BLOCKCHAIN I RAZVOJ MOBILNIH APLIKACIJA ZA SUVREMENO BANKARSTVO

Mrdaković, Mariana

SVEUČILIŠTE U SPLITU

EKONOMSKI FAKULTET

ZAVRŠNI RAD

BLOCKCHAIN I RAZVOJ MOBILNIH APLIKACIJA ZA SUVREMENO BANKARSTVO

Nastavnik/Mentor: Student:

Prof. dr. sc. Željko Garača Mariana Mrdaković

Split,kolovoz,2020.

SADRŽAJ:

1. UVOD 5

1.1 Uvod i sadržaj rada 5

1.2. Metode istraživanja 5

1.3 Struktura rada 6

2. BLOCKCHAIN TEHNOLOGIJA 7

2.1. Pojam i vrste blockchain tehnologije 7

2.1.1 Vrste blockchaina 8

2.2 Karakteristike i princip rada blockchain tehnologije 9

2.2.1 Struktura bloka 9

2.2.2 Hash vrijednost i SHA- 256 10

2.2.3 Novčanik 10

2.2.4 Uloga rudara 11

2.2.5 Proof of work 11

2.2.6 Proof of stake 12

2.2.7 Delegirani proof of stake 12

2.3 Značajke i prednosti blockchain tehnologije 12

3. ELEKTRONIČKO BANKARSTVO 14

3.1 Osnovne odrednice elektroničkog bankarstva 14

3.1.1 E- bankarstvo za građane 15
3.1.2 Sredstva autorizacije 15
3.1.3 Smart kartica 16
3.2 Pozitivne i negativne komponente elektroničkog bankarstva 17
3.2.1 Prednosti i nedostatci sa gledišta banke 17
3.2.2 Prednosti i nedostatci sa klijentovog gledišta 18
3.3 Sigurnost elektroničkog bankarstva 19
3.3.1 SSL algoritam 19
3.3.2 Ostale sigurnosne značajke 20
3.3.3 Sudjelovanje klijenata u sigurnosnom procesu 20
4. ELEKTRONIČKI SUSTAVI PLAĆANJA U APLIKACIJAMA 21
4.1 Vrste transakcija elektroničkim novcem 21
4.2 Vrste elektroničkih novčanih sustava 22
4.2.1 Notacijski sustav 22
4.2.2 Simbolički sustav 23
4.2.3 Centralizirani sustav 23
4.2.4 Decentralizirani sustavi 24
4.3 Protokoli plaćanja elektroničkim novcem 25
4.3.1 Protokol bez anonimnosti 25
4.3.2 Anonimni protokol 26
4.3.3 Konačni oblik protokola plaćanja e- novcem 26

5. IMPLEMENTACIJA BLOCKCHAIN TEHNOLOGIJE U BANKARSKIM APLIKACIJAMA 27

5.1 Potencijal djelovanja blockhaina na poboljšanje cijelog financijskog sektora 27

5.2 Pametni ugovori 29

5.2.1 Koncept rada pametnog ugovora 29

5.2.2 Prednosti i potencijalne primjene pametnog ugovora 30

5.3 Kriptovalute 31

5.3.1 Pojmovno određenje kriptovaluta 31

5.3.2 Odgovor banaka na kriptovalute 31

5.4 Transformacija mreže aplikacija banaka 33

5.5 Sigurnost blockchaina 34

5.6 Blockchain distribuirana glavna knjiga 38

5.7 Izazovi implementacije blockchaina u bankarskom poslovanju 38

6. ZAKLJUČAK 40

7. POPIS LITERATURE 42

1. UVOD

1.1 Uvod i sadržaj rada

Svijet kakvog poznajemo danas nikada nije bio dinamičniji u vidu političkih, kulturnih i ekonomskih odvijanja zbog procesa globalizacije. Cilj tog procesa je postupno smanjivanje i ,u konačnici potpuno ukidanje, restrikcija protoka i razmjene ideja, usluga , proizvoda i ljudi, te se zbog njegovog dijelovanja malo koji tržišni sustav više može gledati kao zaseban, osobito financijski. Financijsko tržište danas na dnevnim bazama služi na korist milijardama njegovih sudionika i transferira bilijunske količine vrijednosti ali se konstantno suočava sa problemom zastarjelosti, koji uzrokuje sve veće probleme kako tržište raste van svog, za njega predviđenog, kapaciteta . Krute i centralizirane financijske institucije godinama nisu osjećale potrebu za promjenom i povećanjem efikasnosti zbog svog sigurnog položaja posrednika na tržištu, što je dovelo do: smanjenja brzine i povećavanja naknada provođenja transakcije, nedovoljno transparentnog načina poslovanja koji korisnicima otežava pristupanje traženim podatcima, ogromnoj količini nepotrebne administracijske dokumentacije koja još dodatno usporava čitavi proces i podložnosti ljudskim greškama prilikom unošenja podataka i ovjere koji mogu biti perspektivan mamac za manipulaciju i krađu podataka i vrijednosti. Nakon Svjetske krize 2007. godine, za koju su djelomično odgovorne i banke, javlja se još veća potreba za potpunom transformacijom poslovanja financijskog sustava. Kao najznačajniji odgovor na nekompetentno i neefikasno poslovanje razvila se blockchain tehnologija koja je glavni predmet ovog rada. U nastavku će se prikazati koncept i struktura njenog djelovanja, načini na koji bi se mogla implementirati u bankarsko poslovanje, te izazovi s kojima bi se mogla suočiti. Zbog boljeg razumijevanja pogodnosti tehnologije, također će se objasniti osnove rada elektroničkog bankarstva i platnih sustava kako bi se potencijalne primjene u pojedinim koracima odvijanja poslovanja lakše mogle uočiti.

1.2. Metode istraživanja

U ovom teoriskom radu rabiti će se različite metode istraživanja, ovisno o tome iz koje su znanstvene literature podatci ekstraktirani, kako bi se došlo do ključnih saznanja o tehnologiji blockchaina i radu novčanog sustava i poslovanja banaka koje su važne za oaj rad. Te metode su

sljedeće:

1) Deskriptivna metoda

2) Metoda analize i sinteze

3) Povijesna metoda

4) Kompilacijska metoda

5) Metoda dedukcije

1.2 Struktura rada

Ovaj završni rad sastavljen je od 5 glavnih poglavlja.

Prvo poglavlje odnosi se na pobliže upoznavanje blockchain tehnologije, njezine strukture, načina rada , vrsta , te prednosti i potencijala za budućnost.

U drugom poglavlju prikazati će se osnovni princip i način rada elektroničkog poslovanja banaka, njegove prednosti i slabosti sa posebnom konentracijom na najvažniji element elektroničkog poslovanja, sigurnost.

U trećem poglavlju obradit će se vrste elektroničkih novčanih sustava koji su nužni za odvijanje transakcija, te osnovne protokole plaćanja elektroničkim novcem

U četvrtom poglavlju će se primjeniti znjanje stečeno u posljednja tri poglavlja kako bi se istaknuli pojedini najpotencijalni aspekti, ali i opasnosti, pri primjeni blockchain tehnolologije u svakodnevnom poslovanju banaka, kao i njezin mogući utjecaj na čitav financijski sektor.

U petom poglavlju iznjet će se sažeti zaključci na kompilirani na osnovu svih činjenica navedenih u ovom radu.

2. BLOCKCHAIN TEHNOLOGIJA

2.1. Pojam i vrste blockchain tehnologije

Blockchain tehnologija predstavlja protokol razmjenjivanja vrijednosti u online transakcijama. To je digitalni javni popis (eng. *ledger)* višestruko decentraliziranih, ovjerenih i zaštićenih elektronskih transakcija koje može pregledati bilo koji pojedinac sa internet pristupom. U toj „knjizi“ su„kriptografski zabilježene sve vrijednosne izmjene i razmjene jedinica kriptovalutakoje su nepromjenjive i neizbrisive“[1],povezivanjem transakcijskih informacija u zasebne blokove, koji se nakon toga povezuju u lance,što nam govori i sam naziv ove tehnologije (pr. *Block- chain – lanac blokova).* Ova tehnologija revolucionarna je za bilo kakav oblik online trgovine upravo zbog njegove koncepcije koja ne zahtjeva provjeru i odobrenje od središnjeg autoriteta, te ne ostavljanja mogućnosti hakiranja i izmjene podataka, što uvelike smanjuje vrijeme obavljanja transkcije i povećava njenu sigurnost. Svaka nova razmjena ima svoj blok koji sadržava sve relevantne informacije o transakciji, informacije o prethodnom bloku i svoj jedinstveni kod koji se zove „*hash“* koji, nakon što biva ovjeren od svih umreženih računala (tzv. *Rudara),* ostaje trajno zapisan. Blokovi imaju točno određen slijed i vezuju se u lanac koji je praktički nepodložan bilo kakvim promjenama i provalama.

Izumitelj i prvi implementator blockchaina je Satoshi Nakamoto koji je s radom ovog koncepta započeo 2008. godine.Iako zvuči kao da je riječ o pojedincu, zapravo se ne zna da li je ovu tehnologiju izmislila skupina, organizacija ili pojedinac nekog drugog imena. Primjenom blockchaina na Bitcoin, prvu digitalnu kriptovalutu o kojoj će biti više riječi kasnije, Satoshi je bio prvi ponuditelj rješenja „duple potrošnje“, velike mane u sustavu digitalne trgovine zbog mogućnosti dupliciranja digitalnih file-ova za transakciju i potencijalne krađe novca, u mreži bez centralnog servera. Ova inovacija donijela mu je veliki uspjeh i „danas

[1]Službene Internetske stranice Europske Unije, (2019.), : Kriptovalute i blockchain – sve što trebate znati, Dostupno na: https://ec.europa.eu/croatia/cryptocurrencies_and_blockchain_all_you_need_to_know_hr

se na njegovu bitcoin adresu pripisuje oko milijun bitcoina koji imaju vrijednost od otprilike 15 milijardi američkih dolara.[2]

Sudionici blockchain tehnologije su klijenti tj. korisnici, koji stvaraju transakcije, i partneri koje izvršavaju različite uloge u sustavu. Najvažniji su tzv. „rudari“ .Oni mogu biti pojedinac ili skupina koja dobrovoljno na svojim računalima obrađuju postojeće i dodaju nove podatke i transakcije, te brinu o održavaju sustava za određenu nagradu u kriptovaluti. Ostali partneri obnašaju sljedeće funkcije:

1. Network routing (hr. *mrežno usmjeravanje*)
2. Održavanje blockchaina
3. Wallet (hr. *Novčanik)* koje ćemo opisati u sljedećem poglavlju.

2.1.1 Vrste blockchaina

Ovisno o ograničenjima za klijenta i partnera razlikujemo tri vrste blockchaina: javni privatni i konzorcijski

1. Javni blockchain

Na javnom blockchain-u svatko može izvršiti transakciju (dok je god valjana), postati rudar,na bilo koji način sudjelovati u koncenzusnom postupku, koji podrazumijeva proces određivanja blokova u lanac, i provjeravati stanje transakcija pomoću blok pretraživača. Transakcije su anonimne ali ipak transparentne.

Ovakav tip blockchaina pogodan je zbog smanjenja i distribucije troškova jer nema potrebe za administratorom sustava, te zato što klijent može bilo kada prekinuti svoje poslovne modele.

U privatnoj verziji također razlikujemo i partnere koji se ovdje dijele na:

1. Rudara
2. Potpunog partnera
3. Novčanik
4. Blockchain partnera.

Svaki je partner zasebno zadužen za mrežno usmjeravanje i autorizaciju novih bilješki transakcija.

Neki od primjera javnog blockchaina su: ethreum, bitcoin, litecoin itd.

[2] Arunović D. (2018.), Što je u stvari blockchain i kako radi?, Dostupno na: https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011

2. Privatni blockchain

Ima veći level restrikcije od javnoga i za klijenta i rudara. Korisnik ne može sudjelovati u ovoj vrsti blockchaina ukoliko nije pozvan od strane organizacije u čijem je vlasništvu i mora se prilagoditi njezinim politikama koje obično uključuju centralizirane dozvole za pisanje i neki stupanj ograničenja uvida u transakcije. Većinom je namijenjen za interne podatke unutar neke organizacije, npr. Računovodstvene ili upravljanje lancima opskrbe, jer pruža veću razinu kontrole i ne riskira se da podatci budu izloženi javnosti. Također usklađuje i pojednostavljuje rukovanje s podatcima i smanjuje troškove.

3. Konzorcijski blockchain

Ova vrsta blockchaina može se smatrati hibridnom vrstom privatnog zbog toga što ima iste pogodnosti u vidu sigurnosti i povećanja kontrole nad podatcima, ali za razliku od njega ima polu centraliziranu dozvolu za pisanje jer je u vlasništvu grupe tvrtki. Pojedinom korisniku se omogučava čitanje i izvršavanje konsenzusnog protokola samo u onom dijelu lanca u kojem su zastupljene njegove transakcije.

2.2 Karakteristike i princip rada blockchain tehnologije

Već smo ranije spomenuli kako se blockchain sastoji od blokova sa sadržajem informacije o transakciji, točno određeno i dosljedno poslagane u lance ali ovom poglavlju će mo se pobliže upoznati sa njihovom konstrukcijom, te pojedinim dužnostima partnera u sustavu.

