ULOGA DIGITALNOG IDENTITETA U DIGITALNOJ EKONOMIJI S OSVRTOM NA PRIMJENU BLOCKCHAIN KONCEPTA U ODABRANOJ INDUSTRIJI

Fijačko, Goran

Master's thesis / Specijalistički diplomski stručni

2018

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Algebra University College / Visoko učilište Algebra**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:225:953052

VISOKO UČILIŠTE ALGEBRA

DIPLOMSKI RAD

ULOGA DIGITALNOG IDENTITETA U DIGITALNOJ EKONOMIJI S OSVRTOM NA PRIMJENU BLOCKCHAIN KONCEPTA U ODABRANOJ INDUSTRIJI

Goran Fijačko

Zagreb, rujan 2018.

Predgovor

Ovim putem zahvaljujem se profesoru i mentoru dr.sc. Leu Mršiću, koji mi je omogućio da napravim svoje prve korake kroz tehnologiju koja polako ali sigurno mijenja svijet na bolje, blockchain tehnologiju. Uz njegova inspirativna predavanja, koja su uvijek prebrzo prolazila, bilo je teško ne imati konstantnu želju i potrebu za novim informacijama. Također mu se zahvaljujem na izrazitoj susretljivosti i pristupačnosti prilikom pisanja Diplomskog rada koje mi je uvelike olakšalo ovo iskustvo i učinilo ga veoma pozitivnim.

Zahvaljujem se i svima koji su na bilo koji način pridonijeli izradi ovog rada.

Posebno se zahvaljujem svojoj obitelji i prijateljima koji mi uvijek pružaju bezuvjetnu podršku u svim segmentima i bez kojih ne bih bio to što jesam.

Goran

Prilikom uvezivanja rada, Umjesto ove stranice ne zaboravite umetnuti original potvrde o prihvaćanju teme diplomskog rada kojeg ste preuzeli u studentskoj referadi

Sažetak

Ovaj rad opisuje blockchain tehnologiju, njenu povijest, način na koji funkcionira i kako utječe na poslovne modele kakve danas poznajemo i sve to držeći se u okviru digitalnog identiteta. Kroz rad će se usporediti tradicionalni poslovni modeli sa modelima koji koriste blockchain i pametne ugovore. Nakon opisa primjene tehnologije u nekim od odabranih industrija u sklopu praktičnog dijela rada biti će predstavljen koncept aplikacije za unos, izdavanje i verifikaciju obrazovnih certifikata baziran na blockchain tehnologiji.

Ključne riječi: identitet, blockchain, pametni ugovori.

Summary

This thesis describes blockchain technology, its history, how it works and how it affects business models we know today and all that through the digital identity framework. The traditional business models will be compared with models that use blockchain and smart contracts. Following the description of the application of the technology in some of the selected indutries, the application concept for creating, issuing and verifying blockchain-based education certificates will be presented in the practical part of the thesis.

Key words: identity, blockchain, smart contracts.

Sadržaj

1. Uvod

Na pitanje što je identitet, vrlo je teško odgovoriti. Stoga u literaturi postoji mnogo subjektivnih stajališta i definicija identiteta. No, u ovom radu bit će obrađen dio identiteta koji se odnosi na identifikaciju pojedinca, njegovu kvalifikaciju i njegov status u društvu, te će u praktičnom dijelu rada poseban naglasak biti na akademskoj kvalifikaciji pojedinca gdje će se kroz primjer blockchain-a prezentirati koncept izdavanja, pohranjivanja i verificiranja obrazovnih diploma.

Kao što je rekla Ginni Rometry[1], generalna direktorica IBM-a, ono što je internet učinio za komunikaciju, smatra se da bi blockchain mogao učiniti za pouzdane transakcije koje se koriste svuda oko nas, svakim danom sve više i više. Blockchain nam omogućava drastično povećanje povjerenja i efikasnosti u izmjeni bilo kakvih podataka.

U ovom će radu, uz digitalni identitet i blockchain tehnologiju, biti opisano kako će se poslovni modeli mijenjati implementacijom ove tehnologije i postaviti će se usporedbe sa tradicionalnim modelima. Kroz opis primjene tehnologije u nekim od odabranih industrija doći će se do praktičnog dijela rada gdje će biti predstavljen koncept izdavanja, postavljanja i verificiranja obrazovnih certifikata na blockchain.

[1] https://flipboard.com/@flipboard/-from-yelp-reviews-to-mango-shipments-ib/f-0cf869ac26%2Fbusinessinsider.com (23.07.2018. u 17:05)

2. Priprema (teoretska osnova)

2.1. Digitalni identitet

Ako govorimo o klasičnom identitetu pojedinca i spominjemo osobnu iskaznicu, rodni list, domovnicu, vozačku dozvolu ili pak diplomu fakulteta, tada pod pojmom digitalnog identiteta pojedinca možemo govoriti o e-osobnoj iskaznici, e-rodnom listu, e-domovnici, e-vozačkoj dozvoli ili pak e-diplomi. Oznaka e- u nazivu označava elektronski, što znači da ti dokumenti imaju i digitalnu komponentu. Ta digitalna komponenta može biti npr. elektronički nosač podataka (čip) na kojem su pohranjeni određeni podaci ili certifikati koji se po potrebi učitavaju u računalo pomoću čitača. Sami podaci koji se prikazuju centralizirani su te za njih garantira i odgovara institucija koja ih izdaje i kod koje su ti podaci pohranjeni.

Digitalni identitet ne mora nužno biti fizička isprava ili dokument. U njega ulaze i naše email adrese te različiti korisnički računi i profili na internetu kao što su npr. korisnički račun u sustavu e-Građani, Facebook profil, email itd.

2.1.1. Osobna iskaznica

Osobna iskaznica je elektronička javna isprava kojom se dokazuje identitet, državljanstvo, spol, datum rođenja i prebivalište. Iskaznica sadrži elektronički nosač podataka (čip) na koji se uz podatke ispisane u vizualnoj zoni kartice, mogu pohraniti jedan ili dva certifikata:

- identifikacijski certifikat koji se koristi za elektroničku potvrdu i autentikaciju prilikom pristupa elektroničkim uslugama
- potpisni certifikat koji se koristi kao podrška naprednom elektroničkom potpisu te zamjenjuje vlastoručni potpis, sukladno zakonu kojim je reguliran elektronički potpis

Elektronička osobna iskaznica na kojoj se nalazi aktivni identifikacijski certifikat služi za prijavu u sustav e-Građani, ali i druge e-usluge. Dok uz potpisni certifikat, ista služi za

obavljanje aktivnosti vezanih uz ovjeru dokumenata elektroničkim potpisom, kao valjanom zamjenom za vlastoručni potpis. [2]

Digitalni certifikati služe kao sredstvo kojim se dokazuje identitet na internetu. Provjeru podataka rade tzv. certifikacijska tijela (CA- Certificate Authority) čija je uloga provjera i utvrđivanje nečijeg identitet i nakon toga izdavanje digitalnog certifikata. Digitalni certifikat sadrži određene podatke o njegovom vlasniku, među kojima su:

- ime vlasnika certifikata
- vlasnikov javni ključ
- nadnevak do kada vrijedi javni ključ
- ime certifikacijskog tijela koje je izdalo certifikat
- jedinstveni serijski broj
- dodatne podatke za identifikaciju

Kada formira neki digitalni certifikat, CA ga na kraju digitalno potpiše svojim tajnim ključem tako da se njegov sadržaj može pročitati korištenjem CA javnog ključa, ali se ne može neovlašteno mijenjati. [3]

2.1.2. Sustav e-Građani

Sustav e-Građani[4] uspostavljen je s ciljem modernizacije, pojednostavljenja i ubrzanja komunikacije građana i javnog sektora te povećanja transparentnosti pružanja javnih usluga.

Navedeni sustav se sastoji od 3 povezane komponente koje predstavljaju zajedničku infrastrukturu javnog sektora te omogućuju sigurnu elektroničku komunikaciju građana i javnog sektora:

- Središnji državni portal
- Osobni korisnički pretinac
- Nacionalni identifikacijski i autentifikacijski sustav

[2] http://stari.mup.hr/42.aspx (20.07.2018. u 18:20)
[3] https://hr.wikipedia.org/wiki/Za%C5%A1tita_podataka#Digitalni_certifikat (20.07.2018. u 21:15)
[4] https://gov.hr/e-gradjani/o-sustavu-e-gradjani/1584 (21.07.2018. u 17:00)

Središnji državni portal[5] je centralno internetsko rješenje za pristup javnim informacijama. Ovaj portal objedinjuje sve informacije državnih institucija i omogućuje građanima da na jednom mjestu pronađu bitne i točne informacije.

Osobni korisnički pretinac[6] služi za komunikaciju između građana i tijela javne uprave. Kroz navedenu komunikaciju građani mogu dobiti osobne informacije vezane za svoje aktivne postupke, statuse i javne usluge. Kroz sustav ih vrlo lako mogu pregledavati, upravljati njima te ih pohranjivati. Osobni korisnički pretinac može se koristiti i kao aplikacija na mobilnim uređajima što korištenje čini još lakšim i praktičnijim jer danas većina ljudi ima pametne telefone, dok računala ne posjeduju svi.

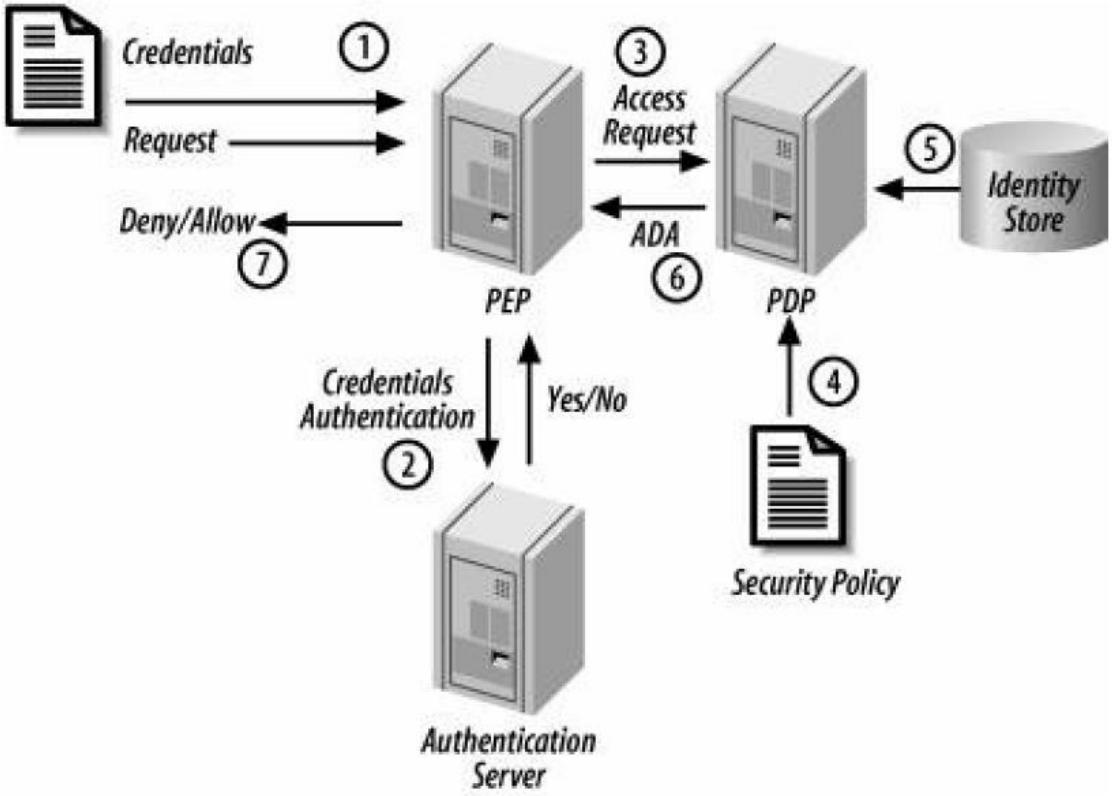
Nacionalni identifikacijski i autentifikacijski sustav (NIAS)[7] je informacijsko-tehnološki sustav središnje identifikacije i autentifikacije korisnika e-javnih usluga. Ako korisnik posjeduje odgovarajuću vjerodajnicu, sustav mu nakon uspješne identifikacije i autentifikacije omogućuje pristup e-uslugama javnog sektora.

Sustavi za identifikaciju i autentifikaciju rade na sljedećem principu[8] (Slika 2.1):

1. Da biste koristili identitet koji omogućava pristup nekom resursu, entitet (u ovom slučaju osoba), uz svoj zahtjev, mora predočiti valjanu vjerodajnicu. Vjerodajnica je dokaz da entitet ima pravo tvrditi da određeni identitet pripada baš njemu.
2. Kada se vjerodajnica dostavi sigurnosnom tijelu, tj. u policy enforcement point (PEP), ono ih ovjerava, najbolje pomoću zasebnog poslužitelja za provjeru autentičnosti.
3. Postoji nekoliko različitih metoda provjere vjerodajnica. Neke od njih su klasično korisničko ime i lozinka, zatim certifikati s najzastupljenijom međunarodnom normom za digitalne certifikate X.509 ili biometrika. Razina provjere autentičnosti je obično proporcionalna riziku koji je prisutan prilikom pristupanja određenom resursu.
4. Nakon ovjeravanja vjerodajnica, sigurnosno tijelo preuzima sigurnosna pravila (eng. *security policy*) za resurs ili ih proslijedi na odvojenu točku za odlučivanje pravila (eng. *policy decision point* – PDP).

[5] Ibid
[6] Ibid
[7] https://nias.gov.hr/Home/TermsOfUse (21.07.2018. u 17:45)
[8] Windley, Phill (2005). Digital identity, str. 36.

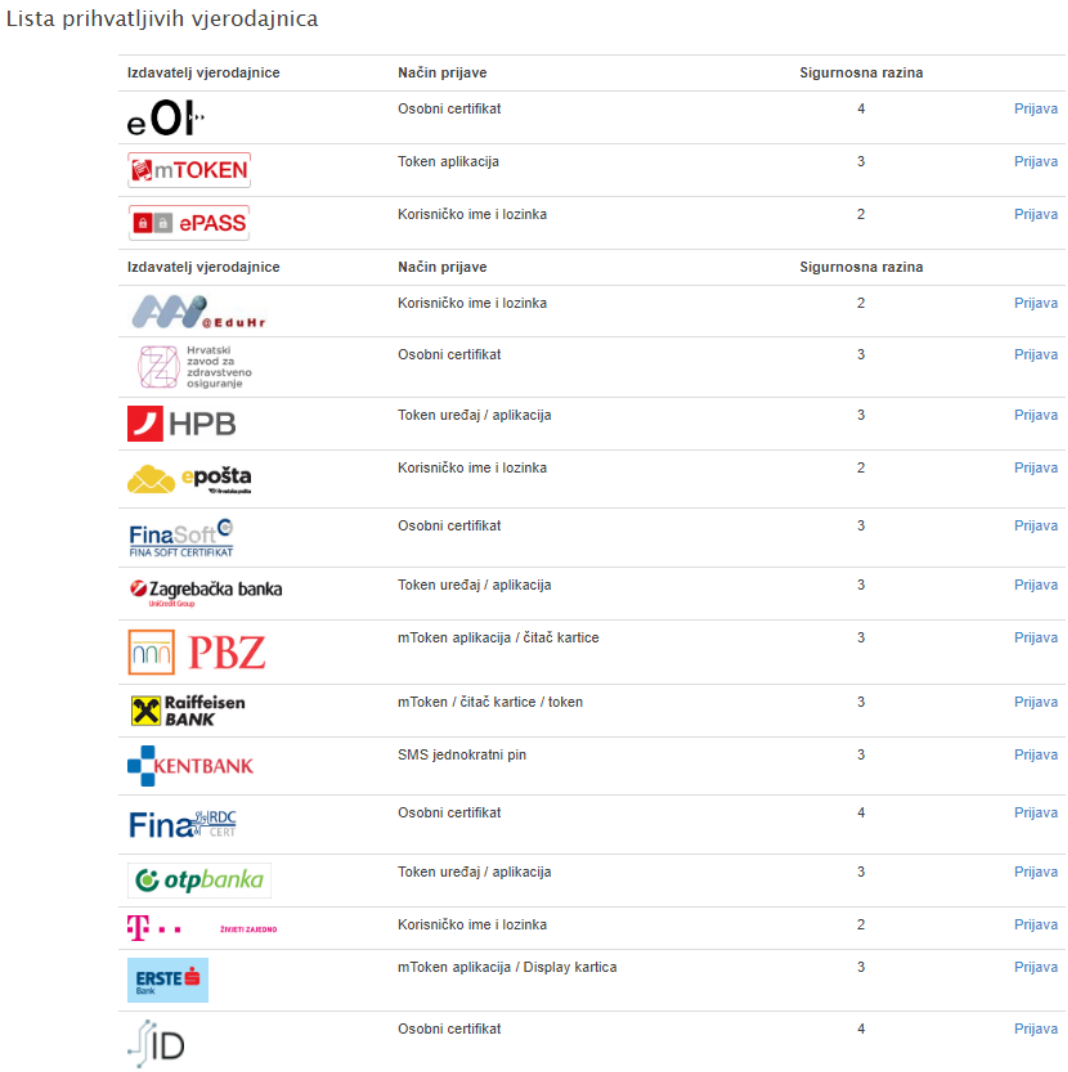
5. PDP koristi dobivena sigurnosna pravila i dani identitet kako bi odredio prava (eng. *entitlements*) i dozvole (eng. *permissions*) povezane s tim resursom za taj identitet. Prava su usluge i resursi kojima dani identitet ima dozvoljen pristup. To npr. može biti stanje na kreditnoj kartici. Dozvole su radnje koje su dozvoljene entitetu kao npr. povlačenje sredstava, kupnja itd.
6. PDP prenosi te podatke natrag na PEP, u obliku tvrdnje o odobrenju (eng. *authorization decision assertion* – ADA).
7. Konačno, PEP sukladno dobivenim podacima dopušta ili odbija radnju koju zahtjeva entitet.



