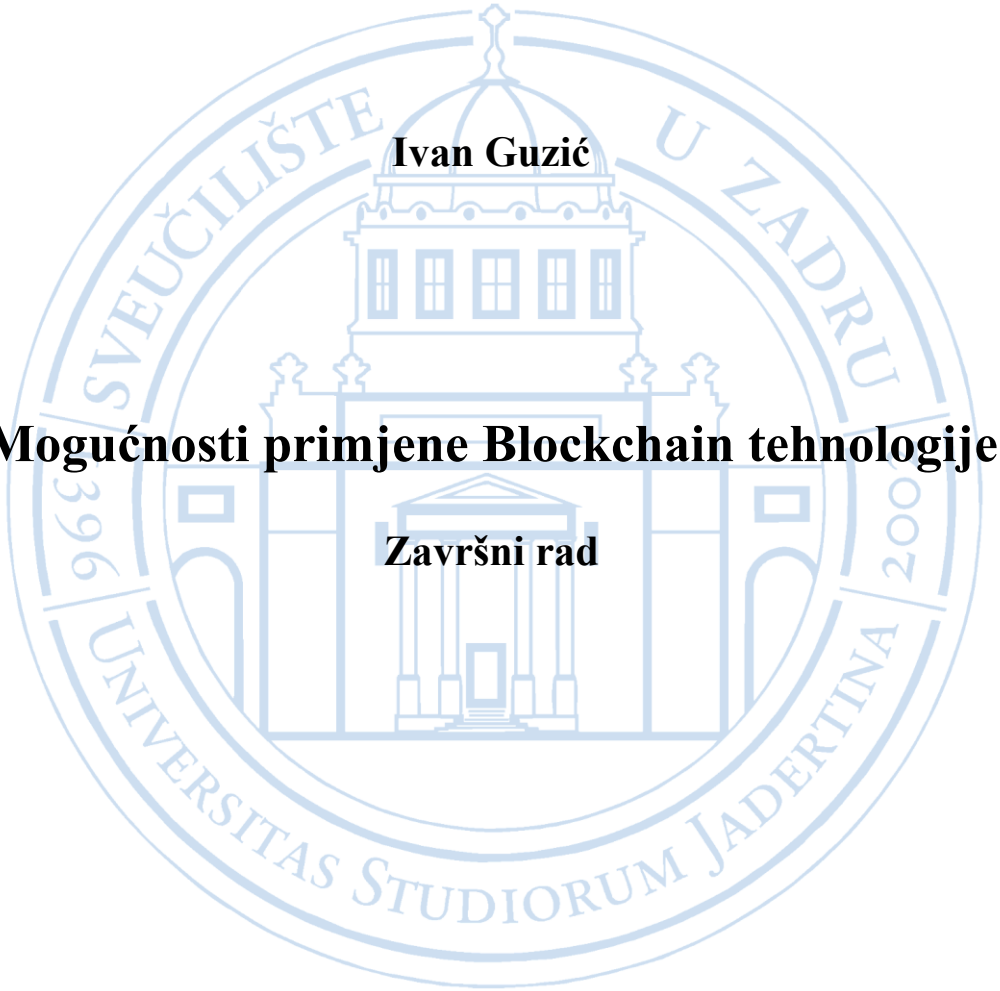
Mogućnosti primjene Blockchain tehnologije

Guzić, Ivan

Sveučilište u Zadru

Odjel za informacijske znanosti
Stručni preddiplomski studij Informacijske tehnologije



Ivan Guzić

Mogućnosti primjene Blockchain tehnologije

Završni rad

Zadar, 2022.

Sveučilište u Zadru

Odjel za informacijske znanosti

Stručni preddiplomski studij Informacijske tehnologije

Mogućnosti primjene Blockchain tehnologije

Završni rad

Student/ica:
Ivan Guzić

Mentor/ica:
Dr. sc. Dino Županović

Zadar, 2022.

Izjava o akademskoj čestitosti

Ja, **Ivan Guzić**, ovime izjavljujem da je moj **završni** rad pod naslovom **Mogućnosti primjene Blockchain tehnologije** rezultat mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Ni jedan dio mojega rada nije napisan na nedopušten način, odnosno nije prepisan iz necitiranih radova i ne krši bilo čija autorska prava.

Izjavljujem da ni jedan dio ovoga rada nije iskorišten u kojem drugom radu pri bilo kojoj drugoj visokoškolskoj, znanstvenoj, obrazovnoj ili inoj ustanovi.

Sadržaj mojega rada u potpunosti odgovara sadržaju obranjenog i nakon obrane uređenoga rada.

Zadar, 19. rujna 2022.

ZAHVALNICA

Ovim putem se zahvaljujem svom mentoru, prof. dr. sc. Dinu Županoviću, koji je spremno prihvatio mentorstvo pri izradi ovog završnog rada. Zahvaljujem se i svojoj obitelji, koja je tijekom cjelokupnog studija zajedno sa mnom prolazila kroz sve obveze koje su me dočekale, te koja mi je bila zaista bila nezamjenjiv oslonac. Naposljetku, posebne zasluge zaslužuje i moj prijatelj Neven. Usprkos mnogim preprekama na koje sam naišao tijekom dosadašnjeg studija, Neven je svojim znanjem i nesebičnim darivanjem vremena uspijevao pronaći način da me usmjerava prema naprijed.

SADRŽAJ

SAŽETAK

Tema ovog završnog rada je Blockchain tehnologija, točnije neke od aktualnih primjena Blockchain tehnologije, te moguće primjene takve tehnologije u budućnosti. Osim samih primjena, nabrajaju se i najznačajnije pozitivne i negativne značajke, kako bi se izgradilo objektivnije stajalište o učinku Blockchain-a na društvo. Sukladno prirodi studija u sklopu kojega je napisan ovaj završni radi, predlaže se i praktični primjer primjene Blockchain-a na problem iz stvarnog svijeta, gdje bi Blockchain svojim karakteristikama mogao doprinijeti pozitivnom pomaku.

KLJUČNE RIJEČI:

Blockchain, tehnologija.

1. UVOD

U svijetu u kojemu malo što može proći nepopraćeno mobilnim uređajima, kamerama, senzorima i ostalom suvremenom tehnologijom, anonimnost i sigurnost su čimbenici koji nam sve više klize iz ruke. Pojavom društvenih mreža sami smo odlučili svoju intimu podijeliti sa svijetom i na taj način smo postali subjektom promatranja, potvrdivši poznatu izreku „ako ne plaćate proizvod, znači da ste vi proizvod.“ Anonimnost i sigurnost na Internetu su problemi modernog doba, pa treba uzeti u obzir kako na njih nismo bili u potpunosti spremni, no svijest o posljedicama se s vremenom razvija. Vraćanje kontrole u vlastite ruke postaje sve bitnije, a spoznaja kako poduzeća naše navike ponašanja u virtualnom svijetu koriste gotovo pa isključivo za vlastitu korist u ljudima stvara iskru otpora. Jednom takvom iskrom se može nazvati i Blockchain.

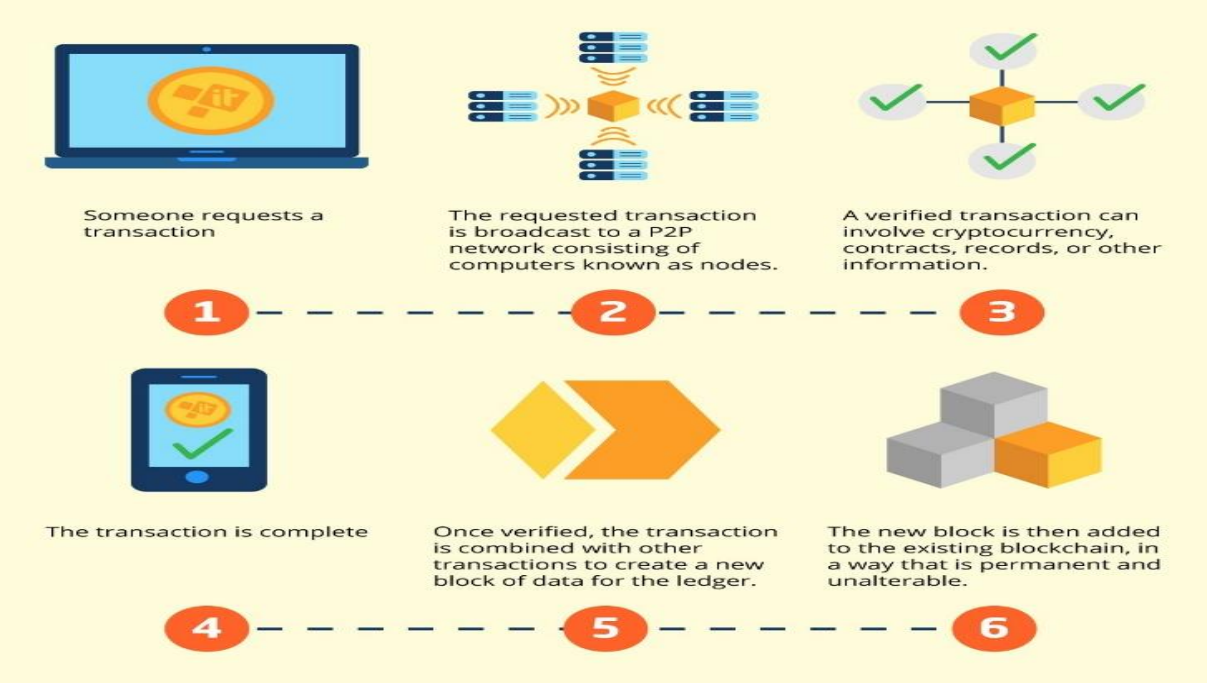
Blockchain sa sobom donosi obećanje u neovisnost o centraliziranim financijskim i drugim sustavima, intimu pri kupovini te nove mogućnosti u upravljanju vlastitom imovinom. Začet na, može se reći, demokratskim idejama, Blockchain pojedincima daje ono što bi im i trebalo pripadati. S druge strane, poduzeća dobivaju moćan alat za unapređenje svojih poslovnih procesa, proizvoda i usluga. Blockchain se, barem na papiru, uistinu čini kao revolucionarna tehnologija. Je li to zaista tako pokušat će se prezentirati u tekstu koji slijedi.

2. BLOCKCHAIN

2.1. Opis

Pri spomenu Blockchain-a kao prva asocijacija se najčešće nameće kriptovaluta Bitcoin. Nastao 2008. godine, a pušten u opticaj početkom 2009. godine, Bitcoin je u međuvremenu postao globalni fenomen i sinonim za kriptovalute. Kao tvorac Bitcoin-a se navodi Satoshi Nakamoto, no osim imena, gotovo da nema drugih informacija vezanih za navedenog individualca ili grupu. Nastao u vrijeme globalne financijske krize, Bitcoin se može smatrati iskazom nepovjerenja prema bankama i bankarskom sustavu, koji su podložni manipulaciji. Kao kriptovaluta s najvećom tržišnom vrijednošću, Bitcoin se temelji na razmjeni kriptovalute putem mreže ravnopravnih računala, gdje se uklanja potreba za posrednicima između strane koja plaća u kriptovaluti i strane koja zaprima kriptovalutu. Mreža ravnopravnih (eng. „peer-to-peer“) računala se sastoji od računalnih sustava koji su direktno povezani jedan s drugim putem Interneta, te koji međusobno mogu razmjenjivati datoteke bez potrebe za centralnim poslužiteljem. Na taj način svako računalo u mreži istodobno može poprimiti funkciju i poslužitelja i klijenta. Navedeno omogućuje izostavljanje utjecaja država, banaka ili nekih drugih financijskih posrednika, te se postiže decentralizirani sustav za razmjenu financijskih sredstava. Upravo taj decentralizirani sustav, odnosno Blockchain, predstavlja revolucionarnu inovaciju na kojoj će se graditi nove tehnologije.

Blockchain se ukratko može definirati kao distribuirana baza podataka. Sukladno tomu, umjesto jednog centraliziranog poslužitelja, Blockchain koristi mrežu računala koja validiraju transakcije, bilo da se radi o transakcijama kriptovaluta, zapisa ili nečeg trećeg. U nastavku se na slici 1 prikazuje pojednostavljeni primjer validacije transakcije kriptovalute.



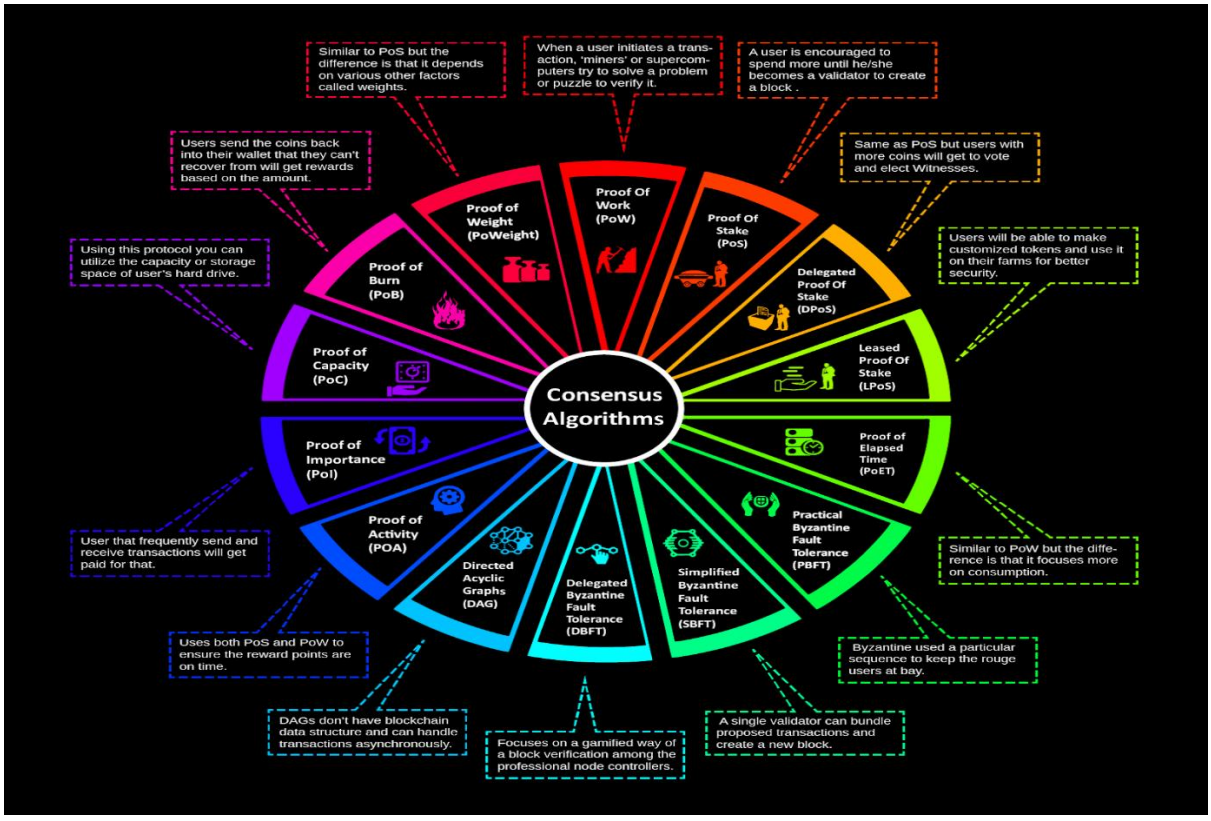
Slika 1: Postupak kreiranja novog bloka u Blockchain-u

Kako je vidljivo na slici 1, proces kreiranja novog bloka u Blockchain-u, odnosno validacija transakcije, započinje zahtjevom za transakcijom. Zahtjev se, zatim, distribuira do svih računala na mreži. Računala na mreži nazivaju se „čvorovima“. „Čvorovi“ (eng. „node“) su svi fizički uređaji u mreži koji su u mogućnosti slati, primati i prosljeđivati informacije, a najčešće se radi u osobnim računalima. Osim osobnih računala, modemi, switch-evi, hub-ovi, bridge-vi, poslužitelji i pisači također predstavljaju čvorove na mreži, kao i ostali uređaju koji se spajaju putem Wi-Fi-ja i Ethernet-a. „Čvorovi“ validiraju transakciju, čime je transakcija dovršena i pridodana prethodnim transakcijama. Naposljetku, novonastali blok se pridodaje postojećem Blockchain-u, na način koji je trajan i neizmjenjiv. Sam postupak validacije transakcija se vrši na način da se „čvorovi“ na mreži natječu u rješavanju kompleksnih algoritama, gdje prvi „čvor“ koji riješi algoritam stječe pravo kreiranja novog bloka te biva nagrađen kriptovalutom. Na taj način „čvorovima“ se daje motivacija za validiranjem transakcija u Blockchain-u. Vezano za same „čvorove“, u pravilu se radi o računalima sa zavidnim hardverskim resursima, najčešće sastavljenima u isključivu svrhu „rudarenja“ kriptovaluta. „Rudarenje“ je jedan od naziva za proces validacije novih blokova u Blockchain-u, a specijalizirana računala za proces „rudarenja“ se nazivaju Application Specific Integrated

Circuit (ASIC) „rudarima“, u čijem slučaju se radi o skupim i kompleksnim komadima hardvera, koji zahtijevaju veliku količinu električne energije.

2.2. Konsenzusi

Blockchain kao sustav, ovisno o kojemu Blockchain-u se radi, temelji se na jednom od nekoliko konsenzusa. Konsenzusi predstavljaju mehanizme za verifikaciju podataka unesenih u Blockchain, na način da se računala u mreži koja čini Blockchain usuglašavaju oko valjanosti podataka. Jednom kada se računala usuglase, kreira se novi blok koji se pridodaje postojećem Blockchain-u. Kroz razne izvore se može naići na više od petnaest različitih konsenzusa, od kojih se kao primjer mogu navesti Proof-of-Authority, Proof-of-Capacity ili Proof-of-Burn. Međutim, primarno se najčešće spominju Proof-of-Work i Proof-of-Stake, budući kako se upravo ti konsenzusi protežu kroz većinu trenutno najviše rangiranih kriptovaluta, ako se u obzir uzmu tržišne vrijednosti.