2.2.1 Struktura bloka

Jedan blok građen je od sljedećih elemenata od kojih svaki ima neku ulogu u očuvanju njegove nepromijenjivosti i nemogućnosti dupliciranja:

1. Indeks bloka- označava redni broj bloka u strukturi lanca.

2. Timestamp- obilježava vrijeme nastanka bloka, odnosno transakcije.

3. Podatke o elektronskoj transakciji

4. Hash vrijednost prethodnog bloka- svojevrsni kodirani digitalni potpis koji se referira na prethodni blok u lancu.

5. Hash vrijednosti aktualnog bloka- također kodirani unikatni digitalni potpis bloka. Značenje i ulogu hash vrijednosti pobliže će mo analizirati u donjem odlomku.

6. Nonce (tj. *broj koji se jednom koristi*)- važan broj koji pokazuje rudaru kolika će biti težina izračuna odgovarajućeg hash-a za taj određeni blok. Nije jednostavan za izračun i

to je jedna od tehnika, ovog danas vrlo kompetitivnog tržišta kojem praktički može pristupiti svaki pojedinac, kojom se mogu eliminirati rudari koji ne posjeduju dovoljno vještina za pravilnu validaciju bloka. Jednom kad izračuna taj hash, rudar dobiva plaću u kriptovaluti.

2.2.2 Hash vrijednost i SHA- 256

Kao što smo već spomenuli hash je digitalni potpis koji predstavlja vrijednost bloka i upravo su oni posebnost ove tehnologije. Proizlazi iz izvođenja algoritma, odnosno kriptografske hash funkcije (obično se u blockchainu koristi SHA-256) nad podacima u bloku, odnosno argumentima hash funkcije, koji mogu biti bilo koje duljine, u svrhu dobivanja rezultata koji je fiksne duljine. Izračunava se relativno jednostavno ali vrlo ga je teško dekodirati ili izmjeniti. Unošenjem samo jednog pogrešnog znaka u zapisu ili ulaznoj informaciji hash informacija će se potpuno promijeniti.

Kriptografska hash funkcija označava matematičku operaciju koja se vrši nad digitalnim podtacima i transformira ih. Jedna od takvih funkcija je SHA- 256 ili SHA-2,nasljednik SHA-1 i jedna od najjačih kriptografskih funkcija danas. Ronald Rivest je ovaj algoritam, pod okriljem američke agencije NSA za nacionalnu sigurnost, osmislio 2002. Godine. Kratica u njegovom imenu znači Secure hash algorithm, a broj 256 količinu bitova hash vrijednosti koju kriptira. U blockchainu se koristi za dvije svrhe:

1) zbog porasta sigurnosti u kreiranju bitcoin adresa i privatnog ključa za pristup
2) za kreiranje tzv. *Proof of work-a* - dokaza o izvršenom rudarenju odnosno pravilnog digitalnog potpisa za blok, kojeg će se kasnije opisati detaljnije.

Nakon kratke analize strukture blockchaina, važno je definirati njegov princip rada i pobliže upoznati uloge partnera. U ovom primjeru upotrijebiti će se javni blockchain sustav jer je on u potpunosti decentraliziran i ravnopravan između uloga partnera dok kod centraliziranog poslužitelj mora spojiti dva klijenta. Ukoliko jedan klijent želi poslati kriptovalutu (uzmimo npr. Bitcoin) drugome prvo mora uplatiti određenu količinu bitcoina u svoj novčanik, čiji će se koncept predstaviti sada.

2.2.3 Novčanik

Novčanik je softwersko rješenje koje predstavlja svojevrsnu adresu korisnika specijaliziranu za primanje kriptovaluta. Ukoliko oba novčanika nisu kompatibilna u vidu valute koju izmjenjuju, transakcija se ne može izvršiti. „Svatko može imati koliko god adresa poželi, i ne postoji način da se adresa poveže s pravim identitetom korisnika, osim ako korisnik sam ne učini neke propuste ili to javno objavi. Na većini blockchainova stanje svačije adrese je javno

– svatko vidi koliko koja adresa ima sredstava. Wallet u kripto svijetu je kao email inbox kojeg svatko može pročitati, ali samo vlasnik može pisati odgovore.“[3]

Određen je s 2 enkripcijska ključa: javnim i privatnim.

Javni predstavlja njegovu identifikacijsku adresu i služi rudaru za dekripciju i provjeravanje transakcije tog klijenta. U slučaju upotrebe bilo čijeg drugog javnog ključa dobiveni podatci neće biti validni.

Privatni ključ zna samo njegov korisnik i pomoću njega se transakcija koju želi obaviti odmah kriptira.

2.2.4 Uloga rudara

Svaka transakcija se sastoji od niza ulaznih i izlaznih podataka.Ulazni podaci podrazumijevaju sve uplate u klijentov novčanik od njegove posljednje transakcijske isplate. Kod izaznih podataka razlikujemo dva tipa: količinu slanja kriptovaluta transakcijom i tzv. *miners fee* koju klijent može i ne mora ponuditi. Ona predstavlja dodatnu naknadu tj. motivaciju za rudara na što bržu obradu transakcije.

Rudari obrađuju transakcije na kopiji aktualnog blockchaina u svom računalu.Svaki rudar ima listu svih transakcija na zasebnom disku, ali samo se nedavne bilježe u radnoj memoriji zbog njihove učestalosti i lakog pristupa. Rudari,iako mogu biti pojedinci, danas se sve češće udružuju u tvz. *mining poolove* koji su pogodniji zbog raspodjele rada. Iako je pool još uvijek klijentu vidljiv kao jedan korisnik, on svoje zadatke, i sukladno zarađene kriptovalute, dijeli svojim članovima. Rudar potvrđuje transakciju izračunavanjem vrijednosti bloka pomoću hash-iranja standardnog algoritma (u slučaju bitcoina SHA-256) i time joj dajući digitalni potpis.

Taj potpis predstavlja njegov dokaz rada koji se u blockchain sustavu naziva *Proof of work.*

2.2.5 Proof of work

Proof of work (PoW) je jedan od dva načina na koji se može vršiti autorizacija transakcija. Ovaj originalni algoritam osmislio je Satoshi Nagamoto. Sastavljen je na način da se čvorovi, odnosno rudari, natječu tko će brže ovjeriti transakciju, zatim ponuđene kriptovalute postaju vlasništvo rudara koji to napravi prvi. Pošto se na kraju izračuna svake transakcije stvaraju novi blokovi, najduži lanac se smatra pobjednikom. Kako svi rudari obrađuju u istom blockchainu, istinitim lancem se smatra onaj u koji je uloženo bar pola ukupne snage svih

[3] Bitfalls, Bruno (2017.), Što je to novčanik (wallet) za kriptovalute i kako do njega?, Dostupno na: https://bitfalls.com/hr/2017/08/31/what-cryptocurrency-wallet/

računala.

Ovaj sustav je ispočetka bio rado privaćen jer pruža mogućnost rudarenja svakome a za uspješan rad zahtjeva samo struju i računalnu opremu. No zbog sve većeg rasta i ,prema tome, povećavanja konkurencije na tržištu,obrada sada zahtijeva složeniju i skuplju opremu a mreža postaje sporija i zbog toga je osmišljen drugi koncept dokaza pod nazivom „*Proof of stake"*.

2.2.6 Proof of stake

Proof of stake (PoS) ne funkcionira na način da ruder kreira i niže nove blokove u lanac, već biva izabran na temelju dva podatka o stanju valuta na njegovom računu (koje se zajednički nazivaju „ulog"): koliko valuta ima i koliko dugo, što znači da rudar sa starijim i brojnijim valutama ima prednost. U ovom slučaju rudarova naknada predstavlja proviziju koju je klijent namijenio za autorizaciju te transakcije.

Glavna prednost PoS-a je osiguranje od postavljaja lažnih transakcija od strane pojedinca i rudara jer, čim se naruši integritet sustava, riskira se narušavanje vrijednosti kriptovalute, što znači da nitko neće moći zaraditiod nje. Pošto ne zahtjeva složeniji proces kreiranja blokova, ova metoda je brža i manje zahtjevna u pogledu potrebne računalne opreme.

Međutim, specifikacije na temelju kojih se rudar bira, otežavaju mogućnost probitka novih rudara zbog favoriziranja uspješnijih i iskusnijih. Zbog toga se rudari mogu odlučiti međusobno udružiti radi povećanja zajedničkog kapitala što dovodi do povećane kontrole sustava. Postoji i inačica Proof of stake-a koja se naziva *delegirani Proof of stake.*

2.2.7 Delegirani proof of stake

Delegirani proof of stake (DpoF) odvija se preko mining pool- ova (od 20 do 100 članova) u kojem se svi članovi međutim izabiru glasanjem. Težina glasa određena je udjelom sredstava u zajedničkom novčaniku jednoga pool-a. Princip naknade i rada ove metode je isti kao Proof of stake samo što klijent tu bira pool umjesto pojedinca. Svaka akcija koju poduzme jedan član poola je javna i može biti osporena i modificirana od strane drugih članova. Ako je akcija neprihvatljiva taj član će biti zamijenjen drugim izabranikom. Iako je ovaj sustav polu centraliziran članovi su ravnopravni i ovakav način rada štedi im vrijeme i manje je podložan greškama. Opasnosti ovog sustava leže u mogućnosti udruživanja skupine unutar organizacije i njene manipulacije i u manjem broju potrebnih ovjera transakcije kako bi bila validna.

2.3 Značajke i prednosti blockchain tehnologije

Ova revolucionarna tehnologija predstavlja korak naprijed u poboljšanju svih ključnih elemenata funkcioniranja finacijskog, poslovno komunikacijskog ali i kojekakvih drugih

sustava poput glasovanja, preuzmanja medicinske ili ovjeravanja drugih važnih dokumentacija. Faktori koji predstavljaju njenu značajnu prednost su decentraliziranost, nepromjenjivost, sigurnost i transparentost.

1. Decentraliziranost- je prva najveća prednost blockchaina, značajna zbog ubrzanja procesa i povišenja sigurnosti transakcija. U centraliziranom sustavu, u kojem samo jedan administrator obnaša sve uloge, veće su mogućnosti hakiranja i kompromiziranja podataka ukoliko doživi problem, te sustav može lakše postati preopterećen velikom količinom podataka. Decentralizirani sustav ne pohranjuje informacije samo u jednom, već u više entiteta ili, u slučaju blockchaina, čvorova zbog čega su podatci dostupniji i teže je s njima manipulirati. Ova prednost se najviše manifestira na bazu podataka. U tradicionalnim bazama podataka klijent može izvšiti bilo koju operaciju i manipulaciju nad podatcima što smanjuje njihovu sigurnost i čini je podležnom manipulacijama dok u blockchainu klijent jedino može dodavati nove podatke, odnosno vršiti transakcije koje nakon dodavanja nemože više izmjeniti.“ S druge strane, baza u blockchainu sastoji se od nekoliko decentraliziranih “čvorova”. Svaki čvor sudjeluje u administriranju: svi čvorovi moraju autorizirati nove dodatke blockchainu i kadri su unijeti nove informacije. Kako bi nova informacija mogla biti unesena, većina čvorova mora postići konsenzus. Mehanizam konsenzusa jamči sigurnost mreže i čini je otpornom na manipulacije. Još jedna bitna razlika je integritet i transparentnost, jer je blockchain javno provjerljiv. Svaki korisnik može biti siguran da su podaci koje ima nekorumpirani od trenutka kada su zabilježeni, i svaki korisnik može utvrditi kako je blockchain bio potvrđivan kroz vrijeme.“[4]

2. Nepromijenjivost- Jednom kada se autorizira, transakciju je gotovo nemoguće izmijeniti ili uništiti zbog kriptiranog, odnosno hash-iranog sadržaja koji, čak i zbog najmanje pogreške, dekriptiran neće imati smisla. Na glavnom popisu blockchaina dostupno je stanje svih računa i popis njihovih ulaznih i izlaznih podataka pa se lako može uočiti bilo kakav pokušaj manipulacije podacima. Također cijeli sustav osmišljen je tako da čvorovi mogu samo dodavati podatka, bez mogućnosti da ih naknadno izmjene ili izbrišu, što rezultira automatiziranom gradnjom sustava povjerenja gdje si korisnici međusobno mogu vjerovati i bez kontrole transakcija od strane posrednika. Prema tome, može se reci da je nefleksiblnost blockchaina jedan od razloga njegovog transaprentnog načina poslovanja.

[4] Jutarnji list, Matanović, I. (2018.), Nemoguće je korumpirati podatke: Najveća prednost blockchaina je njegova transparentnost, Dostupno na: https://novac.jutarnji.hr/novi-svijet/nemoguce-je-korumpirati-podatke-najveca-prednost-blockchaina-je-njegova-transparentnost/7301704/

3. Sigurnost- Zbog već spomenutog matematički složenog kodiranja garantira se da će se klijentovi podaci iščitati samo od osobe koja ih odobrava. Ako itko pokuša pristupiti klijentovim podatcima sustav odmah reagira i dodatno enkriptira datoteke, a uz najmanju pogrešku haker kompromizira stanje kriptovalute i ostaje bez zarade. Potencijalnim hakerima situaciju će dodatno otežati i decentralizirana priroda mreže koja ima više lokalnih kopija podataka raspoređenih po čvorovima, u kojima se lako može provjeriti je li došlo do neke vrste mnipulacije s njima.

4. Transparentnost- Blockchain nudi visoku transparentnost u smislu dostupnosti korisnikovih identifikacijskih podataka u obliku javne adrese, odnosno javnog ključa, i popisa svih stanja ili izmjena vrijednosti na toj adresi, dok, u isto vrijeme, njegov identitet ostaje zaštićen složenim kodovima. Zbog takve vrste transparentnosti lakše se otkrivaju bilo kakve manipulacije podatcima. Zbog, već spomenutog, ugrađenog sustava povjerenja, korisnici imaju veću kontrolu nad svojom transakcijom i nemaju potrebu za posrednicima što dodatno povećava demokratičnost cijelog sustava.