Slika 2.1 Proces autentifikacije. Izvor: Phil Windley, Digital identity, str. 37.

Razina sigurnosti vjerodajnica[9] predstavlja stupanj ranjivosti vjerodajnice prilikom njenog korištenja. U nacionalnom identifikacijskom i autentifikacijskom sustavu postoje 4 razine sigurnosti (Slika 2.2)

Što se tiče sigurnosti vjerodajnica, korisnik je taj koji je isključivo odgovoran za svoju vjerodajnicu te je mora pažljivo čuvati i nikome je ne povjeravati.



Slika 2.2 Lista prihvatljivih vjerodajnica u sustavu e-Građani.

Izvor: https://nias.gov.hr/Authentication/Step2 (22.07.2018. i 18:18)

[9] https://gov.hr/e-gradjani/o-sustavu-e-gradjani/1584 (22.07.2018. u 18:15)

2.2. Blockchain

Blockchain je jedna od disruptivnih tehnologija koja je često nazivana tehnologijom koja će promijeniti svijet i omogućiti mu novu revoluciju. Blockchain predstavlja decentraliziranu bazu podataka koja je javno dostupna svima, putem interneta. Uzmimo za primjer baze podataka i registre koje posjeduju država i njene institucije kao što su ministarstva, zatim banke, mobilni operateri itd., i sve navedene registre i podatke objavimo javno, postavljanjem istih u blockchain. On nam omogućava da svim podacima koji se tiču isključivo nas samih, uz autorizaciju, imamo pristup putem interneta. Isto tako, te iste podatke možemo predstaviti drugoj strani u trenutku kada im trebamo dokazati svoj identitet, valjani podatak ili neku informaciju.

2008. godine, jedna osoba ili skupina ljudi, pod pseudonimom Satoshi Nakamoto, objavili su bijeli papir (eng. whitepaper) u kojem je svijetu predstavljen Bitcoin. Predstavljen je kao prvi Peer-to-Peer sustav elektroničkog novca[10] preko kojeg se mogu izvršavati transakcije između 2 entiteta, preko interneta, bez posredovanja treće strane, u ovom slučaju banke. Sustav je baziran na kriptografiji i pomoću nje rješava glavni problem digitalnog novca koji je postojao do tada, a to je duplo korištenje. Vrlo je lako bilo duplicirati digitalni novac i trošiti ga više od jednog puta. Ovdje je prvi puta predstavljen princip kriptografskog povezivanja svake transakcije sa transakcijom koja joj prethodi i to u obliku u kojem je zapis nepromjenjiv. To svojstvo nepromjenjivosti, Nakamoto je opisao kroz javnu knjigu (eng. public ledger). Iz te javne knjige, preko mreže se mogu pregledavati sve transakcije digitalnog novca.

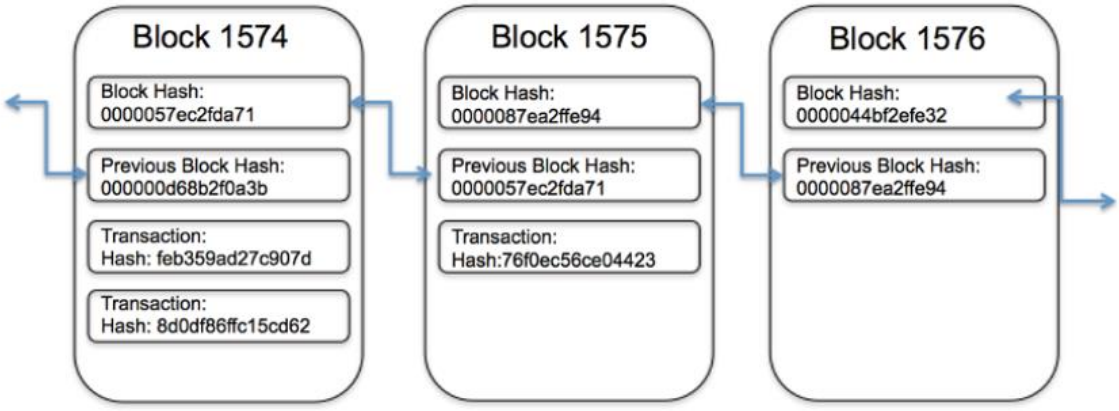
Nekoliko godina Bitcoin je bio u prvom planu, ali zajednica je vrlo brzo prepoznala da on ″leži″ na nečemu što je čak važnije i vrijednije od njega samog, a to je protokol koji ga pokreće tj., blockchain. Došlo se do spoznaje da se blockchain može koristiti na načine koji ne uključuju digitalni novac tj., kriptovalute. U tom trenutku bilo je očito da se radi o nečem velikom što će jednoga dana globalno promijeniti poslovne modele, kao što ih je internet promijenio devedesetih godina.

Glavna svojstva blockchain-a su transparentnost i decentraliziranost, čime se današnji sustavi nikako ne mogu pohvaliti. Digitalni identitet u kombinaciji sa blockchain

[10] https://bitcoin.org/bitcoin.pdf (18.09.2018. u 17:00)

tehnologijom omogućiti će ljudima mnogo brže, jednostavnije i sigurnije obavljanje određenih radnji koje uključuju dokazivanje identiteta, činjenica, stanja i podataka. Nevjerojatno zvuči činjenica da bi traženje novih zaposlenika, provjera podataka o kandidatima i sama prijava za posao mogli biti proces koji bi se odvio u svega nekoliko klikova mišem na računalu i to sa stopostotnom sigurnošću u dobivene podatke. No, blockchain upravo to i nudi. Postavljanjem svih podataka o našem identitetu na njega, uz kriptografiju, koja cijelu stvar čini sigurnom, a ujedno transparentom i uvijek dostupnom putem interneta, svo utrošeno vrijeme na dokazivanje identiteta, podataka, činjenica i stanja stvari, možemo potrošiti na bitnije stvari. Zamislite da uz prijavu za posao možemo priložiti i 3 kriptografska ključa pomoću kojih poslodavac vrlo lako, sa stopostotnom sigurnošću, može provjeriti jesmo li zaista završili fakultet koji smo naveli u svom životopisu, jesmo li nekažnjavani i jesmo li mi uopće ta osoba koja tvrdimo da jesmo. Taj proces bi trajao otprilike nekoliko minuta, dok taj isti proces danas traje nekoliko dana, ako ne i tjedana, pošto se verifikacija podataka vrši pisanim upitima u svaki od tih sustava iz kojih podaci dolaze.

Blockchain je svoj naziv dobio po načinu na koji pohranjuje podatke transakcija koje se događaju. Pohranjuje ih u blokove (eng. *blocks*) koji zajedno povezani čine lanac (eng. *chain*) (Slika 2.3).



Slika 2.3 Prikaz transakcija pohranjenih u blokove koji međusobno povezani tvore lanac.
Izvor: Gupta, M., Blockchain for dummies, 2nd IBM Limited Edition, 2018., str. 14.

Porastom broja transakcija koje se odrađuju, raste i veličina samog lanca u kojemu one nastaju. U blokovima se zapisuju slijed i vrijeme transakcija koje se zatim zapisuju u lanac

unutar mreže i to prema određenim sigurnosnim pravilima dogovorenim među sudionicima. Svaki blok sadrži *hash,* tj. digitalni otisak ili jedinstveni identifikator, zatim vremenski označene valjane transakcije i *hash* prethodnog bloka. *Hash* prethodnog bloka matematički povezuje blokove u lanac i onemogućava bilo kakvu promjenu podataka i informacija u prethodnim blokovima ili pak umetanje novih blokova između postojećih. Tako se svakim sljedećim blokom povećava sigurnost cijelog lanca i smanjuje već ionako mala šansa za manipulaciju i promjenu vrijednosti ili podataka u lancu. [11]

Postoji nekoliko vrsta blockchaina, u ovom radu ćemo spomenuti 2 najčešće vrste:[12]

- Javni blockchain, kao što je Bitcoin blockchain (prva i najpoznatija kriptovaluta bazirana na ovoj tehnologiji), velika je distribuirana mreža koja se izvodi uz izdavanje nativnog tokena. Javni blockchain je vidljiv i otvoren svima za korištenje, na svim razinama. Otvorenog je koda koji održava zajednica programera.
- Privatni blockchain je manjeg obujma i obično se ne izvodi uz izdavanje tokena. Članstvo u ovoj vrsti blockchaina je izrazito kontrolirano te ga često koriste organizacije koje imaju povjerljive članove ili trguju povjerljivim informacijama.

Svi tipovi blockchaina koriste kriptografiju kako bi omogućili svakom sudioniku da koristi mrežu na siguran način, i što je najvažnije, bez potrebe za centralnim autoritetnim tijelom koje provodi pravila. Zbog toga se blockchain smatra revolucionarnim jer je to prvi način kojim je postignuto povjerenje pri slanju i zapisivanju digitalnih podataka.

Najčešće korišteni kriptografski algoritam je SHA-256 algoritam. Kod njega se kao ulaz može koristiti bilo koja količina i tip podataka (tekst, dokument itd.), te se kroz algoritam dobiva jedinstveni podatak fiksne veličine, dužine 32 znaka.

Primjer, tekst mog imena, Goran, prolaskom kroz SHA-256 algoritam daje rezultat dbe08c149b95e2b97bfcfc4b593652adbf8586c6759bdff47b533cb4451287fb.[13] Riječ Goran će uvijek kao rezultat dati identičnu *hash* vrijednost. Dodavanjem bilo kojeg znaka ili slova kod ulaza, mijenja kompletan izgled *hash-a,* ali naravno, spomenuta duljina od 32 znaka

[11] Gupta, M., Blockchain for dummies, 2nd IBM Limited Edition, 2018., str 13.
[12] Laurence, T., Blockchain, 2017., 1. poglavlje
[13] https://www.xorbin.com/tools/sha256-hash-calculator (24.07.2018. u 22:45)

uvijek ostaje identična. Primjer, riječ Gordan, daje rezultat 48fa1be7c33664e5a0c61a006d21592cf20272aab7228b09add728aa0f11ffc7.[14]

Uz spomenute blokove i lanac koji oni međusobno povezani čine, postoji još jedan vrlo važan segment, a to je mreža. Mreža se sastoji od čvorova (eng. *node*) i potpunih čvorova (eng. *full node*). Uređaj koji se spaja i koristi neku blockchain mrežu postaje čvor, no da bi taj uređaj postao potpuni čvor, on mora preuzeti kompletan zapis svih transakcija od samog početka kreiranja tog lanca i pridržavati se sigurnosnih pravila koje definiraju lanac. Potpuni čvor može voditi bilo tko i bilo gdje, jedino što je potrebno je računalo i internetska mreža. No to nije tako jednostavno kako zvuči.

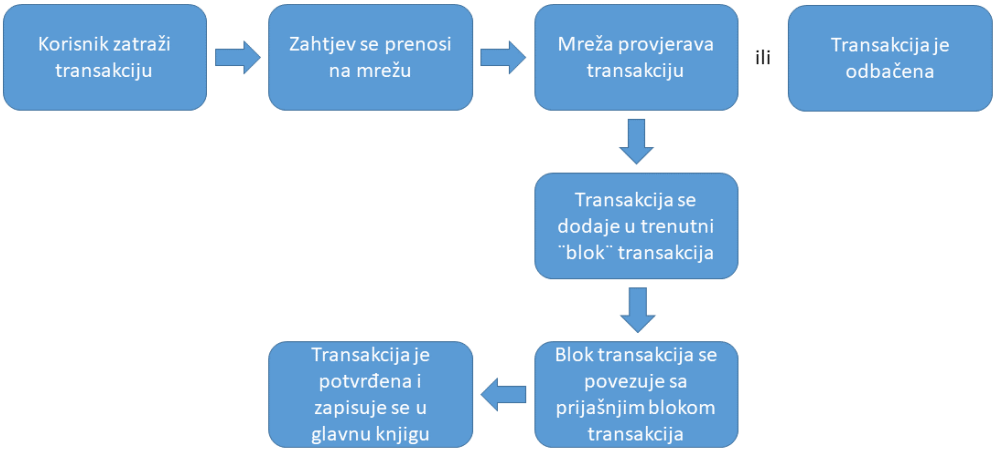
Mnogo ljudi miješa pojmove Bitcoin i blockchain ili ih pak krivo koristi. To su dvije različite stvari. Blockchain tehnologija je predstavljena 2008. godine, ali je tek godinu dana kasnije krenula u pogon i to u obliku kriptovalute Bitcoin. Bitcoin je dakle kriptovaluta koja ima svoj blockchain. Taj blockchain je protokol koji omogućava siguran prijenos i praćenje kriptovalute Bitcoin, sve od nastajanja njenog prvog bloka (eng. *genesis block*) i prve transakcije. Bitcoin je smišljen isključivo kao kritpovaluta s vizijom da jednog dana u potpunosti zamijeni fiat (papirnati) novac i sruši barijere prijenosa novca koje su danas prisutne. Kroz godine koje su prolazile, zajednica je ustanovila da je blockchain moćniji nego što se prvotno mislilo, stoga ako Bitcoin kao kriptovaluta ne zaživi globalno u svakodnevnom životu, iza sebe će ostaviti jedan revolucionaran izum koji potencijalno može promijeniti tehnološki svijet koji trenutno poznajemo.

Blockchain kroz svoj mehanizam konsenzusa eliminira centralne autoritete kakve danas poznajemo i na kojima se bazira današnja tehnologija.

[14] Ibid (24.07.2018. u 22:50)

2.2.1. Konsenzus (Validacija transakcija)

U svijetu blockchaina, postizanje konsenzusa, tj. trajno zapisivanje informacija (verifikacija transakcija) u lanac je proces postizanja sporazuma među skupinom dioničara koji su međusobno nepovjerljivi. To su prethodno spomenuti potpuni čvorovi. Oni potvrđuju transakcije koje su unesene u mrežu i zapisuju ih kao dio glavne knjige (eng. *ledger*) (Slika 2.4). Ako se ustanovi da je transakcija lažna, potpuni čvorovi je vrlo lako prepoznaju i po automatizmu je odbacuju. Postoji nekoliko metoda validacija transakcija. Najčešće i najpoznatije su dokaz radom (eng. *Proof of Work* - POW) i dokaz ulogom (eng. *Proof of Stake* - POS). Algoritam dokaza radom za postizanje konsenzusa koriste dvije od poznatijih kriptovaluta, Bitcoin i Ethereum. Iako su oboje kriptovalute, Bitcoin i Ethereum su vrlo različiti. Bitcoin je isključivo napravljen kao digitalna valuta s vizijom da zamijeni fiat novac, dok je Ethereum baziran na programskom jeziku (Solidity)[15] i pametnim ugovorima, o kojima ćemo u sljedećem poglavlju.



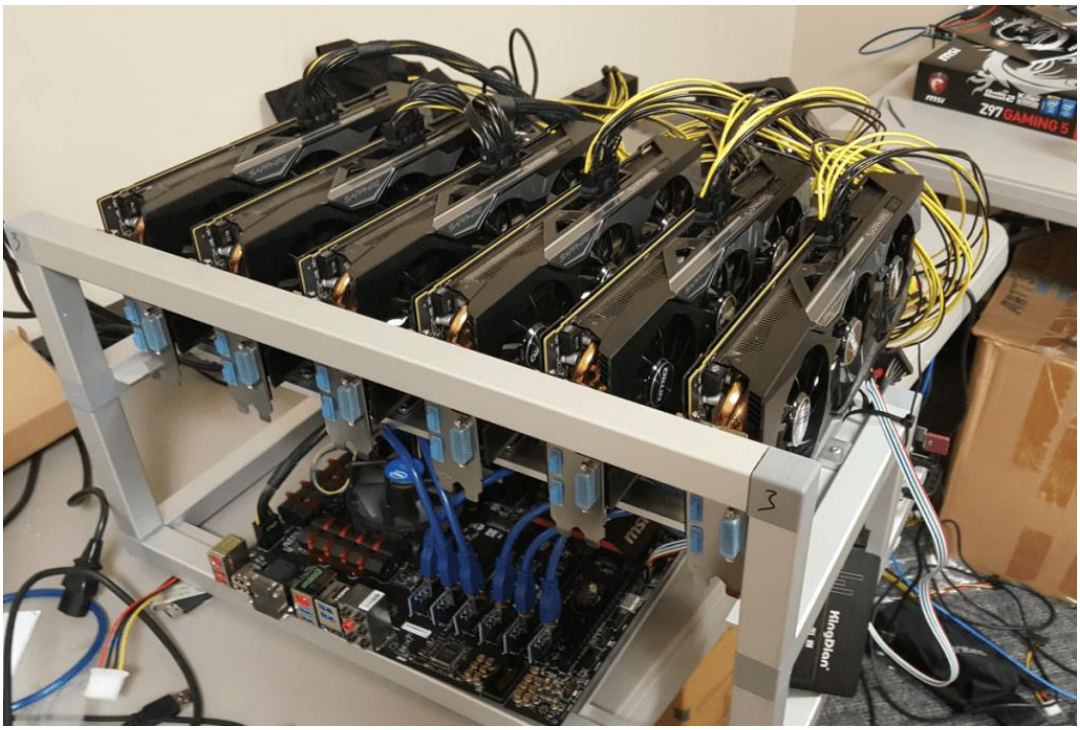
Slika 2.4 Proces kako blockchain postiže konsenzus. Izvor: vlastita grafika

[15] http://solidity.readthedocs.io/en/v0.4.24/ (25.07.2018. u 18:45)

Metodu dokaza radom je razvio tzv. Satoshi Nakamoto, tvorac Bitcoina. Ta se metoda bazira na rudarenju (eng. *mining*). Posebna računala (tzv. *mining rig*) (slika 2.5) ili uređaji namijenjeni rudarenju kao npr. ASIC uređaji (slika 2.6), rješavaju izrazito kompleksne matematičke probleme i nakon uspješnog rješavanja istih bivaju nagrađeni kriptovalutom koju rudare te se tom lancu dodaje novi blok sa svim pripadajućim transakcijama. Matematički problemi rješavaju se metodom pokušaja i promašaja rezultata. Povećanjem uređaja koji rudare raste i kompleksnost matematičkih problema koji se rješavaju i zbog toga se uređaji preko internetske mreže udružuju u rudarska udruženja (eng. *mining pool*) gdje udružuju svoju resursnu snagu (eng. *hash power*).