Slika 2: Blockchain konsenzusi

Na prethodnoj slici su prikazani neki od konsenzusa na kojima se Blockchain temelji, no pored navedenih, postoje još neki, kao što su Proof-of-History ili Proof-of-Person.

2.2.1. Proof-of-Work

Proof-of-Work je mehanizam koji koristi kriptovaluta Bitcoin, sinonim za kriptovalute i od samih početaka na vrhu po tržišnoj vrijednosti. Nadalje, Blockchain-i pogonjeni Proof-of-Work konsenzusom trenutno zauzimaju više od 90% tržišne kapitalizacije postojećih kriptovaluta. Princip Proof-of-Work konsenzusa se temelji na ulaganju računalnih resursa u izračune složenih algoritama. Upravo složenost algoritama osigurava vjerodostojnost Blockchain-a kao distribuirane baze podataka, i to, između ostalog, putem hash-iranja. Hash-iranje označava proces u kojemu kriptografska funkcija niz znakova bilo koje duljine putem ugrađene kompresijske funkcije uvijek pretvara u niz znakova koji imaju istu duljinu, a detaljnije će biti opisano u zasebnom paragrafu.

Budući kako je sam proces „rudarenja“ na Blockchain-ima pogonjenima Proof-of-Work konsenzusom hardverski zahtjevan i rezultira visokom potrošnjom električne energije, potrebno ga je motivirati putem nagrađivanja, odnosno kriptovalute. „Rudari“ se nagrađuju kriptovalutom po završenom procesu validacije blokova u Blockchain-ima, odnosno za kreiranje novih blokova.

2.2.2. Proof-of-Stake

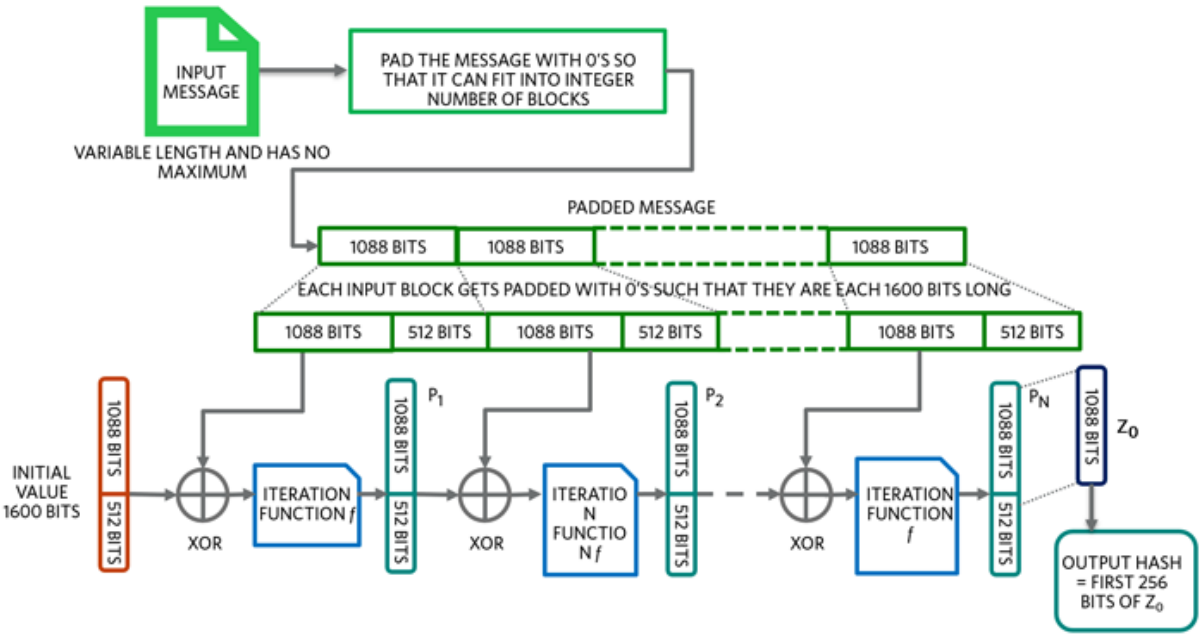
Proof-of-Stake konsenzus, za razliku od Proof-of-Work konsenzusa, ne iziskuje maksimizaciju hardverskih resursa radi povećavanja vjerojatnosti za validacijom i kreiranjem novih blokova na Blockchain-u. Baziran na principu nasumičnog odabira „rudara“, odnosno validatora, Proof-of-Stake konsenzus se smatra ekološki prihvatljivijom varijantom Blockchain-a, uzevši u obzir kako smanjenje potrebe za snažnim hardverom posljedično smanjuje i potrebu za utroškom

električne energije. Potrošnja električne energije je čest argument protiv Proof-of-Work konsenzusa, stoga je jasno kako je potrebno u obzir uzeti i alternativne načine za pogon Blockchain-a.

Na Blockchain-ima temeljenima na Proof-of-Stake konsenzusu nagrada se, također, dodjeljuje kada se kreira novi blok, no validatori se nasumično odabiru sukladno ulozima u sustavu, odnosno određenom iznosu kriptovalute položenom kao osiguranje. Vidljivi nedostatak ovakvog pristupa je činjenica kako se bogatijim „čvorovima“ na Blockchain-u, odnosno „čvorovima“ koji su u mogućnosti uložiti veće uloge u kriptovalutama, daje bolja prilika da povećaju svoje bogatstvo u odnosu na „čvorove“ s manjim početnim ulozima.

2.3. Hash-iranje

Blockchain se blisko veže uz kriptografiju, odnosno kriptografske hash funkcije. Kako je već ranije spomenuto, hash-iranje označava proces u kojemu kriptografska funkcija niz znakova bilo koje duljine putem ugrađene kompresijske funkcije uvijek pretvara u niz znakova koji imaju istu duljinu. Kao primjer se može navesti algoritam za kriptiranje Secure Hashing Algorithm (SHA), jedan od najpoznatijih algoritama te vrste, a koji će po završetku kriptiranja uvijek rezultirati heksadekadskim nizom znakova duljine 40, tzv. „hash-em“, radi ugrađene kompresijske funkcije. SHA je razvijen od strane američkog instituta National Institute of Standards and Technology (NIST) i sigurnosne agencije National Security Agency (NSA), gdje je prva inačica izdana 1993. godine kao “ Federalni standard za obradu informacija“ (FIPS-180). SHA-1 funkcionira na način da se ulazna poruka postavlja i podjeljuje na 512-bitne blokove. Zatim se nad svakim od 512-bitnih blokova primjenjuje kompresijska funkcija od 80 koraka. Funkcija sadrži dva tipa ulaza, ulančani ulaz od 160 bita i unos poruke od 512 bita. Rezultat zadnjeg poziva kompresijske funkcije je hash poruke. Pored SHA-1, danas postoje i SHA-2 te SHA 3 inačice SHA algoritma za kriptiranje, koje dolaze u nekoliko varijanti. Slika u nastavku prikazuje postupak kreiranja „hash-a“ poruke putem SHA-3 algoritma, u varijanti SHA-3 256.



Slika 3: Postupak kreiranja „hash-a“ poruke

Hash poruke, kao produkt hash funkcije, je zapravo ključan faktor pri validaciji blokova u Blockchain-u. Naime, bilo kakva promjena u podacima rezultira potpuno drugačijim „hash-em“, čime „čvorovi“ na Blockchain-u dobivaju jasnu naznaku kako se s određenim blokom pokušalo manipulirati. Kako bi blok na Blockchain-u bio validiran, potrebno je dobiti validaciju od strane više od 50% „čvorova“, čime se osigurava pouzdanost Blockchain-a. Vezano za natpolovičnu većinu „čvorova“, interesantno je spomenuti tzv. „Napad 51%“. Radi se o napadu u kojemu sudjeluje više od 50% „čvorova“ na određenom Blockchain-u, koji su radi svoje natpolovične većine u stanju kontrolirati Blockchain i manipulirati transakcijama. Takvo nešto je izrazito teško izvesti na velikim Blockchain-ima kao što su Bitcoin i Ethereum, na zabilježeno je više napada na manjim Blockchain-ima. U slučaju uspješnog „Napada 51%“, napadačima se otvara mogućnost višestrukog trošenja iste kriptovalute te su u mogućnosti odbacivati transakcije koje im ne odgovaraju.

2.4. Pametni ugovori

Još jedna bitna karakteristika Blockchain-a su pametni ugovori. Radi se o programima koji se automatski izvršavaju, sukladno zadanim parametrima, čime se eliminira potreba za ljudskim intervencijama. Odmah na početku potrebno je ukazati na razliku između pametnih ugovora i decentraliziranih aplikacija. Decentralizirana aplikacija je aplikacija bez posredništva poslužitelja, rasprostranjena na ravnopravnim računalima na određenom Blockchain-u, kao što je npr. Ethereum, dok je pametni ugovor konsenzus napisan izravno u programski kod, kao algoritam koji decentralizirana aplikacija može pozvati.

Kako je vidljivo iz kratkog opisa pametnih ugovora, radi se o izrazito korisnom mehanizmu koji može pronaći široku primjenu. Uzme li se u obzir samo primjer iz područja financija, a koji se često spominje u kontekstu kriptovaluta, pametni ugovori omogućuju izuzimanje banaka i drugih financijskih institucija iz uloga posrednika u financijskim transakcijama, koje svoje uloge posrednika uvijek i naplaćuju. Nadalje, vrijedi navesti i kako je transakcije obavljene putem Blockchain-a mnogo teže povezati sa samom sudionicima transakcija, odnosno teže je pratiti put kriptovalute, čime se osigurava anonimnost sudionika transakcija. Naravno, sama anonimnost sudionika transakcija putem Blockchain-a potencijalno donosi i negativne posljedice, budući kako omogućava različite nezakonite radnje, kao što je npr. trgovina oružjem ili ukradenim bankovnim podacima. Navedena problematika svakako zahtjeva sredstva regulacije, koja na Blockchain-u u puno slučajeva mogu biti nedostižna.

Pored navedenog, pretpostavka je kako se transakcije validirane putem Blockchain-a mogu smatrati manje podložnima manipulaciji i napadima od onih obavljenih putem centraliziranih baza podataka, kao što su bankarski sustavi. Decentralizirani karakter Blockchain-a ulijeva više povjerenja od provedbe financijskih transakcija putem zatvorenih sustava kao što su banke, a u isto vrijeme pruža i anonimnost i određeni stupanj transparentnosti, budući kako su transakcije dostupne i vidljive svim „čvorovima“ na Blockchain-u.

2.5. „Rudarenje“

U kontekstu Blockchain-a i kriptovaluta, „rudarenjem“ se naziva proces validacije transakcija na Blockchain-u. Radi se o hardverski zahtjevnom procesu, gdje se na izračun složenih matematičkih problema ulažu pozamašni računalni resurs, koji također koriste i pozamašne količine električne energije. Kako je već ranije spomenuto, praksa u današnje vrijeme je „rudarenje“ putem ASIC računala, koja su svojim performansama prilagođena za rješavanje matematičkih problema na kojima se Blockchain bazira. Međutim, potrebno je napomenuti kako su početci „rudarenja“ kriptovaluta ne baziraju na ASIC računalima, odnosno ASIC „rudarima“.

Pojavom Bitcoin-a „rudarenje“ se provodilo putem centralnih procesorskih jedinica[1] na računalima, koja su se u određenoj mjeri optimizirala za proces „rudarenja“. Centralne procesorske jedinice se sastoje od samo nekoliko aritmetičko-logičkih jedinica[2] i kontrolnih jedinca, što je za proces „rudarenja“ poprilično ograničavajući čimbenik. Budući kako je proces „rudarenja“ kontinuirano postajao sve složeniji, „rudarenje“ putem centralnih procesorskih jedinica je postalo hardverski nedostatno za bilo kakve ozbiljnije pothvate.

[1] Central Processing Unit (CPU) je primarna komponenta računala koja procesira instrukcije. Izvor: https://techterms.com/definition/cpu.

[2] Arithmetic Logic Unit (ALU) je dio centralne procesorske jedinice zadužen za sve potrebne izračune. Izvor: https://www.techopedia.com/definition/2849/arithmetic-logic-unit-alu.

Slika 4: Platforma za „rudarenje“ putem centralnih procesorskih jedinica

Kako je vidljivo na slici 3, prikazana je platforma za „rudarenje“ s dvije matične ploče na kojima su, između ostalog, montirane centralne procesorske jedinice koje na vrhu imaju montirane velike ventilatore za hlađenje.

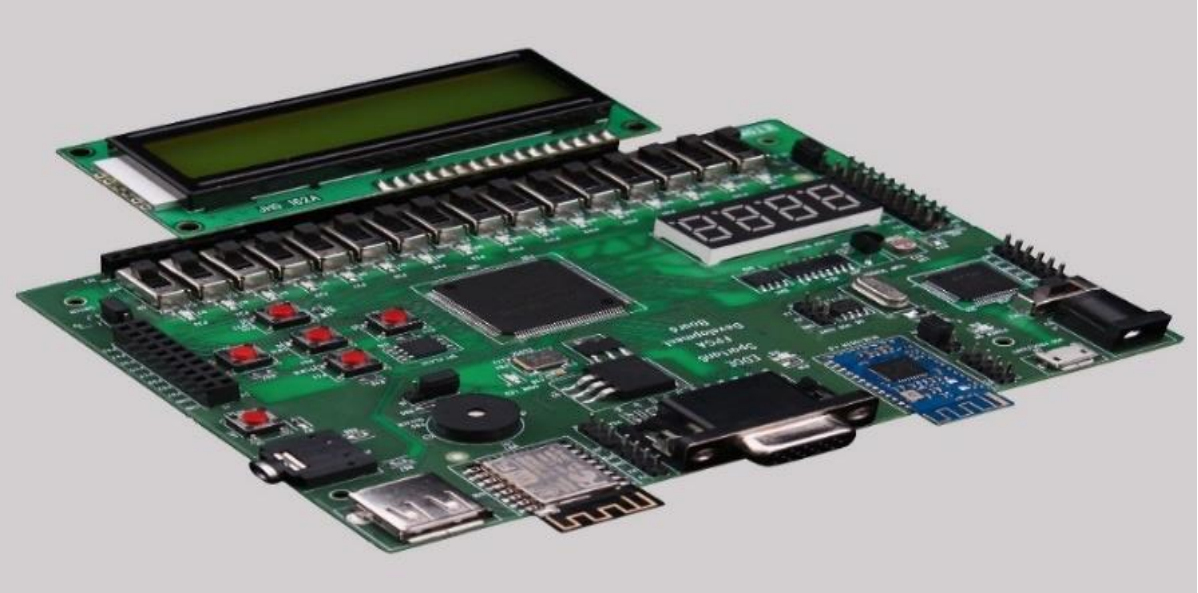
„Rudarenje“ se, potom, s centralnih procesorskih jedinca većinski prebacilo na grafičke procesorske jedinice[3]. Poznato je kako, za razliku od centralnih procesorskih jedinica, grafičke procesorske jedinice sadrže na tisuće jezgri. Ukoliko se u obzir uzme izuzetna sposobnost grafičkih procesorskih jedinica za brzom obradom velikog broja matematičkih podataka i sposobnost paralelnog izvršavanja više procesa odjednom, jasne su koristi koje donose u području „rudarenja“, baziranom na izračunu složenih matematičkih operacija.

[3] Graphics Processing Unit (GPU) je komponenta računala dizajnirana za paralelno procesiranje, ima širok raspon primjena, uključujući grafiku i obradu videa. Izvor: https://www.intel.com/content/www/us/en/products/docs/processors/what-is-a-gpu.html.

Slika 5: Platforma za „rudarenje“ putem grafičkih procesorskih jedinica

Slika 4 prikazuje platformu sa montiranih 6 grafičkih kartica, odnosno grafičkih procesorskih jedinica. Platforma je otvorenog tipa, kako bi se dobio što veći protok zraka, budući kako proces „rudarenja“ stvara velike količine topline.

U relativno kratkom razdoblju nakon pojave „rudarenja“ putem grafičkih procesorskih jedinica, a prije pojave ASIC računala, „rudarenjem“ su dominirali Field-Programmable Gate Array (FPGA) „rudari“. Radi se o logičkim sklopovima koji se mogu korisnici mogu konfigurirati za specifičnu namjenu. Kao bitan čimbenik je potrebno naglasiti da su u vrijeme nastanka FPGA ploče bile do pet puta energetski učinkovitije od „rudarenja“ putem grafičkih procesorskih jedinica. Slika u nastavku prikazuje jednu FPGA ploču.



Slika 6: EDGE Spartan 6 FPGA ploča

Naposljetku, kao alati za „rudarenje“, a koji se i danas koriste u svojim unaprijeđenim verzijama, pojavila su se ASIC računala. ASIC računalima se naziva specijalizirani hardver koji sadrži čip s integriranim krugom, dizajniran za specifičnu namjenu. Računala s ASIC čipovima su najčešće sastavljena kako bi „rudarila“ jednu specifičnu kriptovalutu, a od svakodnevnih računala se razlikuju po hardverskoj snazi i većoj učinkovitosti pri rješavanju kompleksnih matematičkih problema. Slika 6 prikazuje jedno takvo računalo.

Slika 7: ASIC računalo

Međutim, potrebno je napomenuti kako su određeni Blockchain-i svjesno uveli ograničenja na „rudarenje“ putem ASIC računala, točnije ne dopuštaju da se isto provodi. Takvi Blockchain-i se karakteriziraju kao „otporni na ASIC“, od kojih su među najpoznatijima Ethereum, Monero i Ethereum Classic, a otpornost postižu putem specifičnih algoritama za hash-iranje.