3. ELEKTRONIČKO BANKARSTVO

3.1 Osnovne odrednice elektroničkog bankarstva

Rijetko koja inovacija je unijela toliko promijene u bankarsko poslovanje kao elektroničko bankarstvo. Njegova je revolucija dala priliku bankama za proširenje.mijenjanje strategije i pružanje velikog broja novih mogućnosti svojim korisnicima. Iz klijentove perspektive, najveća prilika koju je elektroničko bankarstvo donijelo je povećanje transparentnosti poslovanja, koje im, između ostalog, olakšava odabir između konkurentskih banaka. Iz bankine perspektive, nedvojbeno je najveća prednost smanjenje njenih operativnih troškova.[5]

Sa stajališta optimizacije poslovanja banaka, internet kao distribucijski kanal prilagodljiviji je promjenama i konstantnoj evoluciji bankarskog sustava, u pogledu dostupnosti pokriva najšire područje klijenata i povećava brzinu transakcija te, sukladno tome, ih može obavljati više i profitabilno funkcionirati sa nižim naknadama što je velika prednost za klijenta.

Nova grana koja je proizašla iz elektroničkog, odnosno internet bankarstva, je mobilno, na čijem se prilagođenom sučelju može izvršiti veći operacija kao što su: pregled primitaka, izdataka i stanja računa, nadzor dospijeća i limita svih kartica, informacije o kartičnim transakcijama, obavljanje deviznih i kunskih transakcija, itd..

[5] Impact Journals, Chavan, J., (2013), (8str.), Internet banking- benefits and challenges in an emerging economy-2str., Dostupno na:
file:///D:/Antonija/Downloads/INTERNET_BANKING_BENEFITS_AND_CHALLENGES.pdf

Internet bankarstvo još uvijek doživljava stalni uspon u broju korisnika, čak i onih koji imaju određeno nepovjerenje u njegovu sigurnost, zbog svoje brzine i efikanosti. U hrvatskoj ga koristi oko ¼ stanovništva i više od 200 000 poslovnih korisnika. Većina banaka opciju e-bankarstva danas nudi besplatno ili po niskim cijenama, u okviru njihovih paketa, a jedna od najzatupljenijih je e-bankarstvo za građane.

3.1.1 E- bankarstvo za građane

E- bankarstvo za građane nudi opciju kontrole i izvršenja transakcija na svom računu bilo kada i bilo gdje. Osmišljeni način zaštite korisniku pruža privatnost, mogućnost autorizacije identiteta klijenta i mogućnost digitalnog potpisivanja naloga. Banka također pruža mogućnost mijenjanja informacija i dodatne zaštite čitanja pri transferiranju naloga od klijenta do nje.

Ova širokoopsežna usluga nudi: potpunu provjeru računa, te kreditnog limita i transakcija, kunsko i devizno plaćanje i konverziju valuta, primanje i podmirivanje elektronskih i ostalih računa, plaćanje kreditnih rata te plaćanje pre-paid bonova ta telefonsku mrežu.

3.1.2 Sredstva autorizacije

Za razumijevanje funkcioniranja ovakvog sustava, potrebno je malo detajnije analizirati način identifikacije, to jest autorizacije korisnika. Na temelju načina autorizacije razlikuju se 2 tipa izvršavanja ovoga sustava. Za privatne korisnike uvriježeni su tokeni i TAN, dok se pravnim osobama nudi moćnost upotrebe smart kartice. U nastavku slijedi pobliži opis svakog načina autorizacije

1. Token- Otvaranjem svog računa klijent dobiva uređaj namijenjen isključivo za autorizaciju njegovog računa, koji se zove token. To je samostalni, mal i kompanktan uređaj zaštićem klijentovom lozinkom četveroznamenskaste duljine koji služi ovjerama identiteta i transakcije sa minimalnom mogučnošću neovlaštenih akcija. Prilikom svakog pristupa, nakon početne lozinke, token pruža jednokratni serijski broj koji je također obvezan za rad aplikacije. Kripcijski je zaštićen i prilikom upisa pogrešne inicijalne lozinke tri puta, aplikacija se automatski gasi i ponovno je može aktivirati samo poslužitelj.

2. TAN- odnosno *Transaction identification number* je popis više brojevnih nizova koje banka tj. administrator šalje klijentu. Taj niz naoko izgleda kao telefonski broj kako bi se smanjila mogućnst manipuliranja autorizacijom. Svaki od njih samo jednom može

poslužiti za autorizaciju i unos podataka što znači da banke šalju nove liste ili izdaju karticu i dopunjavaju je određenim količinom na upit klijenta. Pozitivna strana ovakve identifikacije je što se nemora koristiti dodatan uređaj, no administracijski troškovi za banku u odnosu na token su puno viši zbog toga što mora postojati baza podataka sa svim prethodno iskorištenim i dodijeljenim TAN-ovima.

3.1.3 Smart kartica

U slučaju e- bankarstva pravnih osoba, token nije dovoljan jer se neke transakcije rade offline a svaka se mora potpisati od strane banke i vratiti pravnoj osobi u obliku digitalne mape. Zato se u ovom slučaju najčešće upotrebljava smart kartica.

Smart kartica izgledom je ista kao i obična a njezina je fizička konstrukcija defenirana međunarodnim ISO- 7810 standardnom ali može rukovati, pohranjivati i obrađivati veliku količinu podataka.

Njena specifičnost ogleda se u posjedu jedne od dvije kombinacije sljedećih komponenti:

1) memorijskog čipa i mikropocesora ili

2) memorijskog čipa sa neprogramabilnim sustavom.

Kod kartica sa prvom kombinacijom moguće je manipulirati podatcima (izmjeniti ih ili brisati) dok druga kombinacija dozvoljava izvršavanje samo unaprijed određenih aktivnosti. Jedno od najznačajnih poboljšanja u njezinoj tehnologiji je mogučnost dodavanja izvršnog programa tojest koda koji je čini programljivom, a samim time i praktičnijom i sigurnijom.

Ostale softwerske komponente njene građe uključuju: procesor, RAM odnosno radnu ili trenutnu memoriju , ROM (eng. *Read Only memory)*, elektronički izbrisivu memoriju dostupnu samo za čitanje te ulazne i izlazne jedinice.

Čitač smart kartice nužan je za njezinu uporabu jer on, pravilno instaliran, služi kao prijenosnik njenih podataka na računalo. Za pristup podatcima također je potreban i korisnički PIN.

Rad kartice osmišljen je pomoću KPI (eng. *Public Key Infrastructure*) sustava koji kodira podatke kombiniranjem javnih i privatnih ključeva. Kao što mu samo ime govori, javan ključ je dostupan svima dok je privatni poznat samo klijentu. Kad se podatci kriptiraju i pošalju primatelj ih mora dekriptirati vlastitim privatnim i javnim ključem pošiljaoca.

3.2 Pozitivne i negativne komponente elektroničkog bankarstva

Sudionici u sustavuelektroničkog bankarstva imaju različite prioritete i potrebne ključne elemente koji će im pospješiti zadovoljstvo njime stoga će biti pojedino obrađene prednosti i mane sustava od strane klijenata, kao i od strane banke.

3.2.1 Prednosti i nedostatci sa gledišta banke

S bankarskog aspekta očituju se slijedeće prednosti:

1) Administratinvni i transakcijski troškovi višestruko se smanjuju, pogotovo u slučaju uporabe token-a, zbog pospješenja brzine i otklanjanja nepotrebnih hodova automatizacijskim radom sustava. Zaposlenici se dodatno rasterećuju, što znači da mogu obavljati druge poslove i povećati ukupnu odrađenu količinu.

2) Povećanje konkurentnosti zbog primjene općenito prihvaćenog i odobravanog sustava, što podiže imidž i gradi reputaciju banke, te , sukladno tome, povećava povjerenje postojećih i potencijalnih klijenata. Također, razvijanje i potreba za konstantnim ažuriranjem procesa potiče bržu reakciju na promjenu internih i eksternih čimbenika poslovanja.

3) Veću pokrivenost tržišta i osiguravanje zadovoljstva trenutnih i potencijalnih klijenata koji žive dalje od njihovih podružnica zbog ubrzavanja samog procesa i uklanjanja nepotrebne radnje dolaska.

4) Pružanje prilike za dodatni kanal marketinške distribucije banke i njezinih paketa i aktivnosti. Veća je šansa da će klijent uočiti oglas koji bi ga mogao zainteresirati u perifernom dijelu zaslona, nego u podružnici, listajući brošure ili odvajajući dodatno vrijeme pri obavljanju transakcije za raspitivanje o dodatnom pružanju usluga.

Iako ovaj sustav dokazano predstavlja korak unaprijed za bankarsko poslovanje, ipak sadrži i neke potencijalne probleme. Najveća mana je što se on sastoji od samo jednog poslužitelja tj. banke koja ima za zadatak pohraniti, odobriti i izvršiti ostale akcije nad transakcijama svih klijenata. Takva centraliziranost sustava čini ga ranjivijim i podložnim malfunkcijama zbog preopterećenosti, zbog potencijalnog gubljenja informacija koje su pohranjene na samo jednom mjestu i lakšeg mogućeg hakerskog napada koji treba ciljati samo na jednog administratora.

3.2.2 Prednosti i nedostatci sa klijentovog gledišta

Iz klijentove prerspektive gledišta također postoji mnogo prednosti, ali i nekoliko nedostataka e- bankarstva. U nastavku se nalaze neki od najvažnijih, faktora za i protiv.

Prednosti:

1) Efikasnost i brzina za klijenta- većina usluga klijentu je dostupna 24 sata na dan što uvelike pojednostavnjuje proces i drastično smanjuje vrijeme čekanja. Ako klijent ima nekih problema sa korištenjem elektronskog bankarstva uvijek se može obratiti korisničkoj službi, telefonski ili online. Također klijent će ažurnije prepraviti u računu informacije koje su se promijenile poput broja mobitela, e maila, adrese,... .

2)Mogućnost pogodnijih kamata- Pošto e bankarstvo uvelike smanjuje infrastrukturne troškove banki, postoji mogućnost da će banka, sukladno smanjenju plaćanja obveza, sniziti troškove plaćanja kamata na hipoteke ili povećati mjesečnu postotnu naknadu za oročenje štednje.

3) Povećana kvaliteta i dostupnost usluge- banke u kojima postoji mogućnost elektroničkog bankarstva nude mogućnost korištenja besplatnih dodatnih financijskih i poslovnih alata poput alata za analizu i planiranje financijske mogućnosti, kreditnih kalkulatora i alata za investicijsku analizu. Ovakve dodatne pogodnosti obično se ne mogu naći na klasičnim web stranicama banaka

4) Prilagodljivost u vidu mobilne tehnologije- Mobilno bankarstvo kao nova grana internet bankarstva postoji već neko vrijeme ali konstantno se ažuriraju ili stvaraju nove aplikacije koje ispravljaju svoje eventualne prethodne probleme s radom i prilagođavaju se svim modelima današnjih pametnih telefona.

5) Brzina transfera transakcija- e- bankarstvo nudi mogućnost automatskog prihvaćanja transfera klijenata kao i uplate naknada za vrlo nisku ili nepostojeću naknadu, čak i ako je riječ o drugim bankarskim institucijama.

6) Jednostavnost korištenja- Online korisnički račun može se otvoriti u samo nekoliko klikova i ne zahtjeva nikakvo dodatno informatičko znanje i iskustvo, no u slučaju pojave bilo kakvih problema klijent uvijek ima opciju kontaktiranja online ili telefonske korisničke podrške.

7) Ne šteti okolišu- Kako se sve transakcije i ovjere izvode digitalno, eliminira se potreba za većim korištenjem papira i uzročno- posljedično smanjuju trošak nekretnina i uredske opreme bankarske institucije te goriva klijenata koje bi potencijalno iskoristili

za obavljanje transakcije.

Iako klijenti možda isprve nisu svjesni nedostataka e-bankarstva oni svakako postoje i slijede u nastavku:

1) Smanjenje bliskog i personalnog odnosa sa bankom- Odlazak u tradicionalne bankarske ustanove pomaže klijentu da stekne osobniji odnos sa njezinim zaposlenicima koji mogu spoznati njegove individualne potrebe i pravilnije usmjeriti njegov kapital ili mu predožiti neku posebnu uslugu illi podršku u slučaju nekih problema.

2) Mogučnost problema izvršavanja pojedinih transakcija preko interneta- Neke kompleksnije usluge banaka zahtjevaju osobnu naznočnost klijenta pogotovo ako su transakcije međunarodnog tipa.

3) Nemogućnost obavljanja svih financijskih transakcija koje nudi banka preko elektroničkog bankarstva- Online bankarstvo često ne nudi mogučnost dodatnog osiguranja, kao ni ovjeravanje ni digitalno potpisivanje i pečatiranje banke što mnogo pravnih i financijskih dokumenata zahtjeva. Nadalje tradicionalne banke nude svojim lojanim klijentima posebne usluge poput investicijskog savjetovanja ili povoljnijih kamata.

