PRIMJENE I MOGUĆNOSTI BLOCKCHAIN TEHNOLOGIJE SA NAGLASKOM NA PAMETNE UGOVORE

Ćuže, Matej

SVEUČILIŠTE U SPLITU
EKONOMSKI FAKULTET

ZAVRŠNI RAD

PRIMJENE I MOGUĆNOSTI BLOCKCHAIN TEHNOLOGIJE SA NAGLASKOM NA PAMETNE UGOVORE

Mentor:
izv.prof.dr.sc. Maja Ćukušić

Student:
Matej Ćuže

Split, lipanj, 2019.

SADRŽAJ:

1.UVOD 4

1.1. Definicija problema 5

1.2. Cilj rada 5

1.3. Metode rada 5

1.4. Strukture rada 5

2. BLOCKCHAIN TEHNOLOGIJA – POJAM, KARAKTERISTIKE I ZNAČAJ 6

2.1. Pojam blockchain tehnologije 6

2.1.1. Povijest blockchain tehnologije 7

2.2. Karakteristike blockchain tehnologije 8

2.2.1 Kriptografija 8

2.2.2. Kriptografija u blockchain tehnologiji 9

2.2.3. Dokaz rada („Proof of work“) 10

2.2.4. Metoda „Proof of stake“ 12

2.2.5. Sigurnost u blockchain tehnologiji 12

2.2.6. Privatni i javni ključ 13

2.3. Značaj blockchain tehnologije 15

3. TRENUTNA PRIMJENA BLOCKCHAIN TEHNOLOGIJE 16

3.1. Virtualne valute 16

3.2. Blockchain Hyperledger 19

3.2.1. Privatni i javni blockchain 19

3.3. Utjecaj na okoliš 20

3.4. Blockchain u Republici Hrvatskoj 21

4. POTENCIJALNE PRIMJENE BLOCKCHAIN TEHNOLOGIJE 22

4.1. Financijski sektor 22

4.2. Zdravstveni sektor 24

4.3. Javna uprava 25

4.3.1. Evidencija digitalnih identiteta pravnih i fizičkih osoba 25

4.3.2. Katastar 25

4.3.3. Nadzor lanca opskrbe 25

5. PAMETNI UGOVORI – POJAM, KARAKTERISTIKE, ZNAČAJ I MOGUĆNOSTI PRIMJENE 26

5.1. Pojam pametnog ugovora 26

5.2. Karakteristike pametnih ugovora 27

5.2.1. Ethereum platforma 27

5.3. Značaj pametnih ugovora 29

5.4. Mogućnosti primjene pametnih ugovora 30

5.4.1. Osiguranje 30

5.4.2. Ugovori o radu 30

5.4.3. Iznajmljivanje i kupoprodaja nekretnina 30

6. ZAKLJUČAK 31

LITERATURA 32

GRAFIČKI PRILOZI 35

SAŽETAK 36

SUMMARY 37

1.UVOD

U ovome radu će biti objašnjena blockchain tehnologija, njezine trenutne primjene te potencijalne mogućnosti primjene u budućnosti. Također poseban naglasak će biti stavljen na pametne ugovore, kako na njihovo tehničko uporište u blockchain tehnologiji tako i na njihovu potencijalne primjene u ekonomiji. Iako se blockchain tehnologija obično povezuje sa virtualnim valutama, posebice sa Bitcoinom, ona je zapravo puno više od toga.

Na temelju ubrzanog razvoja informatike i znanosti općenito u posljednjih nekoliko desetljeća došlo je do transformacije gospodarstva iz tradicionalnih načina poslovanja u potpuno ili djelomično digitalni način poslovanja. Vrlo važnu ulogu u toj transformaciji su imale i još uvijek imaju baze podataka koje su omogućile sveobuhvatno poboljšanje poslovnih procesa u globalnoj ekonomiji. Neke djelatnosti kao i pripadajuća radna mjesta su u potpunosti nestala, dok su nove djelatnosti nastale i još uvijek nastaju. Uz pomoć baza podataka i interneta koji je sve te baze učinio povezanim na globalnoj razini došlo je do značajnih promjena ne samo u gospodarstvu nego i u svakodnevnici običnih građana. Plaćanje karticama, podizanje novca na bankomatu, korištenje društvenih mreža, putne navigacije i još mnogo toga omogućuju upravo povezane baze podataka. Sve baze podataka se nalaze fizički spremljene negdje na serveru te su centralizirane, što znači da u slučaju napada na centralnu jedinicu sustava, svi korisnici te baze gube pristup podacima i uslugama te baze. Zbog toga podatkovni centri su strogo čuvani i štićeni od fizičkih napada i kibernetičkih napada. Također postavlja se pitanje povjerenja i pouzdanosti administratora te baze podataka zbog same prirode čovjeka čiji osobni interesi nisu uvijek u skladu sa općim interesom korisnika te baze podataka tzv. „moral hazard“.

Javlja se i kontradikcija između privatnosti korisnika i transparentnosti prilikom upravljanja bazom. U slučaju povećanja transparentnosti dolazi do povećanog otkrivanja osjetljivih podataka iz baze te povećanja sigurnosne ranjivosti baze.

Razlog spominjanja baza podataka u ovome radu je upravo taj što je i sam blockchain zapravo baza podataka koja ima potencijal riješiti sve gore navedene nedostatke tradicionalnih baza.

Upravo zbog toga blockchain nalazi toliko raznih mogućnosti primjene jer zapravo omogućava zamjenu tradicionalnih baza podataka koje se posvuda koriste sa novim i naprednijim tipom baze.

U ovom radu će biti objašnjeno na koji način blockchain tehnologija rješava nedostatke tradicionalnih centraliziranih baza podataka i omogućava unapređenje svih procesa koji se odvijaju u društvu te posebno u globalnom gospodarstvu.