2.6. ICO (Initial Coin Offering)

ICO označava ograničeno razdoblje u kojemu je kriptovaluta dostupna javnosti za ulaganje. ICO poduzećima ili pojedincima pruža mehanizam za prikupljanje početnih ili dodatnih financijskih sredstava, nužnih za pokretanje određenog poslovnog ili drugog projekta. Prije nastanka Blockchain-a, financijska sredstva je bilo moguće prikupiti npr. izdavanjem i prodajom vlastitih dionica na burzi. Na taj način kupci dionica stječu određena pri donošenju poslovnih odluka u poduzeću čije dionice su kupili. Ipak, ICO ima neke značajno drugačije karakteristike. Ovaj mehanizam za prikupljanje sredstava je sličan kampanjama masovnog financiranja po uvjetima korištenja digitalnih platformi i odsutnosti uobičajenih financijskih posrednika. Međutim, ono što zaista razlikuje ICO-e od ostalih alternativnih mehanizama za financiranje je izdavanje kriptografskih tokena.

Kriptografski token je digitalna jedinica vrijednosti koja prebiva na Blockchain-u. Postoje četiri glavna tipa; platežni tokeni, uslužni tokeni, sigurnosni tokeni i nezamjenjivi tokeni. Platežni tokeni, koji se još mogu nazivati i „stablecoin“, podrazumijevaju kriptovalute kojima se mogu vršiti plaćanja roba i usluga. Uslužni tokeni omogućuju pristup određenim uslugama, a kao primjer se može navesti Ether, kriptovaluta na Blockchain-u Ethereum. Poduzeća grade decentralizirane aplikacije (DApps) na Ethereum Blockchain-u te lansiraju ICO-e koristeći ERC20 Ethereum standard, koji je najčešći tip uslužnog tokena. Naposljetku, kao četvrti tip tokena se navode nezamjenjivi tokeni, u javnosti puno više poznati po akronimu NFT (eng. „Non-Fungible Token“). Kako im i samo ime kaže, radi se o digitalnim entitetima koji su jedinstveni te koji zbog svoje jedinstvenosti imaju poseban značaj. Bilježeći nagli rast u popularnosti i financijskim sredstvima koja se za NFT-e izdvajaju tijekom posljednjeg desetljeća, NFT-i su postali financijski instrument kojeg se ne smije zanemariti te su danas, kao i Bitcoin te Blockchain, i NFT-i zaista globalni fenomen. Radi svojeg naglog rasta u

relativno kratkom vremenu i česte prezentacije kroz aktualne trendove u umjetnosti, videoigrama ili nekoj drugoj sferi aktualnih trendova, u pojedinim krugovima se NFT-e smatra prolaznom pojavom, no budući kako otvaraju neke nove mogućnosti u razmjeni dobara na koje se svijet sve više privikava, čini se kako bi se NFT-i još barem neko vrijeme mogli zadržati. Radi svoje istaknute uloge, o NFT-ima će biti više riječi u zasebnom dijelu ovog rada, koji govori o trenutno značajnim primjenama Blockchain-a.

3. PREDNOSTI I NEDOSTACI BLOCKCHAIN-A

Iako se koncept na kojemu se Blockchain zasniva bez sumnje čini kao nedvojben korak naprijed te čak i revolucija u pojedinim područjima, Blockchain za sebe veže i određene nedostatke, a za dio kojih će se tek daljnjim razvojem i primjenom Blockchain-a moći konkretnije utvrditi opseg i značaj nedostataka ili zlouporaba. Prije pregleda nedostataka, u nastavku se prvo navode prednosti Blockchain-a, upravo koje ga i čine tehnologijom budućnosti te subjektom vrijednim pažnje i razvoja.

3.1. Prednosti Blockchain-a

Blockchain kao tehnologija već danas nailazi na značajan broj primjena u kojima pokazuje prednosti u odnosu na dosadašnje prakse. Prednosti su mnoge, a u nastavku će biti nabrojan samo jedan dio.

3.1.1. Decentralizacija

Vjerojatno prva prednost koja pada na pamet kod spomena Blockchain-a je decentralizacija. Budući kako se Blockchain prema osnovnoj definiciji može okarakterizirati kao distribuirana baza podataka, jasno je kako se podaci ne nalaze na jednom mjestu, već na većem broju uređaja povezanih u mrežu. Na taj način se minimizira mogućnost manipulacije podacima od strane pojedinaca, čime podaci na Blockchain-u postaju značajno pouzdaniji od podataka na centraliziranim bazama. Nadalje, ovakvim mehanizmom se umanjuje utjecaj država, banaka i korporacija pri pohrani i razmjeni podataka.

3.1.2. Anonimnost

Druga velika prednost Blockchain-a je anonimnost, primarno kada se govori o transakcijama. Iako su transakcije na Blockchain-u vidljive svima, što je jedan od uvjeta da bi se mogle validirati, transakcije se ne mogu jednostavno povezati niti sa jednim određenim sudionikom transakcije, barem ako se radi o jednokratnim transakcijama koje se provode samo jednom s iste adrese. Na taj način se onemogućuje praćenje, bilo da se radi o praćenju od strane države ili od strane neke druge organizacije. Navedena karakteristika ulijeva pouzdanje u čitav takav sustav, budući kako je anonimnost na Internetu nešto što postaje sve veći luksuz.

Ipak, ne može se reći kako je Blockchain apsolutno anoniman. Budući kako svaka transakcija ostavlja nekakav trag, s vremenom i povećanjem broja transakcija povećava se i mogućnost kako će sudionici transakcija izgubiti prvotnu anonimnost. Postoje različiti pristupi koji se bave navedenim problemom, putem enkripcije eliptičnim krivuljama, zamjenom jedne kriptovalute za tokene nekog drugog Blockchain-a ili miješanjem transakcija na način da transakcije idu preko „tumbler“ servisa, kao što su npr. Blender, UniJoin ili SmartMixer, kako bi se prikrio izvorni pošiljatelj. Također, Ring Signature u kriptografiji predstavlja vrstu digitalnog potpisa kojeg može provesti bilo koji član grupe u kojoj svatko ima svoj zaseban ključ. Cilj je potpisati poruku kao određena grupa ljudi, kako bi bilo računalno nemoguće odrediti čiji ključ od članova grupe je iskorišten za kreiranje potpisa. Kriptovaluta Monero je bila prva koja je usvojila ovu metodu za anonimizaciju transakcija.

Naravno, u digitalnom svijetu ništa nije u potpunosti sigurno i prikriveno, pa ni prethodno spomenuti pristupi ne mogu garantirati apsolutnu anonimnost, no uvelike je mogu pospješiti. Međutim, anonimnost sa sobom donosi i određene poteškoće, od kojih se primarno mogu spomenuti one vezane za svakojaku trgovinu, o čemu će biti više riječi u zasebnom dijelu ovog rada.

3.1.3. Automatizam

Kao idući u nizu pozitivnih karakteristika Blockchain-a se može navesti automatizam, i to primarno putem pametnih ugovora, koji su već ranije opisani u zasebnom poglavlju. Kako je već ranije spomenuto, pametni ugovori su programi koji se automatski izvršavaju, sukladno zadanim parametrima, čime se eliminira potreba za ljudskim intervencijama. Na taj način se postiže visoka razina povjerenja, a smanjuje mogućnost zlonamjernih utjecaja na ishode pametnih ugovora. Ako se uzme primjer financijskih transakcija, pametni ugovori omogućavaju izuzimanje financijskih posrednika kao što su npr. banke. Posljedično, eliminira se i plaćanje naknada bankama, a izostankom financijskog posrednika, iz procesa se eliminira i jedna karika koja predstavlja potencijalni sigurnosni rizik.

3.1.4. Učinkovitost i brzina

Nastavno na prethodni paragraf, odnosno automatizam, vidljivo je kako se u slučaju Blockchain-a radi o učinkovitom sustavu koji, jednom kada se pusti u rad, zahtjeva minimalne ljudske intervencije. Budući kako se pametni ugovori izvršavaju automatski te bez ljudskog utjecaja, razne transakcije se provode neprestano, neovisno o dobu dana i lokaciji. Nadalje, transakcije ne zahtijevaju nikakav ručni rad, već se sve odvija elektronički, pa se stoga uglavnom radi o poprilično brzim procesima. Brzine variraju prema vrstama Blockchain-a, a za komparaciju valja uzeti nekoliko primjera. Bitcoin, koji u vrijeme pisanja ovog rada ima prosječno vrijeme transakcija od 40 minuta, može se uzeti kao primjer sporijeg Blockchain-a. Ethereum zahtjeva mnogo manje vremena, pa vrijeme transakcija iznosi 5 minuta. Međutim, postoje i mnogo brži Blockchain-i, kao što su Cardano ili Solana, čije transakcije se izvršavaju gotovo trenutno. Vrijeme transakcije je pod utjecajem nekoliko čimbenika, uključujući vrijeme bloka, veličinu bloka, naknade za transakcije i mrežni promet. Kao dodatno pojašnjenje valja navesti kako vrijeme bloka predstavlja mjernu jedinica vremena koje je „rudarima“ ili validatorima unutar mreže potrebno za potvrdu transakcije unutar jednog bloka te za kreiranje novog bloka u Blockchain-u, a kao primjer veličine bloka se može navesti Bitcoin, čija veličina bloka iznosi 1 MB.

3.1.5. Sigurnost i neizmjenjivost

Kako je već ranije spomenuto u ovom radu, svaki novi blok na Blockchain-u sadrži podatke o prethodnim blokovima, odnosno transakcijama. Ti blokovi su povezani putem prethodnih hash vrijednosti. Ukoliko bi napadač došao korigirati podatke, hash vrijednost će se izmijeniti, a što će utjecati na cjelokupni lanac. Na taj način se garantira dosljednost i kredibilitet novonastalih blokova, a mogućnost manipulacije pri kreiranju novih blokova je svedena na minimum, kao i mogućnost izmjene starijih blokova koji su prethodno već validirani na Blockchain-u. Na karakteristiku neizmjenjivosti se u slučaju Blockchain-a posljedično nadovezuje i karakteristika sigurnosti. Naime, budući kako bi za izmjenu podataka na Blockchain-u sa namjerom manipulacije bilo potrebno upravljati s najmanje 51% „čvorova“, kako je već ranije u ovom radu opisano kao „Napad 51%“, radi se pothvatu za koji nije izvjesno kako će biti uspješno proveden. Naravno, prethodno spomenuti pothvat je teže izvesti što je Blockchain veći, odnosno gdje je broj „čvorova“ veći. Ako se u obzir uzme kako se izmjenom i najmanjeg pojedinačnog podatka mijenja hash vrijednost bloka, te je uz novonastali blok potrebno korigirati i sve prethodno kreirane blokove, jasno je kako napade na Blockchain-ove nije jednostavno provesti, čime se ističe čimbenik sigurnosti.

3.2. Nedostaci Blockchain-a

Kako je vidljivo iz prvog dijela poglavlja o prednostima i nedostacima Blockchain-a, Blockchain obilježavaju značajne pozitivne karakteristike, radi čega je njegov kontinuirani rast i razvoj ne dolazi kao nešto neočekivano, već je u potpunosti opravdan. Prednosti Blockchain-a nabrojane u ovom poglavlju predstavljaju samo jedan dio, no pored prethodno nabrojanih, svako valja spomenuti i još neka područja u koja Blockchain donosi poboljšanja, kao što su transparentnost, troškovi, autorska prava, kontrola kvalitete ili sprječavanje prijevara. Međutim, kao i svaka nova tehnologija, Blockchain sa sobom donosi i neke nedostatke koji nisu zanemarivi. U nastavku se navode neki od nedostataka za koje se može tvrditi kako imaju popriličan značaj.

3.2.1. Potrošnja električne energije

Opće poznato je kako proces „rudarenja“ zahtjeva značajnu količinu resursa. Bilo da se radi o osobnim računalima koja su nadograđena s dodatnim grafičkim procesorskim jedinicama ili o ASIC „rudarima“, hardverske komponente potrebne za „rudarenje“ snagom i cijenom često puta višestruko nadmašuju one potrebne za prosječnu upotrebu. Posljedično, već snaga hardverskih komponenti rezultira i većom potrošnjom električne energija. Upravo potrošnja električne energije je u samom vrhu nedostataka koji se povezuju s Blockchain-om.

Vezano za potrošnju električne energije, zanimljivo je spomenuti podatak iz travnja tekuće godine, a koji kaže kako na svjetskoj razini samo Bitcoin, najveća svjetska kriptovaluta, trenutno godišnje potroši 150 teravat sati električne energije, više od cijele Argentine, države s 45 milijuna stanovnika. Sukladno navedenom, Bitcoin kao kriptovaluta se na svjetskoj razini rangira među tridesetak država koje troše najviše električne energije. Ako se uzme u obzir kako je Bitcoin pušten u rad početkom 2009. godine te je značajniji rast zabilježio tek nekoliko godina kasnije, a već sada potrošnja električne energije je na jako visokoj razini, bojazan kako će ionako visoka trenutna potrošnja električne energije i dalje nastaviti eskalirati definitivno nije neopravdana. Valja napomenuti kako se velika potrošnja energije primarno veže za „rudarenje“ sukladno Proof-of-Work konsenzusu, što predstavlja jedan od argumenata za prebacivanje s Proof-of-Work konsenzusa na npr. Proof-of-Stake konsenzus.

3.2.2. Nepovoljan utjecaj na okoliš

Na prethodno spomenutu visoku potrošnju električne se direktno veže i negativan utjecaj Blockchain-a na okoliš. Ipak, treba uzeti u obzir kako sama visoka potrošnja električne energije nije dovoljan pokazatelj negativnog utjecaja na okoliš. Naime, potrebno je razmotriti i izvore iz kojih se električna energija dobiva. Budući kako električna energija dobivena iz fosilnih goriva nanosi više štete okolišu od električne energije dobivene iz obnovljivih izvora energije, kao što je npr. električna energija dobivena putem solarnih panela, problematika visoke potrošnje električne energije potrebne za rad Blockchain-a zahtjeva da se u obzir uzme i

struktura izvora električne energije. Nažalost, za sada je i dalje ne postoje u potpunosti točni podaci koji bi dali jasniju sliku o izvorima električne energije koja se koristi isključivo za pogon Blockchain-a, budući kako se radi o sustavu koji je distribuiran diljem cijelog svijeta te se razlikuje od države do države, ili čak i među regijama unutar većih država.

3.2.3. Crno tržište i „deep/dark web“

Prije nego se opiše uloga Blockchain-a u trgovini na crnom tržištu, odnosno na „deep web-u" ili "dark web-u“, potrebno je objasniti od čega se sastoji Internet. Internet, kao globalna mreža, sastoji se od više usluga, kao što su npr. e-pošta, prijenos datoteka ili spajanje na udaljena računala, te koje funkcioniraju putem svojih protokola, od kojih se kao primjer mogu navesti HyperText Transfer Protocol Secure (HTTPS), vezan za World Wide Web (WWW), Simple Mail Transfer Protocol (SMTP), vezan za e-poštu, File Transfer Protocol (FTP), vezan za prijenos datoteka, ili Telnet, vezan za spajanje na udaljena računala. Većina korisnika Interneta pristupa Internetu putem usluge WWW, koja označava globalnu mrežu na kojoj se nalaze internetske stranice, a kojima se pristupa putem internetskog preglednika. Internetske stranice kojima se pristupa putem WWW-a su indeksirane, što znači da su prošle kroz proces u kojemu pretraživači pretražuju Internet kako bi otkrili internetske stranice i informacije o njima pohranili u organiziranu bazu podataka zvanu indeks. Pretraživanje u svrhu indeksiranja se vrši pomoću „pauka“, softvera koji pronalazi i indeksira stranice na Internetu, stoga je pristup takvim stranicama maksimalno olakšan. Međutim, WWW predstavlja samo jedan manji, „površinski“ sloj Interneta, za koji se uglavnom pretpostavlja kako sačinjava najviše 5% Interneta.

Pored „površinskog“ sloja Interneta, postoje još i „deep web“ te „dark web“. „Deep web“ se odnosi na kategoriju sadržaja na Internetu koji, iz različitih tehničkih razloga, nije indeksiran od strane pretraživača, te mu se zbog toga ne može pristupiti putem tradicionalnih pretraživača. Za „dark web“ se može reći kako predstavlja još dublji dio „deep web-a“. Budući kako se stranicama na „deep web-u“ i „dark web-u“ se ne može pristupiti na način kakav se viđa na „površinskom“ sloju Interneta, pristupa im se ili putem autentikacije, a što se može vršiti putem npr. korisničkog imena i lozinke, (u slučaju „deep web-a“) ili putem specijaliziranih

internetskih pretraživača (u slučaju „dark web-a“), od kojih je svakako najpoznatiji Tor, no postoje i I2P, Yandex, Tails i Freenet te drugi.

„Dark web“ je sloj Interneta zloglasan po raznim ilegalnim sadržajima, koji bi na „površinskom“ sloju Interneta brzo bili cenzurirani ili uklonjeni. Međutim, radi anonimnog karaktera koji „dark web“ posjeduje, a koji se postiže posebnim karakteristikama specijaliziranih internetskih pretraživača koji prikrivaju adrese korisnika te korištenjem VPN-ova, „dark web“ je prepun sadržaja koji se ciljano prikrivaju od dohvata korisnika „površinskog“ Interneta. Vezano za VPN-ove, radi se o privatnim virtualnim mrežama koje maskiraju IP adresu korisnika, kako bi onemogućila praćenje pri pretraživanju Interneta. Neki od primjera trgovine ilegalnim sadržajima na „dark web-u“ koji se mogu navesti su ilegalna prodaja oružja, narkotika, ukradenih bankovnih podataka i trgovina ljudima. Radi se o teškim kršenjima zakona, stoga trgovci i kupci takvih sadržaja uglavnom ulažu velike napore kako bi svoje identitete sačuvali anonimnima. Upravo ovdje Blockchain igra veliku ulogu, primarno putem kriptovaluta. Kako je već ranije spomenuto u dijelu koji ovog rada koji govori o prednostima Blockchain-a, odnosno anonimnosti, kriptovalute se uvelike koriste za kupovinu ilegalnih proizvoda i usluga, budući kako je takvoj metodi plaćanja poprilično ući u trag. Radi navedenog se može reći kako karakteristika anonimnosti koja obilježava Blockchain u isto vrijeme predstavlja i prednost i nedostatak Blockchain-a.

