podijeliti nagradu u obliku novih tokena. S obzirom na takav nedostatak gdje bi veći entiteti preuzeli kontrolu nad potvrdom transakcija postoje obrambeni mehanizimi kao *slashing* gdje se u slučaju netočnog potvrđivanja ili zlonamjernih radnji *validator* kažnjava s oduzimanjem dijela zaključanih tokena. Također sukladno problemu nastaje sličan način rada tj. delegirani *proof of stake* gdje *validatori* glasaju za tj. delegiraju posao *validatoru* s obzirom na njegov broj tokena, dosadašnje vrijeme provedeno potvrđujući transakcije i slično[14]. Lanci zasnovani na *proof of stake* načinu rada su se pokazali bržim, efikasnijim i ekonomičnijim u odnosu na njihovu konkurenciju zasnovanu na *proof of work* načinu. Također omogućuju manjim ulagačima sudjelovanje u potvrđivanju transakcija i nadogradnji ekosistema s minimalnim ulozima.

4. PREGLED I PROCJENA OPTIMALNOSTI POSTOJEĆIH LANACA

Odabir ekonomičnog i efikasnog lanca je ključan za uspješnu realizaciju zamišljene ideje. Bez optimalnog lanca ideja studentske iskaznice pada u vodu te čak i u slučaju razvoja tehnologije koja bi trenutno omogućila pohranu i slanje kriptovaluta pomoću iste bez brzog i dovoljno jeftinog lanca provedba ideje je nemoguća.

4.1. Bitcoin

Bitcoin je uvjerljivo najpoznatija *blockchain* i kriptovaluta te i sam začetnik istih. Njegova globalna popularnost pa i sama popularnost među ljudima neupoznatim s kriptovalutama predstavlja dobar preduvjet za lakšu prilagodbu plaćanja kriptovalutama. Postavlja se kao potencijalan kandidat za odabir lanca zbog svoje sigurnosti, niskih transakcijskih naknada te već postojećoj raširenosti u svijetu tj. korištenosti gdje se u transakcijama šalju i po stotine milijuna dolara. Troškovi transakcije se u zadnjih par godina vrte oko jednog dolara no u najprometnijim danima su znale doseći i sedamdeset dolara. Unatoč navedenim prednostima Bitcoin funkcionira na *proof of work* načinu rada čije su mane već objašnjene, a tranzicija na drukčiji način rada se najvjerojatnije neće nikad ni ostvariti. No trenutni način rada ima svoje prednosti pošto Bitcoin nikad nije pretrpio 51%-tni napad značeći da nitko nikad nije preuzeo kontrolu nad 51% svih računala koja se ponašaju kao rudari. Ovaj napad bi predstavljao problem za puno manjih *proof of work* lanaca, ali zbog ogromnog broja računala te njihove raširenosti oko svijeta za Bitcoin to predstavlja uvelike umanjen rizik. Takav pothvat bi bio izuzetno novčano i energetski zahtjevan te se smatra skoro pa nemogućim što se očituje u tome da Bitcoin dosad nijednom nije bio hakiran. Nažalost Bitcoin sukladno slici 4.1. od svojeg začetka u najboljem izdanju vrši nešto više od osam transakcija po sekundi, a u najlošijem samo jednu transakciju po sekundi. S obzirom da su takve oscilacije rijetke možemo tvrditi da se većinu vremena transakcije kreću od dvije do pet po sekundi što je daleko od optimalnog za implementaciju studentske iskaznice s obzirom koliko ljudi globalno koristi Bitcoin. Broj dnevnih transakcija se kreće od dvjesto do četiristo tisuća, a sam podatak da je prosječnoj transakciji potrebno deset minuta da se obradi nam govori da je Bitcoin unatoč svojim brojnim prednostima neoptimalan kandidat za implementaciju rješenja. Bitcoin se zbog svojeg načina rada te skoro pa nikakvih promjena od začetka dovodi do upitne skalabilnosti koja je nužna za rješenje.