1.1. Definicija problema

Blockchain kao tehnologija postaje sve prisutnija u svakodnevnom životu, posebice u financijskom sektoru u obliku virtualnih valuta.
Ovaj rad raspravlja o trenutnoj primjeni ove tehnologije te o potencijalnim mogućnostima primjene blockchain tehnologije na druge sektore gospodarstva.
Naglasak je stavljen na pametne ugovore kojima je glavna odlika uklanjanje posrednika iz transakcija, samim time i značajno smanjenje troškova.

1.2. Cilj rada

Ciljevi ovog završnog rada su istražiti i objasniti trenutnu primjenu blockchain tehnologije te predložiti mogućnosti primjene tehnologije u drugim sektorima, posebice kroz model pametnih ugovora te budućnost blockchain tehnologije.

1.3. Metode rada

Za izradu ovoga rada koristit će se sljedeće metode: analiza, sinteza, eksplanacija ,klasifikacija i komparacija.

1.4. Strukture rada

Rad se sastoji od ukupno šest poglavlja. Prvo poglavlje je uvod, drugo poglavlje objašnjava blockchain tehnologiju kao takvu te njezina tehnička uporišta kao kriptografiju, hash funkcije, sigurnosne aspektne i opće karakteristike. U trećem poglavlju se izlažu trenutne primjene blockchain tehnologije sa naglaskom na primjene u virtualnim valutama, pametnim ugovorima i financijskim uslugama. Četvrto poglavlje se bavi mogućnostima primjene tehnologije u budućnosti kroz primjene u medicini, javnoj upravi, lancima opskrbe, utvrđivanju porijekla robe i raznim drugim primjenama. Naposljetku u petom poglavlju detaljno se objašnjavaju pametni ugovori, njihove tehničke karakteristike te Ethereum platforma za programiranje ugovora. Također istražuju se potencijale mogućnosti primjene pametnih ugovora u budućnosti te nedostatke koje tek treba riješiti.

2. BLOCKCHAIN TEHNOLOGIJA – POJAM, KARAKTERISTIKE I ZNAČAJ

2.1. Pojam blockchain tehnologije

Po definiciji blockchain je lista blokova u kojima su zapisani podaci, a sami blokovi su povezani pomoću kriptografije na način da se sprječava promjena podataka u blokovima koji su već dodani na lanac. Svaki blok sadržava takozvani kriptografski „hash" prethodnog bloka, vrijeme kada je nastao „timestamp" i podatke o transakciji.

Blockchain se može zamisliti kao otvorenu knjigu u koju se upisuju transakcije između dvije strane, koje se verificiraju prije upisa i ostaju trajno zapisane u blockchainu. Pošto se radi o otvorenoj i distribuiranoj knjizi da bi se spriječilo upisivanje pogrešnih podataka potreban je validacija tj. provjera istinitosti podataka prije dodavanja novog bloka koji sadrži te podatke više od pola sudionika koji su uključeni u validaciju novog bloka.[1]

Blockchain se najbolje može objasniti na primjeru bitcoin transakcije između dvije osobe, neka se zovu Ivica i Marica. Ivica želi poslati 10 bitcoina Marici. Sve što je potrebno za slanje je da Ivica zna adresu novčanika od Marice te da upiše iznos koji želi poslati. Nakon što Ivica obznani transakciju ostatku mreže u proces transakcije se uključuju „rudari" koji provjeravaju ispravnost zadane transakcije. Točnije provjeravaju ima li Ivica zaista 10 bitcoina koje želi poslati. Pošto se rad o lancu blokova potrebno je zapravo provjeriti ulazne i izlazne transakcije i utvrditi ima li Ivica 10 ili više bitcoina kako bi mogao izvršiti transakciju. „Rudari" koji obavljaju ovaj posao su motivirani time što za svaku verifikaciju prime određenu količinu virtualne valute tako da mogu pokriti trošak infrastrukture i energije uložene u sami proces verifikacije. Druga vrsta nagrade za „rudare" je tzv. „miner fee" koji određuju sami korisnici. Svrha ove naknade je dodatna motivacija „rudarima" da brže verificiraju određenu transakciju. Transakciju je moguće zadati i bez dodatne naknade, ali posljedica toga je sporija verifikacija. Nakon što „rudari" verificiraju transakciju blok se nadoda na lanac i time je transakcija završila. U slučaju pokušaja prevare mreže u smislu da Ivica pokuša poslati 10 bitcoina kojih zapravo nema mreža će odbiti transakciju. Da bi se transakcija verificirala potrebna je suglasnost više od pola mreže „rudara" što osigurava povjerenje u sustav sve dok je pola rudara „pošteno".

U slučaju manipulacije sa više od 50% rudara mreža bi postala nepovjerljiva. [2]

[1] https://en.wikipedia.org/wiki/Blockchain (pristupljeno 10.06.2019.)

[2] https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011 (pristupljeno 10.06.2019.)

2.1.1. Povijest blockchain tehnologije

Početak blockchain tehnologije seže u 1991. godinu kada su Stuart Haber i W. Scott Stornetta objavili rad na temu lanca blokova povezanih pomoću kriptografskih metoda. Jedna od prvih implementacija ovih ideja je nastala u obliku bitcoin virtualne valute. U objavljenom „white paper“ dokumentu nepoznati autor ili skupina njih pod imenom Satoshi Nakamoto objavila je dokument u kojem je uvedeno poboljšanje sustava kroz hashcash metodu. Dizajn je 2009. godine implementiran u virtualnu valutu bitcoin baziranu na blockchain tehnologiji. Također je zanimljivo napomenuti da je u izvornom „white paper“ dokumentu na kojem se temelji blockchain i virtualne valute termin pisan razdvojeno „block chain“ , no ipak vremenom se ustalila inačica blockchain. [3]

Bitno je također spomenuti i pojavu Ethereum sustava koji je iniciran od strane Vitalika Buterina koji je jedan od programera koji je radio na bitcoin sustavu. Vitalik Buterin je inicirao Ethereum blockchain zbog limitiranosti bitcoin sustava. Za razliku od bitcoina, ethereum blockchain omogućava programiranje pametnih ugovora, pozajmica i sličnih instrumenata. To omogućava široku paletu potencijalnim primjena u gospodarstvu što prepoznaju i velike kompanije koje uočavaju potencijal pametnih ugovora u svrhu smanjenja troškova i povećanja efikasnost poslovanja.
Ethereum sustav je počeo sa radom u 2015. godini.[4]

[3] https://en.wikipedia.org/wiki/Blockchain (pristupljeno 10.06.2019.)
[4] https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#1d8f7c157bc4 (pristupljeno 10.06.2019.)