4) Sigurnosni problemi- Svi online računi, kao i oni u tradicionalnim institucijama danas su zaštićeni softwerskom enkripcijom zakonski regulirani od strane FDIC-a (eng. *Federal Deposit Insurance Corporation*) ali sistem je još uvijek podložan hakiranju podataka i njihovoj manipulaciji.[6]

3.3 Sigurnost elektroničkog bankarstva

Sigurnost je u elektroničkom bankarstvu najvažnija za uspješno odvijanje sustava i igra glavnu ulogu u pridobivanju klijentovog povjerenja koji ne želi da informacije o njegovim transakcijama budu dostupne nikome osim administratoru. Podaci se zato složeno kriptiraju i algoritmiraju primjenom, već prethodno spomenute, PKI tehnologije koja kombinira javni i privatni. U bankarskim sustavima postoji nekoliko standardnih algoritama koji se vrše pri obradi podataka a mnoge države, uključujući Republiku Hrvatsku koriste SSL algoritam.

3.3.1 SSL algoritam

SSL (eng. *Secure Socket Layer*) je sigurnosni protokol razvijen od strane Netscape-a,

[6] ResearchGate, Koskosas, I., (2011.), (11 str.), The rpos and cons of internet banking: A short review, 7.-9. str., Dostupno na: file:///D:/Antonija/Downloads/THE_PROS_AND_CONS_OF_INTERNET_BANKING_A_SHORT_REVI.pdf

američke tvtrke za računalne usluge, koji enkriptiranom vezom spaja web stranicu odnosno administratora i klijenta. Prenosi osjetljive podatke poput vjerodajnica i brojeva socijalnog osiguranja te kartica, koji su u mogućnosti pročitati samo korisnici koji posjeduju ključ za dekodiranje.

„Internetske stranice koje su zaštićene SSL certifikatom započinju izrazom https, umjesto http, u kojem *s* označava *secure,* odnosno *sigurno*. Stranice koje počinju s http se smatraju nedovoljno sigurnima jer preko njih napadači mogu dobiti pristup povjerljivim podacima, kao i online računima koje korisnik internetske stranice ima. Također, posjedovanje SSL-a se može prepoznati i po tome da pored adrese internetske stranice stoji mala ikona lokota ili je prostor u kojem se nalazi ta web adresa zelene boje.“[7]

3.3.2 Ostale sigurnosne značajke

Za ovjeru transakcija koristi se bankin digitalni potpis, kreiran pomoću njenog privatnog ključa koji nikom drugom nije poznat, i kojim se potvrđuje identitet pošiljatelja, njegovo neporecivo sudjelovanje u transakciji te integritet i vjerodostojnost transakcijskih informacija. Njegov jedini nedostatak je što nije tajan.

Mobilne aplikacije za e- bankarstvo uz ovaj standradni sigurnosni sustav nude dodatne sigurnosne mjere poput automatskog gašenja nakon 3 minute nakon prestanka aktivnosti ili zaključavanje nakon 3 pogrešna PIN unosa.

3.3.3 Sudjelovanje klijenata u sigurnosnom procesu

U poboljšanju preventivnih mjera sudjeluju i klijenti kojima banka pruža smjernice u vidu opreznosti i tehničkih komponenti uređaja s kojima pristupaju svom računu jer hakeri danas najčešće dijeluju i upadaju u sustav, indirektno upadajući u korisnikovo računalo putem virusa. Najčešće to rade tako da: „zaraze računalo spywareom i ukradu identitet, zatrpaju računalo skočnim prozorima i zaraze virusima, šalju spam i lažne e-poruke, nagovore da otvorite privitak iz lažne e-poruke, nagovore da posjetite lažne stranice i otkrijete im svoje osobne podatke i / ili pristupe vašoj bežičnoj mreži“[8]

Savjetuje se posebna opreznost u otvaranju bilo kakvih neočekivanih e-mail poruka nepoznatog pošiljaoca, posebice ako sadrže privitak ili internetski link. Za poboljšanje sigurnosti uređaja preporuča se korištenje najnovijeg i ažuriranog operativnog sustava, po

[7]ForgeBit, Radoš, M., (2018.), Što je SSL certifikat i zašto je važan?, Dostupno na: https://forgebit.com/2018/03/08/sto-je-ssl-certifikat-i-zasto-je-vazan/

[8] Samoborska banka d.d. (2017.), (11str.), Preporuke za sigurnost korisnika internet bankarstva, 2str., Dostupno na: https://ibank.sabank.hr/doc/Preporuke_sigurnost_korisnika_internet_bankarstva.pdf

mogućnosti kao regularni korisnik a ne administrator. Pri pristupu Internetu korisnik bi trebao uključiti antivirusnu zaštitu i koristiti različite lozinke za različite usluge koje sadrže minimalno 12 znakova.

U slučaju da su podaci kompromizirani, odnosno sustav se zarazi virusom, treba pokušati ekstraktirati podatke i poslovne podatke i programe korištenjem antivirusnih programa poput McAfee antivirusa, AVG-a, BitDefender-a itd., koji će eliminirati sadržaj kompromiziranih datoteka. Česta opasnost pri zarazi virusom je kreiranje velikog broja spam poruka u kratkom vremenu za koje korisnik uopće ne zna, pa se za eliminaciju takvog problema preporuča instalacija anti- spam programa poput StopZilla, AddAware i dr.

4. ELEKTRONIČKI SUSTAVI PLAĆANJA U APLIKACIJAMA

Elektronički novac predstavljaspremanje gotovinskih vrijednosti na informatičkom uređaju koji može služiti kao platno sredstvo u situaciji trgovanja s ostalim subjektima koji nisu izdavatelji te vrijednosti.[9]Jedina razlika između njega i drugih valuta je što se njima trguje virtualno. Može postojati u potpuno digitalnom obliku, pri korištenju na osobnim računalima vlasnika ili u fizičkom u obliku kartice čiji se novac digitalizira i pregledava čitačem za karticu.

4.1 Vrste transakcija elektroničkim novcem

Transakcije elektroničkim novcem uvelike su slične onima s realnim, a dijele se na dva tipa po tome kako i kada novac prelazi u primateljevo vlasništvo. Prva vrsta je notacijsko, odnosno bezgotovinsko plaćanje, a druga simboličko ili gotovinsko.

1. Notacijsko plaćanje temelji se na izdavanju naloga, svojevrsnog dokumenta koji se predstavlja banci i na temelju kojeg ona prebacuje sredstva s jednog na drugi račun. . Sredstva pri kojima se korisri su kreditna i debitna kartica, e-ček,...

2. Simboličko plaćanje podrazumijeva da simbol, odnosno e-novac, nosi vrijednost sam po sebi i ne zahtjeva popratni nalog.

[9] ECB pages, (2017.), What is money?, Dostupno na: https://www.ecb.europa.eu/explainers/tell-memore/html/what_is_money.hr.html

4.2 Vrste elektroničkih novčanih sustava

Elektroničke novčane sustave možemo podijeliti na dva načina:

1. Po načinu njihove povezanosti razlikujemo:

1. Online sustave- koji zahtjevaju konstantnu komunikaciju banke i klijenta, te provjeru valjanosti novčanih sredstava prije izvršavanja svake transakcije. Pomoću ovog sustava se obavlja se plaćanje kreditnom karticom.

2. Offline sustave- koji zathjevaju povremenu interakciju klijenta i banke. Provjera novčanih sredstava može se vršiti naknadno jer se pri transakciji serijski broj novčanice popisuje u bankinu bazu podataka kao korišten i svaki drugi pokušaj korištenja će se podrazumijevati kao krivotvorina.

2. Klasičnom podjelom- elektronički sustavi dijele se na:

1. Notacijske
2. Simboličke
3. Centralizirane
4. Decentralizirane

4.2.1 Notacijski sustav

Kao što je već ranije spomenuto, u notacijskom sustavu klijent putem elektroničkog naoga signalizira banci koliko će sredstava i kome prebaciti. U ovom sustavu nalog ne predstavlja nikakvu vrijednost, ona je pohranjena na računu.

Notacijski sustav dijeli se na tri podkategorije, ovisno o tome kojim sredstvom se korisnik koristi pri plaćanju: narudžbe za elektroničko plaćanje prenošene preko mreže, naplate kreditne kartice preko mreže i notacijske sustave temeljeni na pametnim karticama.

1. Sustav narudžbi za elektroničko plaćanje prenošene preko mreže- su poznati još kao i „plati odmah“ sustavi zbog toga što polog novca prebacuju odmah nakon što klijent inicira zahtjev. Izravno se povezuje sa vrijednosti jer podiže novac sa klijentovog računa. Ovakav se sustav primjenjuje kod čekova i debitnih kartica.

2. Naplatom kreditne kartice preko mreže-korisnik prihvaća njegovu odgovornost za svaku transakciju i ona se izravno veže za tu vrijednost na njegovom računu. Za izvršavanje transakcija u ovom sustavu koristi se kriptirana kreditna kartica ili autorizacijski broj. Kao što joj i sam naziv govori, kriptirana kartica osigurava sigurnost

podataka tako što ih kriptira prije slanja u računalnu mrežu dok u sustavu autorizacijskih brojeva postoji posrednik odnosno autorizator, koji provjerava i odobrava transakcije na temelju spomenutog broja.

3. Notacijski sustavi temeljeni na pametnim karticama- su kreirani specifično za pametne kartice čiji su rad i namjena opisani u prethodnom poglavlju (Osnovne odrednice elektroničkog bankarstva) i većinom su namijenjene za poslovne korisnike, čije složenije transakcije zahtijevaju veću prilagodljivost korisnikovim potrebama te sigurnost u vidu složene kriptografije podataka koji su čitljivi samo vlasniku. Njihova se tehnologija danas proširila i na druge funkcije osim elektroničkog poslovanja pa se ona danas koristi i u telekomunikacijskim i televizijskim djelatnostima.

Ovisno o tome je li potreban kontakt za transfer sredstava na primateljev račun, pametne kartice možemo podijeliti na:

1) Kontaktne- Ovaj tip pametne kartice se mora spojiti na čitač kartice kako bi se preko elektroničkog modula prenijele informacije pohranjene u čipu.

2) Bezkontaktne- U ovom slučaju nije potreban kontakt sa čitačem jer kartica ima ugrađenu antenu koja pri transferu sredstava signalizira informacije centralnoj anteni za primanje.

4.2.2 Simbolički sustav

Naziva se još i gotovinski zbog toga što je najsrodniji gotovinskom plaćanju. Razlika između ovog i prethodnog sustava je što u prethodnom slučaju novac ostaje sačuvan u banci, dok u simboličkom sustavu klijent u banci prediže određeni iznos e-novčanica sa svoga računa i koristi ih jednako kao što bi koristio i realan gotovinski novac. Zbog toga taj novac sam po sebi nosi vrijednost i njegova se autentičnost može kasnije provjeriti serijskim brojem. U trenutku kada korisnik predigne svoju e- gotovinu iz banke sam postaje odgovoran za njezin gubitak ili bilo kakvu kompromizaciju.

4.2.3 Centralizirani sustav

Glavna značajka koja karakterizira ovaj sustav je postojanje samo jednog središnjeg poslužitelja koji upravlja, nadzire i povezuje cijeli sustav, te vrši kontrolu toka podataka i transakcija. U ovakvim sustavima primjenjuje se tzv. Plaćanje unaprijed, na način da korisnik mora prvo kupiti elektroničku valutu,direktno od poslužitelja ili preko treće stranke, prije nego što obavi transakciju. Razlikuju se 2 podkategorije elektroničkih valuta to su:

1) elektronički novac- odnosno e-gotovina, koja se u mrežnom sustavu ponaša kao realan novac

2) elektronički novčanik- koji podrazumijeva korištenje pametne kartice koja svoje vrijednosti čuva na čipu

Centralizirani sustavi primjenjuju se u poslovanju banaka, kao i u mnogim drugim sustavima elektroničkih plaćanja od kojih je najpoznatiji PayPal.

Ova internetski orijentirana tvrtka koja pruža financijske usluge u vlasništvu je Ebay-a, jedne od najvećih tvrtki specijaliziranih za aukcijsku kupnju i prodaju, od 2002. godine. Popularnost na online tržištu je stekla zbog svoje sigurnosti i anonimnosti, jer jedini je jedini vidljivi korisnikov podatak adresa njegove elektroničke pošte. Ne zahtjeva unošenje podataka o računu ili kartici, korisnik samo šalje obavijest sustavu da prebaci određenu uplatu na primateljev račun. Za pružanje ove usluge PayPal naplaćuje proviziju, koja varira zavisno korisnikovom prebivalištu, odabranom tipu plaćanja i e-valuti i samom iznosu transakcije.

4.2.4 Decentralizirani sustavi

Svaka računalna mreža sastoji se od čvorova, od kojih svaki ima svoju svrhu i namjenu pri postavljanju i obradi podataka. Kod centraliziranih sustava diferencijacija čvorova je jasno vidljiva jer postoji jedan centralni koji pohranjuje i verificira podatke (poslužitelj) i oni koji stvaraju i pregledavaju podatke (korisnici). Kod decentraliziranog mrežnog sustava čvorovi su raspodijeljeni na temelju ravnopravnog partnerstva, što je omogućeno korištenjem partnerske mreže (eng. *Peer to Peer)*. koju karakterizira sljedeći način rada:

„1)svaki čvor je ravnopravan, uključujući mogućnosti prihvaćanja upita o podacima od korisnika ili drugih čvorova,
2) komunikacija između čvorova je izravna (bez međukoraka kao što su poslužitelji),
3) čvorovi samostalno prikupljaju informacije o dostupnosti drugih čvorova,
4) pojedinačni čvorovi imaju u svom lokalnom sustavu za pohranu na raspolaganju samo dio podataka, odnosno podskup ukupnih podataka dostupnih na mreži.“[10]

Najpoznatiji primjer decentraliziranog novčanog sustava je Bitcoin koji je jedan od najpoznatijih primjera korištenja Blockchain tehnologije smišljen od strane Nakamota Satoshia. „Bitcoin je sustav otvorenog koda, jer ga nitko ne posjeduje i svatko može

[10]Nacionalni CERT, (2010.), (26.str.), Elektronički novac, 11.str., Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-09-311.pdf

sudjelovati u njegovoj primjeni i razvoju. Ne postoje centralizirane institucije u ekoustavu Bitcoina da prikupljaju naknade i transakcije se mogu odraditi u roku nekoliko minuta, čak iako šaljete novac na drugu stranu svijeta. To je valuta koja nije ograničena državnim granicama.“[11]

Dakle, prednosti bitcoina uključuju jeftino i jednostavno transferiranje sredstava, koja su stabilna i sa minimalnom mogućnosti inflacije, bez potencijalnog manipuliranja podataka od treće stranke.