Glavni nedostatak ove metode je velika potrošnja električne energije pošto procesori i grafičke kartice u navedenim uređajima prilikom rudarenja konstantno koriste svu svoju raspoloživu snagu. Još jedan potencijalni nedostatak je tzv. 51% napad.[16] To najlakše možemo usporediti s preuzimanjem kontrole nad nekom tvrtkom stjecanjem 51% vlasništva te tvrtke. Takav napad je u ovom slučaju izvediv samo ako jedan rudar ili grupa rudara posjeduje 51% ukupne resursne snage neke kriptovalute i lanca. Tako da kao što je spomenuto prije, što je lanac duži to ga je teže prevariti i manipulirati. Pošto je ovo prva metoda postizanja konsenzusa, s vremenom sve njene mane izlaze na vidjelo te se kroz posljednjih nekoliko godina razvilo mnogo drugih metoda koje ispravljaju poznate mane, ali također nisu savršene.

[16] https://bitfalls.com/hr/glossary/#51-napad (27.7.2018. u 19:15)



Slika 2.5 Konfiguracija za rudarenje (mining rig). Izvor: https://blockoperations.com/build-6-gpu-zcash-headless-mining-rig-ubuntu-16-04-using-claymore/ (25.07.2018. u 20:15)

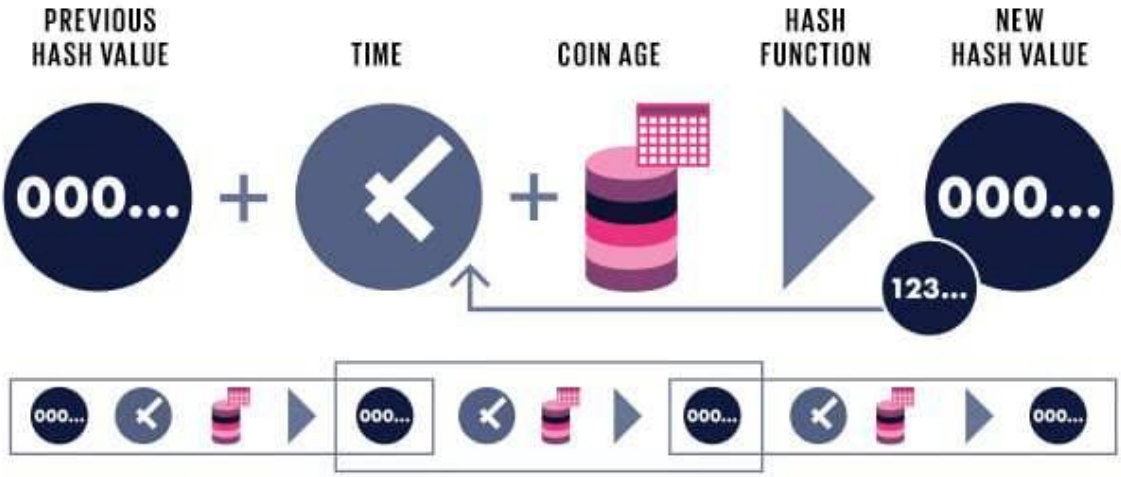
Druga spomenuta metoda konsenzusa je dokaz ulogom i ona se u potpunosti razlikuje od prethodno spomenute metode dokaza radom. Ova metoda ne samo da brže odrađuje transakcije nego je i ekološki prihvatljivija zato što ne traži veliki utrošak električne energije i ne zahtijeva poseban hardver kao metoda dokaza radom. Umjesto izrade novih blokova na temelju rada računala, tvorac bloka se određuje udjelom novaca na računu, tj. ulogom. [17]

[17] https://coincentral.com/making-sense-of-proof-of-work-vs-proof-of-stake/ (27.07.2018. u 20:30)

Slika 2.6 ASIC uređaj za rudarenje. Izvor: https://www.amazon.co.uk/Bitmain-AntMiner-S5-1155Gh-Bitcoin/dp/B00RCTIY4G (25.07.2018. u 20:15)

Neke od poznatijih kriptovaluta koje koriste ovu metodu su Waves, Cardano, OmiseGo te se Ethereum uskoro planira prebaciti na spomenutu metodu i u tijeku pripreme i prilagodbe za postupak prebacivanja. U ovom sustavu, tvorci blokova se biraju na temelju uloga valute i starosti tog uloga. Ako npr. imamo 10.000 novčića (eng. *coin*) kriptovalute Waves, kroz ovaj sustav imamo veću mogućnost biti odabrani kao tvorac bloka nego netko tko na svom računu ima 5.000 istih novčića. Također, ako netko ima isti broj novčića kao i mi, onda će se gledati tko ih duže posjeduje u svom novčaniku (eng. *wallet*) (slika 2.7).

Postoji još nekoliko metoda postizanja konsenzusa kao što su npr. delegirani dokaz radom (eng. *Delegated Proof of Stake* - DPoS), dokaz kapacitetom (eng. *Proof of Capacity* - PoC), bizantinski model zatajenja (eng. *Byzantine Fault Tolerance* - BFT) i dr.



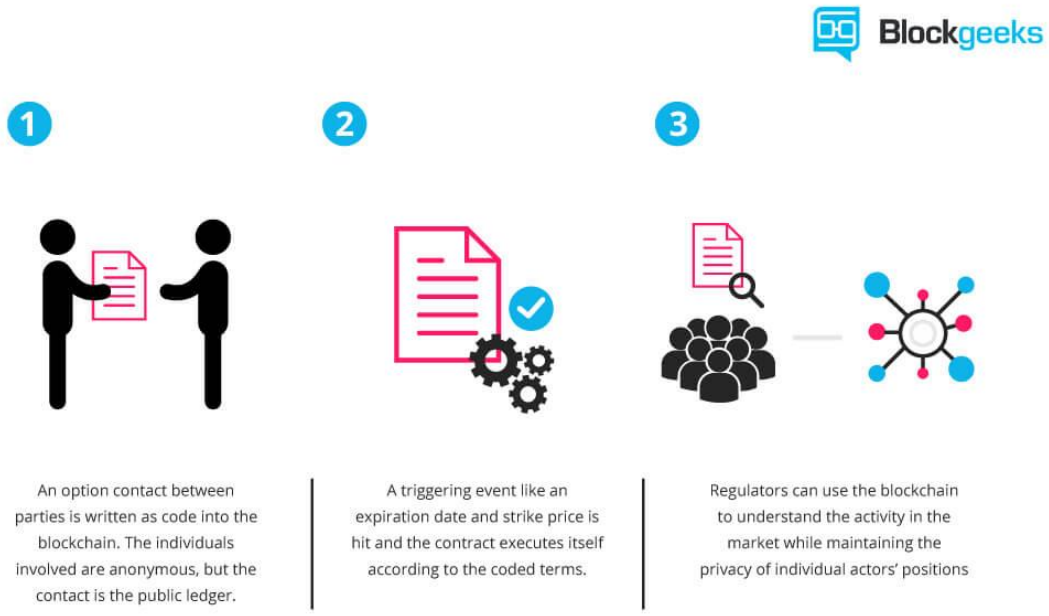
Slika 2.7 Prikaz kako se provodi metoda dokaza ulogom. Izvor: https://coincentral.com/making-sense-of-proof-of-work-vs-proof-of-stake/ (27.07.2018. u 21:00)

2.3. Pametni ugovori

Uz pomoć pametnih ugovora u blockchain se može upisati programski kod ili čak cijele aplikacije. Pametnim ugovorima definiraju se odnosi i ponašanje dviju ili više strana u blockchainu koji posjeduju neku kriptovalutu ili pak neku drugu informaciju ili vrijednost (slika 2.8). Uz ovu vrstu primjene blockchain tehnologije postoji mogućnost da u budućnosti neće biti potrebne standardne usluge odvjetnika, trgovačkih sudova, javnih bilježnika i sličnih. Dobar dio usluga koje oni trenutno nude bit će moguće vrlo lako zamijeniti pametnim ugovorima zato što se odnos korisnika i pružatelja navedenih usluga može vrlo precizno definirati kroz programski kod i unijeti u pametne ugovore koji se kasnije realiziraju ispunjavanjem svih uvjeta, u sklopu transakcije. Realizacija usluga je automatizirana i izuzetno brza što u današnjem obliku nikako nije. Korištenje pametnih ugovora omogućuje isključivanje čitavog niza posrednika u različitim procesima i samim

time omogućava brže i lakše obavljanje aktivnosti, privatnih i, što je bitnije, poslovnih. Mogu se koristi npr. u:[18]

- U osiguranju: ako autorizirani agenti u blockchain upišu da su uvjeti za isplatu osiguranja zadovoljeni, isplata će se automatski odraditi
- U medicinskom osiguranju: ako liječnik ustanovi da je pacijent bolestan i nije u mogućnosti izvršavati poslovne obaveze, u blockchain unosi te podatke, bolesniku se automatski počinje isplaćivati naknada za bolovanje
- U mirovinskom osiguranju: ako autorizirana osoba ili državno tijelo potvrdi da je osoba ispunila uvjete za mirovinu, osobi će se automatski isplaćivati mirovina
- U audio i video industriji: ako korisnik uplati sredstva za gledanje ili slušanje određenog materijala, on automatski dobiva pristup i pravo na kupljeni materijal
- U kladionicama: Korisnik koji uplaćuje okladu, uplaćuje je na račun pametnog ugovora. Nakon što se događaj završi, autorizirana strana upisuje podatke o pobjedniku u blockchain te oni koji su uspješno pogodili rezultati automatski dobivaju isplate



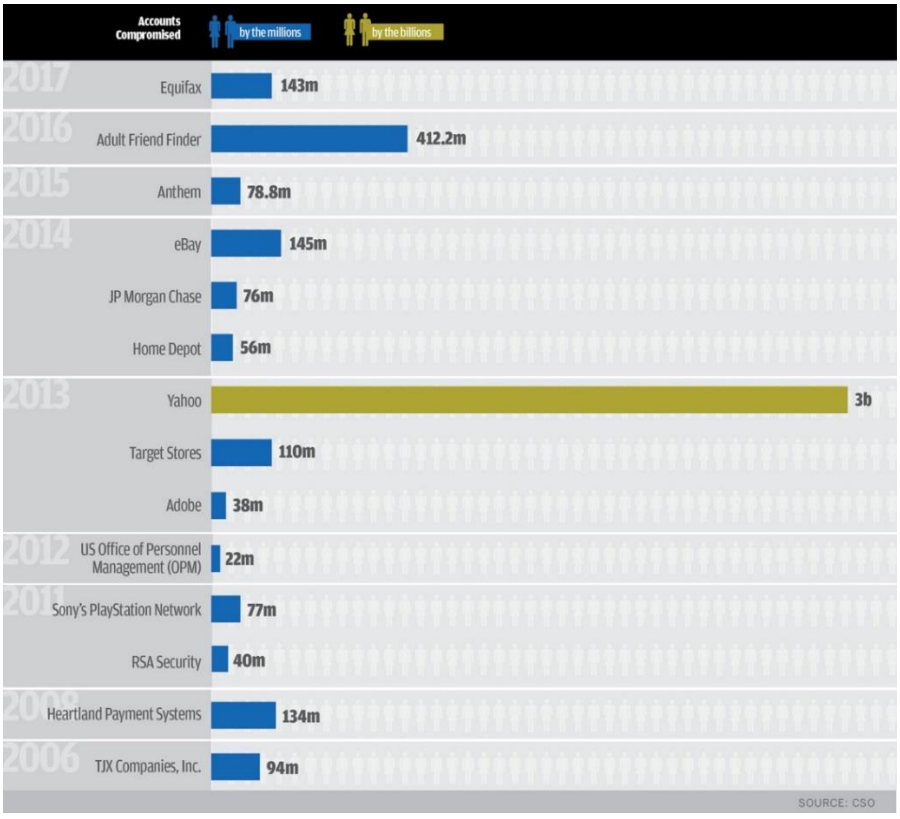
Slika 2.8 Prikaz kako funkcioniraju pametni ugovori. Izvor: https://blockgeeks.com/guides/smart-contracts/ (29.7.2018. u 20:15)

[18] https://ubik.hr/2018/03/26/sto-su-pametni-ugovori-uvod/ (29.7.2018. u 18:30)

3. Platforma

3.1. Blockchain kao tehnologija za razvoj poslovnih modela koji koriste digitalni identitet

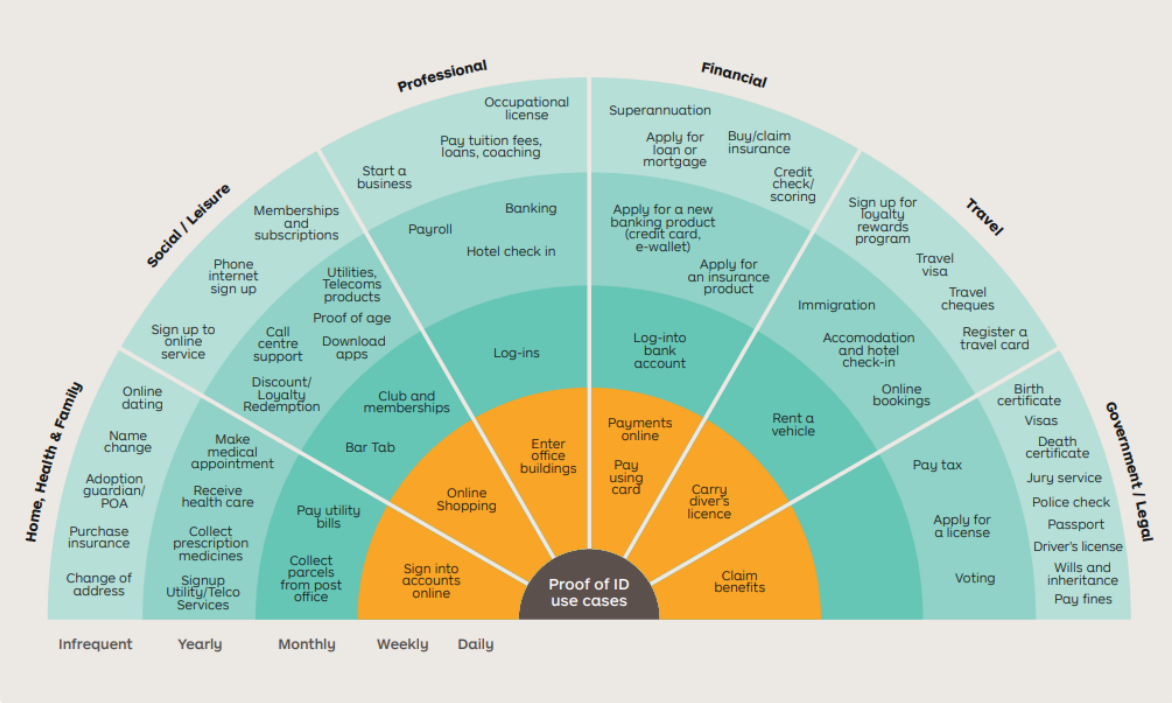
Identitet je vrlo vrijedan no mi, a ni institucije, se danas ne ponašamo u skladu s time. Što zbog manjka svijesti i edukacije o samom identitetu, to zbog digitalne i fizičke centralizacije baza i podataka o našim identitetima koja stvara neizbježne slabe sigurnosne točke koje narušavaju sustavnu vrijednost naših osobnih podataka. Centralizirani sustavi predstavljaju dobar plijen za napadače s lošim namjerama zato što ako provale u sustav vrlo lako mogu ukrasti (kopirati) velike količine podataka koji su pohranjeni u tom sustavu. Svjedoci smo nebrojeno puno napada na centralizirane sustave i to ne na sustave malih tvrtki, nego velikih i globalno utjecajnih tvrtki kao što su Yahoo, eBay, Adobe, JP Morgan Chase, Sony i mnogi drugi (Slika 3.1).