2.2. Karakteristike blockchain tehnologije

Glavna karakteristika blockchaina je da je potpuno decentraliziran, što znači da nema vlasnika, nema fizičku adresu niti je kontroliran od stane neke institucije ili organizacije. Blockchain može koristiti svatko, bez ograničenja i bez potrebe za osobnim podacima korisnika sustava.
Kao što je već spomenuto blockchain je zapravo baza podatak koja sadrži podatke, najčešće o financijskim transakcijama kao u slučaju bitcoin blockchaina.

Glavno pitanje koje proizlazi iz gore navedenog je na koji se način ovaj sustav koji nema jasnog regulatora održava sigurnim.
Tri su ključna faktora koja osiguravaju sigurnost blockchaina:

- Kriptografija
- Rudarenje
- Decentraliziran i distribuiran sustav

U nastavku će se služiti primjerom virtualnih valuta u svrhu objašnjenja karakteristika sveukupne tehnologije koja stoji iza blockchaina. [5]

2.2.1 Kriptografija

Definicija kriptografije glasi: „Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati.„
Kriptografija ima dugu povijest, te je već korištena kod starih Grka i Rimljana.
Svrha kriptografije je omogućiti dvjema osobama komunikaciju putem nesigurnog kanala tako da osoba koja ima pristup tom kanalu ne može razumjeti poruke koje osobe izmjenjuju.
Nakon što primalac primi tekst koji je šifriran potrebno je znati unaprijed dogovoreni ključ pomoću kojeg je moguće pročitati pravo značenje teksta. Kriptografski algoritam označava matematičku funkciju koja služi za šifriranje i dešifriranje. U kriptografiji se također primjenjuju javni i privatni ključ. Kod asimetričnih kriptosustava imamo javni ključ koji je svima dostupan za šifriranje ali iz njega se ne može praktično izračunati ključ za dešifriranje. [6]

[5] https://www.netokracija.com/sto-je-blockchain-132284 (pristupljeno 10.06.2019.)
[6] https://web.math.pmf.unizg.hr/~duje/kript/osnovni.html (pristupljeno 10.06.2019.)

2.2.2. Kriptografija u blockchain tehnologiji

Svaki blok je zapravo paket koji sadrži podatke, odnosno sadrži podatke o transakcijama u nekom vremenu. Blokovi se vežu jedan na drugi uz pomoć kriptografskog potpisa koji ima istu vrijednost na starom i na novom bloku. Taj potpis se zove hash. Hash je zapravo niz znakova koji na prvi pogled nemaju smisla. Ti znakovi su dobiveni uz pomoć složene hash matematičke funkcije koja bilo koji digitalni sadržaj putem matematičkih operacija pretvara u digitalni potpis. Tako možemo od bilo koje slike, pdf dokumenta ili nekog brojčanog zapisa dobiti hash. Bitna karakteristika hasha je da je uvijek iste duljine, nebitno o vrsti i količini ulaznih podataka. Bitno je također naglasiti da ako na iste datoteke primjenjujemo hash funkciju da ćemo uvijek dobiti isti hash. No ako se i najmanji dio te datoteke izmjeni, dobiveni hash će izgledati potpuno različito. U prikazu ispod možemo vidjeti primjer hash funkcije te na koji način dodavanje samo zareza uzrokuje potpuno različit rezultat.[7] U ovome primjeru ćemo koristiti hash funkciju SH – 256.

Slika 1: Rezultat hash funkcije

Izvor: http://www.sha1-online.com/

Slika 2: Rezultat hash funkcije nakon dodavanja zareza

Izvor: http://www.sha1-online.com/

[7] https://www.netokracija.com/sto-je-blockchain-132284 (pristupljeno 13.06.2019.)

U blockchain sustavu na ovaj način se potpisuju blokovi sa transakcijama. Generirani potpis na bloku automatski postaje dio sadržaja idućeg bloka. U slučaju pokušaja izmjene podataka u bloku, to automatski uzrokuje neispravnost potpisa. Ako napadač pokuša generirati ispravan potpis preko hash funkcije za izmijenjene podatke, dolazi automatski do greške u idućem bloku jer je on potpisan hash vrijednošću koja je dobivena na osnovu starog potpisa. Samim time idući blok postaje neispravan. Na taj način se u slučaju napada događa lančana reakcija, što znači da napad na blockchain ne može ostati neprimijećen. Ova osobina blockchain tehnologije je jedna od glavnih poluga sigurnosti cijelog sustava.[8]

2.2.3. Dokaz rada („Proof of work“)

Dokaz rada ili proof of work na engleskom jeziku je još jedna postavka koja omogućuje sigurnost blockchain sustava. Naime, izvršavanje hash funkcije ne iziskuje veliku procesorsku snagu računala. Samim time se otvara mogućnost napada na blockchain jer je moguće istovremeno promijeniti sve potpise u lancu i na taj način uspješno manipulirati cijelim sustavom. No idejni tvorci Blockchain su uspjeli riješiti i taj problem na način da blok nije moguće potpisati sa bilo kojim hash vrijednošću. Da bi hash bio valjan, mora počinjati sa određenim brojem nula. [9]