4.3 Protokoli plaćanja elektroničkim novcem

Protokol plaćanja elektroničkim novcem podrazumijeva svaki korak koji je nužno obaviti kako bi se transakcija izvršila. U pokušaju razvitka protokola koji maksimizira zaštitu klijentovih podataka a minimalizira mogućnost prijevare, kreirana su tri protokola u plaćanju elektroničkim novcem, od kojih je svaki nosio potencijalno rješenje na problem prošlog: protokol bez anonimnosti, anonimni protokol, te konačni oblik platnog protokola. Sva tri sastoje se od virtualno istih koraka: Podizanje novca, plaćanje i polaganje novca u banku, međutim oni se razlikuju u izvedbi njihovih pojedinih komponenata.

4.3.1 Protokol bez anonimnosti

Pri podizanju novca iz banke, korisnik šalje upit za određenu količinu novca banci, koja skine tu svotu sa njegovog računa i uručuje je natrag korisniku u obliku e-gotovine. Svaka novčanica ima digitalni potpis koji omogučuje da banka kasnije provjeri njezinu vjerodostojnost, te serijski broj koji popisuje u svoju bazu podataka kako bi spriječila bilo kakav pokušav njenog dupliranja ili višestrukog korištenja.

Pri plaćanju,korisnik transferira sredstva trgovcu koji prvo vlastoručno provjerava je li digitalni potpis autentičan.

Zatim trgovac šalje elektronički novac batrag u banku gdje se još jednom provjerava njezin serijski broj, te ga uvrštava u bazu podataka primljenih novčanica. Ukoliko se u kasnijem poslovanju pojavi druga novčanica istog serijskog broja banka će je automatski odbiti kao krivotvorinu. Nakon uspješne autentifikacije, gotovina se prebacuje na račun trgovca i on šalje predmet kupnje platitelju.

Glavni zaostatak ovog sustava je što ne pruža anonimnost jer postoji mogućnost da

[11]Kriptomat, (2019.), Što je Bitcoin i kako radi?, Dostupno na: https://kriptomat.io/hr/kriptovalute/bitcoin/sto-je-bitcoin-i-kako-radi/

banka zapamti vezu između korisnika i serijskih brojeva njegovih novčanica i kasnije prati njihovo kretanje i udio u transakcijama. U nastojanju ispravljanja ovoga problema osmišljen je sljedeći sustav.

4.3.2 Anonimni protokol

Ovaj protokol, kao što mu i samo ime govori, onemogućava povezivanje klijenta sa novčanicom od strane banke osiguravajući mu anonimnost. Spomenuti problem ovdje je rješen ispravljanjem postupka klijentovog podizanja novca, koji se odvija na način da on kreira svoje novčanice sa serijskim brojem, kriptira ih i šalje banci koja je ih u ovome slučaju ovjerava tzv. slijepim digitalnim potpisom s djelomičnim uvidom u sadržaj.

Slijepi digitalni potpis s djelomičnim uvidom u sadržaj podrazumijeva kripciju podataka njihovim množenjem sa nasumično izabranim brojem koji se zove faktor slijepoće i podržava javni ključ banke. Pošto banka ne može vidjeti serijski broj novčanica uklanja se potencijalna opasnost njihovog povezivanja sa korisnikom. Banka zatim šalje korisniku zahtjev za slanje dekripcijskog ključa određenog broja novčanica, provjerava njihovu vjerodostojnost, digitalno potpisuje i provjerene i ostale novčanice te skida taj iznos s njegovog računa.

Posljednja dva koraka odvijaju se na jednak način kao i kod protokola bez anonimnosti.

Međutim, kod ovog tipa protokola javlja se problem u vidu otežanog otkrivanja pojedinca koji pokuša duplicirati svoju novčanicu ili je višestruko koristiti, stoga je kreiran posljednji tip protokola koji nudi rješenje i na ovaj problem.

4.3.3 Konačni oblik protokola plaćanja e- novcem

Ovaj najevoluiraniji oblik protokola dosada pruža privatnost korisniku svojstvenu anonimnim sustavima, osim u slučaju pokušavanja bilo kakve prijevare elektroničkom novčanicom. U tom slučaju banka može identificirati korisnika pomoću informacija o identitetu integriranih u samu novčanicu. U ovom su slučaju djelomično izmjenjena sva tri koraka u svrhu njihovog poboljšanja.

Pri podizanju novca korisnik, kao u prethodnom protokolu, kreira, kriptira i šalje novčanice banci. Potom banka njemu šalje zahtjev za parcijalnom dekripcijom nasumičnih novčanica i identifikacijskim podatkom, u svrhu njihove provjere. Identifikacijski podatak može sadržavati bilo kakvu važnu informaciju o korisnikovom identitetu npr. ime ili kontakt broj, i jednom kada se verificira zajedno sa vrijednosti

novčanica, traženi iznos se uklanja s računa.

Pri plaćanju korisnik šalje određeni iznos e- novčanica trgovcu, koji prvo vlastoručno provjerava njezin digitalni potpis. Dodatni način zaštite u ovom koraku osigurava se tako što trgovac šalje slučajni odabirući niz, koji se sastoji od nula i jedinica (koji predstavlja zahtjev za različitim podatcima) korisniku koji mu zatim vraća potrebne podatke za usporedbu identifikacijskog podatka u novčanici. Informacije koje korisnik šalje, razdvojeni nemogu otkriti nikakv identifikacijski podatak dok ih trgovac ne hash-ira i usporedi sa istima na e-novčanici.

Trgovac zatim predaje zahtjev za polaganjem novca u banku zajedno sa informacijama o njegovom računu, i svim podatcima vezanim za novčanicu uključujući identifikacijski niz. Banka prvo provjerava autentičnost serijskog broja u bazi podataka upotrebljenih novčanica, a zatim ga unosi zajedno sa ostalim specifikacijama poslanih od trgovca. Nakon toga potvrđuje završetak transakcije trgovcu koji korisniku isporučuje plaćenu robu.

Uz već spomenuta poboljšanja u vidu anonimnosti i sigurnosti, ovo je prvi protokol u kojem je, pomoću identifikacijskih podataka, moguće otkriti da li novčanica zaista pripada tom korisniku ili je ukradena.

5. IMPLEMENTACIJA BLOCKCHAIN TEHNOLOGIJE U BANKARSKIM APLIKACIJAMA

5.1 Potencijal djelovanja blockhaina na poboljšanje cijelog financijskog sektora

Iako je svrha ovog rada prikazati poboljšanja koju bi primjena blockchaina donijela u bankarski sustav, veoma je važno je istaknuti kako bi implementacija ove tehnologije također unijela i velike promjene u globalni, za potrebe današnjeg sverastućeg tržišta, pomalo zakržljali financijski sektor. Zbog monopolističke prirode i važnosti financijskog sektora zanemarila se potreba za njegovom aktualizacijom i poboljšanjem što je rezultiralo sporim sustavom, podložnim greškama ljudskog faktora, koji ima visoke troškove transakcije održavanja, i prema tome, više provizije za njegove korisnike. Jedno od potencijalnih objašnjenja slabijoj prilagodbi modernim promjenama, u prvom redu banaka i ostalih institucija koje se bave trgovinom vrijednosnih papira, je što njihov pozadinski sustav poslovanja fukcionira na četrdesetak godina staroj tehnologiji dok se korisnicima, u vidu

njihovog sučeljnog pružanja usluga nude najnovije tehnologije poput internet bankarstva. Iako su na prvi pogled modernizirane, zastarjeli elementi poslovnog procesa poput potrebne količine vremena za proknjižavanje transakcija spriječavaju institucije u ostvarivanju većeg napretka.

Blockchain će na ovaj sektor najviše utjecati na slijedećih 8 načina:

1. Validacija podataka i identiteta- za autentifikaciju i odobrenje ovih informacija sudionici se najčešće oslanjaju na posredstvo banaka i drugih institucija dok je u blockchain tehnologiji takav potreban sustav povjerenja već utkan u njegovu mrežu. Korisnicima su međusobno vidljive samo javne adrese a ostali podaci koji bi trebali biti povjerljivi zaštićeni su kripcijom privatnih ključeva.

2. Prenošenje vrijednosti- Implementacija ove tehnologije osigurala bi brži prijenos veće količine transakcija sa manje otpora tijekom same transakcije, što bi znatno smanjilo cijenu transakcijskih troškova i uzrokovalo rast profita.

3. Pohranjivanje vrijednosti- Funkcionalni mehanizam transakcija koji karakterizira visoka kriptiranost podataka i vrijednosti pruža korisnicima povjerenje i eliminira veću potrebu korištenja banaka i ostalih financijskih institucija u svrhu kreiranja korisničkih računa.

4. Povećanje efikasnosti za sve korisnike- Primjenom ove tehnologije, svaki pojedinac će moći direktno, bez bankarskog posredstva, izdavati i primati sredstva što će mu ubrzati čitav proces, osigurati transparentnost procesa i smanjiti troškove istog. Pojam sredstva u ovom slučaju ne odnosne se samo na elektroničke novčanice već i na financijske instrumente poput zajma.

5. Razmjena sredstava- Vrijeme potrebno da se obrade transakcije vrijednosnih papira i drugih financijskih instrumenata može se mjeriti u tjednima što uzrokuje nepotrebno čekanje korisnika, dok bi u blockchainu bilo kakva transakcija mogla biti proknjižena u samo nekoliko minuta.

6. Pojednostavljenje investiranja- Financijske institucije bi i dalje igrale ulogu posrednika između investitora i predmeta ulaganja ali broj sudionika na ukupnom tržištu bi se povećao jer bi svaki pojedinac imao jednaku priliku za brzo, jeftino i sigurno ulaganje.

7. Jamstvo vrijednosti i kontrola rizika- Zbog decentralizirane prirode blockchain sustava koja podržava isto takav način osiguranja, rukovanje fincancijskim sredstvima za upravljanje rizikom postat će transparentnije.Osiguravajući fondovi imati će priliku povećati kontrolu

rizika poslovnih pothvata u koje ulažu, te moći bolje oblikovati sliku o statusu klijenta na temelju njegovih investicijskih pothvata, kapitala i drugih parametara analiziranihkroz blockchainove reputacijske sustave.

8. Transformacija računovodstvenog sustava- Vođenje ovog poslovanja u ovom sustavu također će biti transparentnije. Veliko poboljšanje koje bi blockchain sustav donio računovodstvu je mogućnost financijskog izvještavanja i analize u stavrnom vremenu, koristeći svoju tehnologiju distribuiraneglavne knjige (eng. *Distributed Ledger* Tehnology) transakcija o kojoj će malo više riječi biti poslije.[12]

5.2 Pametni ugovori

Ugovorni sporazum u današnje vrijeme predstavlja temeljni regulator društvenog i organizacijskog funkcioniranja i zbog toga pametni ugovor predstavlja jedno od najperspektivnijih područja blockchaina koji bi mogao unijeti promjene u mnogobrojnim djelatnostima poslovanja, pogotovo u financijskoj.

Riječ ugovor rabi se u imenu ove tehnologije zbog njezine inicijalne pozanosti sa trgovanjem kriptovalutama (novčanim sredstvima blockchaina) na temelju određenih uvjeta i zbog sličnosti s karakteristikama klasičnog pravnog ugovora na papiru: odvija se između stranaka koje su pojedinčno prihvatile njegove uvjete i ispoštovale ih, ili snosile posljedice za njegovo kršenje.

5.2.1 Koncept rada pametnog ugovora

Struktura pametnog ugovora građena je pomoću klasične blockchain tehnologije nizanja lanaca s blokovima, s tim da se u ove blokove ne unose podatci, već programski kodovi. Također, njihov u programski kod je unsena automtski prijenos i kontrola sredstava ukoliko su dogovoreni uvjeti zadovoljeni.

Stvaranje pametnog ugovora sastoji se od 3 koraka: Prvi je transformacija i unos informacija o pravilima razmjene između sudionika u programski kod, koji se zatim unosi u blokove te niže u lanac. Sudionici ostaju anonimni dok su pravila javno dostupna. Drugi nastupa nakon odvijanja događaja za koji je određen da će potaknuti pokretanje procesa (eng. *trigger event*) izvršavanja ugovora prema unaprijed određenim pravilima. U trećem koraku omogućava se ostalim korisnicima sustava da čitaju blokove ugovora kako bi ispitali njegove rezultate.[13]

[12] Tapscott, D. & Tapscott, A., Blockchain Revolution, (2016.), (324str.), 68.-70. str.
[13]Blockgeeks, Rosic, A. (2019.), Smart Contracts: The Blockchain Technology That Will Replace Lawyers, Dostupno na: https://blockgeeks.com/guides/smart-contracts/

5.2.2 Prednosti i potencijalne primjene pametnog ugovora

Tri su najveće prednosti pametnog ugovora naspram običnog: najprije sudionicima jamči dodatnu sigurnost podataka u vidu složene kriptografije kodova. Njegov način strukturiranja blokova u lance, razlog je njegove druge prednosti: nemogućnosti bilo kakve izmjene i brisanja podataka zbog čega se sustav povjerenja između sudionika automatski generira. Zbog toga što se faktor povjerenja automatski uspostavlja, eliminira se potreba za posrednikom koji bi kod klasičnih ugovora osigurao izvršenje uvjeta od strane učesnika.