Slika 3.1 Prikaz najvećih napada na informacijske sustave u 21. stoljeću i broj korisničkih računa koji su kompromitirani u tim napadima. Izvor: https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html (1.8.2018. u 18:40)

Blockchain tehnologija nudi rješenje za taj problem koji postaje sve veći zbog konstantne potrebe, povećanja potražnje i korištenja digitalnog identiteta. No, kao što smo prije spomenuli, ovo je nova tehnologija i tek je u fazi samih početaka i još se zapravo istražuju sve mogućnosti i primjene ove tehnologije.

S potrebom za dokazom našeg identiteta susrećemo se svakodnevno i na različitim mjestima (Slika 3.2). Na poslu, u banci, u dućanu, na putovanjima, u državnim institucijama i na još mnogo različitih mjesta.

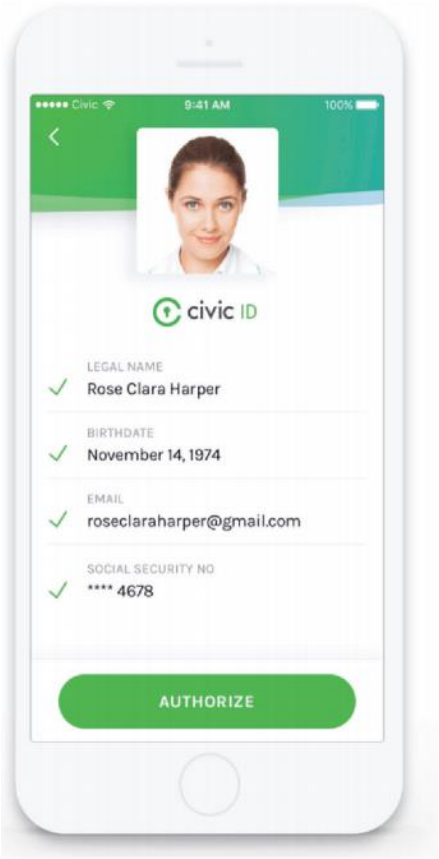


Slika 3.2 Prikaz koliko često i gdje imamo potrebu za dokazom vlastitog identiteta. Izvor: https://auspostenterprise.com.au/content/dam/corp/ent-gov/documents/digital-identity-white-paper.pdf (1.8.2018. u 20:15)

Trenutno ima mnogo novih i perspektivnih projekata i mladih tvrtki koje se bave ovim problemom i pokušavaju pronaći svoje mjesto na tržištu. U ovom dijelu rada ćemo spomenuti neke od njih i pobliže objasniti njihove poslovne modele.

3.1.1. Civic

Civic je tvrtka koja razvija identifikacijski sustav koji korisnicima omogućava selektivno dijeljenje identifikacijskih informacija s tvrtkama. Njihova platforma ima mobilnu aplikaciju (slika 3.3) u koju korisnici unose svoje osobne podatke koji onda pohranjuju u kodiranom (eng. *encrypted*) formatu. Cilj tvrtke je sklopiti partnerstva s državnim vladama i bankama, tj. svima onima koji mogu potvrditi podatke o identitetu korisnika i nakon toga ostaviti pečat ovjere u blockchainu. Sustav radi kriptirani *hash* svih ovjerenih podataka i pohranjuje ga u blockchain te sve osobne podatke korisnika briše s vlastitih servera.

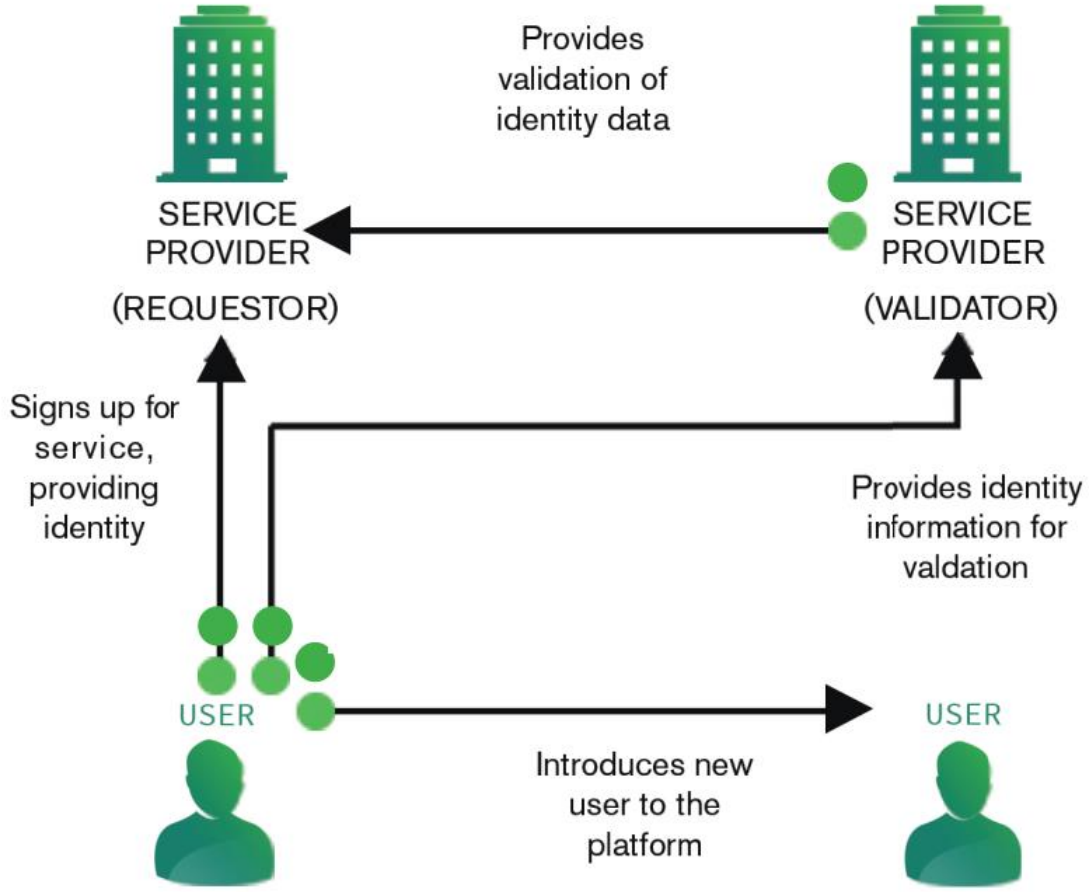


Slika 3.3 Prikaz Civic aplikacije. Izvor: https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf (2.8.2018. u 17:25)

Kao što je tvrtka napisala u svojem White paperu[19], Civic ekosustav je osmišljen tako da potakne sudjelovanje pouzdanih tijela za provjeru identiteta, koje nazivaju „validatori". „Validatori" mogu biti već spomenute državne vlade, banke, zatim razne financijske institucije, itd. Isto kao što Civic trenutno potvrđuje informacije o identitetu korisnika kroz svoju aplikaciju, „validatori" imaju mogućnost potvrditi identitet pojedinca ili tvrtke koji su „korisnici" aplikacije. Zatim „pečatiraju" (eng. *stamp*) tu potvrdu i postavljaju je u blockchain u obliku zapisa poznatog kao „ovjerenje" (eng. *attestation*). To „ovjerenje" je zapravo *hash* osobnih podataka korisnika. Stranke poznate kao „davatelji usluga" (eng. *Service Providers*) koji žele provjeriti iste podatke o identitetu korisnika, više ne bi trebale samostalno provjeravati te iste informacije nego umjesto toga mogu koristiti provjerene informacije za koje garantiraju „validatori" tih istih informacija (Slika 3.4). Cilj je da korisnik ostane „vladar" svog identiteta i da ima potpunu kontrolu nad osobnim informacijama tako da mora dati suglasnost prije svake transakcije informacija o njegovom identitetu između validatora i davatelja usluga. Pomoću pametnih ugovora validatori imaju mogućnost prodavati svoje ovjere davateljima usluga, ali i davateljima usluga omogućuju da vide po kojim cijenama različiti validatori nude svoje ovjere. Svaki validator može objaviti cijenu za koju je spreman prodati osobne informacije korisnika. Nakon što korisnik, validator i davatelj usluga potvrde transakcije putem sustava pametnih ugovora, davatelj usluga plaća validatoru traženi iznos i to u obliku CVC tokena. Nakon toga pametni ugovor će raspodijeliti CVC tokene te će korisnik dobiti svoj dio zbog sudjelovanja. Korisnik može koristiti svoje tokene za kupnju produkata i usluga na Civic platformi. Kao što sam spomenuo, korisnik je taj koji je odgovoran za svoje podatke i pohranjuje ih na neki od svojih osobnih uređaja koristeći Civic aplikaciju te se preporučuje i backup osobnog računa na cloud sustav. Pošto podaci o identitetima korisnika nisu centralizirani, tj. ne nalaze se na poslužiteljima tvrtke Civic ne postoji mogućnost za masovnu krađu identiteta jer se podaci svakog korisnika zapravo nalaze na njihovim uređajima i da bi se ti podaci ukrali, potrebno je provaliti u svaki uređaj zasebno. Taj podatak uvelike pomaže u suzbijanju crnog tržišta osobnim podacima. Npr. crno tržište podataka o kreditnim karticama je dosta raširenо zato što se transakcije mogu odrađivati samo poznavanjem tih podataka, bez znanja korisnika. Ako broj kreditne kartice treba

[19] https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf (2.8.2018. u 18:15)

proći kroz blockchain-ov mehanizam dokazivanja gdje za svaku transakciju treba pristanak korisnika, onda crno tržište takvih podataka polako gubi svoj smisao i vrijednost.



Slika 3.4 Princip rada Civic sustava. Izvor:
https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf (2.8.2018. u 23:05)

3.1.2. HYPR

HYPR[20] je mlada tvrtka, osnovana 2014. godine. Njihov poslovni model je baziran na spajanju biometričkih metoda identifikacije i blockchain tehnologije. Identifikacija biometrikom može zamijeniti klasičnu identifikaciju korisničkim imenom i lozinkom, brža

[20] https://news.bitcoin.com/hypr-3-million-blockchain-biometrics/ (4.8.2018. u 22:05)

je i sigurnija. Biometrikom se mogu prepoznavati različiti dijelovi ljudskog tijela kao npr. geometrija dlana, otisak prsta, šarenica oka, miris, lice i mnogi dugi fiziološki elementi jedinstveni za pojedinca. Biometrika predstavlja vrlo dobar način verifikacije identiteta pojedinca jer ju je vrlo teško, ili pak ne moguće, krivotvoriti.

HYPR[21] stoga nudi platformu za autentifikaciju bez lozinke putem biometrijske enkripcije. Tvrtka se ne bavi razvojem i proizvodnjom uređaja za identifikaciju, nego razvija distribuirani sigurnosni sustav. Kao što je prije spomenuto, svaki digitalni podatak se može ubaciti neki od kriptografskih algoritama i dobiti svoj *hash*. Taj *hash* se može koristiti za provjeru validnosti tih digitalnih podataka bez potrebe da validator ima kopiju tih podataka. Npr. očitamo naš prst na čitaču otiska prsta na mobilnom telefonu i tvrtka koja ima pristup *hashu* našeg otiska u digitalnom obliku može potvrditi naš identitet, i to bez mogućnosti da se lažno predstavljaju kao mi. Digitalni otisak je samo dio mogućnosti koji se nudi. HYPR podržava mnogo tipova biometričkih podataka, od jednostavnih autentifikacijskih algoritama za prepoznavanje lica i govora do puno kompleksnijih algoritama kao što su način na koji tipkamo po tipkovnici, ritam kojim pišemo poruke na mobilnim uređajima ili pak način na koji hodamo. Uz pomoć blockchaina i decentralizacije podataka, autentifikacija postaje mnogo brža i jednostavnija. Svaki korisnik je odgovoran za svoje biometrijske podatke koji se nalaze npr. na njegovom mobilnom uređaju. Tako se izbjegavaju masovne krađe podataka, dok su pojedinačne krađe i dalje moguće, ako korisnik nije dovoljno oprezan kod zaštite svojih podataka i uređaja. Ovakav sustav baziran na blockchain tehnologiji otporan je na napade uskraćivanja usluga (eng. *Denial of service* - DoS) koji su boljka centraliziranih sustava. DoS napadi su napadi na neki računalni servis s ciljem da se onemogući njegovo korištenje. U ovom slučaju umjesto napada na jedan poslužitelj koji se koristi za autentifikaciju podataka, DoS napadači bi trebali identificirati i napasti sve blockchain nodove tog sustava. Iz tvrtke naglašavaju da je uz zaštitu od DoS napada jednako važna i interoperabilnost poslovnih procesa. Trenutno ne postoji mogućnost autentifikacije između dva različita korporativna entiteta kao što su npr. banka i tvrtka za osiguranje. Svaka od tvrtki ima drugačiju bazu identiteta i one nisu interoperabilne. Koristeći blockchain tehnologiju, možemo imati interoperabilnu distribuiranu glavnu knjigu identiteta između više entiteta bez potrebe za složenom i

[21] https://www.forbes.com/sites/jonathanchester/2017/04/28/how-blockchain-startups-will-solve-the-identity-crisis-for-the-internet-of-things/#1a87dafb5c63 (6.8.2018. u 19:45)

skupom infrastrukturom. Tako tvrtka za osiguranje može dokazati naš identitet banci kroz biometrijske podatke.

3.1.3. Blockverify

Problem dokazivanja identiteta ne pojavljuje se samo kod ljudi. On također može biti prisutan i kod različitih proizvoda kao npr. lijekovi, luksuzni proizvodi, dijamanti, elektronika, glazba, softver itd. Navedeni proizvodi često su krivotvoreni i time se proizvođačima nanosi šteta u bilijunskim iznosima. (Tablica 3.1)

Tablica 3.1 Krivotvoreni proizvodi i njihova vrijednost u dolarima. Izvor: https://www.havocscope.com/counterfeit-goods-ranking/ (7.8.2018. 20:45)

Lijekovi	200 milijardi
Elektronika	169 milijardi
Softver	63 milijarde
Hrana	49 milijardi
Auto dijelovi	45 milijardi
Dječje igračke	34 milijarde
Glazba	12.5 milijardi
Obuća	12 milijardi
Odjeća	12 milijardi
Video igrice	8.1 milijardi
Kozmetika	3 milijarde
Oružje	1.8 milijardi
Diplome	1 milijarda

Ljudi koji stoje iza Blockverify projekta žele smanjiti broj krivotvorenih proizvoda na tržištu sprječavanjem pojave duplikata. Različite tvrtke iz različitih industrija mogu registrirati i pratiti svoje proizvode pomoću Blockverifya i blockchain tehnologije.

Iz tvrtke smatraju da se poboljšanje mjera protiv krivotvorenih proizvoda može postići jedino korištenjem decentraliziranog, skalabilnog i od napada sigurnog rješenja. Blockverify[22] ima svoj privatni blockchain, ali koristi i Bitcoinov blockchain u koji bilježi važne promjene u svom lancu. Njihov lanac je vrlo skalabilan i transparentan kako bi svaki proizvedeni proizvod u njega mogao ući kao sredstvo (eng. *asset).* Nakon toga svaki od tih *asseta* će biti dodan u blockchain te će im biti dodijeljen jedinstveni *hash.* Bilo tko, pomoću tog *hasha* može pristupiti blockchainu i provjeriti je li proizvod valjan ili ne. Primarni cilj tvrtke je riješiti problem krivotvorenih lijekova koje je prvo na ljestvici krivotvorenih proizvoda, ali ujedno i jedan od opasnijih krivotvorenih proizvoda jer direktno utječe na zdravlje ljudi i uzrokuje milijune smrtnih slučajeva godišnje. Još jedan problem koji tvrtka želi riješiti je problem verifikacije vlasništva. Zahvaljujući blockchain tehnologiji, promjene vlasništva se vrlo lako mogu trajno zabilježiti. Ovakvim načinom je onemogućeno da pojedinci rade duple zapise i neautorizirane promjene.