U hash funkcija ulaze sljedeće varijable:

- indeks bloka
- hash prethodnog bloka
- podaci o transakciji
- nonce ili promjenjiva vrijednost

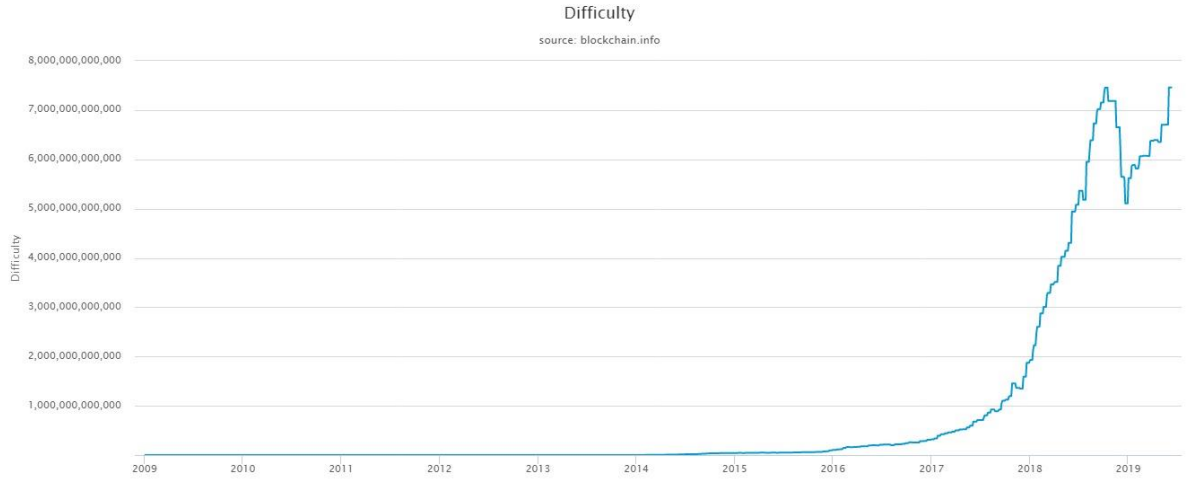
Varijabla nonce je jedina varijabla koju ju dopušteno mijenjati od svih podataka koji ulaze u hash funkciju. Pošto je hash vrijednost vrlo jednostavno izračunati postavlja se pitanje zašto rudari troše toliko sredstava na infrastrukturu i na električnu energiju za verificiranje novih blokova. Razlog tome leži u već spomenutoj postavki blockchaina da hash mora počinjati sa određenim brojem nula. Parametar koji se koristi kao mjera težine izračuna se zove „difficulty“. Kada algoritam odluči da novi blok mora imati na početku četiri nule, rudar mora tražiti hash sve dok ne zadovolji zadani kriterij. Od svih varijabli koje ulaze u hash funkciju jedino se smije

[8] https://www.netokracija.com/sto-je-blockchain-132284 (pristupljeno 14.06.2019.)
[9] https://www.netokracija.com/sto-je-blockchain-132284 (pristupljeno 14.06.2019.)

mijenjati nonce varijabla. Mijenjanje vrijednosti nonce varijable je jedini način da se dođe do tražene hash vrijednosti. Nakon pronalaska ispravne vrijednosti rudar šalje prema mreži ispravan hash. Cilj algoritma unutar mreže je da se novi blok generira svakih 10 minuta. Algoritam mijenja težinu izračuna na bazi prethodnih 2016 generiranih blokova. Sama zahtjevnost izračuna je jako bitna jer čini mogućnost prevare težom. [10]

Također bitno je spomenuti i pojam „Hash rate“ ili „Hash power“ odnosno koliko hash vrijednosti neki rudar generira u jednoj sekundi. Na primjer, računalo koje generira 60 hash vrijednosti u sekundi ima „hash rate“ 60. Za same rudare bitno je nekoliko faktora koji utječu na samu profitabilnost djelatnosti. To su ponajprije cijena električne energije i cijena infrastrukture za rudarenje. [11]

U početku bitcoin blockchaina bilo je moguće rudariti i uz pomoć osobnog računala dok se sada na tržištu mogu naći specijalizirani ASIC uređaji bez kojih rudarenje nema isplativosti. Cijene navedenih uređaja se kreću od 500 američkih dolara pa do nekoliko tisuća dolara. Za uspješnije rudarenje mnogi se udružuju u takozvane bazene rudara ili „mining pool“ na način da udruže procesorsku snagu i tako ostvaruju prednost ispred ostalih individualnih rudara.[12]



Slika 3: Težina rudarenja na bitcoin blockchainu

Izvor: https://www.blockchain.com/en/charts/difficulty?timespan=all

[10] https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011 (pristupljeno 14.06.2019.)
[11] https://www.buybitcoinworldwide.com/mining/hash-rate/ (pristupljeno 14.06.2019.)
[12] https://www.investopedia.com/terms/b/bitcoin-mining.asp (pristupljeno 14.06.2019.)

2.2.4. Metoda „Proof of stake“

Metoda dokaza rada je prvotni princip kojeg je osmislio Satoshi Nakamoto čime je riješen problem vjerodostojnosti. Problem metode dokaza rada je taj što se troši iznimno puno električne energije i procesorske snage pošto se svi rudari natječu tko će prvi naći ispravnu hash vrijednost. Metoda „Proof of stake “ nudi potencijalno rješenje za navedene nedostatke. Ova metoda se temelji na ulaganju postojećih virtualnih kovanica čime se ostvariva pravo na sudjelovanje u verifikaciji transakcija u mreži. Zarada tim korisnicima dolazi od transakcijske naknade koju plaćaju drugi korisnici kada transferiraju virtulanu valutu drugom korisniku. No, ipak postoje mnogi potencijalni nedostatci kod ove metoda, najprije mogućnost da rudar istovremeno verificira više blokova pošto nema troška energije i resursa da se blok potpiše kao u metodi dokaza rada.[13]