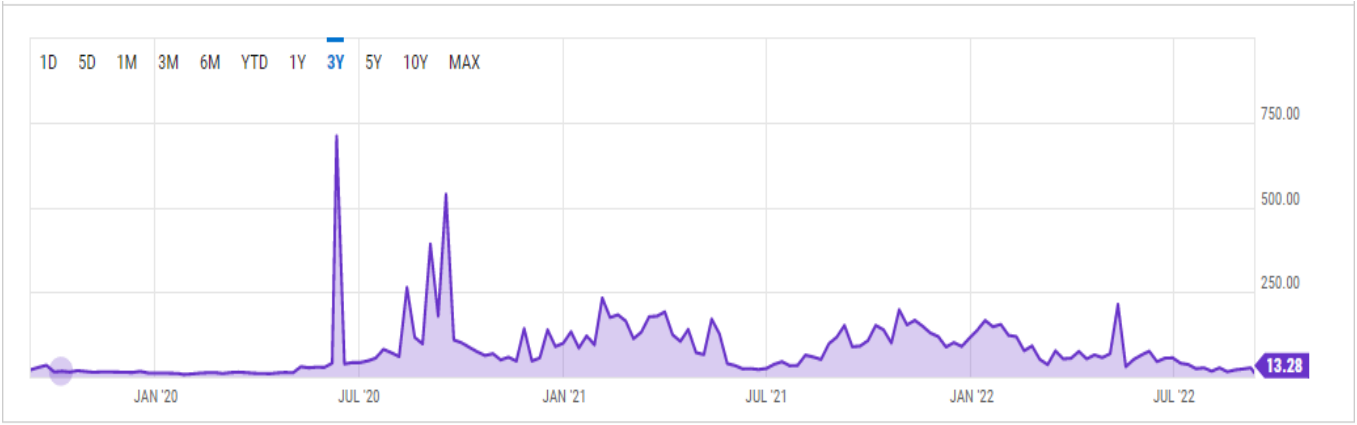
Sl. 4.1. Graf BTC transakcija po sekundi od 2016. do rujna 2022., [15]

4.2. Ethereum

Ethereum je druga najveća kriptovaluta po tržišnom udjelu te najpoznatija među valutama koje nisu Bitcoin. Ethereum je inače vrlo siguran lanac, ali su se u prošlosti već dogodile provale u sustav te krađe od čak par stotina milijuna dolara. U slučaju studentske iskaznice ovaj problem je zanemariv pošto su se napadi dogodili preko takozvanih *bridge-eva* koji služe kako bi se dva lanca koja inače nebi mogla komunicirati, povežu i međusobno si omoguće transakcije, a u slučaju iskaznice rješenje je predviđeno na isključivo jednom lancu. Na slici 4.2. je vidljivo da se prosječna vrijednost transakcija po sekundi kreće od deset do dvadeset, a u začecima je jedva dostizao jednu transakciju po par sekundi. Lanac trenutno operira na *proof of work* načinu rada no tranzicija na *proof of stake* bi se trebala ostvariti u rujnu 2022. što bi značilo da bi Ethereum u bližoj budućnosti mogao obrađivati i po par tisuća transakcija u sekundi. U daljoj se budućnosti , po izjavama tvorca Ethereuma, Vitalika Buterina, može očekivati i do sto tisuća transakcija po sekundi što s obzirom na brz razvoj tehnologije ulančavanja ne čini nedostižno [16]. Iako bi se prijelazom na optimalniji način rada trebala unaprijediti brzina, cijena transakcija će zasad ostati netaknuta što je jedan od najvećih problema Ethereuma kao lanca. Iz grafa na slici 4.3. se može vidjeti kako cijena prosječne transakcije jako varira te se može kretati od deset dolara kad je lanac pod najmanjim opterećenjem pa do čak par stotina dolara kad je promet najveći. Ovakve cijene transakcija su nedopustive za implementaciju nečega kao studentska iskaznica u kojem

slučaju bi se dnevne transakcije za prehranu brojale u tisućama, a samim time bi i troškovi bili nesnošljivi. [17]

Sl. 4.2. Graf ETH transakcija po sekundi od 2015. do rujna 2022., [15]