[22] https://bitcoinist.com/block-verify-turns-bitcoin-life-saving-technology/ (7.8.2018. u 21:30)

3.2. Usporedba tradicionalnih modela s onima baziranim na pametnim ugovorima

3.2.1. Osiguranje od otkaza ili kašnjenja avionskog leta

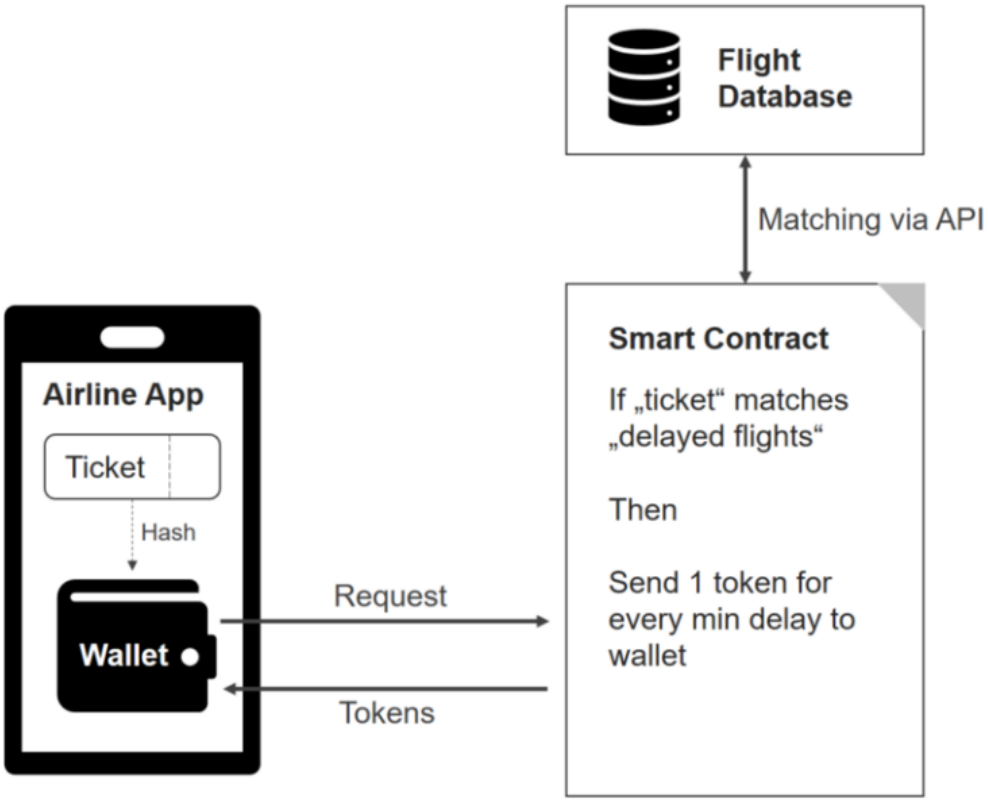
Otkazivanje i kašnjenja avionskih letova su svakodnevna pojava na aerodromima, ali povrat novca korisniku, na koji on potpuno ima prava, nije. Primarni razlog tome je taj što većina ljudi ne zna koja su njihova prava u navedenim slučajevima. Proces dobivanja povrata novca je izuzetno kompliciran i oduzima puno vremena i živaca. Ovakvo stanje stvari izuzetno odgovara i pogoduje aviokompanijama. Naime, da bi pojedinac dobio povrat sredstava, on prvo mora proučiti sva svoja prava kroz postojeću regulativu, zatim napisati žalbu, ponekad čak i u pisanom obliku na papiru, nakon toga mora ispunjavati kojekakve forme s previše informacija i dokazivati svoj identitet i činjenicu da je on stvarno vlasnik te avionske karte čiji je let otkazan ili kasni. U čitavom tom procesu, vrlo vjerojatno će doći do određenih nejasnoća kod korisnika te će možda biti potrebno kontaktirati službu za korisnike koja vrlo često komunicira preko email poruka. Za sve nabrojano, vrlo vjerojatno je potrebno više od jednog dana, ponekad i nekoliko tjedana. Ljudi vrlo često nemaju vremena raditi istraživanja, pisati email poruke i savjetovati se na različitim stranama te odustaju od samog postupka ili usred postupka ako dođe do zastoja procesa zbog nekog problema. No, kada se dobije odgovor aviokompanije, oni najčešće prvo nude kupone koji se mogu iskoristiti za usluge u njihovoj ponudi ili pak nude da će poslati ček. Problem kod toga je što ne znate hoćete li ikada uspjeti iskoristiti kupon koji nude, a problem kod čekova je taj što banka uzima veliku proviziju kod unovčavanja čekova. Stoga se i u ovom slučaju korisnik mora dobro informirati i mora znati da sve ponude aviokompanija mogu odbiti i imaju pravo tražiti da im se uplati iznos putem bankovnog transfera. No ni tu problemima nije kraj, da bi korisnik iskoristio najbolji mogući način povrata sredstava, a to je spomenuti bankovni transfer, korisnik mora imati bankovni račun na kojem je omogućeno uplaćivanje deviza iz inozemstva. Danas čak postoje tvrtke koje se isključivo bave poslom potraživanja sredstava u ime korisnika i naplaćuju se iz uspješno odrađenih poslova uzimajući određeni postotak od vraćenih sredstava.

Rješenje ovog problema možemo naći u blockchainu i pametnim ugovorima. No rješenje nije toliko jednostavno jer korisnici vrlo često svoje karte kupuju na servisima drugih kompanija. Pošto aviokompanije nemaju pristup podacima ostalih kompanija koje vrše prodaju karata, potrebno je omogućiti interoperabilnost sustava koja je moguća uz blockchain.

Blockchain nudi mogućnost da se uspostavi sustav na principu pametnih ugovora koji automatski isplaćuje korisniku tokene u slučaju kašnjenja ili otkaza leta. Korisnik ne mora napraviti ništa jer se sva pravila i uvjeti unose u kod pametnog ugovora i on se automatski realizira. Korisnik kasnije može iskoristiti tokene za usluge aviokompanije ili ih pak može unovčiti na način da ih proda drugom korisniku kojem je možda potrebno nekoliko tokena kako bi imao mogućnost iskoristiti ih za neki od letova. Ovakav način ne samo da smanjuje troškove administracije nego poboljšava odnos između korisnika i aviokompanije i sve sudionike stavlja u tzv. win-win situaciju, što znači da su svi na dobitku.

Kako funkcioniraju pametni ugovori u ovom slučaju? (Slika 3.5) Dakle, novčanik (eng. *wallet*) je direktno integriran u naš korisnički račun kod aviokompanije. Svaki puta kada kupimo kartu aktivira se zahtjev kod pametnog ugovora koji sadrži *hash* naše karte. Pametni ugovor kontinuirano prati podatke o odgođenim letovima i podatke na našoj karti. Ako se dogodi otkaz ili kašnjenje određenog leta, a taj let se nalazi na našoj karti, pametni ugovor će automatski pokrenuti isplaćivanje tokena na naš *wallet* za svaku minutu kašnjenja leta ili određenu količinu tokena u slučaju otkaza leta. Ovakav sustav također može nagrađivati lojalne korisnike koji koriste istu aviokompaniju iako im se dogodilo nekoliko kašnjenja ili otkaza letova. No, što u slučaju da aviokompanije nisu zainteresirane za ovakvo rješenje? Pametnim ugovorima se i dalje može omogućiti, već spomenutim tvrtkama koje se bave isključivo potraživanjem povrata sredstava u ime korisnika, da otkupe još ne vraćenu naknadu od korisnika. Putnici odgođenog leta mogu poslati svoje podatke pametnom ugovoru. On ih ovjerava pomoću javno dostupnih podataka i izdaje token za odgođeni let, koji sadrži sve podatke potrebne za podnošenje zahtjeva prema aviokompaniji. Time je omogućeno trgovanje još neostvarenim povratom. Tako bi svatko mogao otkupiti taj token i pokrenuti postupak povrata sredstava od strane aviokompanije. Ovakvim bi načinom oštećeni putnici dobili možda više novaca nego da su sami krenuli u proces dok bi aviokompanije zasigurno dobile mnogo više zahtjeva za povratom sredstava

što bi ih onda vrlo vjerojatno na kraju prisililo da prihvate ono prvo rješenje koje svima ide u korist.[23]



Slika 3.5 Uloga pametnih ugovora kod kupnje avionskih karata. Izvor: https://medium.com/cashlink-crypto/eliminate-the-hassle-of-flight-delay-compensation-by-using-smart-contracts-a5db3b5c3ed (9.8.2018. u 20:30)

Postoji nekoliko projekata i tvrtki koji se trenutno bave navedenim problemom i razvijaju vlastite platforme bazirane na gore opisanom modelu. Najpoznatiji i najperspektivniji su TustaBit i Fizzy.

[23] https://medium.com/cashlink-crypto/eliminate-the-hassle-of-flight-delay-compensation-by-using-smart-contracts-a5db3b5c3ed (9.8.2018. u 19:45)

3.2.2. Glasanje

Sustav u kojem nije moguće namještanje izbora i lažiranje glasova, sustav koji je 100% povjerljiv i transparentan? Zvuči ne moguće, no u teoriji blockchaina i pametnih ugovora itekako je moguć.

Glasovanje na izborima spada u transakcije visoke vrijednosti i rizika. Stoga, nije ni čudo da se današnja metoda glasovanja ne razlikuje puno od metoda koje su se koristile davno prije. Ipak, glasovanje na papiru je danas stvarno i sigurnije od elektroničkog glasovanja internetom, na centraliziranim sustavima. Danas, proces ide tako da svaka osoba mora fizički doći na određenu lokaciju, identificirati se, dobiti glasačke listiće, zatim odabrati kome će dati svoj glas, nakon toga ubaciti listiće u glasačku kutiju te se nakon završetka izbora svi ti glasovi moraju fizički prebojavati prije objave rezultata. Kao što vidimo, proces je vrlo dug. Potrebno je puno radne snage, sredstava i puno vremena kako bi se sve odradilo bez grešaka. U ovakvom sustavu nerijetko se događa da „glasaju“ ljudi koji su umrli ili da su glasali ljudi koji uopće nisu izašli na biračka mjesta.

U ovom slučaju, implementacijom pametnih ugovora u sustav, riješili bi se navedeni problemi. Pametni ugovori bi se postavili između dvije strane (u ovom slučaju između građana koji ima pravo glasovanja i države) te bi se automatski aktivirali prilikom glasovanja pojedinca. Takvim se principom osigurava da svaki građanin ima samo jedan glas i da se nakon predavanja glasa, odabir ne može mijenjati jer je transakcija trajno zapisana u blockchain. U fazi prebrojavanja glasova vidjeli bi zapravo najveću promjenu u odnosu na trenutni model glasovanja. Naime, završetkom glasovanja u istom trenutku bi se mogli prikazati u potpunosti točni podaci i statistike, bez potrebe za brojanjem glasova, što zaista ubrzava proces i drastično smanjuje njegove troškove. Također, ovakvim bi se pristupom povećala i izlaznost građana na glasovanje jer ljudi vrlo često niti ne stignu doći na biračka mjesta predati svoj glas, možda zbog posla, obaveza, djece, itd. Zbog svega navedenog, da se ljudima omogući sigurna predaja svojih glasova putem svog računala ili pametnog telefona, dobili bi brže, kvalitetnije, i što je najbitnije jeftinije i transparentnije izbore.

Koliko god ovakav princip zvuči primamljivo, također ga nije jednostavno provesti. Djelomično zato što je sama tehnologija blockchaina i pametnih ugovora u vrlo ranoj fazi i još se istražuju i testiraju njihove mogućnosti. No, dugoročno gledajući, uz adekvatnu

edukaciju države i njenih građana, smatram da bi ovakva rješenja svakako dala svoj doprinos, prvenstveno u uštedama novca koji bi se mogao dalje pametno ulagati.

3.2.3. Glazbena industrija

Jedan od većih problema u glazbenoj industriji danas je taj što ne postoji nikakav službeni javni registar glazbenika i njihovih djela.[24] Bilo je pokušaja kreiranja takvog registra, no bezuspješno su potrošeni milijuni dolara bez nekakvog konkretnog rješenja. Postoje agencije koje osiguravaju da tekstopisci, glazbenici, izvođači i izdavači dobivaju svoje zaslužene naknade. Ponovo, to je centraliziran sustav, koji nije imun na manipulacije i namještanje podataka. Kao što to biva u svakom poslovanju koje nije transparentno, ovakav model je podložan mnogobrojnim prevarama a samim time i mnogobrojnim tužbama s odštetama u desecima milijuna dolara. Problemi u glazbenoj industriji zasigurno bi se smanjili kreiranjem javnog registra u koji bi tvorci glazbe unosili svoj materijal. Ljudi koji zapravo proizvode glazbu, vrlo često budu posljednji u redu za isplate zarade na toj glazbi.

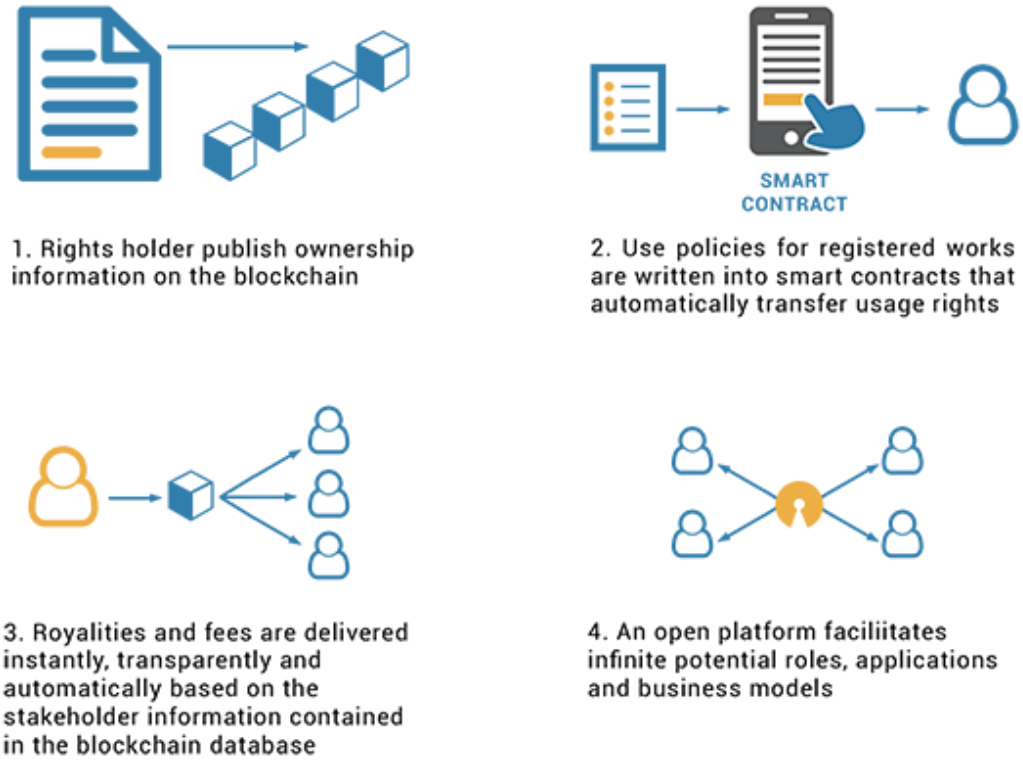
Iskoristimo li mogućnosti pametnih ugovora u ovom slučaju to bi izgledalo ovako: (Slika 3.6)

1. Tekstopisac napiše tekst pjesme
2. Glazbenik/skladatelj napiše glazbu za taj tekst
3. Glazbeni producent snimi, uredi i pripremi glazbu za produkciju

Nakon ovog procesa, svi dionici se dogovaraju koliki je njihov zasluženi postotak zarade koju će generirati novonastala pjesma. Nakon postignutog dogovora, ti podaci se unose u pametni ugovor. Pjesma i pametni ugovor se zatim postavljaju u blockchain, uzmimo za primjer Ethereum. Korisnik koji želi slušati novu pjesmu, ima ju mogućnost kupiti za određenu količinu Ethereuma. Korisnik se odlučuje za kupnju i na račun pametnog ugovora uplaćuje traženi iznos. Pametni ugovor zatim u svom kôdu pregledava unesene podatke i na temelju tih podataka automatski prebacuje dogovorene iznose svim ranije navedenim dionicima. Korisniku se, nakon uplate, automatski ponudi kupljeni materijal na slušanje. Na ovaj način direktno povezujemo tvorce glazbe s njenim korisnicima i

[24] https://hbr.org/2017/06/blockchain-could-help-musicians-make-money-again (11.8.2018. u 19:45)

omogućujemo glazbenicima da bolje upoznaju svoju publiku i na temelju toga stvaraju bolji sadržaj.



Slika 3.6 Pametni ugovori u ulozi isplata honorara. Izvor: https://www.draglet.com/blockchain-services/smart-contracts/use-cases/ (11.8.2018. u 20:30)

3.2.4. Praćenje osobnih zdravstvenih podataka

Zdravstvo je, čini se, u problemima u skoro svakoj državi. Ne može se vrlo često čuti da zdravstveni sustav neke države funkcionira bez problema i poteškoća. Na stranu općih problema u zdravstvu, uočavamo i problem u praćenju zdravstvenih zapisa o pojedincima (pacijentima). Donedavno je svaki pacijent imao svoj zdravstveni karton koji je bio fizički pohranjen kod doktora opće prakse koji je bio zadužen za tog pacijenta. Nakon toga, ti

kartoni su se polako prebacili u digitalni oblik te se sada svi podaci o pacijentima nalaze na računalima, ali u centraliziranom sustavu. U ovakvom obliku pohrane podataka pacijenti nemaju pristup podacima koji se odnose na njihovo zdravlje i što je još gore, pacijenti uopće ne znaju za što se sve njihovi podaci koriste.[25]

Procesi u zdravstvenom sustavu puni su zapisa. Zdravstveni zapisi, povijesti bolesti, laboratorijski nalazi, dijagnostički pregledi, propisani lijekovi, itd. Sve to zahtjeva previše papira, a samim time i usporava proces liječenja pacijenata. Ovo vrlo često stvara problem kod kooperacije više liječnika koji se brinu od istom pacijentu. Ako pacijent želi promijeniti doktora, mora proći kroz mukotrpan proces ispunjavanja papirologije. Drugi primjer su pacijenti s kroničnim bolestima. Oni imaju potrebu za praćenjem i brigom o zdravlju 24 sata dnevno. Ti pacijenti i tim doktora koji se brinu za njegovo zdravlje nemaju adekvatan i učinkovit način pristupa zdravstvenim podacima pacijenta.