2.2.5. Sigurnost u blockchain tehnologiji

Blockchain se među njegovim zagovornicima smatra za jednim o najboljih načina za osiguranje transakcija. Razlog tome je što je svaki blok koji sadrži podatke koji su najčešće transakcije povezan sa svim blokovima ispred i iza sebe. Samim time jako je teško promijeniti jedan zapis jer bi to značilo da treba mijenjati i zapise u povezanim blokovima. Zapisi na blockchainu su osigurani putem kriptografije. Sudionici mreže imaju svoj privatni ključ koji je povezan na njihove transakcije i služi kao osobni digitalni potpis. U slučaju promjene zapisa, potpis će postat nevaljan te će cijela mreža odmah saznati da se nešto dogodilo. U cijelom procesu je bitno da je mreža brzo obaviještena kako bi se spriječila zloupotreba.

Također još jedna temeljna postavka blockchain tehnologije je distribuiranost blockchaina preko cijele mreže. To mu omogućava svojstvo da nema takozvane „single point of failure“ odnosno da se mrežom ne može manipulirati sa jednog mjesta u sustavu.[14]

Jedna od mogućih sigurnosnih ugroza za blockchain je „51% napad“. Pretpostavimo da napadač želi manipulirati mrežom tako da može dva puta potrošiti neku količinu virtualne valute. Kako bi to uspio napadač mora izgraditi lanac koji je dulji od istinitog lanca i počinje se odvajati prije trenutka kad je potrošio virtualnu valutu. Da bi napad bio uspješan svi bi se blokovi morali

[13] https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011 (pristupljeno 14.06.2019.)
[14] https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/ (pristupljeno 14.06.2019.)

ponovno verificirati, a pošto je za to potrebna ogromna procesorska snaga koja bi nadjačala ostatak „poštenih“ korisnika mreže, napada je skoro nemoguće izvesti. [15]

2.2.6. Privatni i javni ključ

Privatni ključ je oblik kriptografskog zapisa koji omogućava korisnica pristup podacima koji su dostupni samo njima. Upotreba privatnog ključa je jedan od temeljnih dijelova cijele blockchain tehnologije. Kod virtualnih valuta svaki korisnik ima javnu adresu i privatni ključ. Javni ključ je kreiran od privatnog ključa uz pomoć kompleksnih matematičkih operacija, no praktično nije moguće od javnog ključa operacijama dobiti privatni ključ.
Privatni ključ im nekoliko različitih formi, obično kao niz brojeva i slova. Sustav privatnog i javnog ključa se najbolje može objasniti uz pomoć primjera poštanskog sandučića. Javni ključ je kao adresa koju svatko zna i svatko može ubaciti u sandučić što god želi ali samo osoba koja ima ključ od sandučića može upravljati sadržajem istog. Zbog toga je bitno čuvati privatni ključ na sigurnom. Digitalni novčanik sprema privatni ključ od korisnika. Kada dođe do transakcije, digitalni novčanik kreira digitalni potpis iz privatnog ključa. Potpis služi kako bi se potvrdilo da transakcija dolazi od nekog korisnika i osigurava da je nije moguće kasnije promijeniti. Ako korisnik izgubi privatni ključ više nije moguće pristupiti niti upravljati svojim računom. Privatni ključ se može spremiti na eksternoj memoriji, u obliku QR koda ili ga samo isprintati na papir. Ključ se može spremiti i putem servisa koji su povezani na internet kao na primjer na mobilne novčanike. [16]

```
E9873D79C6D87DC0FB6A5778633389F4453213303DA61F20BD67FC233AA33262
```

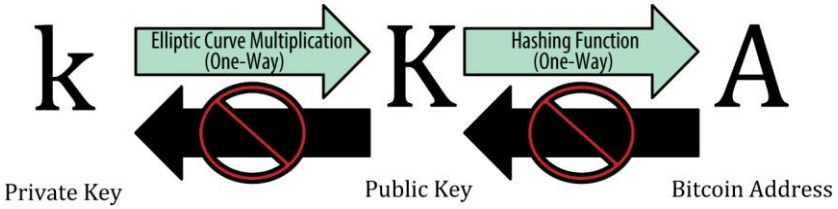
Slika 4: Primjer privatnog ključa u bitcoin blockchainu

Izvor: https://en.bitcoin.it/wiki/Private_key

Iz privatnog ključa se generira javni ključ, a iz javnog ključa se skraćivanjem dolazi od javne adrese. Razlog skraćivanju je iznimno dug niz simbola koji sadrži javni ključ.
Da bi se moglo ući u interakciju sa drugim korisnikom potrebno je obznaniti javnu adresu. Javna adresa se može shvatiti kao broj bankovnog računa. Pošiljatelj mora znati broj računa

[15] Kraft, D. (2015); Difficulty Control for Blockchain-Based Consensus Systems, University of Graz, Graz, str. 3
[16] https://www.investopedia.com/terms/p/private-key.asp (pristupljeno 15.06.2019.)

kako bi mogao poslati novac dok primatelj ima privatni ključ koji mu omogućuje pristup tim sredstvima.[17]



Slika 5: Javni ključ, privatni ključ i javna adresa

Izvor: https://www.oreilly.com/library/view/mastering-bitcoin-2nd/9781491954379/ch04.html

```
3048 0241 00C9 18FA CF8D EB2D EFD5 FD37 89B9 E069 EA97 FC20 5E35 F577 EE31 C4FB C6E4 4811 7D86 BC8F
BAFA 362F 922B F01B 2F40 C744 2654 C0DD 2881 D673 CA2B 4003 C266 E2CD CB02 0301 0001
```

Slika 6: Javni ključ

Izvor: https://www.comodo.com/resources/small-business/digital-certificates2.php

```
1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2
```