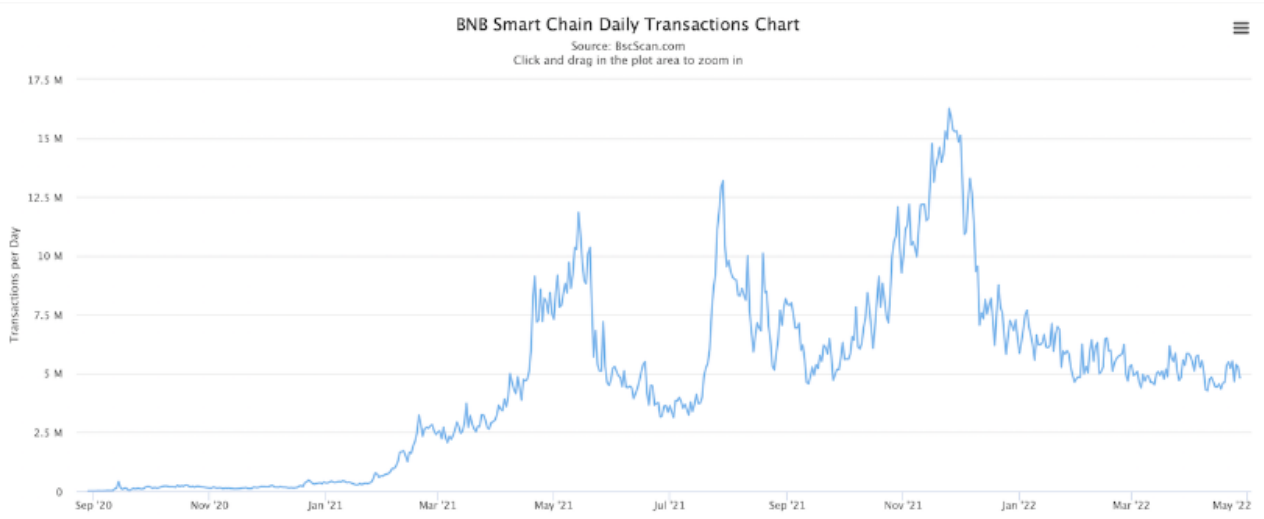


Sl. 4.3. Graf ETH troškova transakcije u dolarima od rujna 2019. do rujna 2022., [15]

4.3. Binance Smart Chain (BSC)

Binance Smart Chain je produkt kompanije i mjenjačnice Binance. Njihov *native* token BNB je treća najveća kriptovaluta po tržišnom udjelu izuzevši stabilne valute. BSC također ima vlastitu, već spomenutu, stabilnu valutu Binance USD (BUSD) koja je treća najveća stabilna valuta po tržišnom udjelu. Samim time, bilo bi za očekivati da se u slučaju izbora BSC kao idealnog lanca za rješenje također implementira BUSD kao valuta kojom će se rukovati. BSC je relativno

sigurna mreža te je dosad napadnuto tek par protokola temeljenih na BSC lancu što je rezultiralo u ukradenih par desetaka milijuna dolara no ništa naspram cijele količine koja se nalazi u cijelom BSC ekosustavu. Troškovi transakcija su jako niski te iznose tek par centa po transakciji što bi bilo pogodno za rješenje. Lanac najčešće bilježi prosjek od par desetaka transakcija po sekundi, a u najboljem slučaju dosegne i do par stotina. Brzina lanca nije optimalna no svejedno je iznad trenutnih mogućnosti Bitcoina i Ethereuma, a i brojevi dnevnih transakcija vidljivih iz slike 4.4. pokazuju da je lanac testiran i pouzdan za obradu više milijuna transakcija dnevno.