Ova tehnologija ima najveću potencijalnu primjenu u djelatnostima različitih osiguravajućih društava i telekomunikacija,pri plaćanju za različite medije i sadržaje ili čak pri sportskom klađenju. Korisnicima pružaju potpunu autonomiju, odnosno kontrolu, nad ugovorom, uštedu vremena i novca zbog eliminacije troška plaćanja raznih posrednika, te automatiziran sustav povjerenja uz visoku sigurnost podataka.

Iako bi pametni ugovor trebao predstavljati opasnost za poslovanje banaka u vidu posredništva i prema tome ubiranju posredničke naknade, zapravo joj pruža priliku da upotrijebi njegovu efikasnu tehnologiju za pružanje mogućnosti usluge sastavljanja sigurnog, transparentnijeg i jeftinijeg ugovora za svoje korisnike u kraćem roku, u kojem ona posreduje na drugi način: kao vjerodostojna, povjerljiva i sigurna eksterna baza podataka u koju se svi sudionici mogu pouzdati za korektan unos informacija iz realnog života koje bi mogle uvjetovati ugovornu transakciju. S obzirom da je pametni ugovor u svojoj osnovi ipak samo programski kod, on treba svoju eksternu bazu podataka (eng. *oracle*) koju može iskoristiti za unošenje realnih i provjeru postojećih podataka.

S obzirom da u kodovima pametnih ugovora može biti zapisan bilo kakav podatak, ne samo oni koji potiču financiranje na temelju ispunjenih uvjeta, on se može transformirati u uvjetovanu aktivnost koja može uvelike automatizirati neke poslovne procese banaka poput:

1. selektivne komunikacije i pružanja mogućnosti uvida u podatke za jedan ili više čvorova

2. Za automatski izračun i analizu podataka u ugovoru za korisnika od strane programskog koda

3. Za provjeru ispravnosti identifikacije pohranitelja odeređenih podataka

4. Za usklađivanje, prilagođavanje i standardizaciju podataka programskim kodom pametnog ugovora, što eliminira potrebu za pojedinačnim unosom podataka od različitih korisnika.

5.3 Kriptovalute

5.3.1 Pojmovno određenje kriptovaluta

Jedan od važnijih izuma proizašlih iz blockchaina koji bi također mogao unijeti velike promjene u financijski sustav su kriptovalute.

Javljaju se tijekom svjetske financijske krize 2009. godine kao odgovor na nekompetentan, krut i centraliziran stav monetarnih politika banaka. Kreirane su kao posebna, geografski neodređena valuta, koja eliminira potrebu za posredovanjem ili obradom transakcija od treće strane, odnosno financijske institucije. Prva kriptovaluta produkt je samog izumitelja blockchaina i naziva se bitcoin, te je i danas jedna od najpoznatijih digitalnih valuta sa nevjerovatnom vrijednosti od 64,980,97 kn po jednome bitcoinu.

Unatoč njihovoj mnogobrojnosti karakterizira ih sljedećih 6 osobina:

1) Vezane su isključivo za računala, odnosno digitalne su

2) Koriste decentraliziranu peer-to- peer mrežu pri transferu vrijednosti

3) Za razliku od realnih valuta, univerzalno su iskoristive bilo gdje

4) Njegova vrijednost nije pohranjena kod treće stranke ili institucije već je decentralizirana unutar mreže

5) Sustav u kojem se njima trguje već ima integriran sustav povjerenja u svoj način rada stoga su ostale provjere suvišne

6) Vrijednost i podatci koje ona uz sebe nosi su kriptirani

Kriptovalute imaju izniman potencijal za transformaciju današnjih financija zbog toga što nisu pod vlasništvom ni jedne zemlje, stoga nisu podložne nikakvoj vladi niti fiskalnoj ili monetarnoj politici. Iako je to velika prednost u vidu lišavanja tržišta od ikakve dominacije institucija, banke, koje bi izgubile ulogu posrednika, nebi više imale utjecaja nad ponudom i potražnjom a države bi potencijalno mogle izgubiti svojstvene valute i izgubiti kontrolu nad inflacijom, što će izazvati nove promjene u načinu zaduživanja i općenitoj ekonomiji.

5.3.2 Odgovor banaka na kriptovalute

Današnje banke još nisu prihvatile kriptovalute kao validno klasično sredstvo plaćanja zbog sumnje u nekolicinu, po njihovom mišljenju, većih propusta unatoč njihovim brojnim potencijalnim prednostima.

„BIS ili središnja banka svih središnjih banaka, kako je poznatija u javnosti, smatra da su kriptovalute prenestabilne, u njihovo nastajanje troši se prevelika količina električne energije te je subjekt previše manipulacija i prijevara da bi mogla biti sredstvo razmjene u globalnoj ekonomiji.

Štoviše, decentralizirana struktura kriptovaluta, za njihove zagovornike jedna od glavnih prednosti, za BIS je jedan od ključnih nedostataka.

Zbog krhkosti decentraliziranih mreža o kojima kriptovalute ovise, povjerenje u njih može nestati praktički "preko noći", smatraju u BIS-u.

Naime, bilo koji oblik novca zahtijeva povjerenje u stabilnost svoje vrijednosti, a to kriptovalute nemaju. Analitičari te institucije također smatraju da bi masovno korištenje kriptovaluta u platnim transakcijama dovelo do zagušenja internetskih veza, te da kod kriptovaluta dobar dio njihovih vlasnika drži nih iz čisto špekulativnih razloga, a ne zato jer njime žele plaćati robu i usluge.“[14]

Unatoč ne prihvaćanju kriptovaluta kao potencijalnih digitalnih valuta budućnosti,nekoliko velikih financijskih poduzeća prepoznalo je potencijal takve tehnologije i 2016. 4 velike svijetske banke, na čelu s UBS grupom, počinju raditi na projektu USC tokena (eng. *Utility Settlement Coin*). Ideja za ovaj projekt proizlašla je iz želje banaka da implementiraju blockchain tehnologiju u svoj sustav poslovanja zbog njene efikasnosti, ali bez korištenja nesigurnih decentraliziranih kriptovaluta čije bi se vrijednost mogla pokazati previše nestabilnom. Stvaranjem USC tokena, posebne digitalne valute koja predstavlja ekvivalent 5 glavnih svjetskih valuta: američkog i kanadskog dolara, britanske funte, eura i japanskog jena, i koja bi imala svrhu sredstva online plaćanja i prenositelja svih transakcijskih podataka, trošak i vrijeme obavljanja transakcija mogli bi značajno pasti. Ovaj sustav bi također eliminirao tri rizika posrednika: rizik namirenosti, druge ugovorne strane i tržišni rizik, pošto su funkcije sva tri navedena već implementirane u blockchain tehnologiju.

Ovaj projekt, koji je još u razradi, prvi je od sličnih koji su uslijedili, a dosada je prikupio 14 banka članica i oko 63,2 milijuna dolara investicija[15]

Ovo je jedan od mnogih vrsta projekata koji imaju za cilj uspješnost implementacije ove tehnologije. 2015. američka tvrtka Consensys koja se bavi primjenom blockchaina, uspješno je pokazala kako bi pametni ugovori, o kojima će više riječi biti kasnije, jedna od

[14] Poslovni Dnevnik, (2018.), “Banka svih banaka” poručila: Bitcoin nikada neće biti novac, Dostupno na: https://www.poslovni.hr/trzista/bis-bitcoin-nikada-nece-biti-novac-342094

[15]Coindesk, (2020.), 14 Banks, 5 Tokens: Inside Fnality’s Expansive Vision for Interbank Blockchains, Dostupno na: https://www.coindesk.com/fnality-utility-settlement-coin-central-bank-token-blockchain

značajnih funkcija ovoga sustava, pospješili rad banaka, a 2016. 40 najvećih svjetskih banki uspješno je izvelo pokušaj prodaje financijskih sredstava na 5 diferenciranih blockchain sustava.

5.4 Transformacija mreže aplikacija banaka

Jedna od komponenti sustava rada banaka koju blockchain tehnologija također može unaprijediti je tip mrežne arhitektekture unutar njenih aplikacija.

Banke trenutno u okviru svog poslovanja upotrebljavaju distribuirani tip aplikacije, oblik koji podržava njezin istovremeni rad na više računala i servera gdje god se oni nalazili, u svrhu izvršavanja njenih zadaća. Ova značajka je najveća prednost sustava, jer ako jedno računalo iskusi probleme bilo kakve s radom, aplikacija se može jednostavno ponovo pokrenuti na drugom.Podijeljena je u dva osnovna dijela: jedan je namijenjen klijentima a drugi poslužiteljima.

Ove aplikacije podržavaju četiri različite arhitekture mreža, a banke danas u svom poslovanju većinom rabe Uslužno orjentiranu arhitekturu.

Uslužno orjentiranu arhitekturu karakterizira konstantna komunikacija između različitih programskih rješenja u smislu razmjenjivanja podataka ili njihovog međusobnog kombiniranja u svrhu izvršenja zadatka. Ovakav tip aplikacije pruža različit broj hijerarhijski raspoređenih usluga koje su neovisne jedna o drugoj i imaju već unaprijed određen tok i ishod. Na svom sučelju korisnik ima mogućnost odabira onih usluga koje su mu potrebne, dok mu druge ostaju skrivene ne ukaže li se potreba i za njima.

Upotreba blockchaina prvenstveno bi unaprijedila distribuirani u decentralizirani tip aplikacije, a uslužnu arhitekturu bi zamijenila *Peer to Peer*(P2P)arhitektura, karakteristična za funkciju sustava u blockchainu.

Decentralizirani tip aplikacije inačica je distribuiranog tipa karakterističnog za blockchain. Njezin princip rada i uslužna logika unaprijed su određeni programskim kodom unutar sustava koji podržava i isti takav oblik P2P ravnopravne partnerske arhitekture. S obzirom da je u ovom slučaju riječ o uvrštavanju ovakve arhitekture u poslovni proces banaka, koje same po sebi predstavljaju posrednika i poslužitelja i u jednu ruku zahtjevaju klijent-server tip arhitekture , idealan za primjenu bio bi poseban oblik P2P-a koji se naziva hibridni P2P.

„Hibridne Peer to Peer mreže možemo promatrati kao mješavinu klijent-server i čiste P2P arhitekture. Hibridni pristup dopušta postojanje preferiranih čvorova tzv. superčvorova koji su

nadređeni ostalima te na razne načine mogu utjecati na mrežu. Klijent-server arhitekutura se odnosi na pretraživanje datoteka, a čisti P2P na njihov prijenos.“[16]

Ovaj tip mreže kombinira sve pozitivne značajke centraliziranog načina čuvanja i zaštite podataka od ostalih čvorova koji nisu nadređeni, što je ključno za povjerljivu prirodu bankarskog poslovanja, te decentraliziranog načina raspodjeljivanja podataka po superčvorovima, od kojih svaki preuzima na sebe određeni dio podataka iz običnih čvorova i raspoređuje ih u datoteke. Ukoliko korisnik, odnosno obični čvor želi pristupiti određenim podatcima, uputiti će zahtjev jednom od superčvorova koji će pretražiti svoju osobnu bazu i eventualno uputiti zahtjev ostalim nadležnim čvorovima ukoliko nema zapisane te podatke, te ih nakon pronalaska emitirati natrag korisniku. Pošto se radi o peer to peer mreži obični korsnici mogu međusobno slobodno komunicirati i razmjenjivati resurse tj. podatke koji su im omogućeni od strane poslužitelja tj. banke Ukoliko korisnik želi dodati nove podatke u sustav, odnosno uspostaviti transakciju, moraju poslati zahtjev centralnim autoritetima, koji provjeravaju valjanost informacija i zapisuju ih u blokove. Svatko tko treba imati pristup zapisanim informacijama dobiva svoj hash-pointer (hash pokazivač) s kojim može provjeriti pokušaje naknadnih falsificiranja

Primjenom ovakvog načina transfera i pretraživanja i zaštite podataka u poslovanju, banke bi uvelike ubrzale pretraživanje podataka iz njihove i klijentove perspektive, rasteretile glavni server i eliminirale potencijalnu preopterećenost daljnim rastom mreže, i uvelike smanjile opasnost kompromiziranja i manipulacije podacima zbog toga što je hakerima teže napasti više čvorova, a sve eventualne izmjene i pokušaji manipulacije podataka lakše će se otkriti uspoređivanjem podataka na drugome superčvoru.

5.5 Sigurnost blockchaina

Kao što je već ranije objašnjeno u tekstu, sigurnost je jedna od ključnih prednosti ove tehnologije u prvom vidu zbog složene matematičke kriptografije podataka, razvijenog identifikacijskog sustava i već ugrađenog sustava povjerenja. Ova značajka mogla bi joj osigurati ne samo perspektivnu budućnost u poslovanju banaka, već i kod bilo kakvih poslovnih ili vladinih sustava kojima je zadatak povjerljiva i efikasna razmjena informacija.