Postavljanjem svih spomenutih zdravstvenih zapisa u blockchain olakšava situaciju i pacijentu i liječniku. Svaki liječnik kod kojeg dođe novi pacijent ne mora provjeravati podatke o zapisima putem telefona ili nekog drugog kanala nego sve podatke ima dostupne na računalu, ako mu za to ovlaštenje da pacijent. Uzmimo za primjer osobu koja ima zdravstveno osiguranje. Pojedinosti njegove police osiguranja zapisuju se unutar njegovog profila unutar blockchaina. Kada pacijent koristi usluge bolnice koje su pokrivene tim osiguranjem, tada se pametni ugovor automatski aktivira i prebacuje sredstva s računa osiguravajuće tvrtke na račun bolnice. Ovakav način bi trebao imati pozitivan utjecaj na pošteno izvršavanje police osiguranja. Smanjio bi neučinkovitost i stres koji nastaju prilikom ispunjavanja obrazaca osiguranja nakon korištenja bolničkih usluga. Postavljanje osobnih zdravstvenih podataka u blockchain i pametne ugovore stvara jedan novi, nepromjenjivi i neovisan sustav u kojem su svi zapisi o pacijentima potpuno sigurni i trajni. Time bi se stvorila nova tzv. digitalna zdravstvena industrija koja ima mnoštvo prednosti nad starim modelom. Najbitnija prednost je transparentnost za obje strane, liječnika i pacijenta. Kao što je gore već spomenuto, trenutni model koji se koristi nije dovoljno transparentan i pacijent zapravo ne zna kako i u koje svrhe su korišteni podaci o njegovom zdravlju. Pomoću blockchaina podaci poput bolesti, liječničkih pregleda, nalaza i propisanih lijekova mogu se kriptirati i postaviti u blockchain nakon čega pacijent dobiva

[25] https://applicature.com/blog/blockchain-healthcare-smart-contracts-2 (11.8.2018. u 22:25)

privatni ključ za pristup tim podacima. Tako pohranjeni podaci su sigurni i samo pacijent ima ovlaštenja drugima dati da provjeravaju njegove podatke. Takvi podaci se također mogu koristiti u istraživačke svrhe, no u ovom slučaju identitet pacijenta ostaje anoniman što definitivno doprinosi napretku zdravstva, bez narušavanja privatnosti i identiteta pacijenta. Također, postoji mogućnost kreiranja liste čekanja za transplantacije organa gdje se donori i primatelji mogu transparentno povezati. Koristeći ovu tehnologiju korisnik bi u svakom trenutku mogao znati gdje se nalazi na listi čekanja i mogao bi biti siguran da će ostati na tom mjestu te da ga nitko ne može od tamo maknuti.

4. Primjena

4.1. Opis primjene tehnologije u odabranim industrijama

4.1.1. Fintech industrija

Fintech industrija je možda najveća i najutjecajnija industrija koja će se implementacijom blockchaina promijeniti na bolje. Bitcoin, koji je prvotno predstavljao prijetnju cijeloj industriji, možda bude katalizator njene disrupcije, jer protokol na kojem je stvoren može biti od velike važnosti za svijet financija. Svaka osoba je na neki način dio ove industrije koja je bazirana na transakcijama, a kao što je ranije spomenuto, blockchain pruža potpuno novi model zapisivanja i praćenja transakcija. Stoga, logičan slijed događaja je prilagodba industrije novoj tehnologiji.

Transakcije su oduvijek bile skup i dugotrajan proces, posebice prekogranične transakcije. Ako se npr. nalazimo u Europi i želimo poslati novac nekome u Ameriku, šaljemo novac preko svoje lokalne banke u lokalnu banku u kojoj osoba kojoj šaljemo novac posjeduje račun. Taj novac mora proći nekoliko konverzija i banaka prije nego što dođe na odredište i postane spreman za isplatu. Postoje mnogi servisi za brzo slanje novaca kao npr. Western Union, no takvi servisi obično su višestruko skuplji od slanja putem bankovnih računa. Blockchain tehnologija drastično može ubrzati taj proces i raskinuti granične barijere koje trenutno usporavaju i poskupljuju proces, a uz to, gubi se potreba i za nizom posrednika. Sve to čini proces mnogo povoljnijim. Trenutni trošak novčanih doznaka iznosi 5-20 %, dok bi se implementacijom blockchain tehnologije dodatni troškovi smanjili na 2-3 % ukupnog iznosa uz sigurne transakcije u realnom vremenu.[26]

Drugi financijski sektor koji također može imati benefita od ove tehnologije je trgovina dionicama. Kupnja, prodaja i posjedovanje dionica oduvijek je uključivala mnoge posrednike. To su prvenstveno burze, na kojima se vrši proces trgovanja, ali i brokeri koji na njima trguju. Današnje burze su centralizirani sustavi, no stvaranjem decentraliziranih

[26] https://www2.deloitte.com/nl/nl/pages/financial-services/articles/1-blockchain-speeding-up-and-simplifying-cross-border-payments.html (27.8.2018. u 19:45)

burzi baziranih na blockchainu kreira se bolja povezanost između ponude i potražnje te se svakom dioniku daje mogućnost da dâ svoju privolu za validaciju transakcija. Takvim se načinom ubrzava proces dogovaranja cijena, omogućava se veća preciznost trgovanja te se iz cijele priče izbacuju posrednici, koji su u ovom slučaju brokeri. Ovakvim bi se pristupom promijenile uloge dionika u procesu trgovanja. [27]

Uz sve dobro što ova tehnologija nudi, postoje mnogi rizici i segmenti na koje treba obratiti posebnu pozornost kao što su npr. privatnost, regulacija i skalabilnost. Ta tri segmenta su vrlo bitna i sve dok se ne omogući sigurnost na svim poljima, ne možemo očekivati globalnu implementaciju i masovno korištenje tehnologije. Trenutno ne postoji niti jedno centralno tijelo ili organizacija koja prati i regulira blockchain protokole. To je veoma osjetljivo područje i zapravo je pozitivno da stvari idu sporijim tokom uz detaljna istraživanja i testiranja mogućnosti tehnologije. Što se tiče skalabilnosti, blockchain tehnologija još nije napredovala do te razine kako bi se mogla koristiti masovno i globalno. To smo najviše osjetili kod drastičnog povećanja zainteresiranosti javnosti i ulagača u kriptovalute krajem 2017. godine. Naime, u tom razdoblju naglog porasta zainteresiranosti, mnoge su burze i mjenjačnice kriptovaluta morale zatvoriti pristup i registracije novih korisnika. Cijela zajednica nije očekivala takav drastičan porast korisnika, no nakon tih početnih problema, blockchain tehnologija je pokazala da je ovdje za duge staze i da će stvarno jednoga dana promijeniti svijet kakvog poznajemo. Nakon otprilike pola godine intenzivnog rada na skalabilnosti, sve je ponovno dovedeno u red te su burze i mjenjačnice opet počele primati nove korisnike. Kao primjer možemo uzeti podatak da je jedna od poznatijih burzi kriptovaluta, Binance, u tom razdoblju na dnevnoj bazi imala i više od 250.000 zahtjeva za registraciju novih korisnika uz dnevni promet trgovanja veći od 9.5 milijardi dolara. [28]

Procijenjeno je da će biti potrebno 7 do 10 godina da tehnologija dosegne tu razinu gdje će se moći koristiti masovno i globalno u komercijalnim i međubankovnim transakcijama. [29]

---

[27] https://www2.deloitte.com/nl/nl/pages/financial-services/articles/2-blockchain-and-the-future-of-share-trading.html (27.8.2018. u 20:15)
[28] https://cointelegraph.com/news/exponential-growth-cryptocurrency-exchanges-are-adding-100000-users-per-day (27.8.2018. u 20:45)
[29] https://blockchainapac.fintecnet.com/uploads/2/4/3/8/24384857/fintech_blockchain_report_v3.pdf (27.8.2018. u 21:00)

4.1.2. Osiguranje

Industrija osiguranja je jedna od najvećih svjetskih industrija. U konstantnom je porastu, što govori podatak da su globalne premije osiguranja u 2017. godini iznosile gotovo 5 bilijuna dolara, što je 1.5% više nego 2016. godine.[30] Stoga se s nestrpljenjem prati istraživanje i razvoj blockchain tehnologije koja bi implementacijom u ovu industriju drastično ubrzala većinu procesa te bi definitivno povećala efikasnost u izvršavanju istih.

U današnje vrijeme osiguravajuće kuće često nude svoje usluge putem telefonskih poziva. Nakon odabira usluge, korisnik dolazi u osiguravajuću kuću sklopiti policu osiguranja. Podaci se vrlo često prikupljaju i obrađuju na papiru. Takav način je sklon pogreškama i za provođenje je potreban konstantan nadzor zbog mogućih pogrešaka u svakom koraku procesa, što naravno, povećava rizik za osiguravajuće kuće. Prebacivanjem procesa i podataka u blockchain, izbjegle bi se potencijalne točke neuspjeha u procesu te bi se drastično umanjio rizik od gubitka podataka, krivo tumačenih polica osiguranja, a smanjilo bi se i vrijeme potrebno za postizanje nagodbi.

Blockchain tehnologija može pridonijeti otkrivanju prijevara i prevenciji rizika. Opisani model kojim se procesuiraju osiguranja podložan je manipulacijama i prijevarama, baš iz tog razloga što je proces spor i što se neki procesi i dalje vrše preko papira. To omogućava kriminalcima da krivotvore i manipuliraju potraživanja od više različitih osiguravatelja, ali isto tako omogućava lažnim prodavačima osiguranja da prodaju police osiguranja i da premije uzimaju sebi. Procjenjuje se da ukupni trošak prijevara osiguranja u Americi iznosi čak i do 40 milijardi dolara godišnje, ne uključujući zdravstveno osiguranje. Ovaj podatak ne ide na štetu samo osiguravajućih kuća, nego to direktno osjete i korisnici osiguranja čije su godišnje premije zbog toga od 400 do 700 dolara veće nego u slučaju da ne postoje navedeni gubitci.[31] Blockchain bi u ovom primjeru omogućio stvaranje ekosustava koji bi se sastojao od distribuiranje glavne knjige u kojoj bi trajno bili zapisani podaci o transakcijama uz, naravno, kontrolirani pristup i zaštitu podataka. Ovakav način bi

[30] http://www.xprimm.com/Swiss-Re-s-sigma-The-global-insurance-market-slowed-down-in-2017%3B-emerging-markets-and-the-US-strengthening-economy-will-lead-future-growth-articol-117,149-11571.htm (3.9.2018. u 19:45)

[31] https://www.cbinsights.com/research/blockchain-insurance-disruption/ (3.9.2018. u 20:30)

omogućio kooperaciju svih osiguravajućih kuća te bi se tako vrlo lako mogle uočiti svi pokušaji kriminalnih radnji.

Ugovor na papiru je sporazum između dvije ili više strana koji je provediv u skladu sa zakonom. Pametan ugovor je također sporazum između dvije ili više strana koji je trajno zapisan na blockchainu i može se izvršiti programskim kodom. Svaki ugovor na papiru se može pretvoriti u programski kod i postaviti u pametni ugovor koji može automatizirati obradu zahtjeva i izračun naknada za sve uključene u proces. Kao primjer možemo uzeti ranije navedeno osiguranje od otkaza ili kašnjenja avionskog leta. Pametan ugovor bi mogao biti povezan s bazom podataka u kojoj se nalaze podaci o letovima, te u slučaju zakašnjelog ili otkazanog leta, automatski pokreće proces povrata sredstava korisniku.

Jedna od najvećih europskih osiguravajućih kuća Allianz nedavno je pokrenula blockchain prototip izrađen na Hyperledger Fabric 1.0 programskom okviru (eng. *framework*). Prototip je, između ostalog, namijenjen osiguranju imovine i povezuje se s CitiConnectovim aplikacijsko programskim sučeljem (eng. *application programming interface,* API) kako bi preuzeo instrukcije i ugovore o isplati. Prototip na blockchain bilježi obnavljanje polica osiguranja, plaćanje premija i obradu potraživanja i uvelike pojednostavljuje protok transakcija između stranaka. Kao što kaže predsjednik Allianz Risk Transfer Gropu, Yann Krattiger, „Automatizirana obrada podataka zamjenjuje razmjenu tisuće email poruka i masivnu količinu podatkovnih datoteka.“ [32]

Blokchain može povećati učinkovitost osiguravajućih kuća, ali isto tako može dovesti i do puno boljeg korisničkog iskustva za korisnike osiguranja. Npr. DocuSign je u partnerstvu s Visa-om nedavno također pokrenuo prototip koji pojednostavljuje proces leasinga i osiguranja automobila elektroničkim putem na blockchainu. Svaka interakcija u tom procesu, od odabira automobila, sve do odabira plana osiguranja i načina plaćanja, bilježi se, ažurira i verificira na blockchainu.[33] (slika 4.1)

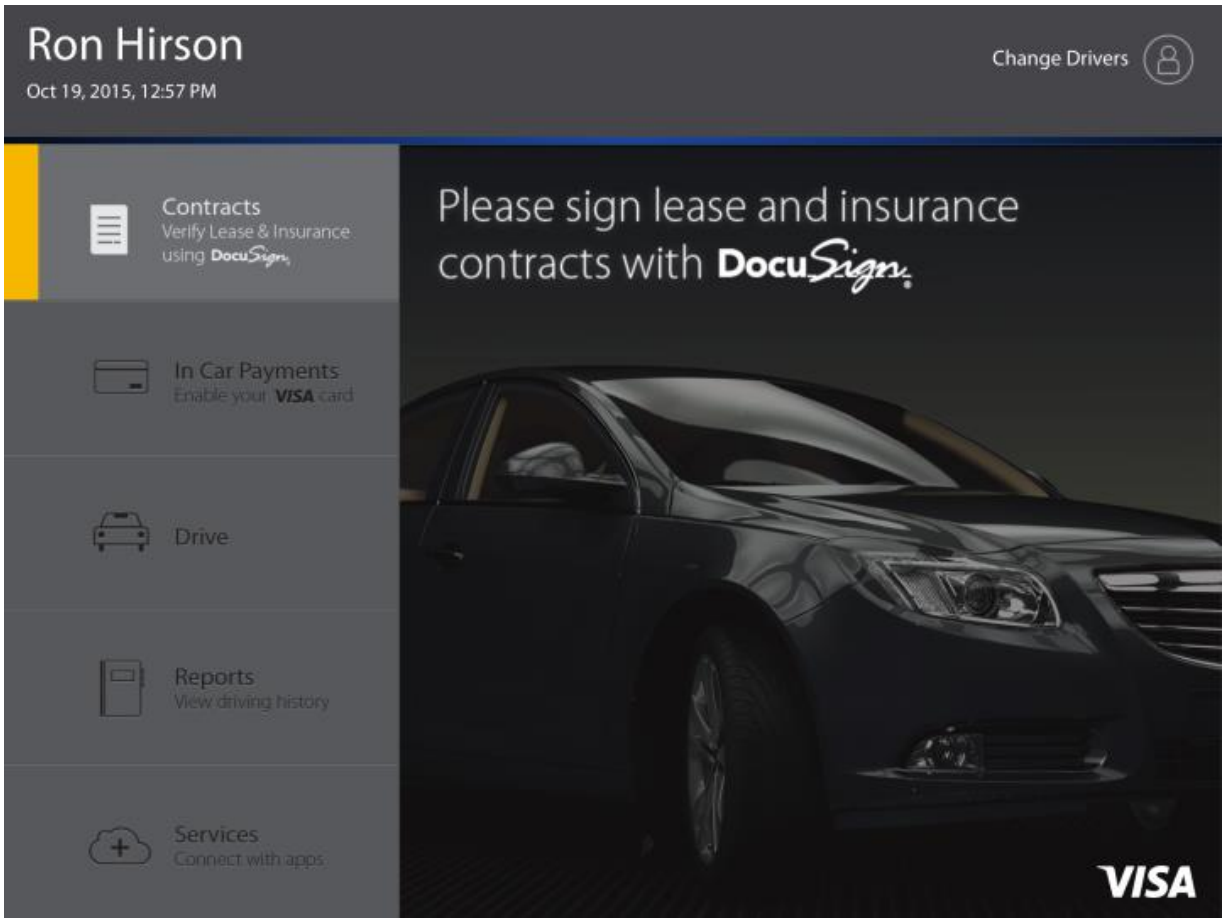
Ranije je spomenuto i zdravstveno osiguranje. Ekosustav zdravstvenog osiguranja je poprilično neučinkovit, što ide na štetu svih dionika: pružatelja usluga, osiguravajućih kuća, ali i pacijenata. Prosječan pacijent tijekom svog života sigurno ima potrebu posjetiti više od jednog liječnika ili specijalista. Zato što je u zdravstvo uključeno više različitih

[32] https://www.agcs.allianz.com/about-us/news/blockchain-prototype-captive-insurance-press-release/ (3.9.2018. u 23:15)
[33] https://www.cbinsights.com/research/blockchain-insurance-disruption/ (3.9.2018. u 23:45)

strana, teško je dijeliti i koordinirati osjetljive medicinske podatke o korisnicima između njih. Medicinski podaci ulaze u različite zdravstvene ustanove i osiguravajuće kuće, a duplicirani i pogrešni zapisi vrlo često dovode do skupih pogrešaka i nepotrebnih obaveza za korisnike kao npr. ponavljanje pretraga, plaćanje krivih lijekova ili terapija, itd. S blockchainom se može kreirati globalno distribuirana, sinkronizirana baza podataka o pacijentima i njihovom zdravstvenim zapisima i što je najbitnije, svojom kriptografskom zaštitom može osigurati privatnost pacijenta, a na kraju i veliku uštedu novaca koji se trenutno ulaže u zdravstvenu industriju. Ovakav pristup daje pacijentima potpunu kontrolu nad svojim zdravstvenim podacima i omogućava im pristup tim podacima ovisno o njihovim trenutnim potrebama. Umjesto prisiljavanja osiguravajućih kuća i pružatelja zdravstvenih usluga na međusobno sinkroniziranje baza podataka o pacijentima, blockchain ekosustav za pohranu medicinskih zapisa mogao bi pohraniti kriptografski potpis za svaki zapis i postaviti ga u distribuiranu knjigu. Potpis kriptografski označava sadržaj svakog dokumenta i daje mu vremensku oznaku te zapravo ne pohranjuje nikakve osjetljive podatke na blockchain.