Jedan od najpoznatijih primjera koji u vezu dovodi crno tržište i kriptovalute je onaj o stranici Silk Road [4]. Tijekom gotovo dvije i pol godine, „podzemna“ internetska stranica poznata kao Silk Road je korištena od strane nekoliko tisuća narko dilera i ostalih nezakonitih trgovaca za distribuciju stotina kilograma ilegalnih narkotika i ostalih nezakonitih dobara i usluga za preko sto tisuća kupaca te za pranje stotina milijuna dolara proizašlih iz tih nezakonitih transakcija. Naposljetku, vrijedi spomenuti i kako nije sav sadržaj na „deep web-u“ i „dark web-u“ ilegalan, budući kako se navedena dva sloja Interneta koriste i za enkriptiranu komunikaciju u vojne

[4] Hrv. „Put svile“, asocira na drevne rute koje su povezivale Kinu i Indiju sa zapadom. Izvor: https://www.britannica.com/topic/Silk-Road-trade-route.

svrhe, u svrhu novinarstva ili izbjegavanja cenzuriranja određenih sadržaja u pojedinim državama.

3.2.4. Financiranje terorizma i pranje novca

Decentralizacija, anonimnost i automatizam, kao jedne od glavnih karakteristika Blockchain-a, predstavljaju plodno tlo za trgovinu i financiranje ilegalnih aktivnosti. Nastavno na prethodni dio o crnom tržištu i „deep/dark web-u“, postoji opravdana bojazan kako će Blockchain, odnosno kriptovalute, uvelike pomoći u financiranju terorizma. Budući kako je Blockchain i dalje relativno nova tehnologija, kriptovalute i dalje nisu zakonski precizno i detaljno regulirane kao klasični novac ili vrijednosni papiri. Pojedine države su u posljednjih desetak godina pokušale zabraniti ili barem strože regulirati kriptovalute, no uspjesi su poprilično upitni.

Transakcijama izvršenim u kriptovalutama putem Blockchain-a je teško ući u trag jer se ne izvršavaju putem jedne centralne institucije, odnosno putem jednog poslužitelja, a adrese sudionika transakcija zapravo ne otkrivaju prave identitete sudionika. Enkripcija je jedan od temelja Blockchain-a, a u kombinaciji sa TOR mrežom računala koja posreduju između računala klijenta i računala poslužitelja, te s VPN-ovima, što sve zajedno izrazito otežava bilo kakvo praćenje ili regulaciju transakcija u kriptovalutama. Iz navedenog je jasno kako Blockchain predstavlja moćan alat za ilegalnu trgovinu i pranje novca, pa ne treba čuditi što pojedine vlade i vladine organizacije nisu oduševljene njegovom pojavom i razvojem.

4. POSTOJEĆE PRIMJENE BLOCKCHAIN-A

Već i površnom pretragom na Internetu s upitom o primjenama Blockchain-a dolazi se do desetaka rezultata, i to u raznim društvenim sferama, bilo da se radi o financijskom sektoru, energetici, zdravstvu, trgovini nekretninama ili nečemu drugom. Aktualnih primjena Blockchain-a je mnogo, a u ovom radu će biti opisan dio za koji se može reći da trenutno među najznačajnijima. Također, i sam Internet je doživio transformaciju pojavom Blockchain-a, pa je u nastavku potrebno i o tome posvetiti dio teksta.

4.1. Web3

Odmah na početku valja napomenuti kako Internet strogo gledano ne poznaje različite verzije, već se nazivi kao što su web1 ili web 2.0. u žargonu koriste kako bi opisali skup noviteta koji svi zajedno doprinose drugačijem iskustvu Interneta. Prvom verzijom Interneta, odnosno web1, može se nazvati Internet u razdoblju koje je trajalo od početaka masovne upotrebe Interneta do kraja prošlog, odnosno početka ovog stoljeća.

Web1 karakteriziraju statičke internetske stranice, kreirane u cijelosti putem HTML-a, jezika za web koji definira strukturu internetskih stranica, te minimalna interakcija korisnika i internetskih stranica. Ukratko, korisničko iskustvo na web1 Internetu je bilo poprilično skromno. Korisničko iskustvo do izražaja dolazi u razdoblju koje se može nazvati web2, a koje okvirno započinje polovicom prvog desetljeću novog milenija. Upotrebom CSS-a , jezika koji precizira na koji način se dokumenti (najčešće HTML) prikazuju korisnicima, odnosno na koji način su stilizirani, postavljeni, itd., te JavaScript-a, skriptnog programskog jezika koji se koristi za kreiranje i kontrolu dinamičkog sadržaja na internetskim stranicama, a koji su poslužili kao dopuna HTML-u, internetske stranice postaju vidno privlačnije korisnicima, upotrebom animacija i stiliziranih fontova te pozadina. Web2 možda ponajviše karakteriziraju društvene mreže, blogovi i prikazivanje video sadržaja, te se može reći kako se i dalje nalazimo u razdoblju u kojemu dominira web2.

Naposljetku, web3 je „sljedeća velika stvar“. Ako se napravi usporedba s Blockchain-om, i web3 se bazira na decentralizaciji i izostanku povjerenja prema trećim stranama, primarno državnim tijelima i privatnim poduzećima. U svojoj srži, web3 koristi Blockchain, kriptovalute i NFT-e kako bi moć vratio natrag korisnicima, u vidu vlasništva. Pod vlasništvom se podrazumijeva činjenica kako će digitalna imovina koju određena osoba posjeduje biti postojana te neće ovisiti o pojedinačnom korisničkom računu, odnosno kako gašenje računa ne znači i nestanak digitalne imovine, već će se imovina moći trajno prodavati, razmjenjivati i prenositi. Na taj način se može govoriti i o NFT-ima. Nadalje, web3 se još naziva i semantički web, što upućuje na to kako se radi o web-u u kojemu bi strojevi obrađivali sadržaj na način kako bi to radio čovjek, gdje bi cjelokupni podaci bili povezani i shvaćeni, konceptualno i kontekstualno, a što bi dovelo do začetka AI-a i ML-a. AI označava skraćenicu naziva Artificial Intelligence, odnosno umjetnu inteligenciju, koja utječe na računala i strojeve kako bi imitirali sposobnosti rješavanja problema i donošenja odluka poput ljudskog uma. ML označava skraćenicu naziva Machine Learning, odnosno strojno učenje, a koje predstavlja granu AI-a i računalne znanosti koja se usredotočuje na korištenje podataka i algoritama, a kako bi imitirala način na koji ljudi uče, postupno poboljšavajući preciznost.

4.2. Internet stvari (IoT)

Pojam „Internet stvari“ (IoT) [5] je po prvi puta 1999. godine iskoristio britanski tehnološki pionir Kevin Ashton, kako bi opisao sustav u kojemu su objekti iz fizičkog svijeta povezani na Internet putem senzora. Na taj način se kreira mreža uređaja koji su svi međusobno povezani te su u mogućnosti razmjenjivati podatke u stvarnom vremenu i prilagođavati se okolini. Danas pod IoT uređajima podrazumijevamo uređaje kod koji se pojavila mogućnost povezivanja na Internet, no koji tu mogućnost ranije nisu imali, a primjeri se mogu naći svugdje od kućnih uređaja, kao što su kućne lampe i zamrzivači, pa sve do sigurnosnih sustava i sustava za poljoprivredu, a kao bitna stavka u radu IoT uređaja se svakako treba navesti njihova autonomija. Kao i u dosta drugih područja, Blockchain je pronašao primjenu i kod IoT uređaja. IoT omogućuje uređajima diljem Interneta slanje podataka privatnim Blockchain mrežama, a kako bi se kreirali zapisi o dijeljenim transakcijama koji su otporni na falsificiranje. Bilo da se

[5] Eng. „Internet of Things“.

radi o uređajima koji prate kretanja pošiljki, mehanizaciji u proizvodnim postrojenjima ili zapisima o redovnim kontrolama i servisima voznog parka, Blockchain može predstavljati bitan čimbenik u osiguravanju točnosti podataka.

Kada se spominju IoT uređaji, važno je napomenuti i kako pored IoT uređaja danas poznajemo i „pametne uređaje“ te „povezane uređaje“. Radi se konceptima sličnim Internetu stvari, no ipak ponešto inferiornijima. Kako im i samo ime kaže, pod pojmom „povezni uređaji“ se podrazumijevaju uređaji na koje se moguće povezati iz daljine. Kao primjer se može navesti kućanski uređaj kojemu je putem mobilne aplikacije moguće zadati naredbu da započne s radom, kako bi po dolasku vlasnika uređaja sve već bilo pripremljeno. Iz navedenog je vidljivo kako „povezani uređaji“ praktički nemaju autonomije, već rade prema uputama na daljinu. Pod „pametnim uređajima“ se podrazumijevaju uređaji koji imaju određeni stupanj autonomije u radu, pa tako nakon što se programiraju za neku specifičnu primjenu pojedine zadatke mogu odrađivati i bez potrebe da sa se korisnik svaki puta s njima povezuje. Također, postoje i uređaji koji predstavljaju kombinaciju „pametnih uređaja“ i „ povezanih uređaja“, čime se postiže više funkcionalnosti.

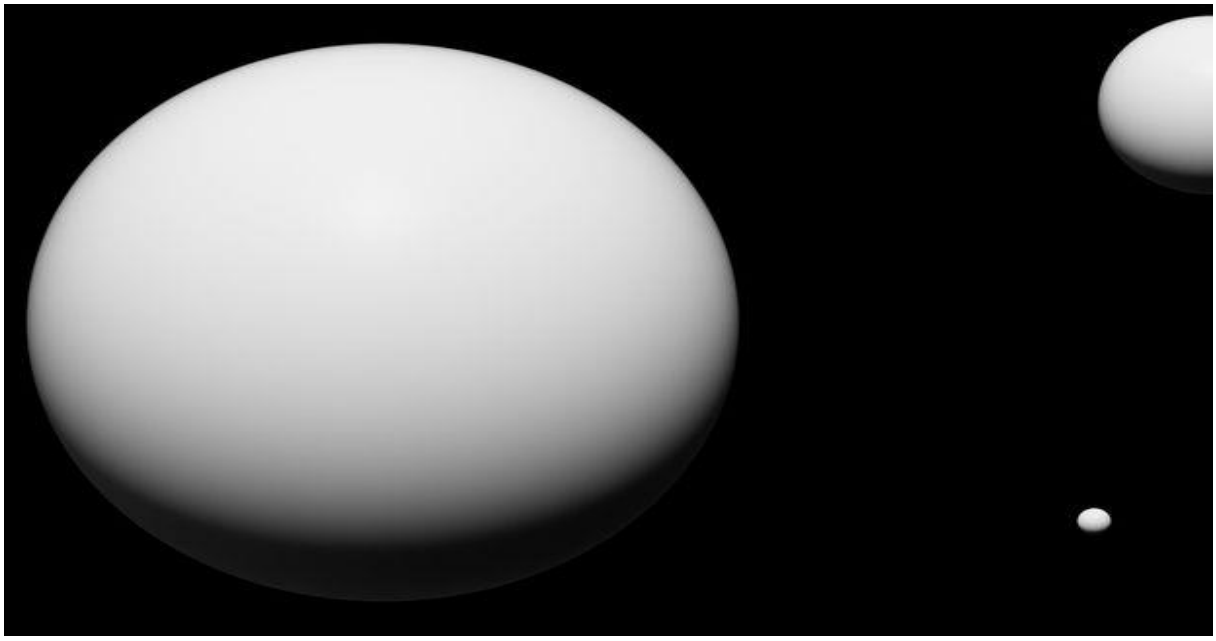
Za kraj, može se spomenuti i kako razni izvori s Interneta predviđaju kako se do 2025. godine očekuje kako će na svijetu postojati između 20 i 30 milijardi IoT uređaja, čime njihova važnost i buduća primjena niti u jednom trenutku ne dolaze u pitanje. Posljedično, povećanjem broja IoT uređaja može se očekivati kako će i Blockchain dodatno dobiti na značaju, ponajviše radi karakteristike sigurnosti.

4.3. Non-Fungible Tokens (NFT)

NFT-i, jedinstveni tokeni ili nedjeljivi tokeni, pored kriptovaluta, vjerojatno predstavljaju trend koji je najviše pripomogao približavanju Blockchain-a široj javnosti. Iako pojedince mogu začuditi novčani iznosi za koje se prodaju pojedini NFT-i, kao što su slike nekih od simbola popularne kulture, treba uzeti u obzir kako su vrijednosti svih valuta, vrijednosnih papira ili dragocjenih materijala u nekoj mjeri samo rezultat društvenog konsenzusa kojim im se daje na

vrijednosti. Specifičnost NFT-a, u odnosu na npr. papirnati novac, dionice ili zlato, jeste što su NFT-i neopipljivi, pa se pri prvoj pomisli čini kako nemaju značajnu vrijednost. Međutim, NFT-i mogu predstavljati digitalni primjerak fizičkog objekta kao što je nekretnina, npr. stambeni objekt. Na taj način se trgovinom NFT-ima zapravo može trgovati fizičkim objektima, koji se u digitalnom obliku manifestiraju kao npr. slike ili animacije. Sama slika ili animacija se često puta ne pohranjuju na Blockchain-u, jer se takva vrsta pohrane smatra skupom, već se pohranjuju ili na centraliziranoj bazi podataka ili na decentraliziranoj bazi podataka, kao što su Interplanetary File System (IPFS) ili Arweave, koje su prikladnije za pohrane većih datoteka. Kao pojašnjenje se može navesti kako IPFS predstavlja sustav za verzioniranje datoteka koji može pohranjivati datoteke i pratiti verzije datoteka kroz vrijeme, poput Git-a. Sami NFT-i se pohranjuju u virtualnim novčanicima kao kod, te upućuju na lokaciju slike ili animacije. U svojoj srži, virtualni novčanik je program koji je u mogućnosti primati, slati i pohranjivati kod koji predstavlja valutu.

Kada se priča o Blockchain-ima na kojima NFT-i prebivaju, najveću ulogu svakako ima Ethereum. NFT-i su po prvi puta predloženi u Ethereum Improvement Proposals (EIP) 721 te su daljnje razvijeni u EIP-1155. Vezano za EIP-e, radi se o prijedlozima za poboljšanje Ethereum Blockchain-a, a sami NFT-i koriste pametne ugovore, koji predstavljaju jednu od glavnih karakteristika Ethereum-a. Osim Ethereum-a, NFT-i se mogu pronaći i na još nekim Blockchain-ima kao što su Solana, Tezos, Hive, Polkadot te još neki, no NFT-i se i dalje primarno spominju u kontekstu Ethereum-a. Neke od najpoznatijih trgovina NFT-ima koje se mogu pronaći na Internetu uključuju Rarible, OpenSea, Binance i Nifty Gateway, no postoji i značajan broj drugih trgovina. Naposljetku, a kako bi se dočarao fenomen NFT-a, valja spomenuti zanimljivost o trenutno najvišem iznosu ikada plaćenom za NFT. Radi se o NFT-u nazvanom „The Merge" (hrv. "Spajanje"), koji se u prosincu 2021. godine prodao za 91,8 milijuna američkih dolara.



Slika 8: „The Merge“ NFT

4.4. Decentralizirane financije (DeFi)

DeFi označava skraćenicu pojma decentralizirane financije. Jedan od glavnih ciljeva decentraliziranih financija je eliminacija potrebe za posrednikom pri izvršavanju financijskih poslova, odnosno transakcija. Na taj način se oduzima kontrola iz ruku državnih i privatnih banaka te drugih financijskih institucija, koje pri izvršavanju klasičnih transakcija imaju uvid u podatke pošiljatelja i primatelja te uvid u detalje samih transakcija. Pri tomu je vidljiva naglašena karakteristika anonimnosti sudionika transakcija koja, naposljetku, predstavlja jedno od primarnih obilježja i cjelokupne Blockchain tehnologije. Nadalje, korištenje određenih usluga decentraliziranih financija omogućuje primjenu jedinstvenih naknada za provođenje transakcija, neovisno o lokaciji na kojoj se odvijaju, a što nije slučaj s klasičnim financijskim posrednicima.

Kao i u slučaju NFT-a, i decentralizirane financije se primarno vežu za Ethereum Blockchain, no postoje i alternative. Kao neke od alternativnih trgovina i mjenjačnica kriptovaluta mogu se spomenuti Venus Finance i PancakeSwap, koji se baziraju na BNB Blockchain-u, Newdex,

baziran na EOS Blockchain-u ili JustLend i JustSwap, bazirani na TRON Blockchain-u. Kao što je slučaj sa bankama, mjenjačnicama ili kreditnim ustanovama, decentralizirane financije također pružaju usluge razmjene valuta i kriptovaluta te pozajmljivanje novca, koristeći se pametnim ugovorima. Međutim, pored nabrojanoga, postoje i neke usluge koje su specifične za decentralizirane financije i kriptovalute, kao što je npr. „omatanje“ Bitcoin-a [6], kako bi se transakcija u Bitcoin-ima mogla izvršiti na Ethereum Blockchain-u. Naime, budući kako se radi o različitim Blockchain tehnologijama, pri prijenosu kriptovalute je potrebno koristiti svojevrsni adapter, odnosno „omatanje“. Pored navedenog, potrebno je istaknuti i mogućnost vezivanja određene kriptovalute za tradicionalnu valutu [7], kao što su npr. euro ili dolar, te mogućnost predviđanja i klađenja na buduće događaje, bilo da se radi o predviđanjima vezanim za fluktuaciju vrijednosti kriptovaluta, rezultate sportskih natjecanja ili čak mogućnosti pojave novih pandemija i ratova.