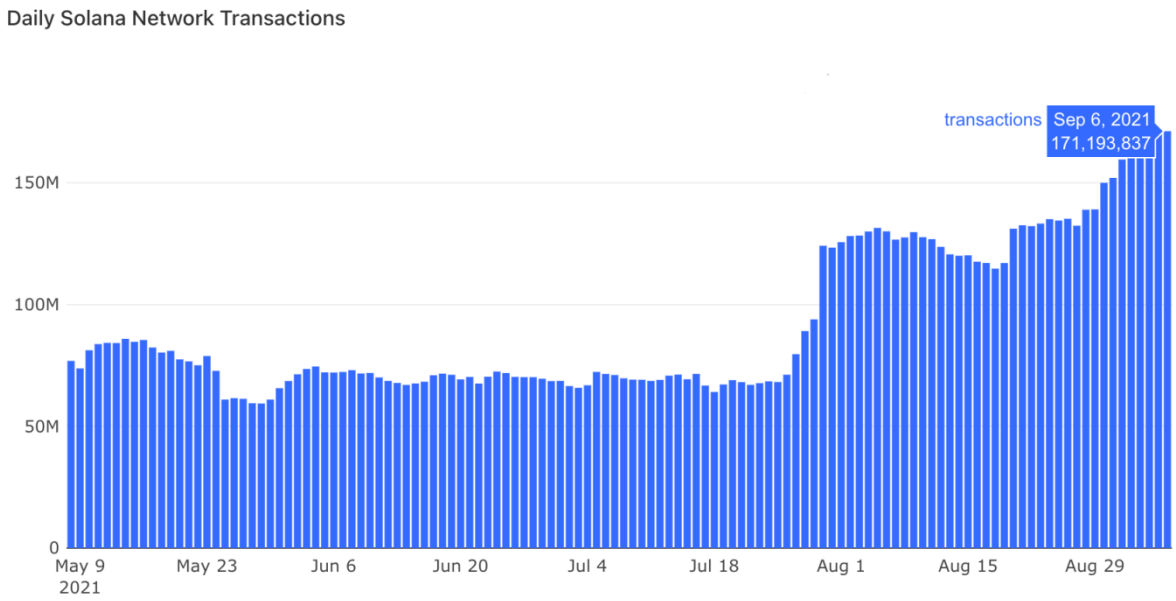


Sl. 4.4. Graf BSC ukupnog broja dnevnih transakcija od rujna 2020. do svibnja 2022., [15]

4.4. Solana

Solana se postavlja kao jedan od ozbiljnijih kandidata za implementaciju rješenja zbog svoje brzine koja iznosi po par tisuća transakcija u sekundi te jeftinih troškova transakcije koji u prosjeku iznose manje od jednog centa po transakciji. Trenutno šesta najjača valuta po tržišnom udjelu isključujući stabilne te doživljava ogroman porast u popularnosti. Zasniva se na delegiranom *proof of stake* načinu rada. Potvrdno istraživanju i testiranjima razvojnih programera spomenutog lanca Solana je vrlo skalabilna te bi u budućnosti trebala moći obrađivati i do stotinu tisuća transakcija po sekundi [18]. Graf na slici 4.5. nam govori o učinkovitosti Solane te pokazuje sposobnost obrade stotina milijuna transakcija dnevno s minimalnim troškovima obrade. Ovakve brojke nam govore kako bi Solana bila idealan kandidat

za implementaciju rješenja, ali naspram ostalih lanaca Solana je doživjela *down time* desetak puta te bi to svakako predstavljalo problem u sustavu studentske prehrane. Padovi sustava su bili riješeni kroz par sati no opet treba uzeti u obzir pouzdanost lanca kao takvog. Solana se također smatra jednim od nesigurnijih među najvećim lancima te je više puta bila izložena hakerskim napadima.



Sl. 4.5. Graf SOL ukupnog broja dnevnih transakcija od svibnja 2021. do rujna 2022. [15]

5. PRIJEDLOG I PREDVIĐENA IMPLEMENTACIJA RJEŠENJA

Prijedlog implementacije rješenja se temelji na već postojećim tehnologijama te su za isto izabrani sukladni kandidati, no zbog trenutnih nedostataka i potencijalnih problema lanaca i valuta predloženo je i alternativno rješenje. U smislu fizičke tehnologije i uporabe rješenje je predloženo kao izvedenica već postojećih i predviđenih tehnologija, no one bi se morale dodatno razviti u budućnosti za ostvarenje rješenja.

5.1. Problem subvencije

Raspodjela subvencije bi se morala prilagoditi sustavu lanca te bi plaćanje trenutnim novčanicama kao što su kune bilo onemogućeno. Samim time raspodjela subvencije koju vrši država bi se morala odvijati u kriptovalutama. Takav pristup bi se mogao riješiti na dva načina. Prvi način je da država, zajednica kao EU ili slično ovisno o magnitudi projekta kupi određenu količinu stabilnih valuta te ih pohrani na sigurno. Pohrana bi stvarala komplikacije pošto bi se novac najsigurnije pohranio na hladni novčanik, no nije sigurno toliku količinu novca držati u jednom novčaniku koji bi mogao biti fizički ugrožen. Preporuka je raspodijeliti novac u više novčanika manjim upravnim jedinicama kao što su županije. Također se problem očituje u tome što bi se novac morao prebaciti s hladnog novčanika na iskaznice te nakon skeniranja predviđene iskaznice uputama *smart contracta* upisanog u transakciju potrošeni novac trebao prebaciti nazad na taj novčanik. Ovo stvara tehnološki nepremostivu prepreku pošto bi hladni novčanik morao biti ukopčan USB-om u uređaj za obradu. Druga, puno optimalnija opcija bi bila stvaranje nove stabilne valute na odabranom ili čak novokreiranom lancu. Valuta bi morala biti isključivo namijenjena svrsi studentske iskaznice tj. prehrane/studentskim popustima kako bi se izbjegli potencijalni hakerski napadi. Valuta bi imala vrijednost isključivo u vlastitom ekosustavu te ju ne bi bilo moguće prodavati na mjenjačnicama. Ovim bi se izbjegla uporaba hladnog novčanika te bi prebacivanje novca iz i u „glavni“ novčanik bilo jednostavno i efikasno uz naravno ostvarene prvotne uvjete brzine i niskih troškova transakcija.