Slika 7: Javna adresa

Izvor: https://en.bitcoin.it/wiki/Address

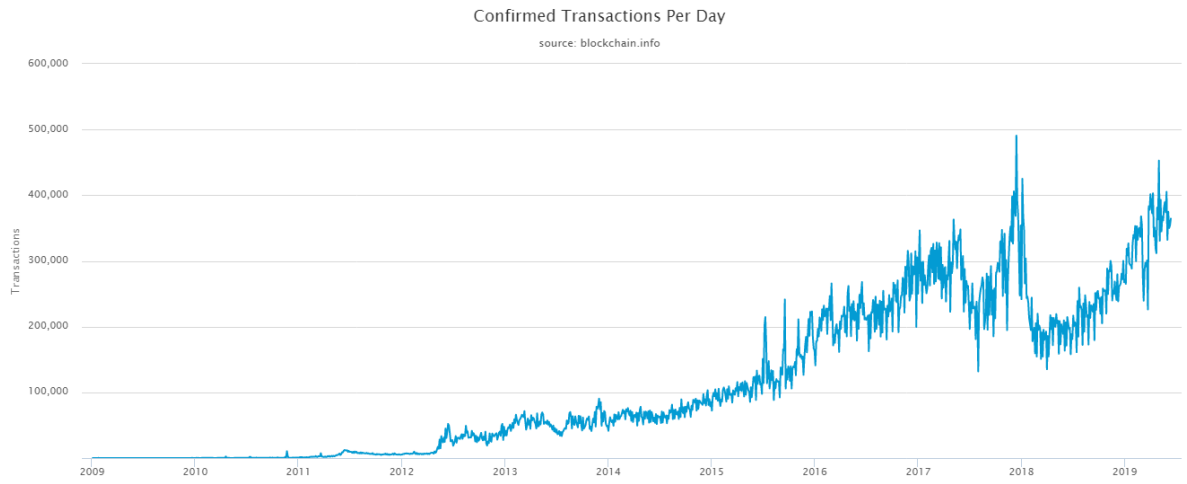
[17] https://www.investopedia.com/terms/p/public-key.asp (pristupljeno 14.06.2019.)

2.3. Značaj blockchain tehnologije

Značaj same tehnologije se ogleda u njezinoj univerzalnosti primjene. Internet je donio revoluciju u sve slojeve života. Ta revolucija se i dalje oslanja velikim dijelom na baze podataka. Samim time što je blockchain distribuirana baza podataka koja nosi mnoge prednosti u odnosu na klasičnu organizaciju i upravljanje podacima, ima veliki potencijal i bezbrojne mogućnosti primjene. Blockchain je već postao novac za internet i može postati „Internet of Money“ za financijske usluge spajajući korisnike na isti način na koji su spojeni uređaji u „Internet of things“ mreži. [18] Unatoč tome utjecaj virtualnih valuta na globalnoj razini je zanemariv. Na dan 14. prosinca 2017. u svijetu je bitcoinom provedeno oko 490 tisuća transakcija dok je ukupan broj prosječnih dnevnih bezgotovinskih platnih transakcija u 2016. godini samo u europodručju iznosio 484 milijuna, a u cijeloj 2016. godini provedene su 122 milijarde platnih transakcija

U Republici Hrvatskoj prosječno se dnevno izvrši više od 2,9 milijuna bezgotovinskih transakcija.

Iz navedenog je jasno da su transakcije bitcoinom kao glavnim predstavnikom virtualnih valuta zanemarive na ukupan broj transakcija. Prema HNB-u upotreba virtualnih valuta u sadašnjem opsegu ne donosi rizik za provođenje ključnih ciljeva središnje banke poput stabilnosti cijena, financijske stabilnosti bankovnog sustava i stabilnosti platnog prometa[19].



Slika 8: Broj transakcija na bitcoin blockchainu

Izvor: https://www.blockchain.com/en/charts/n-transactions?timespan=all

[18] Swan, M. (2015): Blockchain: Blueprint for a New Economy, O'Reilly Media, Sebastopol, str. 5.
[19] https://www.hnb.hr/-/sto-su-virtualne-valute- (pristupljeno 16.06.2019.)

3. TRENUTNA PRIMJENA BLOCKCHAIN TEHNOLOGIJE

3.1. Virtualne valute

Virtualne valute ili kripto valute su digitalni ekvivalent novca. Glavna karakteristika virtualnih valuta je nepostojanje središnje institucije koja ih izdaje ili koja njima na neki način upravlja. Stabilnost samih virtualnih valuta se održava pomoću kompleksnih unutarnjih mehanizama sadržanim u samom protokolu. Za zamjenu iz virtualnih valuta u stvarni novac koriste se burze na kojima se tečaj formira ovisno o ponudi i potražnji za određenom virtualnom valutom.
Virtualne valute trenutno predstavljaju sporno područje po pitanju zakonske regulacije. Glavni uzrok toga je visoka razina privatnosti korisnika mreže, zbog čega je se povezuje sa ilegalnim aktivnostima. [20]
U trenutku pisanja ovoga rada prema stranici www.coinmarketcap.com na tržištu se nalaze ukupno 2245 virtualne valute sa ukupnom tržišnom kapitalizacijom koja iznosi oko 288 milijardi . [21]