Osim pojma decentraliziranih financija, često se koristi i pojam decentraliziranih aplikacija. Iako su zapravo jako slični, navedeni pojmovi ipak nose dvije značajne razlike. Kao prva razlika se ističe činjenica kako su decentralizirane financije izgrađene na decentraliziranim aplikacijama, te se više koriste u komercijalne svrhe. S druge strane, decentralizirane aplikacije imaju primjenu i van područja financija, kao što su razvoj aplikacija za računalne igrice, internetski preglednici, kockanje, edukacija, itd. Druga ključna razlika je što su decentralizirane financije ograničene na Blockchain, dok s druge strane decentralizirane aplikacije rade na mreži ravnopravnih računala, koristeći pametne ugovore za ispravan rad, što zahtjeva konsenzuse za bilo kakve izmjene nakon puštanja u rad.

4.5. Decentralizirane autonomne organizacije (DAO)

Kako je već iz naziva decentraliziranih autonomnih organizacija vidljivo, takve organizacije slijede filozofiju samog Blockchain-a te kroz demokratski i ravnopravan način omogućuju

[6] „Wrapped“ Bitcoins (WBTC).

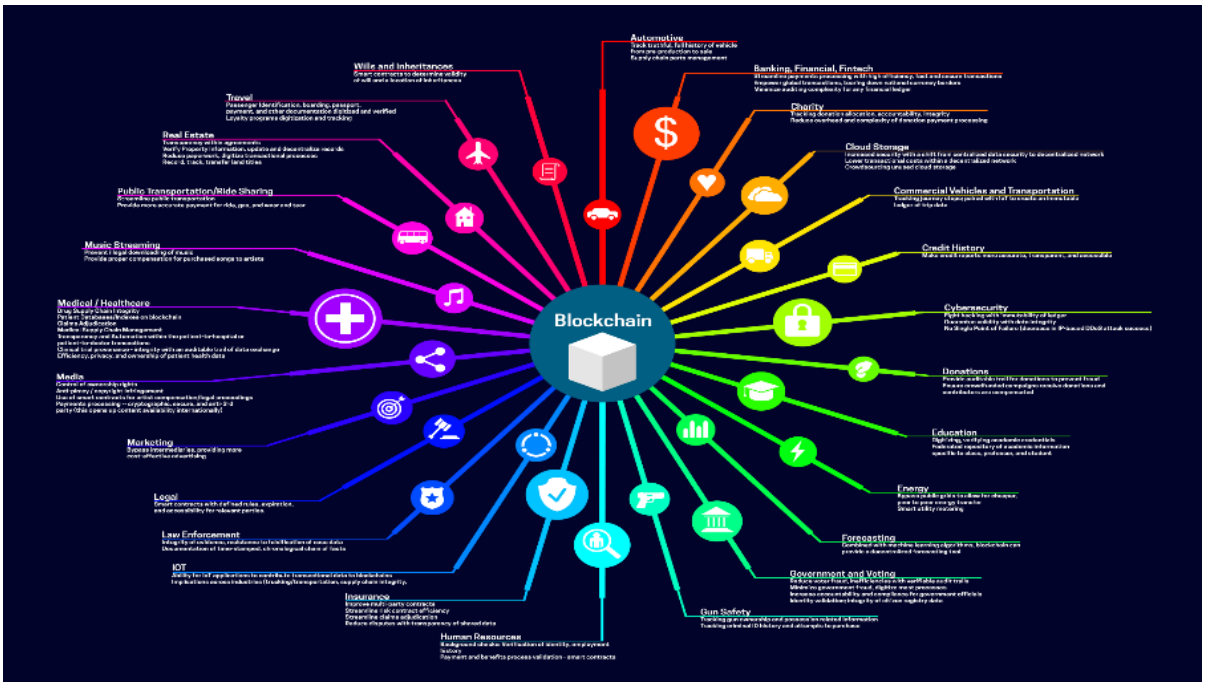
[7] Eng. „stablecoin“.

donošenje odluka koje vode zajedničkim ciljevima svih pojedinaca koji čine takvu organizaciju. Koristeći pametne ugovore, takve organizacije omogućuju pojedincima koji se međusobno nikada nisu osobno upoznali suradnju na projektima uz gotovo potpunu sigurnost kako se sve odluke donose prema unaprijed dogovorenim pravilima. Može se reći kako na neki način pojedinci u decentraliziranim autonomnim organizacijama u isto vrijeme predstavljaju i vodstvo organizacije, budući kako svačiji glas nosi određenu važnost u donošenju odluka te doprinosi usmjeravanju organizacije u određenom smjeru, i zaposlenike organizacije, budući kako kvaliteta donesenih odluka svima diktira uspješnost i očuvanje posla u organizaciji.

Iako u teoriji demokratski pristup pri donošenju odluka, kojim se velikom broju ljudi dopušta ravnopravno sudjelovanje u upravljanju organizacijom, zvuči sjajno, upravo ta demokratičnost i mnogobrojnost sa sobom nose i neke od najvećih poteškoća koje se vežu za decentralizirane autonomne organizacije. Pri klasičnom glasanju pojedinaca u takvim organizacijama, gdje je potrebno postići kvorum, odluke se u praksi donose sporo te se zahtjeva veliki angažman pojedinaca u organizaciji. To znači kako će se u slučajevima gdje je potrebno reagirati na promjene u okolini organizacije koje se oslanjaju isključivo na kvorum pri donošenju odluka naći u nezavidnim pozicijama. Nadalje, svakako treba uzeti u obzir i kako svi članovi unutar organizacije nisu jednako kompetentni u donošenju odluka, pa odluka koja je donesena većinom glasova ne mora nužno biti i najkvalitetnija odluka. Svjesni prethodno navedenih ograničenja koja su prisutna pri klasičnom donošenju odluka većinom glasova, razni kolektivi su razvili više alternativnih modela decentraliziranih autonomnih organizacija. Kao neki od primjera se mogu navesti organizacije čije uloge članova se temelje na tokenima ili udjelima, organizacije sa članstvima temeljenima na reputacijama članova, organizacije Moloch u kojima se odluke donose relativnom većinom glasova, odnosno usporedbom samo glasova „za“ i glasova „protiv“ te izostavljajući neutralne članove. Prethodno navedeni alternativni modeli pokušavaju ublažiti ili u potpunosti ukloniti nedostatke osnovnog modela decentraliziranih autonomnih organizacija. Osim po načinu glasanja, decentralizirane autonomne organizacije se mogu razlikovati i po namjeni, pa tako poznajemo organizacije usmjerene na protokole, investicijske organizacije, organizacije društvenih mreža, kolekcionarske organizacije i filantropske organizacije, iz čijih naziva su zapravo poprilično jasne namjene kojima takve organizacije služe.

5. POTENCIJALNE BUDUĆE PRIMJENE I RAZVOJ BLOCKCHAIN-A

Blockchain već danas broji mnoge primjene u različitim područjima, iako se i dalje radi o relativno mladoj tehnologiji uz koju se primarno vežu kriptovalute, a posebice Bitcoin. Slika u nastavku prikazuje popriličan broj područja koja koriste beneficije Blockchain tehnologije.

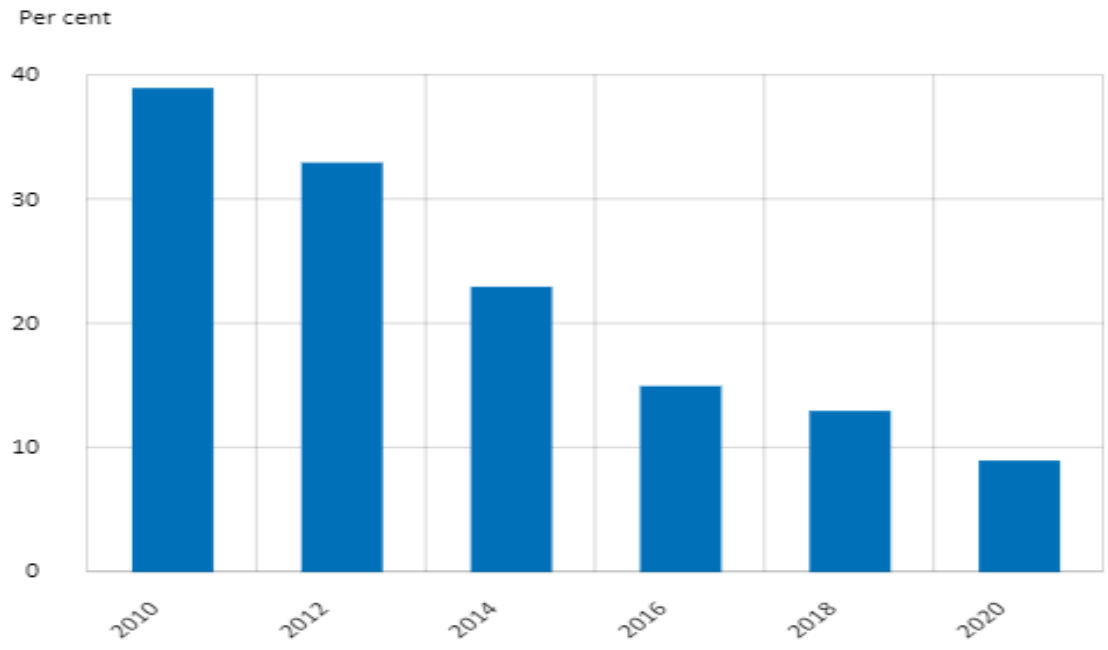


Slika 9: Prikaz nekih od primjena Blockchain-a

Kako je vidljivo iz prethodne slike, Blockchain je pronašao primjene u gotovo pa svim sferama ljudskog djelovanja. Auto industrija, bankarstvo, kibernetička sigurnost, mediji, trgovina nekretninama, ali i mnoga druga područja mogu iskoristiti karakteristike koje sa sobom donosi Blockchain, kako bi se unaprijedila ili u potpunosti transformirala. Jedan dio primjena Blockchain-a prikazanih na slici je opisan u prethodnom poglavlju, a u nastavku se navode neki primjeri potencijalnih budućih primjena Blockchain-a.

5.1. Zamjena fizičkoj valuti

Plaćanje bez posredovanja fizičkog novca, korištenjem bankovnih kartica, već danas predstavlja svakodnevicu koja je općeprihvaćena. Osim što se za plaćanja bankovnim karticama može reći kako predstavljaju bržu i praktičniju metodu plaćanja od plaćanja fizičkim novcem, pojavom epidemije koronavirusa je takav beskontaktni način plaćanja posebice došao do istaknute uloge. Kao država koja je na putu da postane prva država bez fizičkog novca se ističe Kraljevina Švedska. Podaci iz 2020. godine objavljeni na internetskim stranicama švedske Riksbanke pokazuju kako je postotak ljudi koji su u 2020. godini pri svojoj posljednjoj kupovini koristili fizički novac manji od 10%.



Slika 10: Prikaz plaćanja fizičkim novcem u Kraljevini Švedskoj u razdoblju od 2010. godine do 2020 godine.

Značajan podatak s prethodne slike predstavlja i činjenica kako je u relativno kratkom razdoblju od 2010. godine do 2020. godine korištenje fizičkog novca pri posljednjoj kupovini palo za čak 30%. Navedeni podatak pokazuje kako kod ljudi postoji velika spremnost na zamjenu fizičkog novca alternativnim načinima plaćanja. Naravno, Kraljevina Švedska gotovo

pa sigurno ne može se uzeti kao apsolutno mjerilo koji će ostatak svijeta odmah objeručke prihvatiti. Međutim, ipak može poslužiti kao interesantna naznaka mogućeg pravca u kojemu će ići plaćanja u budućnosti, gdje kriptovalute i Blockchain potencijalno mogu odigrati ključnu ulogu.

Vezano za digitalne valute, valja ukazati na razliku između dvije vrste digitalnih valuta. Jedna vrsta digitalnih valuta su valute koje služe specifičnoj svrsi, kao npr. valute koje se koriste u igrama na Internetu, ili koje su pod nadzorom određene financijske institucije. Central Bank Digital Currency (CBDC) predstavlja digitalnu valutu, koju nadziru Federalne rezerve u Sjedinjenim Američkim Državama, a kao primjer digitalne valute specifične za određeno poduzeće se može navesti Amazon Coins. Drugi primjer digitalnih valuta, koji bi potencijalno u budućnosti mogao dobiti još značajniju primjenu, su kriptovalute. Iako primjer Kraljevine Švedske i prijelaza s plaćanja fizičkim novcem na plaćanja bankovnim karticama demonstrira visoku razinu povjerenja koje građani u toj državi imaju prema financijskim institucijama, ono što kriptovalute čini privlačnima je upravo mogućnost izostavljanja financijskih institucija kao posrednika u plaćanjima. Uzme li se u obzir kako banke i druge financijske institucije koriste novac građana za vlastite investicije na financijskom tržištu, nije teško razumjeti zašto bi bilo razumno potražiti alternativne mehanizme za transakcije. Blockchain kao temelj za funkcioniranje kriptovaluta pruža upravo jednu takvu alternativu.

5.2. Lanac opskrbe

Rastom broja proizvođača i distributera te pristupom robi iz svih dijelova svijeta, sve je teže pratiti put robe od proizvođača do potrošača. Bilo da se radi o prehrambenim namirnicama, farmaceutskim proizvodima ili nečemu trećem, može se pretpostaviti kako većina ljudi preferira, ukoliko je moguće, znati od kuda dolaze proizvodi koje konzumiraju. Porijeklo proizvoda u svijesti potrošača često puta garantira kvalitetu, trajnost, zdravlje ili nešto drugo, ovisno o kakvom tipu proizvoda se radi. Sukladno navedenim očekivanjima, proizvođači proizvode koji se percipiraju kao proizvodi koji opravdavaju pozitivna očekivanja naplaćuju po višim cijenama. Ukoliko su potrošači spremni platiti više cijene proizvoda, svakako žele i

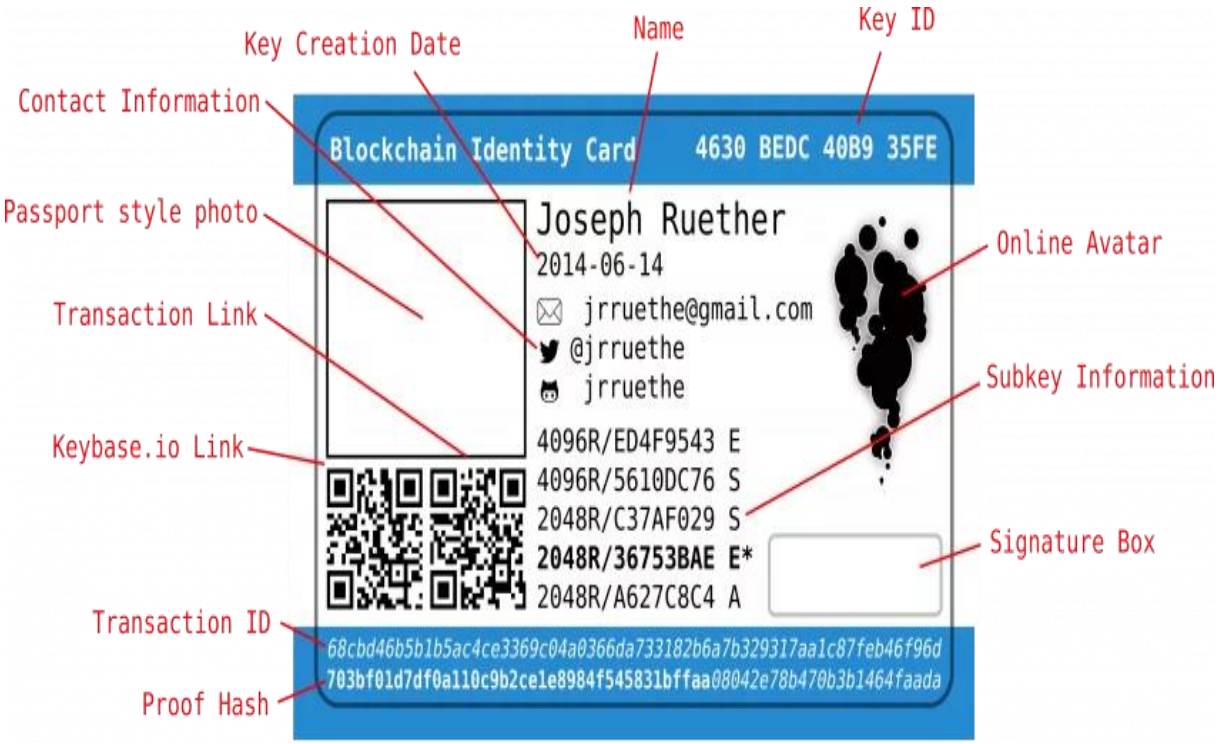
biti u mogućnosti potvrditi porijeklo takvih proizvoda, koje bi opravdalo više cijene. Iz prethodno navedenog je vidljivo kako postoje razni objektivni razlozi za težnju pouzdanim podacima o lancu opskrbe.

Papirnati zapisi su podložni manipulacijama, kao i standardni digitalni zapisi. Međutim, neizmjenjivost kao jedno od svojstava Blockchain-a, spomenuto u ranijem poglavlju ovog rada koje se bavi opisom prednosti i nedostataka Blockchain-a, može uvelike pripomoći pouzdanosti lanca opskrbe. Praćenjem i evidentiranjem robe tijekom cijelog ciklusa, od vađenja sirovina do prodaje gotovih proizvoda potrošačima, Blockchain omogućuje transparentnost i vjerodostojnost podataka o porijeklu proizvoda. Posljedično, raste i povjerenje među samim dobavljačima, koji pri formiranju proizvoda mogu biti sigurni kako dobivaju sirovine koje očekuju. Naposljetku, kao rezultat istovremene umiješanosti više strana u kreiranju zapisa, odnosno blokova u Blockchain-u lanca opskrbe, olakšava se i mogućnost kreiranja jedinstvenih standarda za kreiranje zapisa, čime podaci među više poduzeća postaju međusobno kompatibilni. Na taj način je lakše vršiti razmjenu te analizu podataka o sirovinama i gotovim proizvodima.