„Struktura ovog sistema omogućila je CIA-i da na raspolaganju ima trojstvo cyber sigurnosti

[16] Torrentkb, (2018.), P2P mreže, Dostupno na: https://torrentkb.weebly.com/p2p-mre382e.html

(povjerljivost, integritet i raspoloživost), kaže kaže Tanner Johnson, viši analitičar u oblasti cyber sigurnosne tehnologije i IoT-a u IHS Markitu. "Povjerljivost spriječava neautorizirane pojedince da pristupaju informacijama. Integritet ih spriječava da izmijene ili modificiraju informacije. Dostupnost osigurava da pojedinci koji imaju ovlaštenje uvijek imaju pristup neophodnim informacijama", kaže Johnson. Osim toga, dodao je da neopozivost i autentičnost blockchaina pomaže pri sprečavanju pojedinaca da negiraju svoje akcije počinjene u digitalnom svijetu, jer blockchain pruža dokaze o njihovoj aktivnosti. Svako može pristupiti i vjerovati podacima koji se održavaju u blockchainu, bilo da se podaci dijele na javnoj ili privatnoj mreži. Blockchain ima veliki potencijal kada je u pitanju primjena u oblasti sigurnosti"[17].

U poslovanju banaka sigurnost blockchaina eliminirala bi dugotrajne autentifikacije identiteta i značajno ubrzala transakcijski tok, osiguravajući visoku razinu integriteta podataka, koji se ne mogu mijenjati zbog složene građe strukture blokova na kojima se blockchain temelji i rezervnu pohranu informacija na različitim superčvorovima mreže bnakarskog sustava.

Implementacija blockchaina u obranama od najčešćih napada

U nastavku će se obrazložiti kako bi implementacija ove tehnologije pomogla u elektroničkom poslovanju banaka pri obrani od najčešćih vrsta napada na podatke i digitalne valute:

1. Višekratna uporaba i dupliciranje elektronskih novčanica- protiv ovakvog načina prevare banka se bori tako da digitalno potpisuje sve novčanice koje izdaje i pribraja im serijski broj koji se prvo unosi u bazu izdanih, a po završetku transakcije u bazu potrošenih novčanica. Ukoliko primi neku novčanicu koja je već unesena u bazu, banka je odbija pod sumnjom na krivotvorinu i pomoću identifikacijskog podatka vezanog za nju, lako otkriva počinitelja.

U slučaju offline potrošnje, gdje novac po pridizanju napušta vlasništvo banke, primjenjuje se programski pristup, koji uključuje gore navedeni postupak provjere novčanica pri ponovnom polaganju novca u banku od strane trgovca, te sklopovski pristup. Ovaj pristup namijenjen je poslovanju sa pametnim karticama, uređaju koji već u sebe ima ugrađenu neizbrisivu i nepromjenjivu bazu podataka koja bi otkrila eventualni pokušaj duplikacije njene vrijednosti.

Značajka koja bi učinila blockachain sustav efikasnim za ovu svrhu, je primjena njegove baze

[17]A&S Adria, (2020.), Blockchain tehnologija: Sigurnost i razmjena podataka, Dostupno na: https://www.asadria.com/blockchain-tehnologija-sigurnost-i-razmjena-podataka/

podataka pod nazivom Distribuirana glavna knjiga (eng. *Distributed Ledger*), čiji će se koncept rada detaljnije prikazati u sljedećem poglavlju. Ona bi predstavljala glavnu bazu banke ali, za razliku od njenog uobičajenog centraliziranog pohranjivanja podataka u lokalnu bazu podataka, ovaj sveobuhvatan popis transakcija pohranjivao bi u različitim superčvorovima sustava što bi urokovalo brži proces provjere autentičnosti transakcije i elektroničkog noca, smanjilo pogreške unosa ljudskog faktora i eliminiralo preopterećenje sustava.

2. Krađa elektroničke novčanice- U današnjim protokolima plaćanja, ovakva vrsta prevare suzbija se tako da trgovac provjerava pošiljateljeve podatke pomoću već opisane tehnike slanja slučajnog niza.

Upotreba blockchaina znatno bi skratila sustav provjere identifikacije korisnika, jer je, kako je već spomenuto, sustav povjerenja odnosno asimetrične kriptografije već ukomponiran u ovaj sistem.

Za razliku od simetričnog sustava koji je kriptiran jednim ključem ovaj sustav sačinjavaju dva: javni i privatni. Korisnikov javni ključ bio bi vidljiv banci i ostalim sudionicima transakcije, dok njegov privatni ključ štitio vrijednost koja se prenosi i ostale osjetljive osobne podatke. Prilaganjem svog privatnog ključa banci, korisnik bi dokazao svoj identitet i banka bi ovjerila transakciju.

3. Krivotvorenje novčanica- Ovakvu vrstu prevara banka spriječava ovjerevanjem svake novčanice putem digitalnog potpisa koji je kriptiran privatnim ključem banke dostupnim isključivo njoj. Primjena blockchaina dodatno bi obesrabrila hakere, prvenstveno radi krptografske zaštite podataka i male mogućnosti da se krivotvorenje provede uspješno, te zbog prisutnosti algoritma za provjeru potpisa, pomoću kojeg banka lako može provjeriti autentičnost novca i ostalih podataka vezanih iz transakciju.

4. Sigurnost korpotativnih podataka banke- „Zahvaljujući rastućim mogućnostima cloud računarstva i korporativnih podataka, većina kompanija premjestila je svoju infrastrukturu na internet. To smanjuje potrebu za upravljanjem lokalnim serverima i podatkovnim centrima, ali s druge strane čini infrastrukturu podložnom cyber napadima. Rastuća popularnost blockchaina u pogledu sigurnosti podataka rezultirala je povećanjem broja pružalaca sigurnosnih rješenja zasnovanih na blockchainu. Svaki od njih je kreirao drugačiji pristup i svaki se sa svojim rješenjima fokusirao na razne industrije. Naprimjer, indijski startup Block Armour razvio je sigurni sistem za zaštitu korporativnih podataka na način da ih hakeri ne

mogu vidjeti i ukrasti. Block Armour kombinira privatnu blockchain mrežu i TLS tehnologiju kako bi omogućio napredni, softverski definiran perimetar (SDP) zasnovan na blockchain tehnologiji. SDP je sigurnosni okvir koji je razvila grupacija za cloud sigurnost, a koji kontrolira pristup podacima na osnovu identiteta. Ovaj pristup podrazumijeva to da svi korisnici koji žele pristupiti određenoj infrastrukturi moraju biti autentificirani i autorizirani. Kada je u pitanju *phishing* – česta hakerska strategija kojom napadači pokušavaju doći do načina na koji mogu lažirati identitet – Block Armourovo rješenje sadrži tri autentifikacijska procesa, uključujući lozinke, digitalni korisnički ID te digitalni ID uređaja, čime se hakerima može blokirati pristup sistemu te se korporativni podaci mogu adekvatno osigurati. "Razvili smo Secure Shield arhitekturu (SSA), koja štiti sistem i omogućava siguran pristup mreži. Sistemi su nevidljivi te su zaštićeni od poznatih i nepoznatih prijetnji. Samo je autentificiranim i autoriziranim korisnicima i uređajima dozvoljeno da vide i pristupe tim zaštićenim sistemima", objašnjava Narayan Neelakantan, suosnivač i direktor Block Armoura."[18]

5. Sigurnosni napad na korisnika- Predmet hakerskih napada često nisu sami sustavi poslovanja već individualni korisnici, kako je prethodno opisano u poglavlju Sigurnost elektorničkog bankarstva. Korisnik bi trebao dobro paziti na sigurnost svog privatnog ključa jer to predstavlja najveću potencijalnu priliku za napad na njegov identitet i vrijednosne podatke.

Najčešći tip napada na klijenta je tzv. *Man in the Middle* napad koji se dijeli na svije vrste: *Man in the browser i Close to you*.

Man in the Middle predstavlja maliciozno presretavanje komunikacije između korisnika i servera od strane nekog drugog korisnika. *Close to you* metoda izvodi se na fizički način, presretavanjem rutera korisnika i mreže koja nije dovoljno zaštićena ili u slučaju spajanja korisnika na nezaštićenu javnu mrežu, dok kod *Man in the browser* metode zlonamjerni korisnik nastoji implementirati softwer koji će mu prikupiti podatke bez znanja korisnika. Najčešće korištena metoda je *phishing*- slanje lažnih elektronskih poruka koje mogu prevariti korisnika u ulaženje u njih, pri čemu on daje dopuštenje tom softweru za pristup svim informacijama u njegovom računalu.

Osim zaštitnih koraka koje može primjeniti isključivo sami korisnik, ono što banka može

[18]A&S Adria, (2020.), Blockchain tehnologija: Sigurnost i razmjena podataka, Dostupno na: https://www.asadria.com/blockchain-tehnologija-sigurnost-i-razmjena-podataka/

učiniti je osigurati i učvrstiti identitet vlastite aplikacije kako bi korisnik lakše primjetio da se radi o pokušaju prevare.

5.6 Blockchain distribuirana glavna knjiga

Kao što je prethodno spominjano, jedna od glavnih prednosti primjene blockchaina u poslovanju mnogih djelatnosti, pa tako i banaka je njegova tehnologija dentralizirane Distribuirane glavne knjige koja čini temelj njegove funkcije.

Distribuirana glavna knjiga (eng. *Distributed Ledger*) predstavlja bazu podataka čiji su podatci podijeljeni, replicirani i sinkronizirani i zatim dodatno algoritmirani putem konsenzusa unutar mreže,u slučaju banaka superčvorova,koji se usuglašavaju pri snimanju jedinstvene kopije baze podataka koja bi zakonom vjerovatnosti zbog više istih kopija trebala biti ona autentična. Obuhvaća popis svih transakcija odvijenih u mreži poslovanja i samim time predstavlja poboljšani instrument za autentifikaciju vlasništva elektronskog novca od uobičajenih centraliziranih lokalnih baza servera banke.

Tehnologija distribuirane glavne knjige primjenjuje se i izvan blockchain sustava, no posebnost ove leži u njezinoj matematički složenoj, kriptografskoj građi koja se sastoji lanca određenog kronološkog slijeda. Lanac sačinjavaju blokovi u koje se na točno određen način pohranjuju skupine transakcija, što uvelike otežava mogućnost samog pronalaska i dekriptiranja podataka, a pogotovo njihove izmjene, jer dogodi li se ikakva promjena u lancu, on više nema smisla, sistem se automatski alarmira i izbacuje maliciozni blok. Svi čvorovi osim superčvorova imaju dodijeljenu isključivo mogućnost dodavanja podataka, bez opcije naknadne izmjene i brisanja.

Ova tehnologija potencijalno predstavlja značajni korak prema zaustavljanju bilo kakvih transakcijskih prevara, te prema automatizaciji, što će uzrokovati značajno ubrzanje obavljanja evidencije, koja je u klasičnim bankarskim sustavima još uvijek dosta podložna faktorima ljudskih grešaka.

5.7 Izazovi implementacije blockchaina u bankarskom poslovanju

Iako implementacija blockchaina u bankarske sustave može uvelike pomoći podizanju njeihove transparentnosti i efikasnosti, ipak se radi o relativno novoj tehnologiji koja trenutno nije standardizirana i dovoljno pravno zakonski definirana za korištenje u ovako važnoj djelatnosti koja predstavlja jednog od najvažnijih regulatora svjetske ekonomije. Unatoč tome da se u ovom slučaju primjene radi o privatnom blockchainu sa hibridno decentraliziranom

mrežom a ne javnom, koji bi imao još više potencijalnih poteškoća u svakodnevnoj primjeni, ova tehnologija mogla bi se suočiti sa sljedećim izazovima:

1. Visoki troškovi implementacije i razvoja- Kao što je već poznato, blockchain decentralizirana mreža sastojala bi se od više superčvorova, odnosno većeg broja kvalitetno opremljenih računala koja će trošiti puno više električne energije kako bi provela proces složene matematičke kriptografije nad svim podatcima, što će uzrokovati velike troškove banci, pogotovo one inicijalne. Još jedan trošak koji bi banke mogle iskusiti je pri istraživanju koliko i kako bi ta tehnologija poboljšala njihovo poslovanje i da li je u konačnici isplativa, te pri razvoju i prilagođavanju blockchain tehnologije njihovom sustavu.

2. Nestandardiziranost i nefleksibilnost- Javni blockchain je dencentraliziran i u vidu donošenja odluka o poboljšanju i ažuriranju softwera što je dovelo do kreiranja različitih inačica blockchaina koji se međsobno razlikuju i ne podržavaju što bi rezultiralo manjkom adaptivnosti i interoperativnosti ukoliko bi se primjenio u globalne poslovne sustave banaka. Također, nepromijenjivost blockchaina može predstavljati potencijalni problem zbog toga što se podatci mogu samo dodavati, bez mogućnosti brisanja i izmjene što znači da ostaju trajno zapisani u bazi podataka. Iako se u ovom slučaju radi o sigurnim bazama banaka, napad na starije podatke prigodniji je za hakere jer će sustav sporije uočiti prevaru, opasnost koja pogotovo prijeti tehologiji pametnih ugovora. Ukoliko zlonamjerni korisnik uoči neku grešku u programskom kodu ugovora, on je može upotrijebiti u svrhu krađe vrijednosti definirane ugovorom, a nepromijenjivost blockchaina znatno će otežati raskid kompromiziranog ugovora.