5.2. Implementacija rješenja

Za implementaciju trenutno dostupnog rješenja, preporučen je lanac Solana te stabilna valuta USD Coin (USDC). Solana se pokazala kao skoro pa idealan kandidat zbog svoje izuzetne brzine

od par tisuća transakcija po sekundi i minimalnih troškova od čak manje od centa. Unatoč prednostima, Solana, kao i ostali lanci nije savršen te je više puta u prošlosti iskusio hakerske napade i *down time* što je bez obzira na brzo saniranje problema bitan faktor te bi se takve stvari u budućnosti morale maksimalno sanirati. USD Coin se predstavio kao optimalan izbor valute koja će se koristiti zbog svojih marginalnih oscilacija u cijeni i jako čvrstoj podržanosti u fiat sredstvima. Alternativni prijedlog je stvaranje vlastitog, privatnog lanca te vlastite valute kojom će se rukovati. Subvencija bi se dijelila među studentima početkom mjeseca, a uputama zapisanim u pametnom ugovoru bi se ostatak vraćao u „glavni“ novčanik na kraju mjeseca. Uz uvjet da bi zamišljeni projekt financiralo neko nadležno tijelo kao npr. vlada države, svaki pokušaj zlouporabe tokena ili napada na sustav bi bio zakonski kažnjiv čime bi se sustav dodatno zaštitio. Iz aspekta fizičke tehnologije teško je zamisliti studente kako nose sa sobom nešto kao što su hladni novčanici zbog nekonvencionalne uporabe putem USB-a, a i samim time što novčanici još uvijek nisu spremni pohranjivati valute direktno nego samo pohraniti privatni ključ. U izglednijoj situaciji iskaznica ili sličan izveden uređaj bi morali ili nekako skenirati QR kod koji bi sadržavao upute za transakciju tj. pametni ugovor ili primiti upute pomoću promjene magnetskog toka na isti način na koji rade trenutne kreditne kartice kad se provuku kroz uređaj. Stoga, trenutni je najveći problem direktno pohraniti kriptovalute na iskaznicu. S obzirom na navedene trenutne tehnološke nedostatke, u oba slučaja (privatnog ili javnog lanca) se preporuča razvoj mobilne aplikacije tj. novčanika. Novčanik bi kao i trenutni mobilni novčanici funkcionirao jednostavno pomoću očitavanja QR koda koji sadrži upute o transakciji. Novčanik bi uz čuvanje sredstava, također služio kao identifikacija u sustavu studentskog obrazovanja te bi studenti preko aplikacije mogli primati kupone/sniženja za aktivnosti kao što su odlazak u kino, na bazene i sl.

6. ZAKLJUČAK

Implementacija studentske iskaznice na lanac bi trebao dostižan pothvat s obzirom na dosadašnje tehnološke uspjehe čovječanstva te ranu fazu u kojoj se nalaze kriptovalute. Trenutna tehnologija pokazuje naznake potencijalnog ostvarivanja zamišljenih ideja i čini se da je pitanje želi li se, a ne može li se tehnologija razviti do pretpostavljene razine. Lanci koji podržavaju velike brojeve transakcija i dovoljno su jeftini da bi model bio održiv već postoje, ali također postoje problemi koje bi trebalo sanirati kako bi se rješenje moglo provesti u stvarnost. Ethereum pokazuje da se lanci mogu uvelike promijeniti pa i izvršiti tranziciju s jednog načina rada na drugi. Neupitno je da će i ostali lanci, a i oni nadolazeći težiti onim aspektima koji su bili nužni za odabir optimalnog rješenja. Ovakav sustav plaćanja studentske prehrane, a i općenito plaćanja kriptovalutama bi autoritetima koji ih koriste mogao omogućiti stopostotno točan i siguran uvid u cijelu prošlost transakcija te samim time eliminirati potencijalnu korupciju ili prevare u sistemu. Unatoč moderniziranim načinima plaćanja usluga pomoću mobilnih aplikacija, razvoj nove aplikacije koja implementira tehnologiju ulančavanja pruža bolju sigurnost, transparentnost te efikasnost samog sustava. S obzirom na sve rečeno, još uvijek ne postoje toliko bitni razlozi ili pravi poticaj kako bi se nešto kao studentsko plaćanje kriptovalutama provelo u realnost zbog već relativno lagane uporabe studentske iskaznice i standardiziranosti postojećeg sistema. Uz uvid u točnost i transakcije, lanci i kriptovalute bi u budućnosti morale pružiti neke dodatne prednosti i proširiti već postojeće mogućnosti kako bi nadležna tijela razmotrila ovakvo nešto kao potencijalnu zamjenu postojećeg sustava.