5.3. Digitalni identitet

Pored problema s anonimnošću na Internetu, postoji i značajan primjer utvrđivanja identiteta te krađe identiteta. Podaci iz 2018. godine procjenjuju kako postoji otprilike jedna milijarda ljudi bez službenog dokaza o identitetu. Bez potvrde identiteta nije moguće upisati se u školu, prijaviti se za poslove, napraviti putovnicu ili pristupiti mnogim javnim uslugama, a posjedovanje identiteta je ključno i za pristup postojećim financijskim uslugama. S druge strane, 60% od 2,7 milijardi ljudi koji nemaju račune u bankama posjeduju mobilne telefone, čime je utrt put prema mobilnim rješenjima vezanim za identitet, koji se temelje na Blockchain-u te koji bi bili podobniji potrebama ranjivih građana. Naravno, ne bi se trebalo ograničiti samo na mobilna rješenja. Nadalje, vezano za krađe identiteta, podaci Federalne trgovinske komisije (FTC) u SAD-u navode kako je samo u SAD-u 2021. godine bilo gotovo 1,4 milijuna prijava krađe identiteta. Jasno je kako se radi o izrazito velikoj brojci, a broj je još i veći na razini cijelog svijeta.

Blockchain ima potencijal značajno umanjiti mogućnost krađe identiteta, a predstavlja i način za sigurnije utvrđivanje identiteta. Identifikacija putem Blockchain-a bi se mogla kombinirati s drugim načinima autentikacije, bilo da se radi o biometrijskoj autentikaciji, dvofaktorskoj autentikaciji ili nečemu trećem. Poput Bitcoin-a, koji zahtjeva jedinstveni ključ kako bi se pristupilo sredstvima, osobna iskaznica temeljena na Blockchain-u bi od pojedinca pod čijom je brigom zahtijevala autorizaciju pristupa. U nastavku je na slici prikazan primjer potencijalne osobne iskaznice temeljene na Blockchain-u, kreiran od strane poduzeća DevTeam.Space.



Slika 11: Primjer osobne iskaznice temeljene na Blockchain-u

Kako je vidljivo na slici 11, osobna iskaznica temeljena na Blockchain-u, pored elemenata karakterističnih za klasičnu osobnu iskaznicu kao što su ime, prezime, potpis i fotografija osobe, sadrži i specifične elemente kao što su npr. transakcijski broj (ID) i potvrdni hash.

5.4. Glasovanje

Glasovanje je temelj demokracije, kako na razini država, tako i na nižim razinama kao što su lokalne samouprave ili dionička društva. Budući kako se upravo glasovanjem najčešće donose ključne odluke vezane za izbor rukovodećih osoba te strateške i druge odluke, od iznimne je važnosti da proces glasovanja bude legitiman i oslobođen od bilo kakvog oblika manipulacije. Vrijedi spomenuti primjer predsjedničkih izbora u SAD-u 2016. godine, u kojemu su, prema slijedu događanja objavljenom od strane CNN-a, ruski hakeri prvo preuzeli kontrolu nad jednim od računala Demokratskog nacionalnog odbora, a zatim i putem zlonamjerne e-pošte [8] saznali podatke o lozinkama za prijavu. Iako se čini kako hakeri na kraju ipak nisu direktno utjecali na glasačke uređaje, te time i na broj i opredjeljenje glasova, jasno je o kakvoj se poteškoći radi ukoliko se otvori prostor za manipulaciju.

Iako se glasovanje putem glasačkih listića provodi već stotinama godina, pa se stoga smatra provjerenom metodom za demokratsko donošenje odluka, i proces glasovanja čeka neizbježna sudbina digitalizacije, kao i mnoge druge procese do sada. Digitalizacija bi uklonila potrebu za osobnim dolaskom glasača na glasačka mjesta, nestao bi problem utjecanja na glasače putem nepropisnih isticanja promotivnih materijala kandidata na izborima, u neposrednoj blizini glasačkih mjesta, a eliminirala bi se i mogućnost pronalaska viška glasačkih listića u glasačkim kutijama, radi čega je izbore na takvom glasačkom mjestu potrebno poništavati i ponovno ponavljati. Međutim, s digitalizacijom dolazi i set problema vezanih za sigurnost, od potvrde identiteta glasača do utvrđivanja valjanosti glasova.

Potvrda identiteta putem Blockchain-a je opisana na prethodnoj stranici, a u kombinaciji s evidencijom glasovanja putem Blockchain-a predstavlja potencijalno rješenje za glasovanje u budućnosti. Blockchain-ove karakteristike sigurnosti i neizmjenjivosti u teoriji bi trebale osigurati vjerodostojnost glasovanja. Blockchain je „append-only" [9], što znači da omogućuje

[8] U ovom konkretnom slučaju radi se o „phishing-u", e-pošti koja za cilj ima od primatelja saznati povjerljive informacije o autentikacijskim podacima ili osobnim podacima.

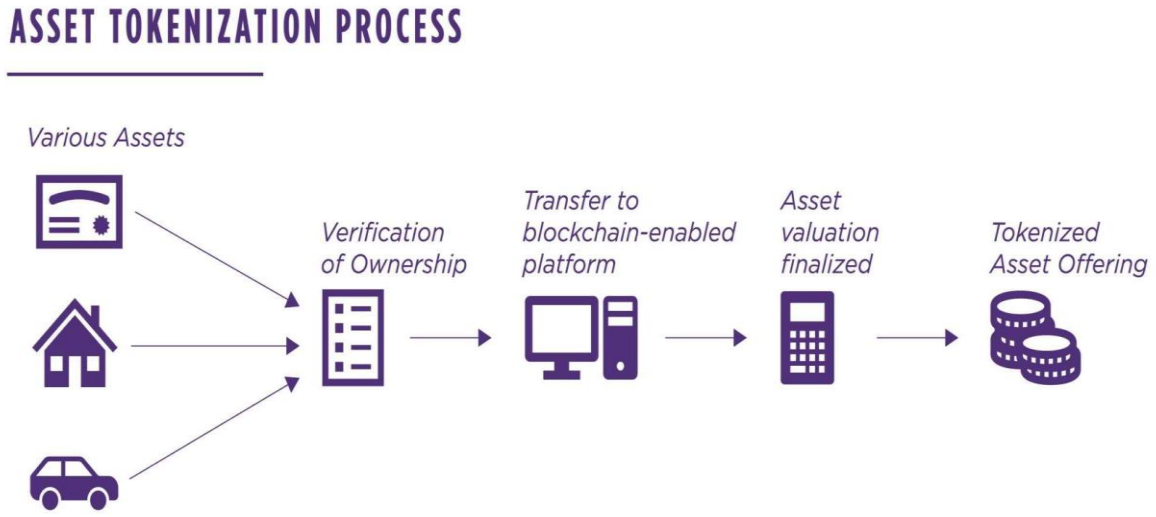
[9] Hrv. „isključivo dodavanje".

dodavanje podataka na kraju, no nikada uklanjanje, a također je i javan te dostupan, što znači da svatko može pročitati podatke te svaki čitatelj vidi zajednički prefiks poretka. Iz navedenog je vidljivo kako bi se, između ostalih, istaknula i karakteristika transparentnosti, kao krucijalan element demokratskog odlučivanja. Naravno, uz korištenje Blockchain-a je potrebno osmisliti i pristupačna korisnička sučelja koja će biti jednostavna i intuitivna za masovno korištenje u procesu glasovanja, neovisno o stupnju informatičke pismenosti korisnika. Također, potrebno je posjedovati i potrebnu informatičku infrastrukturu, s posebnim naglaskom na mrežu povezanih računala na Blockchain-u, koja imaju ulogu distribuirane baze podataka.

5.5. Tokenizacija imovine

U svijetu gdje sve teži povezivanju i brzini, tokenizacija predstavlja alat za pristup imovini koja bi se inače možda činila van dometa. Tokenizacija imovine je proces koji uključuje pretvorbu imovine na Blockchain-u. Obuhvaća materijalnu, kao i nematerijalnu imovinu te se primjenjuje na industrije kao što su financije, umjetnost, trgovina nekretninama i zdravstvena skrb. Radi se o načinu digitaliziranja opipljive i neopipljive imovine i pretvorbe u tokene. Interesantno je što se kroz tokenizaciju imovine materijalna imovina zapravo može raspodijeliti u mnogo malih dijelova, odnosno tokena. Na taj način je moguće sudjelovati u vlasništvu imovine bez potrebe da se ista kupi u cijelosti.

Korištenjem pametnih ugovora, proces kupovine tokena se automatizira, pa se stoga mogu izuzeti posrednici kao što su npr. agencije za promet nekretninama. Trgovinom tokenima preko Blockchain-a se ubrzava sam proces trgovine i prijenosa vlasničkih udjela. Slika u nastavku prikazuje cijeli proces tokenizacije imovine.



Slika 12: Proces tokenizacije imovine

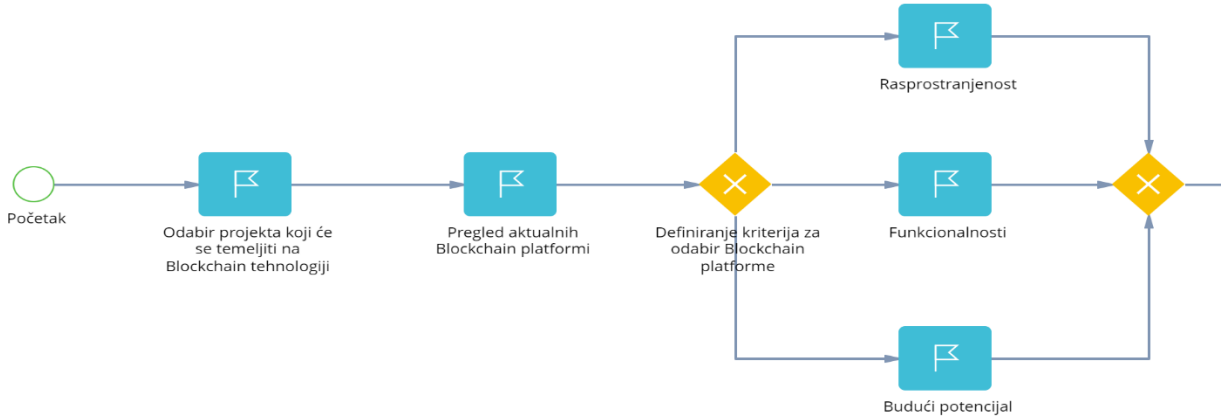
Kako je vidljivo na prethodnoj slici, nakon što se utvrdi vlasništvo nad imovinom, sve se prebacuje na Blockchain, čime se procjena imovine finalizira te se naposljetku nude tokeni koji predstavljaju udjele u imovini.

6. PRAKTIČNI PRIMJER PRIMJENE BLOCKCHAIN-A

Nakon pregleda značajki, prednosti, nedostataka te aktualnih i potencijalnih budućih primjena, u nastavku se navodi i praktični primjer Blockchain-a. Kako će biti vidljivo u nastavku, prije samog kreiranja Blockchain sustava, potrebno je izvršiti značajan broj pripremnih radnji i donijeti odluke u kojemu smjeru će zamišljeni Blockchain ići. Pored tekstualnih opisa, navode se i slikovni prikazi u vidu hodograma, kako bi se uz prikaz potrebnih radnji pobliže dočarala i kronologija događanja. Sam praktični primjer je podijeljen na dva dijela, od kojih prvi dio čini priprema i puštanje u rad Blockchain-a, a drugi dio čini opis zamišljenog Blockchain-a koji je pušten u rad.

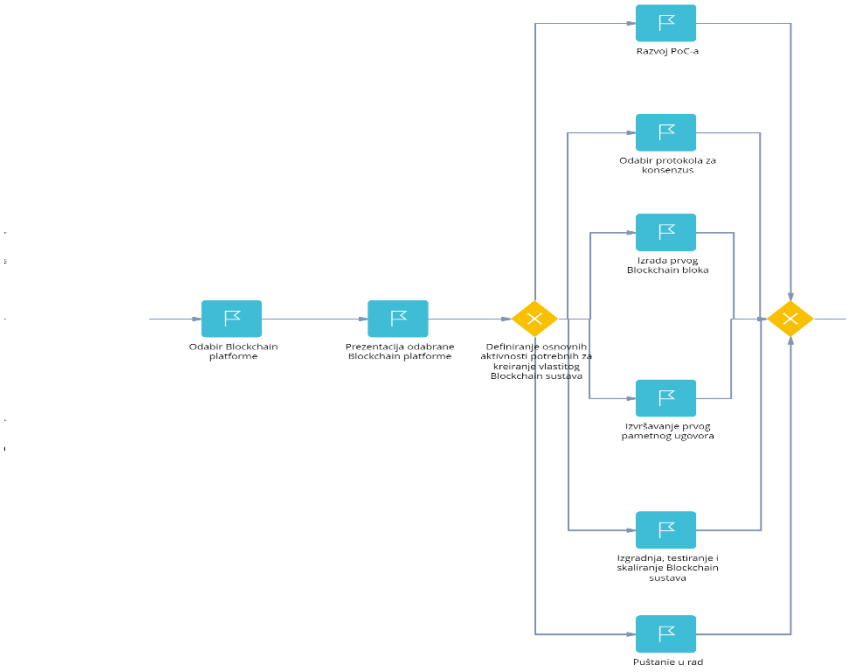
6.1. Priprema projekta

Sve započinje iniciranjem ideje o početku projekta izrade vlastitog Blockchain sustava. Sam projekt za svrhu ima razvoj vlastitog Blockchain sustava za evidenciju dostave pošiljki. Neke od aktualnih Blockchain platformi uključuju Ethereum, Hyperledger Fabric, R3 Corda, Ripple, Quorum, Solana-u, XDC Network, Tezos, Hyperledger Sawtooth, Stellar, EOS, Corda-u, Klaytn, Tron i Hedera Hashgraph. Navedene Blockchain platforme se razlikuju prema popularnosti, namjenama, učinkovitosti, skalabilnosti i sigurnosti. Kako bi se odabrala odgovarajuća Blockchain platforma, prvo je potrebno definirati koji kriteriji će se uzeti u obzir kod donošenja odluke o odabiru. U slučaju ovog projekta, kao tri primarna kriterija su odabrani rasprostranjenost (popularnost) Blockchain platformi te njihove funkcionalnosti i budući potencijal.



Slika 13: Odabir projekta, pregled platformi i definiranje kriterija

Kriterij rasprostranjenosti (popularnosti) je odabran kao bitan kriterij, budući da kao takav čini pokazatelj kako je za očekivati da će odabrana Blockchain platforma i u budućnosti biti relevantna, te kako se može očekivati njen daljnji razvoj. Ovisno o naravi projekta, određene funkcionalnosti Blockchain platformi se nameću kao bitnije od drugih. Neki od primjera su tokeni, pametni ugovori te konsenzusi, odnosno protokoli za konsenzus. Za pretpostaviti je kako se budući potencijal neke Blockchain platforme u značajnoj mjeri direktno nadovezuje i na njenu trenutnu rasprostranjenost (popularnost). Pri provedbi projekta izrade vlastitog Blockchain sustava svakako valja misliti o budućnosti sustava po završetku izrade. Radi navedenog je potrebno pažljivo odabrati odgovarajuću Blockchain platformu za koju postoje naznake kako će i u budućnosti pružati pozitivne rezultate. Po završetku definiranja kriterija za odabir odabire se Blockchain platforma za evidenciju dostave pošiljki.



Slika 14: Odabir platforme i osnovne aktivnosti

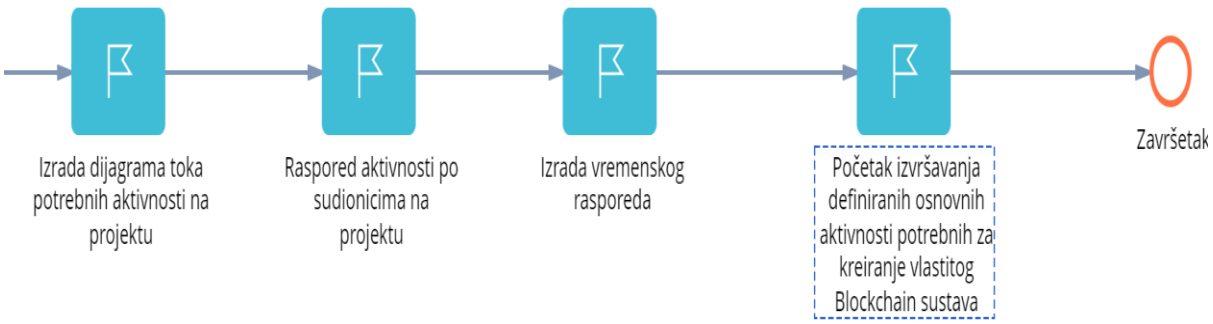
Pri izradi vlastitog Blockchain sustava postoje aktivnosti koje je potrebno provesti neovisno o kojoj Blockchain platformi se radi. Aktivnosti koje se najčešće spominju su razvoj dokaza o konceptu (eng. „Proof of Concept“, odnosno PoC), odabir konsenzus, izrada prvog Blockchain bloka, izvršavanje prvog pametnog ugovora, izgradnja, testiranje i skaliranje Blockchain sustava te puštanje u rad. PoC je dokaz koji je pribavljen iz pilot projekta, a koji se izvršava kako bi se demonstriralo da su ideja proizvoda, poslovni plan ili projektni plan izvedivi. PoC prikuplja povratne informacije od korisnika i spoznaje članova tima, uključujući i one koji inače ne bi sudjelovali, te na taj način izbjegava nepredviđene rizike. Nadalje, potrebno je odabrati odgovarajući protokol za konsenzus, a najrelevantniji protokoli su već ranije spomenuti u jednom od ranijih poglavlja. Protokol za konsenzus garantira kako „čvorovi“ na mreži imaju isto stanje duž cijelog Blockchain-a.