Iako je ova tehnologija još u svojim začecima, već postoji nekoliko obećavajućih projekata i primjena u industriji osiguranja. Velik igrači u ovoj industriji kao što su Allianz i Swiss Re već koriste neka od blockchain rješenja u svojem redovnom poslovanju. Iz perspektive industrije, osiguravajuće kuće moraju uskladiti svoje procese i standarde kako bi omogućile potpunu implementaciju ove tehnologije. Blockchain tehnologija može pružiti bolje alate za suradnju i razmjenu podataka, ali jedan od bitnijih uvjeta je taj da osiguravatelji moraju biti voljni surađivati i dijeliti podatke međusobno. Potrebno je još vremena da razvoj tehnologije dođe do zadovoljavajuće razine. Javni blockchain u kojem svatko ima pristup svim transakcijama u glavnoj knjizi ne odgovara modelu poslovanja osiguravajućih kuća. Prvenstveno iz sigurnosnih i privatnih razloga. Njihov interes je više na strani privatnog blockchaina, koji je još u intenzivnoj fazi istraživanja i razvoja. [34]

[34] https://www.cbinsights.com/research/blockchain-insurance-disruption/ (4.9.2018. u 00:45)



Slika 4.1 Prikaz DocuSign aplikacije za leasing i osiguranje automobila. Izvor: https://www.docusign.com/blog/the-future-of-car-leasing-is-as-easy-as-click-sign-drive/ (3.9.2018. u 23:50)

4.1.3. Nekretnine

Jedna od tradicionalnih industrija, industrija nekretnina, također može imati velikog doprinosa od blockchain tehnologije. Kao što je ranije spomenuto, blockchain nudi siguran način pohrane i organizacije podataka, što je od velike važnosti prilikom trgovine nekretninama. Danas, u procesu transakcija nekretnina, potrebno je obraditi nebrojeno puno papirologije i potrošiti mnogo vremena i resursa. Implementacijom pametnih ugovora u ovaj proces drastično bi se smanjila količina papirologije, vrijeme potrebno za realizaciju transakcija, dok bi najveća promjena bila razina sigurnosti, koja bi se drastično povećala. Primjerice, spriječile bi se mnogobrojne prijevare koje se događaju prilikom elektroničkog plaćanja hipoteka. Švedska, jedna od zemalja koja je prihvatila blockchain tehnologiju,

počela je sa implementacijom iste u svoj sustav za registraciju zemljišta. Projekt se zove Lantmäteriet i započeo je 2016 godine.[35] Magnus Kempe, direktor prodaje i financija u tvrtki Kairos Future, govori kako je plan ovog projekta postaviti sve transakcije u trgovanju nekretninama na blockchain nakon što kupac i prodavač postignu dogovor. Kreirana je distribuirana baza podataka kojoj mogu pristupiti samo verificirani korisnici kao što su npr. vlasnici zemljišta, zaposlenici banaka, kupci nekretnina i brokeri. Oni su tako u mogućnosti pratiti cijeli proces i odgovorni su za verifikaciju i ažuriranje podataka. Ovakvim načinom cijeli proces postaje potpuno transparentan i interoperabilan među različitim sustavima. Kupoprodajne transakcije i postupci danas traju i do pola godine, no uvođenjem ovakvog sustava, to vrijeme se smanjuje na svega nekoliko dana uz drastično povećanje sigurnosti i nemogućnosti manipuliranja podataka. Procijenjeno je da bi ovaj projekt mogao uštediti 100 milijuna eura godišnje, eliminirajući veliku količinu papirologije i prijevara.

Blockchain također može doprinijeti i pojednostavljenju upravljanja imovinom. Pametnim ugovorima se vrlo lako može automatizirati većina repetitivnih radnji, od podešavanja priključaka do određivanja parametara za ugovore o najmu. Većina zapisa o vlasništvu nekretnina nije dostupna javno, na internetu.

4.1.4. Ostale industrije

Kao što je ranije spomenuto, blockchain tehnologija ima sposobnost disrupcije mnogobrojnih industrija. Uz Fintech, te industrije osiguranja i nekretnina, blockchain tehnologija se može primijeniti npr. i u:[36]

1. **Računalnoj sigurnosti** - iako su svi podaci na blockchain-u javni, podaci se verificiraju preko napredne kriptografije i to ih čini vrlo sigurnim
2. **Internet stvari** (eng. Internet of things - IoT) - povezivanje i komunikacija uređaja putem interneta bez centralne kontrolne lokacije (primjeri: Samsung, IBM)

[35] https://qz.com/947064/sweden-is-turning-a-blockchain-powered-land-registry-into-a-reality/ (10.8.2018. u 20:45)
[36] https://www.youtube.com/watch?v=G3psxs3gyf8 - 19 Industries The Blockchain Will Disrupt (17.8.2018. u 17:45)

3. **Upravljanju opskrbnim lancima** - blockchain može drastično smanjiti kašnjenja u isporuci i eliminirati ljudske pogreške (primjeri: Provinance, Fluent, Blockverify, Skuchain)
4. **Privatni transport i dijeljenje prijevoza** - blockchain nudi mogućnost razvoja decentraliziranih peer-to-peer aplikacija koje izbacuju posrednike u ovom procesu i omogućavaju korisnicima direktno postizanje dogovora i angažmana na siguran način (primjeri: Arcade City, La´Zooz)
5. **Online pohrana podataka** - za razliku od podataka koji se nalaze na centraliziranim serverima, podaci na decentraliziranim sustavima su višestruko sigurniji (primjer: STORJ)
6. **Dobrotvorne organizacije** - blockchain omogućava donatorima da prate svoje donacije i budu u potpunosti sigurni da će one doći do osoba kojima su stvarno namijenjene (primjer: BitGive)
7. **Upravljanje energijom** - postoje projekti na ethereum blockchain-u koji nude mogućnost trgovanja energijom na peer-to-peer bazi, bez posrednika (primjer: TransActiveGrid)

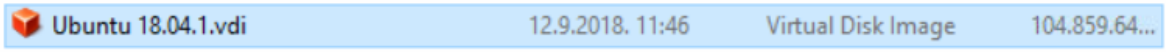
5. Primjer baziran na izdavanju obrazovnih certifikata (aplikacija za unos, izdavanje i provjeru obrazovnih certifikata)

5.1. Opis izrade koncepta aplikacije

Kao platformu za izradu koncepta aplikacije za unos, izdavanje i provjeru obrazovnih certifikata odabran je MultiChain. MultiChain je platforma otvorenog koda koja omogućava kreiranje vlastitog blockchaina, ili više njih, te upravljanje njegovim mogućnostima. Optimizirana je za kreiranje lanaca u kojima se daju dozvole (eng. *permissioned blockchains*). MultiChain je kompatibilan s Linux, Windows i Mac operativnim sustavima. Trenutno je optimiziran za Linux operativne sustave. Pošto sam korisnik Windows operativnog sustava, za potrebe praktičnog dijela ovog rada, odlučio sam podići virtualnu mašinu na kojoj sam instalirao Linuxov 64-bitni Ubuntu 18.04.1 operativni sustav. Virtualnu mašinu sam podigao na jednom fizičkom serveru pomoću Oracle VM VitrualBoxa.

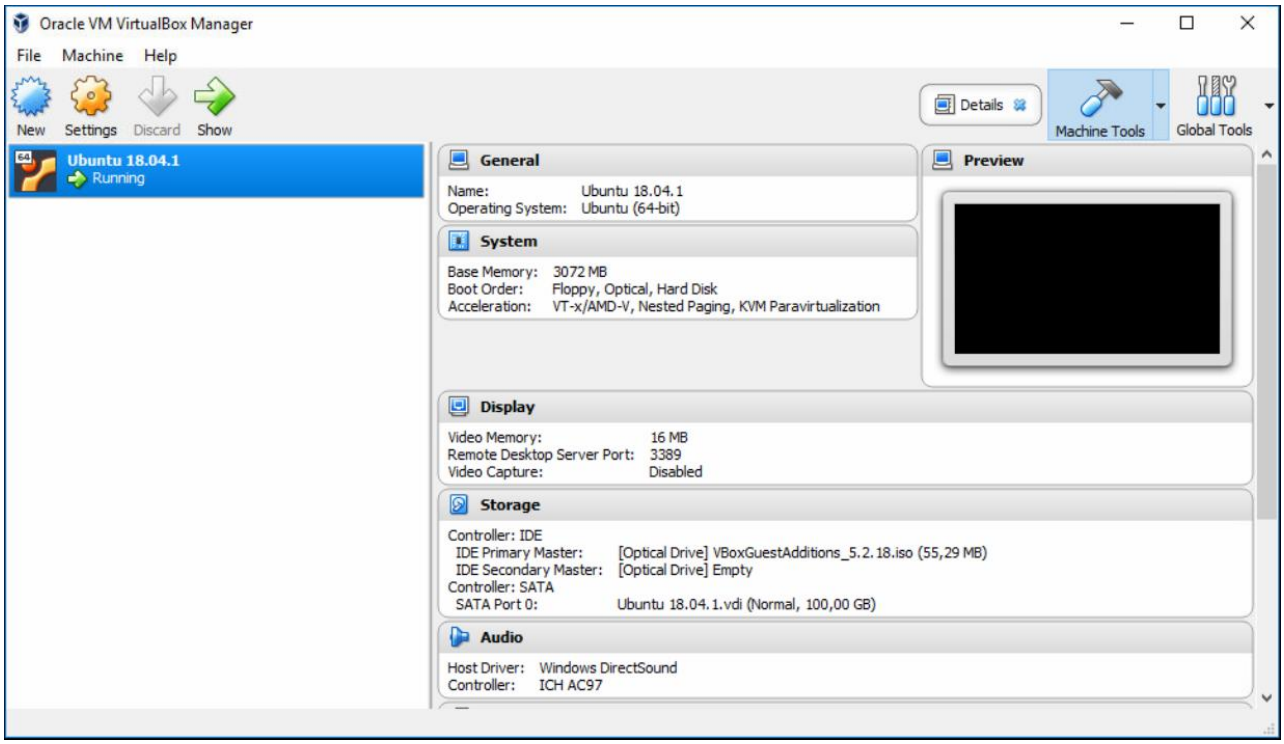
Virtualizacija operativnih sustava nam omogućava da na jednom serveru, radnoj stanici ili računalu imamo više operativnih sustava i koristimo ih istovremeno. Svi operativni sustavi dijele računalne resurse. Broj virtualnih mašina je neograničen, tj. ovisi o količini diskovnog prostora i memorije računala na kojem su ugošćene (eng. *hosted*).

U radnoj konzoli Oracle VM VirtualBox-a (slika 5.2) nalazi se radni izbornik (*File, Machine, Help),* ikone za najvažnije aktivnosti na virtualnim mašinama (*New, Settings, Discard, Show*), a ispod njih se nalazi prozor u kojem se prikazuju instalirane virtualne mašine. Kao što se vidi na slici 5.2. instalirana je i pokrenuta Ubuntu virtualna mašina kojoj sam za rad dodijelio 100GB diskovnog prostora i 3GB radne memorije. Prije instalacije operativnog sustava bilo je potrebno kreirati virtualni disk navedene veličine koji će mašina koristiti (slika 5.1).



Slika 5.1 Prikaz virtualnog disk-a. Izvor: Vlastiti screenshot

Kompletna radna konzola i instalacija virtualnih mašina je vrlo intuitivna i jednostavna. VirtualBox nudi mogućnost odvojivog (eng. *deatachable*) pokretanja virtualnih mašina što nam omogućava da se cijeli proces vrti bez otvorenih prozora i grafičkog korisničkog sučelja (eng. graphical user interface - GUI)



Slika 5.2 Prikaz Oracle VM VirtualBox sučelja. Izvor: Vlastiti screenshot

Nakon instalacije i podešavanja virtualne mašine potrebno je preuzeti i instalirati MultiChain aplikaciju. Preuzimanje, instalacija, ali i sve ostale radnje unutar MultiChaina vrše se preko Terminal sučelja Ubuntu operativnog sustava. Za preuzimanje i instalaciju koriste se sljedeće naredbe:

```
wget https://www.multichain.com/download/multichain-1.0.6.tar.gz
tar -xvzf multichain-1.0.6.tar.gz
```

```
cd multichain-1.0.6

mv multichaind multichain-cli multichain-util /usr/local/bin[37]
```

Posljednja linija naredbe prebacuje najbitnije datoteke u *bin* folder radi lakšeg pozivanja kroz naredbe u sljedećim koracima.

Nakon instalacije MultiChain aplikacije, prvi korak je kreiranje vlastitog lanca (slika 5.3). Pošto je cilj aplikacije unos, izdavanje i provjera valjanosti obrazovnih certifikata, za potrebe ovog projekta, lanac sam nazvao *BlockchainDiploma*. Navedeno odrađuje sljedeća funkcija:

```
multichain-util create BlockchainDiploma
```

Pomoću ove naredbe kreiramo lanac navedenog naziva sa zadanim (eng. *default*) postavkama. Nakon toga, potrebno je pokrenuti kreirani lanac pomoću sljedeće naredbe (slika 5.3):

```
multichaind BlockchainDiploma -daemon
```

Lanac je pokrenut i kreiran je njegov prvi blok (eng. *genesis block*). Nakon pokretanja, novokreirani lanac dobiva svoju IP adresu i port preko kojega mu se može pristupiti s drugog uređaja. Uređaj na kojemu je kreiran lanac postaje prvi glavni čvor (eng. *nod*), te svako sljedeće računalo koje se spoji na taj lanac preko njegove IP adrese i zadanog porta, preuzima podatke kompletnog lanca i također postaje čvor. Za potrebe ovoga rada korišten je samo jedan čvor, no u produkciji se nikako ne preporučuje korištenje samo jednog čvora, naravno, iz sigurnosnih razloga spomenutih ranije u radu.

Ako bi se drugo računalo spajalo na ovaj lanac, ono također mora imati instaliranu MultiChain aplikaciju i mora pokrenuti naredbu:

```
multichaind BlockchainDiploma@[ip-adresa]:[port]
```

Nakon spajanja drugih računala/čvorova, prvi čvor jedini ima ovlaštenja za dodjeljivanje određenih prava, kao npr. *read* i *write* prava, drugim čvorovima.

[37] https://www.multichain.com/download-install/ (4.9.2018. u 18:15)

MultiChain, između ostalog, ima mogućnost pohrane podataka u blockchain koristeći tzv. *stream*. Uz pohranu, nudi i mogućnost vađenja podataka. Ova funkcionalnost je najbitnija za koncept aplikacije koji se ovdje prikazuje. Dakle, na glavnom čvoru potrebno je kreirati novi *stream,* koji ćemo u ovom primjeru nazvati **diplome.** Navedeno izvodimo naredbom:

```
create stream diplome false
```

Izraz `false` u naredbi znači da u taj *stream* mogu zapisivati samo one adrese kojima se eksplicitno daje dozvola. Pošto u ovom primjeru imamo samo jedan čvor koji je i kreirao taj *stream,* nije potrebno dodjeljivati posebna prava. Ako postoji drugi čvor i neka druga adresa s koje se želi nešto zapisati na taj isti *stream,* s prvog čvora je potrebno dodijeliti prava za svaku adresu posebno naredbom `grant`.