LITERATURA

[1] „How Blockchain Is Used in Education“, https://online.maryville.edu/blog/blockchain-in-education/ [14.09.2022.]

[2] „Welcome to the Binance Card“, https://www.binance.com/en/cards [30.06.2022.]

[3] „Crypto.com Cards“, https://crypto.com/eea/cards [30.06.2022.]

[4] „Crypto Payments Explained“, https://academy.binance.com/en/articles/crypto-payments-explained [30.06.2022.]

[5] „Hardware Wallets Explained“, https://medium.com/radartech/hardware-wallets-explained-da8bd93ce801 [30.06.2022.]

[6] „Ledger to Ledger transfers are now possible – Radar Relay“, https://coingeek.com/ledger-to-ledger-transfers-are-now-possible-radar-relay/ [30.06.2022.]

[7] https://www.ledger.com [30.06.2022.]

[8] „Stablecoin Market Capitalization“, https://www.statista.com/statistics/1255835/stablecoin-market-capitalization/ [08.09.2022.]

[9] https://coinmarketcap.com [08.09.2022.]

[10] „Why a Blockchain-Based Digital Student ID Is The Next Big Innovation“, https://www.linkedin.com/pulse/why-blockchain-based-digital-student-id-next-big-christopher-williams/ [14.09.2022.]

[11] A. Lewis, „The basics of Bitcoins and Blockchains: an Introduction to Cryptocurrencies and Technology that Powers them“, Ingram Publisher Services UK, 2018.

[12] „Blockchain Facts: What Is It, How It Works, and How It Can Be Used“, https://www.investopedia.com/terms/b/blockchain.asp [08.09.2022.]

[13] A. Tapscott, D. Tapscott, „Blockchain revolution“, Penguin Publishing Group, 2016.

[14] „What Are Proof of Stake and Delegated Proof of Stake?“, https://www.gemini.com/cryptopedia/proof-of-stake-delegated-pos-dpos [10.09.2022.]

[15] https://www.blockchain.com [08.09.2022.]

[16] „Revolution in Ethereum (ETH) Scalability: Vitalik Buterin Shares "All In" Roadmap With 100,000 Maximum TPS“, https://u.today/revolution-in-ethereum-eth-scalability-vitalik-buterin-shares-all-in-roadmap [10.09.2022.]

[17] A. Antonpoulos, „Mastering Ethereum“, O'Reilly Media, Inc., 2018.

[18] „Inside Solana's Internal Scalability Test“, https://solana.com/news/inside-solana-s-internal-scalability-test [10.09.2022.]

SAŽETAK

Pojava kriptovaluta i tehnologije ulančavanja je stvorila nove mogućnosti te redefinirala način na koji se šalje novac ili potvrđuje legitimnost nečega kao fakultetska diploma. U radu su objašnjene tehnologije koje bi mogle pomoći u implementaciji studentske iskaznice na lancu. Opisane su specifikacije te trenutno stanje najpoznatijih postojećih lanaca kao i sam način na koji lanac funkcionira. Naposlijetku je, s obzirom na sve opisano u radu, predstavljeno „idealno“ rješenje te implementacija studentske iskaznice na lancu.

Ključne riječi: kriptovalute, lanac, studentska iskaznica

ABSTRACT

Student ID card on a chain

The appearance of cryptocurrencies and blockchain technology has created new posibilities by redefining the way money is being sent or legitimacy of something like a college degree being confirmed. The paper explains technologies that could be of help in the implementation of the student identification card. Specifications of the most popular blockchains and their current state, aswell as the way the chain itself operates has been explained. Finally, considering everything described in the work, an „ideal“ solution and the implementation of the student card has been presented.

Keywords: cryptocurrencies, blockchain, student ID

ŽIVOTOPIS

Autor ovog rada, Juraj Marinčić, rođen je 23.12.2000. u Osijeku. Osnovno obrazovanje stječe u Osnovnoj školi „Retfala“, a srednjoškolsko u „III. Gimnazija“ u Osijeku. 2019. upisuje studij računarstva na „Fakultet elektrotehnike, računarstva i informacijskih tehnologija“ čiji je redovni student.