Po završetku odabira odgovarajućeg konsenzusa, može se pristupiti kreiranju prvog bloka [10]. Kako bi se kreirao Blockchain, prvi blok se kreira ručno, a sadrži sve karakteristike lanca. Sve se potom podijeli sa „čvorovima“ na mreži. Prvi blok se definira ispunjavanjem datoteke u

[10] Prvi blok se naziva i „blok nastanka“ (eng. „genesis block“).

JSON (JavaScript Object Notation) datoteci. Potom klijentska platforma kreira mapu koja sadrži Blockchain te ga inicijalizira. Kada se kreira prvi blok mogu se početi izvršavati pametni ugovori. Pametni ugovori se mogu izvršavati putem "if" uvjetnih naredbi ili "when ... then" uvjetnih naredbi, a trebali bi se automatski izvršavati po nekom od predodređenih uvjeta, kao što su određena količina nečega, određena satnica ili neki drugi uvjet.

Prije konačnog puštanja Blockchain-a u rad, kao logičan korak se nameće testiranje. Kako bi se provelo testiranje, poželjno je razviti jedan segment od ukupnog skupa podataka za Blockchain. Narav samog Blockchain sustava čini proces testiranja i uklanjanja pogreški izrazito složenim, budući kako se mora kreirati novi blok te se mora pričekati kako bi Blockchain propagirao implementirane izmjene. Ukoliko su razvoj dokaza o konceptu, odabir protokola za konsenzus, izrada prvog Blockchain bloka, izvršavanje prvog pametnog ugovora, izgradnja i testiranje Blockchain sustava dovršeni, Blockchain sustav se može pustiti u rad. Potrebno je napomenuti kako pored aktivnosti specifičnih za kreiranje Blockchain sustava hodogrami na prethodnim slikama 13 i 14, te na sljedećoj slici 15, prikazuju i poneke aktivnosti koje su zajedničke i projektima nevezanima za Blockchain.



Slika 15: Završne aktivnosti

Kada je sve definirano, potrebno je donijeti konačnu odluku o odabiru adekvatne Blockchain platforme. U ovom slučaju se radi o odabiru Ethereum-a, i to iz nekoliko razloga. Ethereum predstavlja razvijen i provjeren open-source Blockchain sustav s nekoliko tisuća decentraliziranih aplikacija i desecima tisuća developera. Prijelaz Ethereum-a s Proof-of-Work na Proof-of-Stake konsenzus možda i nije značajan faktor za privatne Blockchain sustave, no tako velik zahvat pokazuje ulaganje u budućnost Ethereum-a što opravdano daje optimizam kako će se Ethereum razvijati i u budućnosti. Vezano za sigurnost, na Ethereum-u ne postoji broj „čvorova" kao što ih ima na Bitcoin-u (iako razni izvori na Internetu poprilično variraju s iskazom), pa stoga nije u istoj mjeri zaštićen od potencijalnog „Napada 51%", no Ethereum se stalno razvija kroz open-source zajednicu i organizacije koje tvore Ethereum Foundation, pa nije neuobičajeno mišljenje kako se radi o tehnološki najnaprednijem Blockchain sustavu. Nadalje, Ethereum pruža mogućnost pristupa iz privatnog Blockchain-a u javni Blockchain, a samo jedna od prednosti koja se time postiže je mogućnost komunikacije više privatnih Blockchain-a preko javnog Ethereum Blockchain-a. Naposljetku, ističe se možda i najvažnija značajka, a to je kako je Ethereum sinonim za pametne ugovore, a koji jednostavno rečeno rezultiraju automatizacijom. Ispunjenjem zadanih kriterija se izvršava specifični algoritam, bez potrebe za ljudskom intervencijom. Takav pristup se čini idealan za repetitivne i relativno jednostavne aktivnosti, kao što je u slučaju ovog praktičnog primjera evidencija dostave pošiljki.

6.2. Primjer sustava za evidenciju dostava pošiljki

Pojavom epidemije virusa SARS-CoV-2 krajem 2019. godine do izražaja su došle pogodnosti koje pruža kupovina preko Interneta, od kojih se, između ostalog, može navesti ušteda vremena. Ušteda vremena se postiže na način da kupac više nije obvezan osobno odlaziti u trgovine, već iz udobnosti vlastitog doma putem Interneta odabire proizvod, a proizvod se zatim dostavlja na adresu kupca. Upravo čimbenik dostave čini jedan od najbitnijih čimbenika kod kupovine preko Interneta, gdje se očekuje pouzdanost pri dopremanju proizvoda i relativno kratko vrijeme od odabira proizvoda do pristizanja proizvoda do adrese kupca. Međutim, pored kupnje preko Interneta, iste značajke se očekuju i kod dostave drugih pošiljki. Često puta primatelji pošiljki nisu sami inicirali proces dostave, već se dostava inicira od strane drugih osoba, bilo da se radi o fizičkim osobama, poduzećima ili javnim institucijama. Promotivni

materijali i čestitke zapravo i ne predstavljaju jako bitne pošiljke za većinu primatelja, no pošiljke javnih institucija često imaju popriličan značaj, posebice kada se odlučuje o pravima i obvezama primatelja takvih pošiljki. Iz navedenog razloga se takve pošiljke često dostavljaju po posebnim propisima, a što može predstavljati poteškoću.

Određeni pojedinačni akti, kao što su npr. rješenja Porezne uprave ili jedinica lokalne uprave te pozivi sudova, dostavljaju se prema poreznom postupku, upravnom postupku ili parničnom postupku, ovisno o naravi stvari radi koje se dostava pokušava. Jedna od glavnih zajedničkih značajki za oba postupka je nužnost da se dostava, u slučaju prvog neuspješnog pokušaja dostave pošiljke, dostava ponovno pokuša nakon ostavljene obavijesti i roka koji je u takvoj obavijesti najavljen. Datumi navedeni na dostavnicama koji označavaju pokušaje dostave su od velike važnosti, budući da se protekom određenog roka može izgubiti neko od zajamčenih prava, kao što je npr. pravo primatelja rješenja na ulaganja žalbe na rješenje. S druge strane, nepropisnom dostavom i javna institucija koja šalje određeni pojedinačni akt ne može utvrditi određenu obvezu, već se cijeli postupak dostave mora ponoviti prema propisima. Kako je vidljivo iz prethodno navedenog, nepropisna postupanja s pošiljkama predstavljaju podjednak problem i za primatelje i za pošiljatelje. Problem koji se često pojavljuje u praksi je evidentiranje pokušaja dostave pošiljke, iako se takvo nešto zapravo fizički i nije izvršilo te dostavljač uopće nije dolazio na adresu primatelja pošiljke. Na taj način primatelj ne bude ni obaviješten o terminu u kojemu će se pokušati ponovljena dostava, čime se povećava mogućnost kako ni naredni pokušaj dostave neće biti uspješan. Budući kako dostavljač obavijest o pokušaju dostave pošiljke može elektronički ispisati neovisno o lokaciji na kojoj se nalazi, ostavlja se prostor za manipulaciju. Međutim, u navedenoj problematici Blockchain bi mogao naći konkretnu i korisnu primjenu.

Realizacijom Blockchain-a na način da se kod primatelja postavi QR kod kojemu je potrebno fizički pristupiti kako bi se potvrdio pokušaj dostave, te se podaci relevantni za pokušaj dostave evidentiraju na Blockchain-u, učinili bi veliki pomak u pouzdanosti dostave pošiljki. Koristeći pametne ugovore kao jednu od najbitnijih značajki Ethereum-a, već samim fizičkim dolaskom dostavljača na adresu primatelja se može automatski izvršiti algoritam predviđen za situacije u kojima se primatelj ne zatiče na svojoj adresi prebivališta ili boravišta. Uzevši u obzir značajku neizmjenjivosti Blockchain-a, podaci se mogu smatrati pouzdanima, te se ostavlja minimalan

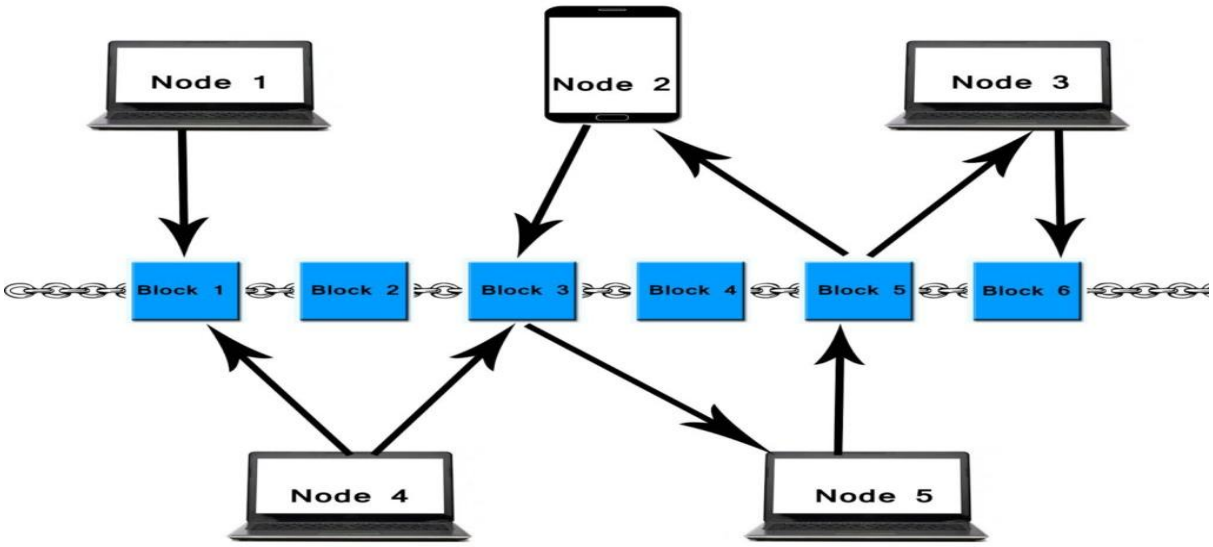
prostor za manipulaciju. Također, treba uzeti u obzir da, iako mogu nositi poprilično značenje za primatelje, uobičajene dostave pošiljki uglavnom nemaju značajniju vrijednost za eventualne napadače na Blockchain koji bi pokušali profitirati iz takvog napada. Na taj način bi se Blockchain za evidenciju dostave pošiljki mogao smatrati relevantno sigurnim, posebice ukoliko bi se čitav sustav odvijao na „čvorovima“ koji bi bili u cijelosti na mreži dostavljača, odnosno na privatnom Blockchain-u.

6.2.1. Privatni Ethereum Blockchain

Radi naravi problematike koja se pokušava riješiti sustavom za evidenciju dostave pošiljki, čitav sustav bi se trebao odvijati na privatnom Blockchain-u, budući kako bi „čvorove“ van sustava trebalo motivirati kriptovalutom ili nekim drugim sredstvom, a što se za ovakav specijalizirani i zatvoreni sustav ne čini prikladnim. Blockchain bi se, dakle, izvršavao na „čvorovima“ koji bi bili unutar mreže određenog dostavljača. Neke od prednosti privatnih Blockchain-a su veća fleksibilnost u vidu definiranja prilagođenih pravila po kojima će privatni Blockchain funkcionirati, definiranje visine transakcijskih naknada ili njihovo potpuno uklanjanje, što posljedično ima utjecaj i na vrijeme transakcija. Kako je već ranije spomenuto, vrijeme transakcije je pod utjecajem nekoliko čimbenika, uključujući vrijeme bloka, veličinu bloka, naknade za transakcije i mrežni promet. Vezano za sam Ethereum, razni izvori navode kako vrijeme bloka iznosi od 12 do 17 sekundi, no to vrijeme se može značajno skratiti u privatnom Blockchain-u. Ukoliko se kao čimbenik uklone transakcijske naknade te se uzme u obzir kako se očekuje da je na privatnom Blockchain-u mrežni promet manji od onog na javnom Ethereum Blockchain-u, može se postići vrijeme koje premašuje, ionako zadovoljavajuće za tip sustava koji se predlaže, prosječno vrijeme transakcija od 5 minuta na javnom Ethereum Blockchain-u.

6.2.2. Infrastruktura potrebna za privatni Ethereum Blockchain

Budući kako Blockchain predstavlja decentraliziranu bazu podataka, iz definicije je jasno kako je za distribuciju takve baze podataka potrebno osigurati više od jednog računala. Sam broj računala ovisi o stupnju decentralizacije koji se želi postići, odnosno koliko broj „čvorova“ se želi osigurati kako bi se postigla veća sigurnost i distribucija moći u Blockchain-u. Veći broj računala svakako znači veću pouzdanost, budući kako na taj način više strana vrši validaciju transakcija, pa to predstavlja nešto što je potrebno uzeti u obzir pri formiranju privatnog Blockchain sustava. U nastavku se slikovito prikazuje jednostavna shema mreže računala u privatnom Blockchain-u.



Slika 16: „Čvorovi“ na Blockchain-u

Kako se u ovom slučaju radi o privatnom Blockchain sustavu, što podrazumijeva samostalno definiranje vremena potrebno za transakciju, validacije od strane „čvorova“ na Blockchain-u se ne moraju izvršavati na izrazito snažnim računalima, posebice uzevši u obzir Ethereum-ov prijelaz na Proof-of-Stake konsenzus, koji zahtjeva značajno manju hardversku snagu od Proof-of-Work konsenzusa.

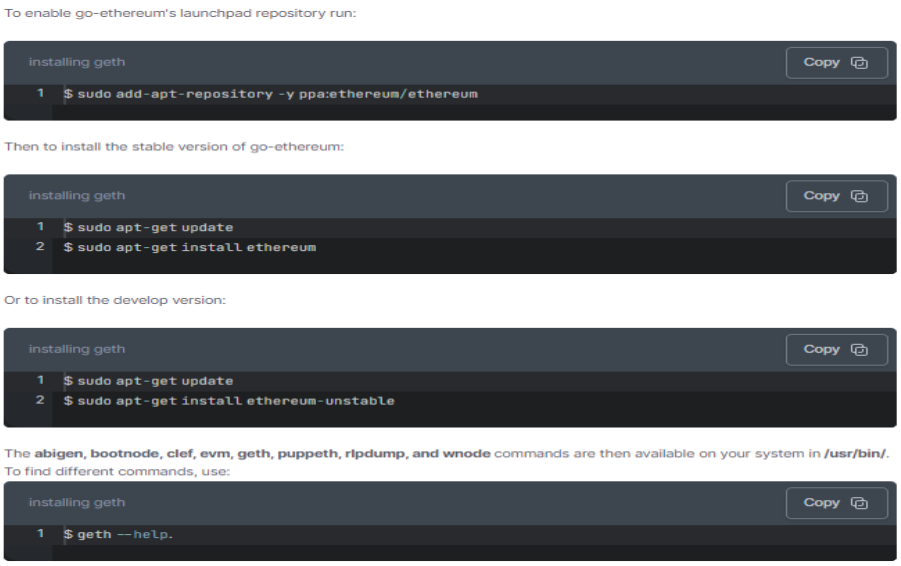
Međutim, ovdje valja spomenuti kako postoji alternativa formiranju vlastite infrastrukture s „čvorovima“, barem što se tiče početne faze uspostave privatnog Blockchain sustava. Naime, platforma Infura pruža mogućnost da umjesto kreatora privatnih Ethereum Blockchain-a vrši interakciju s Blockchain-ima, odnosno da pokreće „čvorove“ . Ipak, odmah je vidljivo kako takav pristup od kreatora privatnih Blockchain-a oduzima element decentralizacije i samostalnosti, budući kako se podaci, iako u enkriptiranom obliku, ipak predaju jednom subjektu.

6.2.3. Kreiranje privatnog Ethereum Blockchain-a

Nakon što se pruži potrebna infrastruktura koja će pogoniti privatni Blockchain, potrebno je odraditi softverski dio aktivnosti. Primjer u nastavku se u osnovnoj formi djelomično oslanja na primjer sa web sjedišta Topflight Apps [11].

Prije stvaranja prvog bloka, odnosno „bloka nastanka“, jedan od uobičajenih koraka bi bio preuzimanje i instalacija Geth klijenta. Geth (koji ima značenje „Go Ethereum“) je sučelje naredbenog retka koje se koristi za pokretanje Ethereum „čvora“ implementiranog u Go programskom jeziku, a koji developerima omogućuje „rudarenje“ Ether-a, kriptovalute srodne platformi Ethereum, validacije transakcija Ether-a i izvršavanje pametnih ugovora na Ethereum mreži. Na slici u nastavku se prikazuju naredbe potrebne za instalaciju Geth-a na Linux operacijskom sustavu.

[11] Web adresa: https://topflightapps.com/ideas/how-to-make-a-private-blockchain/.



Slika 17: Instalacija Geth-a na Linux-u

Nakon izvršenog preuzimanja i instalacije Geth klijenta, definiraju se parametri privatnog Blockchain-a kreiranjem „bloka nastanka“, nakon čega slijedi dodjela adresa „čvorovima“ na privatnom Blockchain-u. Slika u nastavku prikazuje primjer jednog „bloka nastanka“, a sam JSON dokument s „blokom nastanka“ se kreira u zasebnoj mapi unutar kreiranog Blockchain projekta.