Sljedeći korak je pohrana podataka u kreirani *stream* **diplome**. Podaci se pohranjuju u heksadecimalnom obliku. U ovom primjeru ću pohraniti vlastito ime i prezime i OIB pomoću naredbe

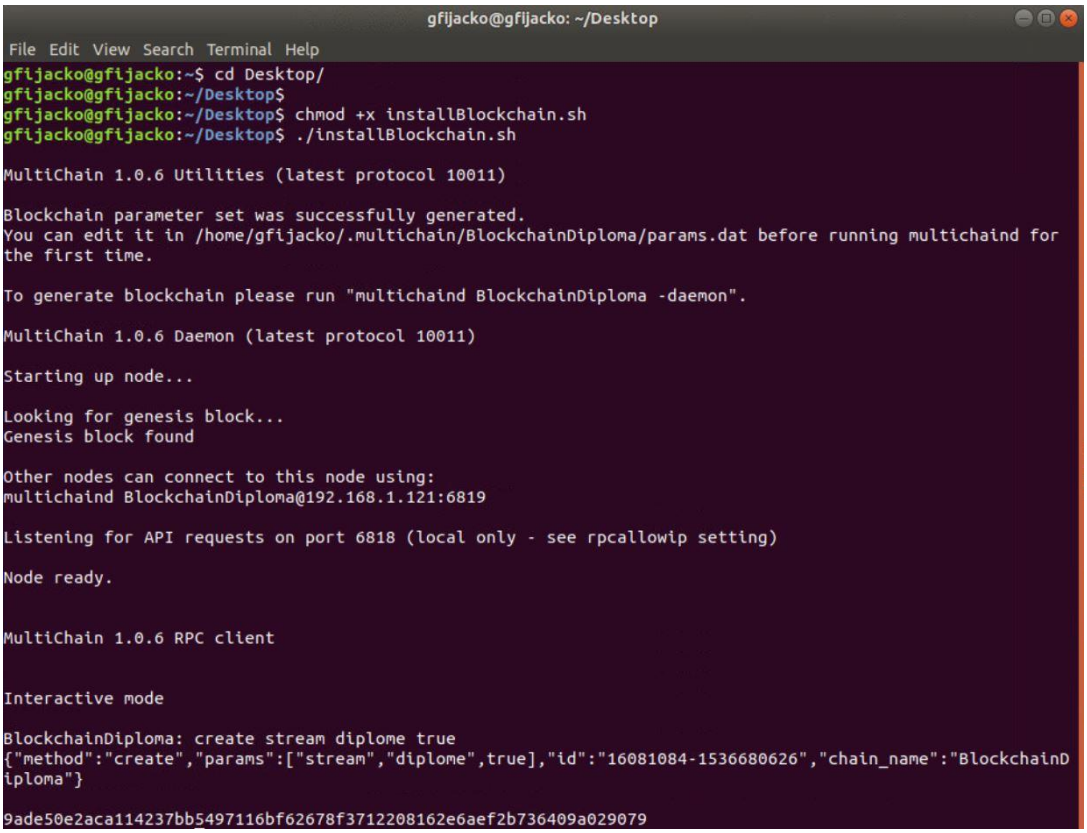
```
publish diplome key1
476f72616e2046696a61636b6f203638383136393734393035
```

Heksadecimalni broj 476f72616e2046696a61636b6f203638383136393734393035 pretvoren u tekstualni oblik daje vrijednost: *Goran Fijačko 68816974905*. [38]

Nakon zapisivanja podataka, pomoću upita (eng. query) možemo dobivati podatke zapisane u *stream.* Sljedeća naredba nam daje sve podatke zapisane u *stream* **diplome**

```
liststreamkeys diplome
```

[38] http://www.unit-conversion.info/texttools/hexadecimal/ (4.9.2018. u 22:15)



Slika 5.3 Prikaz tekstualnog (CLI) sučelja u kojem je prikazano kreiranje lanca, pokretanje lanca i kreiranje *streama* **diplome**. Izvor: Vlastiti screenshot

5.2. Funkcionalnosti

Ovakav tip aplikacije je namijenjen privatnom blockchainu. To znači da bi svaka obrazovna ustanova trebala imati svoj *stream* na koji samo osobe iz te ustanove imaju ovlaštenja pohraniti diplome. Svi *streamovi* su pohranjeni u glavnoj knjizi koja je distribuirana na sve čvorove, tj. obrazovne ustanove u ovom primjeru. Što je više čvorova u lancu, to bolje, jer lanac postaje sve jači i sigurniji.

Aplikacija se sastoji od tri modula:

1. Modul za unos diploma
2. Modul za provjeru diploma
3. Modul za ispis diploma

Prvi modul služi za unos diploma. On prebacuje unesene podatke u heksadecimalni oblik i pohranjuje ih u lanac te natrag vraća ID transakcije (*txid*). ID transakcije je privatni ključ koji se daje diplomiranom studentu jer pomoću njega se mogu provjeriti podaci o diplomi u lancu.

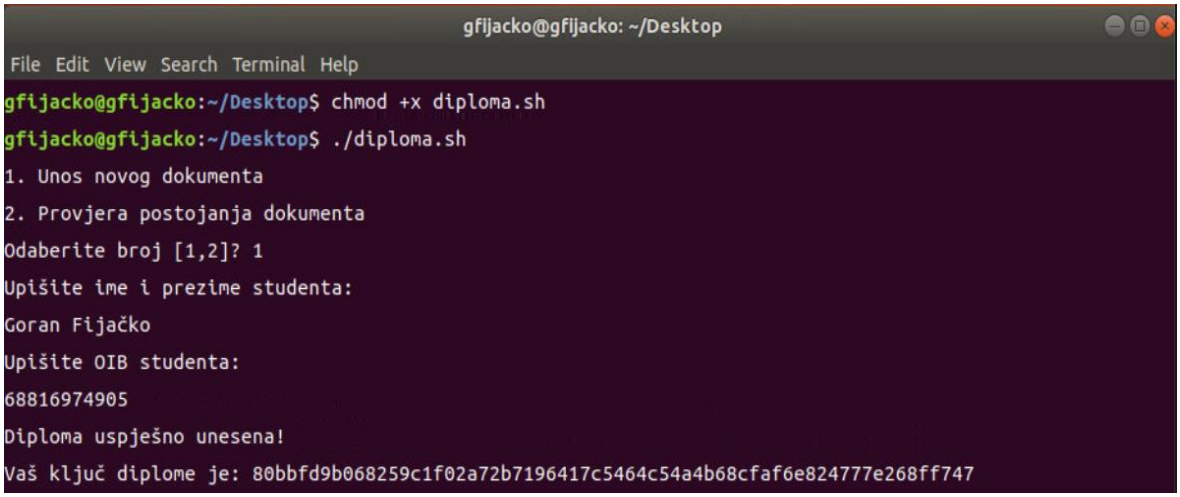
Modul za provjeru diploma, uz kombinaciju OIB-a i ID-a transakcije, šalje upit u lanac i provjerava postoji li zapis u lancu. Nakon toga daje pozitivan ili negativan odgovor, ovisno o tome postoji li zaista tražena diploma u lancu i poklapa li se za unesenim OIB-om.

Modul za ispis diploma ispisuje diplomu na ekranu u PDF obliku.

Svi navedeni moduli u ovom primjeru prikazani su u komandnom tekstualnom sučelju, tj. u Terminalu Ubuntu operativnog sustava. Oni se također mogu programirati i u web aplikaciju i koristiti u WEB preglednicima.

5.3. Korisničke role

Nakon što student uspješno završi fakultet i obrani svoj diplomski rad, u sustav fakulteta se unosi podatak da je taj student diplomirao. Pomoću ove aplikacije i modula za unos diploma, ovlaštena osoba na fakultetu unosi ime, prezime i OIB diplomiranog studenta te se taj podatak sprema u lanac. Kao povratnu informaciju dobiva ID transakcije (slika 5.4) koji daje studentu i upisuje na originalni ispis diplome. Moguće ga je ispisati i u obliku bar koda čije skeniranje daje vrijednost ID-a transakcije.



Slika 5.4 Prikaz modula za unos diplome. Izvor: vlastiti screenshot

Student dobiva svoju zasluženu diplomu i svoj privatni ključ diplome koji je u ovom slučaju 80bbfd9b068259c1f02a72b7196417c5464c54a4b68cfaf6e824777e268ff747. On se zatim prijavljuje za posao i nakon poziva poslodavca odlazi na razgovor za posao. Poslodavac ga traži diplomu kako bi provjerio njegovu stručnu spremu. Trenutno se postupak vrši tako da poslodavac kontaktira obrazovnu ustanovu kako bi provjerio valjanost diplome i to najčešće pisanim putem. Taj proces je dugotrajan i troši mnogo resursa. No, u ovom slučaju poslodavac dobiva diplomu na kojoj se nalazi privatni ključ. Poslodavac zatim u aplikaciju upisuje OIB osobe koja se prijavila za posao i javni ključ koji se nalazi na diplomi (slika 5.5). Ovakav način u djeliću sekunde vraća informaciju o valjanosti diplome.

Slika 5.5 Prikaz modula za provjeru diplome. Izvor: vlastiti screenshot

Nakon potvrdnog odgovora aplikacije, dobiva se ispis na ekranu. U ispisu piše ime i prezime studenta, obrazovna institucija, usmjerenje, datum i mjesto diplomiranja. Poslodavac na kraju ima opciju ispisa kopije diplome za vlastitu arhivu. Ako izabere opciju za ispis, diploma će se generirati i otvoriti u PDF obliku (slika 5.6)

Radi lakšeg korištenja aplikacije nakon puštanja u produkciju, bolji je izbor korištenje u obliku WEB aplikacije. To znači da bi se sve prikazano premjestilo na nekakav web server te bi se aplikaciji pristupalo putem *https* protokola (npr preko URL-a https://www.diplome.hr) u web preglednicima. To znači da je korisnicima potrebna jedino internetska veza i korisnički račun u aplikaciji kako bi brzo i sa stopostotnom sigurnošću provjerili validnost diplome.

Slika 5.6 Prikaz ispisa diplome iz modula za ispis. Izvor: https://thumbs.dreamstime.com/z/certificate-diploma-blank-template-vector-illustration-31569678.jpg; dorađeno u Adobe Photoshopu (10.9.2018. u 23:15)

Zaključak

U ovom radu predstavljena je blockchain tehnologija, njena povijest te princip kako funkcionira u okviru digitalnog identiteta. U dijelu teoretske osnove postavljena je usporedba ¨klasičnog¨ identiteta i digitalnog identiteta koji je opisan kroz primjere osobnih iskaznica i sustava e-građani. Zatim, nakon uvoda u blockchain tehnologiju i opisa metoda postizanja konsenzusa i zapisivanja transakcija, opisan je princip pametnih ugovora koji nude mogućnost upisivanja kôda ili čak potpunih aplikacija i postavljanja istih u blockchain omogućavajući tako automatiziranje mnoštvo procesa.

U trećem poglavlju koje obrađuje platformu, kroz 3 primjera (Civic, HYPR, Blockverify), opisani su poslovni modeli koji koriste blockchain kao platformu na kojoj razvijaju svoje procese bazirane na digitalnom identitetu. Također, uspoređeni su tradicionalni modeli s onima baziranim na pametnim ugovorima. Kroz primjere osiguranja od otkaza ili kašnjenja avionskih letova, glasanja, glazbene industrije i praćenja osobnih zdravstvenih podataka ustanovljeno je koliko su zapravo postojeći modeli spori, neučinkoviti i skloni manipulacijama te je kroz primjere implementacije blockchain-a u iste, pokazano kako bi ti sustavi funkcionirali brže, transparentnije i što je najvažnije, sigurnije.

U četvrtom poglavlju opisuje se primjena tehnologije u nekoliko industrija, od Fintech industrije, pa sve do industrije osiguranja i nekretnina. Opisani su koncepti i testna rješenja koja se polako implementiraju u produkcijske faze i pokazuju izvrsne rezultate. Iz tog razloga smatram da će takvih rješenja iz godine u godinu biti sve više te da ćemo uskoro vidjeti sve veću adopciju blockchain tehnologije na globalnoj razini.

U posljednjem, praktičnom dijelu rada, odrađeno je istraživanje postojećih rješenja koja nude kreiranje vlastitog blockchain-a te je odabrana platforma MultiChain. Za potrebe ovog rada bilo je potrebno kreirati Ubuntu virtualnu mašinu u Oracle VM VirtualBox-u, na koju sam zatim postavio MultiChain. Kroz Ubuntu-ov Terminal predstavljen je koncept aplikacije za unos, izdavanje i verifikaciju diploma fakulteta te su opisane sve funkcionalnosti i korisničke role u tom procesu.

Tko zna, možda ova tehnologija promijeni način na koji koristimo računala u svakodnevnom životu i možda poslužitelji kakve danas poznajemo i koristimo u svim

segmentima informatike i poslovanja, postanu obsolit. U svakom slučaju, na dobrom je putu da se tako nešto i ostvari, ali ipak, još smo na samim počecima razvoja i istraživanja mogućnosti blockchain tehnologije, tako da ne preostaje ništa drugo, nego strpljivo čekati, promatrati i ako je ikako moguće doprinijeti zajednici u toj uzbudljivoj avanturi revolucije u tijeku.

Student vlastoručno potpisuje diplomski rad iza zaključka s datumom i oznakom mjesta završetka rada te naznakom:

„Pod punom odgovornošću pismeno potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada“.

U Zagrebu, datum.

Popis kratica

CA	*Certificate Authority*	Tijelo za izdavanje certifikata
NIAS	*Integrated Services Digital Network*	Nacionalni identifikacijski i autentifikacijski sustav
PEP	*Policy enforcement point*	Točka provođenja pravila
PDP	*Policy decision point*	Točka za odlučivanje pravila
ADA	Authorization decision assertion	Tvrdnja o odobrenju
SHA	Secured Hash Algorithm	Osiguran Hash Algoritam
POW	Proof of work	Dokaz radom
POS	Proof of stake	Dokaz ulogom
DPoS	Delegated Proof of Stake	Delegirani dokaz ulogom
PoC	Proof of Capacity	Dokaz kapacitetom
BFT	Byzantine Fault Tolerance	Bizantinski model zatajenja
DoS	Denial of service	Uskraćivanje usluga
API	Application programming interface	Aplikacijsko programsko sučelje
GUI	Graphical user interface	Grafičko korisničko sučelje
CLI	Command Line Interface	Tekstualno sučelje
URL	Uniform Resource Locator	Ujednačeni lokator sadržaja
IoT	Internet of things	Internet stvari

Popis slika

Popis tablica

Literatura

[1] WINDLEY, P. *Digital identity*. O´Reilly, 2005.

[2] GUPTA, M. *Blockchain for dummies*. 2nd IBM Limited Edition, 2018.

[3] LAURENCE, T. *Blockchain*.1. poglavlje, 2017.

[4] https://flipboard.com/@flipboard/-from-yelp-reviews-to-mango-shipments-ib/f-0cf869ac26%2Fbusinessinsider.com (23.07.2018. u 17:05)

[5] http://stari.mup.hr/42.aspx (20.07.2018. u 18:20)

[6] https://hr.wikipedia.org/wiki/Za%C5%A1tita_podataka#Digitalni_certifikat (20.07.2018. u 21:15)

[7] https://gov.hr/e-gradjani/o-sustavu-e-gradjani/1584 (21.07.2018. u 17:00)

[8] https://nias.gov.hr/Home/TermsOfUse (21.07.2018. u 17:45)

[9] https://gov.hr/e-gradjani/o-sustavu-e-gradjani/1584 (22.07.2018. u 18:15)

[10] https://bitcoin.org/bitcoin.pdf (18.09.2018. u 17:00)

[11] https://www.xorbin.com/tools/sha256-hash-calculator (24.07.2018. u 22:45)

[12] http://solidity.readthedocs.io/en/v0.4.24/ (25.07.2018. u 18:45)

[13] https://bitfalls.com/hr/glossary/#51-napad (27.7.2018. u 19:15)

[14] https://coincentral.com/making-sense-of-proof-of-work-vs-proof-of-stake/ (27.07.2018. u 20:30)

[15] https://ubik.hr/2018/03/26/sto-su-pametni-ugovori-uvod/ (29.7.2018. u 18:30)

[16] https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf (2.8.2018. u 18:15)

[17] https://news.bitcoin.com/hypr-3-million-blockchain-biometrics/ (4.8.2018. u 22:05)

[18] https://www.forbes.com/sites/jonathanchester/2017/04/28/how-blockchain-startups-will-solve-the-identity-crisis-for-the-internet-of-things/#1a87dafb5c63 (6.8.2018. u 19:45)

[19] https://www.havocscope.com/counterfeit-goods-ranking/ (7.8.2018. 20:45)

[20] https://bitcoinist.com/block-verify-turns-bitcoin-life-saving-technology/ (7.8.2018. u 21:30)

[21] https://medium.com/cashlink-crypto/eliminate-the-hassle-of-flight-delay-compensation-by-using-smart-contracts-a5db3b5c3ed (9.8.2018. u 19:45)

[22] https://hbr.org/2017/06/blockchain-could-help-musicians-make-money-again (11.8.2018. u 19:45)

[23] https://applicature.com/blog/blockchain-healthcare-smart-contracts-2 (11.8.2018. u 22:25)

[24] https://www2.deloitte.com/nl/nl/pages/financial-services/articles/1-blockchain-speeding-up-and-simplifying-cross-border-payments.html (27.8.2018. u 19:45)

[25] https://www2.deloitte.com/nl/nl/pages/financial-services/articles/2-blockchain-and-the-future-of-share-trading.html (27.8.2018. u 20:15)

[26] https://cointelegraph.com/news/exponential-growth-cryptocurrency-exchanges-are-adding-100000-users-per-day (27.8.2018. u 20:45)

[27] https://blockchainapac.fintecnet.com/uploads/2/4/3/8/24384857/fintech_blockchain_report_v3.pdf (27.8.2018. u 21:00)

[28] http://www.xprimm.com/Swiss-Re-s-sigma-The-global-insurance-market-slowed-down-in-2017%3B-emerging-markets-and-the-US-strengthening-economy-will-lead-future-growth-articol-117,149-11571.htm (3.9.2018. u 19:45)

[29] https://www.cbinsights.com/research/blockchain-insurance-disruption/ (3.9.2018. u 20:30)

[30] https://www.agcs.allianz.com/about-us/news/blockchain-prototype-captive-insurance-press-release/ (3.9.2018. u 23:15)

[31] https://www.cbinsights.com/research/blockchain-insurance-disruption/ (3.9.2018. u 23:45)

[32] https://www.cbinsights.com/research/blockchain-insurance-disruption/ (4.9.2018. u 00:45)

[33] https://qz.com/947064/sweden-is-turning-a-blockchain-powered-land-registry-into-a-reality/ (10.8.2018. u 20:45)

[34] https://www.youtube.com/watch?v=G3psxs3gyf8 - 19 Industries The Blockchain Will Disrupt (17.8.2018. u 17:45)

[35] https://www.multichain.com/download-install/ (4.9.2018. u 18:15)

[36] http://www.unit-conversion.info/texttools/hexadecimal/ (4.9.2018. u 22:15)