Cryptocurrencies ▾ Exchanges ▾ Watchlist USD ▾ ← Back to Top 100

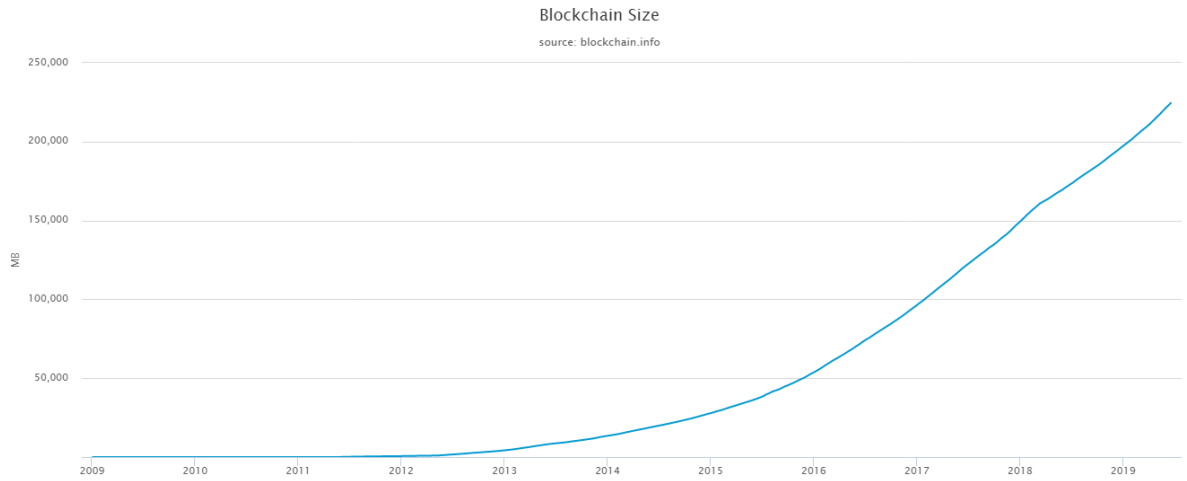
#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	$166,238,839,760	$9,354.90	17,770,237	$16,659,680,493	0.14%	2.39%	13.98%
2	Ethereum	ETH	$28,603,371,071	$268.40	106,570,658	$5,810,807,612	0.02%	0.30%	3.43%
3	XRP	XRP	$18,207,414,868	$0.428390	42,501,950,124 *	$1,233,927,691	0.44%	-0.99%	6.57%
4	Litecoin	LTC	$8,364,000,907	$134.23	62,312,550	$3,910,024,188	-0.27%	-3.24%	0.77%
5	Bitcoin Cash	BCH	$7,315,636,816	$409.88	17,848,438	$1,237,634,094	-0.13%	-0.67%	-0.95%
6	EOS	EOS	$6,207,866,350	$6.75	919,927,033 *	$1,811,104,182	0.06%	-1.15%	3.69%
7	Binance Coin	BNB	$5,171,038,524	$36.63	141,175,490 *	$665,132,291	0.81%	3.72%	4.59%
8	Bitcoin SV	BSV	$3,830,887,828	$214.66	17,846,248	$352,068,867	-0.02%	-3.47%	2.24%
9	Tether	USDT	$3,544,895,029	$1.00	3,537,715,309 *	$15,825,858,060	0.00%	0.06%	-0.06%
10	Stellar	XLM	$2,366,347,382	$0.121920	19,408,944,603 *	$254,166,095	0.29%	-1.71%	-3.17%

Slika 9: Najpoznatije virtualne valute

Izvor : https://coinmarketcap.com/all/views/all/

[20] D. Buterin, E. Ribarić, S. Savić (2015): Bitcoin – nova globalna valuta, investicijska prilika ili nešto treće, Zbornik Veleučilišta u Rijeci, Vol. 3, No. 1, pp. 148-149
[21] https://coinmarketcap.com/all/views/all/ (pristupljeno 20.06.2019.)

Virtualne valute se pohranjuju u digitalnim novčanicima koji su zapravo aplikacije koje sadrže privatni i javni ključ vlasnika. Korisnici mogu generirati neograničen broj javnih adresa. Vjerojatnost da se generiraju dvije iste adrese je zanemarivo mala. Nakon obavljanja transakcije mijenja se vlasništvo nad virtualnom valutom. U slučaju da korisnik izgubi privatni i javni ključ, pristup jedinicama je nepovratno izgubljen. Zbog toga je potrebno uspostaviti sigurnosne kopije javnih i privatnih ključeva. Blockchain virtualne valute može zauzeti veliku količinu memorije pošto su u njemu sadržane sve transakcije od početka postojanja virtualne valute. Rješenje se može naći u obliku web novčanika koji ipak imaju niži stupanj sigurnosti.



Slika 10: Veličina bitcoin blockchaina

Izvor: https://www.blockchain.com/en/charts/blocks-size?timespan=all

Dva načina koja se najviše koriste za kupnju virtualnih valuta su kupnja za gotovinu i kupnja na burzi. Lokalna kupnja se odvija neposredno sa prodavačem na dogovorenom mjestu. Prodavači i kupci se mogu nalaziti preko internetskih stranica. Drugi način je kupovina preko burza virtualnih valuta gdje se valute ponašaju slično kao i dionice.[22]

Jedan od problema koji se javlja prilikom korištenja virtualnih valuta je i računalna ranjivost tzv. kripto mjenjačnica. Jedna od najvećih mjenjačnica Mt. Gox je bankrotirala upravo zbog hakerskih napada na njihove sustave. Događanje takvih incidenata utječe na virtualne valute. Upravo zbog nereguliranosti i decentraliziranosti dolazi do velike volatilnosti jer se cijena određuje isključivo na temelju ponude i potražnje za valutom za razliku od tradicionalnih valuta. Također javlja se i sigurnosni rizik zbog kompleksnosti blockchaina koji stoji iza

[22] D. Buterin, E. Ribarić, S. Savić (2015): Bitcoin– nova globalna valuta, investicijska prilika ili nešto treće, Zbornik Veleučilišta u Rijeci, Vol. 3 , No. 1, pp. 150-151

virtualnih valuta. Osobe koje nemaju informatičko obrazovanje mogu počiniti pogreške i na taj način ostati zbog svojih sredstava. Neke od pogreške su gubitak podataka o ključevima, nenamjerno odavanje informacija o ključevima, krađa ključeva itd.[23]

Usprkos tome cijena virtualnih valuta dostiže visoke vrijednosti. Najveća zabilježena cijena bitcoina iznosila je čak 19.524 američka dolara na dan 17.12.2017. godine.[24]

Slika 11: Kretanje cijene bitcoina

Izvor : https://www.blockchain.com/charts/market-price?timespan=all

[23] D. Buterin, E. Ribarić, S. Savić (2015): Bitcoin – nova globalna valuta, investicijska prilika ili... Zbornik Veleučilišta u Rijeci, Vol. 3 , No. 1, pp. 154-155

[24] https://www.blockchain.com/prices (pristupljeno 20.06.2019.)