3.Pravno reguliranje- Ova tehnologija danas je različito regulirana zavisno o zakonima države koji se odnose na zaštitu podataka i novčane tokove u kojoj se primjenjuje, što predstavlja problem pri njenom uvođenju u globalno poslovanje banaka. Standardizacija ove tehnologije također bi podrazumijevala osmišljavanje potpuno nove pravne regulative, umjesto nadopune starih koji nisu stvoreni za pružanje njenog punog potencijala. Hibridni blockchain, koji je ovdje predmet slučaja, imao bi manje problema sa zakonima o zaštiti podataka, no još uvijek bi se mogao nositi sa raznim poteškoćama poput oprečnosti GDPR zakonu koji vrijedi za, ne baš zanemarivo, tržište Europske Unije. „GDPR određuje da svaka fizička osoba čiji se podaci obrađuju ima pravo na ispravak osobnih podataka koji se na njega odnose te “pravo na zaborav” (eng. *a right to be forgotten*) ispuni li se neka od GDPR-om propisanih pretpostavki. Međutim, blockchain je podoban samo za dodavanje podataka, a to ne utječe na postojanje onih prethodno zapisanih. Blockchain je koncipiran tako da svaki dio

sustava sadržava informacije o cijelom sustavu. Drugim riječima, podaci, jednom učitani na blockchain, ne samo da zauvijek ostaju, već ostaju dostupni svima koji se koriste tim blockchainom.“[19]

4) Problem ograničene vizije- Problemi s kojima će se blockchain suočiti ne moraju biti samo tehničke prirode, već i bihevioralne, uzrokovane manjkom edukacije i perspektivnosti. Pojedine institucije zbog svoje ograničene vizije potencijalno neće htjeti preći preko inicijalnog troška uvođenja ove tehnologije jer ne gledaju dovoljno dugoročno njegovu potencijalnu vrijednost ili misle da će tehnologija služiti za ispravljanje samo dijela poslovnih usluga što je ne čini dovoljno korisnom za ozbiljnije razmatranje ukomponiranja u poslovanje.

5) Centralizirana priroda ove hibridne mreže-, uz svu sigurnost blockchain tehnološke strukture, učinila bi je ranjivom na ljudske pogreške i potencijalno podobnijom za različite vrste napada.

6. ZAKLJUČAK

„Blockchain je jedna od velikih tehnologija digitalnog doba, usporediva s internetom ili cloud computingom. Ona ima potencijal da eliminira pouzdane posrednike i tako zamijeni skupe institucije i često kompleksne tokove, i to sve koristeći automatske algoritme.“[20]

Ova relativno nova decentralizirana tehnologija javila se kao odgovor na Svjetsku krizu potaknutu bankama i njihove zastarjele i spore poslovne procese neprimjerene za konstano rastuće globalno tržište prisutno danas. Njezina složena struktura, sustav asimetričke kriptografije i nemogućnost izmjene podataka što dodatno podiže sigurnost i transparentnost transakcije, uz eliminiranje troškova posrednika, privukla je mnogo pažnje i to ne samo u financijskom sektoru. Ova tehnologija pokazala se jednako perspektivna u raznolikim situacijama poput elektronskom planiranju poslovanja ili sigurnoj razmjeni bilo kakvih osjetljivih podataka ili medija, a mogla bi potaknuti i značajan napredak u medicini, računovodstvenim sustavima ili čak i u osmišljavanju elektronskog sustava glasovanja pri izborima.

[19] Legaltech, Batarelo, M., B., Bodlaj, D., Bohaček, K., M., (2019.), (8 str.), Okršaj titana: Pravo vs. Blockchain, 4.-5 str., Dostupno na: https://parser.hr/wp-content/uploads/2019/10/Mreza_blockchain.pdf

[20]Lider, Oršulić, N., (2019.), Igor Pejić: Blockchain može bankama i uštedjeti 20 milijardi dolara i opako srezati zaradu, Dostupno na: https://lider.media/aktualno/igor-pejic-blockchain-moze-bankama-i-ustedjeti-20-milijardi-dolara-i-opako-srezati-zaradu-26948

Banke, kao i druge današnje financijske institucije inertne su i sklone tradicionalnim i uhodanim metodama i klasičnoj, centraliziranoj mreži. Unatoč tome što su neki dijelovi njihovog poslovanja zastarjeli, ipak nastoje modernizirati i povećati efikasnost barem svog sučelnog sustava, namijenjen korištenju klijenata, kako bi zadobili njegovo povjerenje i zadovoljstvo, te si osigurale konkurentnu prednost.Iako je blockchain osmišljen kao sustav kojemu je cilj eliminiranje banaka u transakcijskom procesu, one ga nebi trebale promatrati kao prijetnju, već kao odskočnu dasku za podizanje efikasnosti, sigurnosti i, u konačnici, smanjenje operativnih i transakcijskih troškova, te rast profita.

Primjenjujući određene komponente ove tehnologije za poboljšanje pojedinih poslovnih procesa poput automatizacije identifikacijskih provjera i transakcijskih obrada, decentraliziranja baze podataka i složenijeg kriptiranja podataka, banke će biti u mogućnosti povećati transparentnost i efikasnost poslovanja, biti manje podložne hakerskim napadima i greškama nastalim pri unosu od ljudske ruke, te smanjiti transakcijske provizije na klijentovo zadovoljstvo. Njihov polucentralizirani privatni sustav blockchaina sadržavao bi implementacije svih prednosti blockchaina, istovremeno pružajući klijentima povjerenje da autorizacijskim čvorovima upravlja povjerljiva institucija i baza podataka, na kojoj će njihovi privatni ključevi i ostali podatci uistinu biti sigurni.

Još od 2015. Financijske institucije polako spoznaju potencijal blockachaina i počinju ulagati u različite projekte, uključujući razvijanje standardizirane digitalne valute i primjenu pametnih ugovora te prodaje drugih financijskih derivata u blockchain sustavu. Sigurno je da ova tehnologija zahtjeva još mnogo ulaganja u istraživanje kako bi se mogla implementirati u svakodnevne poslovne sustave banaka, ali, gledano iz dugoročne perspektive, investitori koji počnu ulagati u nju sad mogli bi ostvariti višestruki povrat na svoja sredstva. Ova tehnologija sigurno će mnogim institucijama postati privlačnija kada se pronađe štedljiviji način u obradi transakcija u obliku potrošene električne energije, te kada se ona standardizira u jedan cjeloviti sustav sa potpuno određenom pravno regulativom. S obzirom na nagli uzlet popularnosti i perspektivnosti ove tehnologije, ne bi trebalo proći dugo vremena prije nego što se, barem djelomično, otklone njezini potencijalni problemi i ona postane standardni dio poslovanja, kako i banaka, tako i čitavog financijskog sektora.

7. POPIS LITERATURE

Internet izvori:

1. Tockanai.hr (2020.): Što je to blockchain?, dostupno na: https://tockanai.hr/tehnologija/sto-je-blockchain-32409/

2. Investopedia (2020.): Blockchain explained, dostupno na: https://www.investopedia.com/terms/b/blockchain.asp

3. Službene Internetske stranice Europske Unije (2019.), : Kriptovalute i blockchain – sve što trebate znati, Dostupno na: https://ec.europa.eu/croatia/cryptocurrencies_and_blockchain_all_you_need_to_know_hr

4. Bug.hr, (2018.), Što je u stvari blockchain i kako radi?, Dostupno na: https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011

5. Bitfalls, (2017.), Što je to novčanik (wallet) za kriptovalute i kako do njega?, Dostupno na: https://bitfalls.com/hr/2017/08/31/what-cryptocurrency-wallet/

6. Jutarnji list, (2018.), Nemoguće je korumpirati podatke: Najveća prednost blockchaina je njegova transparentnost, Dostupno na: https://novac.jutarnji.hr/novi-svijet/nemoguce-je-korumpirati-podatke-najveca-prednost-blockchaina-je-njegova-transparentnost/7301704/

7. ResearchGate, Koskosas, I., (2011.), (11 str.), The pros and cons of internet banking:A short review, Dostupno na: file:///D:/Antonija/Downloads/THE_PROS_AND_CONS_OF_INTERNET_BANKING_A_SHORT_REVI.pdf

8. ForgeBit, Radoš, M., (2018.), Što je SSL certifikat i zašto je važan?, Dostupno na: https://forgebit.com/2018/03/08/sto-je-ssl-certifikat-i-zasto-je-vazan/

9. Samoborska banka d.d. (2017.), (11str.), Preporuke za sigurnost korisnika internet bankarstva, 2str., Dostupno na: https://ibank.sabank.hr/doc/Preporuke_sigurnost_korisnika_internet_bankarstva.pdf

10. Movable Type Scripts,SHA- 256 Cryptographic Hash Algorithm, https://www.movable-type.co.uk/scripts/sha256.html

11.Nacionalni CERT, (2010.), Elektronički novac, (11.str.), Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-09-311.pdf

12.Blockgeeks, Rosic, A. (2019.), Smart Contracts: The Blockchain Technology That Will Replace Lawyers, Dostupno na: https://blockgeeks.com/guides/smart-contracts/

13. Poslovni Dnevnik, (2018.), "Banka svih banaka" poručila: Bitcoin nikada neće biti novac, Dostupno na: https://www.poslovni.hr/trzista/bis-bitcoin-nikada-nece-biti-novac-342094

14. Coindesk, (2020.), 14 Banks, 5 Tokens: Inside Fnality's Expansive Vision for Interbank Blockchains, Dostupno na: https://www.coindesk.com/fnality-utility-settlement-coin-central-bank-token-blockchain

15. A&S Adria, (2020.), Blockchain tehnologija: Sigurnost i razmjena podataka, Dostupno na: https://www.asadria.com/blockchain-tehnologija-sigurnost-i-razmjena-podataka/

16. Lider, (2019.), Igor Pejić: Blockchain može bankama i uštedjeti 20 milijardi dolara i opako srezati zaradu, Dostupno na: https://lider.media/aktualno/igor-pejic-blockchain-moze-bankama-i-ustedjeti-20-milijardi-dolara-i-opako-srezati-zaradu-26948

17. Legaltech, (2019.), (8 str.), Okršaj titana: Pravo vs. Blockchain, Dostupno na: https://parser.hr/wp-content/uploads/2019/10/Mreza_blockchain.pdf

18. Torrentkb, (2018.), P2P mreže, Dostupno na: https://torrentkb.weebly.com/p2p-mre382e.html

19. Christidis, K. i Devetsikiotis, M. (2016) Blockchains and Smart Contracts for the Internet of Thing,. Dostupno na: https://mycourses.aalto.fi/pluginfile.php/378344/mod_resource/content/1/Christidis%20and%20Devetsikiotis.pdf

20. Dalton, D. (2017) Blockchain Control Principles, Dostupno na: https://www2.deloitte.com/ie/en/pages/technology/articles/blockchain-control-principles.html

21. McWaters, R.J. (2016) The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services, Dostupno na: http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf

22.Morini, M. (2017) From "Blockchain Hype to a Real Business Case for Financial Markets, 45, str., Dostupno na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2760184

23. Raskin, M. i Yermack, D. (2016.) Digital Currencies, Decentralized Ledgers, and the Future of Central Banking, Dostupno na: https://www.nber.org/papers/w22238

24. Kelly, J. (2016), UBS leads team of banks working on blockchain settlement system,

Dostupno na: https://www.reuters.com/article/us-banks-blockchain-ubs-idUSKCN10Z147

25. Chavan, J., (2013), Internet banking – benefits and challenges ina an emerging economy, Impact Journals, [Online], Dostupno na: http://www.academia.edu/13233924/INTERNET_BANKING-BENEFITS_AND_CHALLENGES_IN_AN_EMERGING_ECONOMY

26. Dragos, P., (2010), Electronic banking advantages for financial services delivery, Dostupno na: http://anale.steconomiceuoradea.ro/volume/2010/n2/106.pdf

27. Logicno, L. R., (2020.), Utjecaj blockchain tehnologije na bankarstvo, Dostupno na: https://www.logicno.com/novac-posao-ekonomija/utjecaj-blockchain-tehnologije-na-bankarstvo.html

Knjige:

1.Popovska Kamnar, N., Korištenje elektroničkog novca i njegov utjecaj na

monetarnu politiku, JCEBI 1(2), 2014

2. Swan, M. (2015) Blockchain: Blueprint for a New Economy. Sebastopol, CA: OReilly.

3. Tapscott, D. i Tapscott A. (2016) Blockchain Revolution: How the Technology behind Bitcoin Is Changing Money, Business, and the World. Toronto, Ontario: Portfolio/Penguin.

4. Rose, P. S., Hudgins, S. C., Upravlajnje bankama i financijske usluge, Mate

d.o.o., Zagreb, 2015.

SAŽETAK

U ovome radu obrađivati će se pojmovno značenje blockchain strukture i njezina struktura, u svrhu boljeg razumijevanja kako bi se takva tehnologija mogla implementirati u sve aspekte života, s naglaskom na financijski sektor i bankarske institucije. Također će se obraditi trenutni način poslovanja i zaštite koje danas primjenjuju klasične banke, te protokoli plaćanja novcem i njegovi novčani sustavi, radfi boljeg razumijevanja potrebe nadograđivanja pojedinih aspekata te djelatnosti.

KLJUČNE RIJEČI: Blockchain, Internet bankarstvo, financijski sustav

SUMMARY

This paper will adress the conceptual meaning of the blockchain structure and its structure in order to better understand how such technology could be implemented in all aspects of life, with an emphasis on the financial sector and banking institutions. It will also discuss the current way of doing business and the protection applied today by traditional banks, as well as payment protocols with money and its monetary systems, in order to better understand the need to upgrade certain aspects of this activity.

KEY WORDS: Blockchain technology, internet banking, financial sector.