Slika 18: Primjer „bloka nastanka“

Pored „bloka nastanka“, potrebno je i napisati programski kod za pametne ugovore. U slučaju Ethereum Blockchain-a, najčešća praksa je pisanje pametnih ugovora u Solidity programskom jeziku. Slika koja slijedi prikazuje primjer programskog koda pametnog ugovora.

```
pragma solidity 0.4.18;

// Contract to test unsigned integer underflows and overflows
// note: uint in solidity is an alias for uint256

// Guidelines: Press "Create" to the right, then check the values of max and zero by clicking "Call"
// Then, call overflow and underflow and check the values of max and zero again

contract OverflowUnderFlow {
    uint public zero = 0;
    uint public max = 2**256-1;

    // zero will end up at 2**256-1
    function underflow() public {
        zero -= 1;
    }
    // max will end up at 0
    function overflow() public {
        max += 1;
    }
}
```

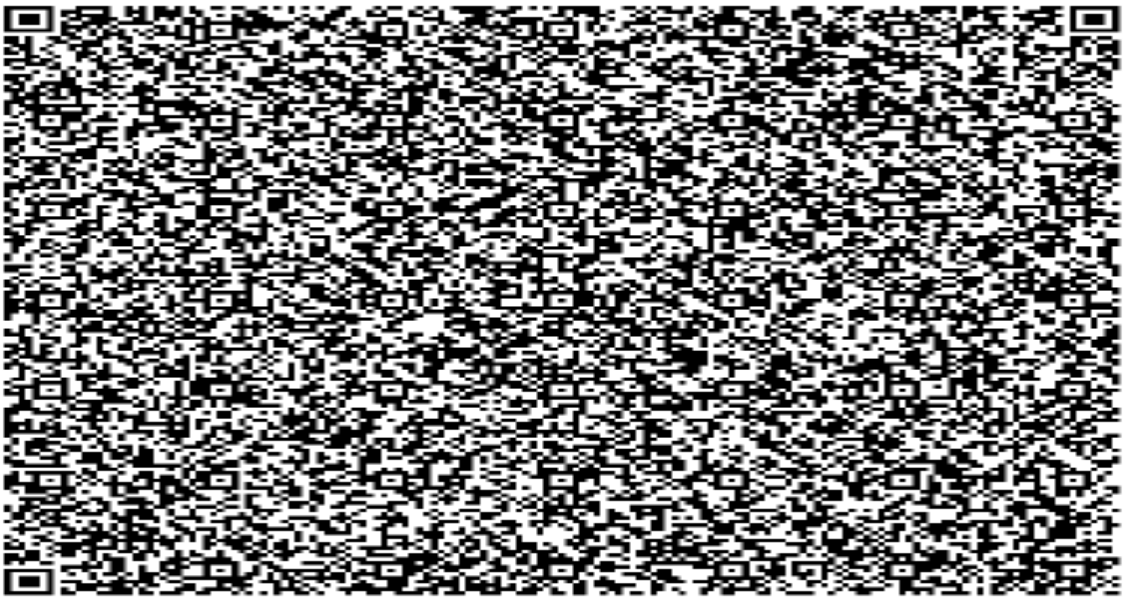
Slika 19: Primjer Solidity programskog koda za pametni ugovor

6.2.4. Kreiranje decentralizirane aplikacije

U ovom koraku se primarno kreira sučelje za interakciju s korisnikom, koji je u ovom slučaju dostavljač pošiljki. Radi prirode dostavljačkog posla, decentralizirana aplikacija se mora izvoditi i na mobilnim uređajima koje će dostavljači koristiti za evidenciju dostava pošiljki. Budući kako se tijekom radnog dana može pojaviti potreba za dostavom više desetaka pošiljki, korištenje mobilne decentralizirane aplikacije bi trebalo biti maksimalno jednostavno i brzo za korištenje. Osnovna funkcija koju bi mobilna decentralizirana aplikacija trebala sadržavati je očitavanje QR koda koji predstavlja adresu primatelja pošiljke, a koji se fizički nalazi na kućnoj adresi korisnika, čime se zaista potvrđuje pokušaj dostave pošiljke. Očitanjem koda se evidentiraju datum i vrijeme pokušaja dostave pošiljke te identitet dostavljača. Budući kako pošiljke već prije otpreme za dostavu dobivaju naznaku radi li se o pošiljci po poreznom, upravnom ili nekom drugom postupku, takva naznaka bi se također mogla evidentirati pri pokušaju dostave, kako bi se definirao adekvatan način postupanja.

6.2.5. Distribucija QR kodova za evidenciju dostava

Kao završni korak u realizaciji privatnog Blockchain sustava za evidenciju dostava pošiljki je potrebno izvršiti distribuciju QR kodova zainteresiranim korisnicima. Na taj način svaki korisnik, odnosno potencijalni primatelj pošiljki, može osigurati sredstvo za pouzdanu evidenciju izvršenih dostava pošiljki. Kako bi se osnažila vjerodostojnost pri evidenciji dostava, mogu se koristiti tzv. „sigurni QR kodovi“, koji mogu biti enkriptirani te imaju ugrađene slike, URL adrese ili oboje. Također, dodatna mjera osiguranja može predstavljati uparivanje učitanog QR koda na adresi korisnika s trenutnom GPS lokacijom dostavljača, koja se evidentira putem mobilnog uređaja. Iako bi se GPS lokacija mogla koristiti i kao zasebni čimbenik pri evidenciji pošiljki, ista često može zakazati u preciznosti lociranja, pa je tako u stambenom naselju s više stambenih zgrada koje imaju više etaža teško potvrditi preciznu lokaciju. Na slici u nastavku se prikazuje jedan primjer QR koda.



Slika 20: Primjer kompleksnog QR koda

7. ZAKLJUČAK

Kako je vidljivo iz prethodnih paragrafa, Blockchain već danas pronalazi primjenu u širokom spektru područja te nadilazi kriptovalute, koje i dalje predstavljaju glavnu asocijaciju pri spomenu Blockchain-a. Decentralizacija financijskog sustava, potpuna povezanost svih električnih uređaja ili ukidanje fizičkog novca se i danas mogu smatrati utopijskim idejama, no detaljnijim pregledom projekata u kojim je korišten upravo Blockchain, bilo da se radi o DeFi trgovinama i mjenjačnicama, IoT uređajima ili Bitcoin-u, nije teško zamisliti budućnost koja donosi sve od navedenog. Iako Blockchain sa sobom donosi i određene nedostatke, može se pretpostaviti kako će daljnji razvoj tehnologije, ali i pojava novih ideja, doprinijeti razvoju Blockchain-a u sustav na kojemu će se graditi nove inovacije i unapređivati postojeće tehnologije. Vrijedi spomenuti kako je u trenutku pisanja ovog rada izvršena tranzicija Ethereum Blockchain-a s Proof-of-Work konsenzusa na Proof-of-Stake konsenzus, čime se pad u potrošnji električne energije procjenjuje za ogromnih 99%. Time je postignut još jedan korak prema ekološki prihvatljivom sustavu, a za pretpostaviti je kako nas još mnogo novina tek očekuje.

POPIS REFERENCI

[1] TechTerms, »P2P,« Sharpened Productions, 2006. [Mrežno]. Available: https://techterms.com/definition/p2p. [Pokušaj pristupa 26 July 2022].

[2] T. Fisher, »What Is a Node in a Computer Network?,« Lifewire, 27 September 2021. [Mrežno]. Available: https://www.lifewire.com/what-is-a-node-4155598. [Pokušaj pristupa 25 July 2022].

[3] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf i S. Capkun, »On the security and performance of proof of work blockchains,« u *On the Security and Performance of Proof of Work Blockchains*, Vienna, 2016.

[4] M. Memon, U. A. Bajwa, A. Ikhlas i S. S. Hussain, »Blockchain beyond Bitcoin: Blockchain Technology Challenges and Real-World Applications,« u *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*, Southend, 2018.

[5] National Institute of Standards and Technology, »Secure hash standard,« National Institute of Standards and Technology, Gaithersburg, 1995.

[6] C. De Cannière i C. Rechberger, »Finding SHA-1 Characteristics: General Results and Applications,« u *International Conference on the Theory and Application of Cryptology and Information Security*, Shanghai, 2006.

[7] D. Dujak i D. Sajter, »Blockchain Applications in Supply,« u *Dujak, Davor; Sajter, Domagoj*, Osijek, Springer International Publishing AG, 2019, p. 29.

[8] M. B. Taylor, »The Evolution of Bitcoin Hardware,« *Computer*, p. 63, 2017.

[9] A. C. Moxoto, P. Melo i E. Soukiazis, »Initial Coin Offering (ICO): a systematic review of the literature,« u *Hawaii International Conference on System Sciences*, 2021.

[10] Metaco, »(Cryptographic) Tokens,« 24 June 2022. [Mrežno]. Available: https://www.metaco.com/digital-assets-glossary/cryptographic-tokens/.

[11] The UtilitySmarts Team, »What Are Utility Tokens?,« 24 June 2022. [Mrežno]. Available: https://www.utilitysmarts.com/utility-bills/what-are-utility-tokens/.

[12] J. Kozioł, »Is it possible to have anonymous transactions on the public blockchain?,« Pragmatic Coders., 27 December 2019. [Mrežno]. Available: https://www.pragmaticcoders.com/blog/anonymous-transactions-on-the-public-blockchain. [Pokušaj pristupa 1 August 2022].

[13] Statista, »Average transaction speed of 66 cryptocurrencies with the highest market cap as of March 2022,« 30 June 2022. [Mrežno]. Available: https://www.statista.com/statistics/944355/cryptocurrency-transaction-speed/.

[14] J. Frankenfield, »Block Time,« Investopedia, 14 December 2021. [Mrežno]. Available: https://www.investopedia.com/terms/b/block-time-cryptocurrency.asp. [Pokušaj pristupa 1 August 2022].

[15] L. Kenny, »The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed,« Medium, 30 January 2019. [Mrežno]. Available: https://towardsdatascience.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44. [Pokušaj pristupa 1 August 2022].

[16] S. Remya i A. Aneena, »A Review on BlockChain Security,« u *International Conference on Recent Advancements and Effectual Researches in Engineering Science and Technology (RAEREST)*, 2018.

[17] J. Hinsdale, »Cryptocurrency's Dirty Secret: Energy Consumption,« 1 July 2022. [Mrežno]. Available: https://news.climate.columbia.edu/2022/05/04/cryptocurrency-energy/.

[18] Tutorials Point, »Internet Services,« Tutorials Point, [Mrežno]. Available: https://www.tutorialspoint.com/internet_technologies/internet_services.htm#. [Pokušaj pristupa 1 August 2022].

[19] K. Finklea, »Dark Web,« Congressional Research Service, Washington, 2017.

[20] A. Brill i L. Keene, »Cryptocurrencies: The Next Generation of Terrorist Financing?,« 2014.

[21] Ethereum, »Introduction to Web3,« 4 July 2022. [Mrežno]. Available: https://ethereum.org/en/web3/.

[22] A. Samsukha, »Web2 vs. Web3: Complete Guide,« 4 July 2022. [Mrežno]. Available: https://www.emizentech.com/blog/web2-vs-web3.html.

[23] IBM Cloud Education, »Artificial Intelligence (AI),« IBM, 3 June 2020. [Mrežno]. Available: https://www.ibm.com/cloud/learn/what-is-artificial-intelligence. [Pokušaj pristupa 1 August 2022].

[24] IBM Cloud Education, »Machine Learning,« IBM, 15 July 2020. [Mrežno]. Available: https://www.ibm.com/cloud/learn/machine-learning?mhsrc=ibmsearch_a&mhq=ml. [Pokušaj pristupa 1 August 2022].

[25] K. Rose, S. Eldridge i L. Chapin, »The Internet of Things: An Overview,« The Internet Society (ISOC), 2015.

[26] IBM, »Build trust in your IoT data with blockchain,« 10 July 2022. [Mrežno]. Available: https://www.ibm.com/topics/blockchain-iot.

[27] K. Kwatra, »What is IPFS?,« Wolverine Blockchain, 15 March 2018. [Mrežno]. Available: https://medium.com/wolverineblockchain/what-is-ipfs-b83277597da5. [Pokušaj pristupa 26 July 2022].

[28] Q. Wang, R. Li, Q. Wang i S. Chen, »Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges,« 2021.

[29] N. Lambert, »Top 10 Most Expensive NFTs Ever Sold! (Updated 2022),« 18 July 2022. [Mrežno]. Available: https://bynicklambert.com/top-10-most-expensive-nfts-updated-2022/.

[30] R. Kaur, »What is the difference between Dapps and Defi-apps?,« 20 July 2022. [Mrežno]. Available: https://medium.datadriveninvestor.com/what-is-the-difference-between-dapps-and-defi-apps-922c7e69bac5.

[31] Sveriges Riksbank, »Payments in Sweden 2020,« Sveriges Riksbank, 29 October 2020. [Mrežno]. Available: https://www.riksbank.se/en-gb/payments--cash/payments-in-

sweden/payments-in-sweden-2020/1.-the-payment-market-is-being-digitalised/. [Pokušaj pristupa 4 August 2022].

[32] World Bank Group, »ID4D Data: Global Identification Challenge by the Numbers,« 2018. [Mrežno]. Available: https://id4d.worldbank.org/sites/id4d.worldbank.org/files/2018-08/ID4D%20Data%20Notes%20revised%20082918.pdf. [Pokušaj pristupa 6 August 2022].

[33] Consensys, »Blockchain in Digital Identity,« Consensys, [Mrežno]. Available: https://consensys.net/blockchain-use-cases/digital-identity/. [Pokušaj pristupa 6 August 2022].

[34] Federal Trade Commision, »New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021,« Federal Trade Commision, 22 February 2022. [Mrežno]. Available: https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0. [Pokušaj pristupa 6 August 2022].

[35] A. Davies, »How To Use Blockchain Technology For Identity,« DevTeam.Space , [Mrežno]. Available: https://www.devteam.space/blog/how-to-use-blockchain-technology-for-identity/. [Pokušaj pristupa 6 August 2022].

[36] S. Park, M. Specter, N. Narula i R. L. Rivest, »Going from Bad to Worse: From Internet Voting to Blockchain Voting,« *Journal of Cybersecurity*, svez. VII, br. 1, 2021.

[37] C. A. Engr, »The Complete Guide for Asset Tokenization on Blockchain,« Litimus, 21 February 2022. [Mrežno]. Available: https://litimus.com/the-complete-guide-for-asset-tokenization-on-blockchain/. [Pokušaj pristupa 7 August 2022].

[38] W. Malsam, »What Is Proof of Concept (POC)? Definition, Steps & Best Practices,« ProjectManager.com, Inc., 1 December 2021. [Mrežno]. Available: https://www.projectmanager.com/blog/proof-of-concept-definition. [Pokušaj pristupa 23 August 2022].

[39] Success Synergy Enterprises, »How to Start Your Own Blockchain Project in 5 Simple Steps,« Success Synergy Enterprises, [Mrežno]. Available: https://neenadayal.com/how-

to-start-your-own-blockchain-project-in-5-simple-steps/. [Pokušaj pristupa 23 August 2022].

[40] CW Lab OÜ, »What is Geth?,« CW Lab OÜ, [Mrežno]. Available: https://cryptowallet.com/glossary/geth/. [Pokušaj pristupa 18 September 2022].

POPIS SLIKA

1.medium.com%2Fmax%2F2000%2F1*rRuZqum3gwp_IxvyBhHqbQ.png&f=1&nofb=1.

10. Prikaz plaćanja fizičkim novcem u Kraljevini Švedskoj u razdoblju od 2010. godine do 2020. godine. Izvor: https://www.riksbank.se/en-gb/payments--cash/payments-in-sweden/payments-in-sweden-2020/1.-the-payment-market-is-being-digitalised/cash-is-losing-ground/.
11. Primjer osobne iskaznice temeljene na Blockchain-u. Izvor: https://www.devteam.space/wp-content/uploads/2018/05/blockchain.png.
12. Proces tokenizacije imovine. Izvor: https://external-content.duckduckgo.com/iu/?u=https%3A%2F%2Fwww.wavestone.com%2Fapp%2Fuploads%2F2019%2F09%2FAsset-tokenization.jpg&f=1&nofb=1.
13. Odabir projekta, pregled platformi i definiranje kriterija. Izvor: Vlastita izrada u web aplikaciji Studio Creatio, https://app.creatio.com/.
14. Odabir platforme i osnovne aktivnosti. Izvor: Vlastita izrada u web aplikaciji Studio Creatio, https://app.creatio.com/.
15. Završne aktivnosti. Izvor: Vlastita izrada u web aplikaciji Studio Creatio, https://app.creatio.com/.
16. „Čvorovi“ na Blockchain-u. Izvor: https://theblockchainland.com/wp-content/uploads/2018/08/network-of-nodes-blockchainland-1024x1024.jpg.
17. Instalacija Geth-a na Linux-u. Izvor: https://www.quicknode.com/guides/infrastructure/how-to-install-and-run-a-geth-node.
18. Primjer „bloka nastanka“. Izvor: https://external-content.duckduckgo.com/iu/?u=https%3A%2F%2Fwww.samsclass.info%2F141%2Fproj%2FpEth1-33.png&f=1&nofb=1.
19. Primjer Solidity programskog koda za pametni ugovor. Izvor: https://medium.com/loom-network/how-to-secure-your-smart-contracts-6-solidity-vulnerabilities-and-how-to-avoid-them-part-1-c33048d4d17d.
20. Primjer kompleksnog QR koda. Izvor: https://external-content.duckduckgo.com/iu/?u=https%3A%2F%2Fi.stack.imgur.com%2FBDY0Q.png&f=1&nofb=1.

FUTURE APPLICATIONS OF THE BLOCKCHAIN TECHNOLOGY

ABSTRACT

The subject of this final thesis is the Blockchain technology, more precisely its current applications, as well as possible future applications. In addition to the applications, positive and negative properties are also listed, in order to help form a more objective opinion on the Blockchain's impact on the society. Due to the very nature of the faculty under which this final thesis was written, a practical example of real world Blockchain application is also suggested, in which the Blockchain, given its characteristics, could contribute to a positive change.

KEY WORDS:

Blockchain, technology.