3.2. Blockchain Hyperledger

Hyperledger ili u slobodnom prijevodu glavna knjiga je program otvorenog koda (engl. open source) kreiran za napredna blockchain tehnološka rješenja u gospodarstvu. Projekt se provodi u okviru Linux zaklade. Cijeli projekt je lansiran 2016. godine sa tehničkom i organizacijskom strukturom od 30 osnivačkih kompanija. Početno su u projekt ušla dva programska okvira (eng. frameworks), „Hyperledger Fabric“ od IBM-a te Hyperledger Sawtooth od Intel-a.
Glavna ideja Hyperledger projekta je razvoj blockchain programskih okvira i platformi koji su univerzalno primjenjivi.
Glavni ciljevi Hyperledger projekta su:

- kreiranje programa otvorenog koda u svrhu potpore izvršavanju poslovnih transakcija
- pružanje neutralne, otvorene i zajednicom upravljane infrastrukture
- izgradnja zajednice za razvoj blockchain tehnologije
- edukacija javnosti o blockchain tehnologiji
- promoviranje upotrebe raznih programskih okvira i platformi[25]

3.2.1. Privatni i javni blockchain

Temeljna razlika između privatnih i javnih blockchain je u tome da privatnom blockchainu mogu pristupiti samo određeni korisnici, dok javnom mogu pristupiti svi. Javni blockchain obično ima neke mehanizme za privlačenje novih korisnika, poput bitcoin blockchaina. Jedan od nedostataka javnog blockchaina je potreba za procesorskom snagom da bi se ostvario konsenzus u mreži. Još jedan nedostatak je i sama otvorenost mreže, što smanjiva razinu privatnosti.
Kod privatnog blockchaina korisnik mora biti pozvan da bi pristupio mreži. Tvrtke koje uspostave privatni blockchain određuju tko može pristupiti i čemu taj korisnik može pristupiti. Nakon što dobije odobrenje za pristup blockchainu korisnik sudjeluje u održavanju blockchain mreže. Primjer privatnog blockchaina je Hyperledger Fabric.[26]

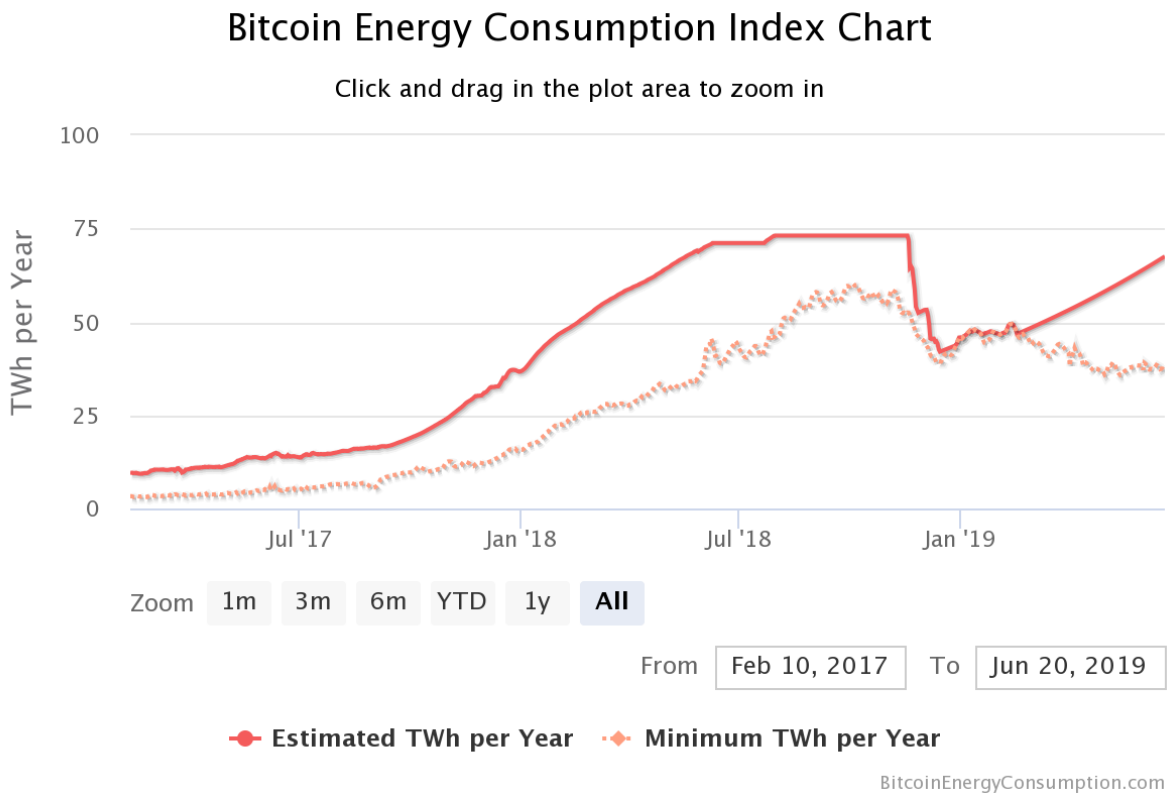
[25] https://www.hyperledger.org/about (pristupljeno 21.06.2019.)
[26] https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/ (pristupljeno 21.06.2019.)

3.3. Utjecaj na okoliš

U istraživanju o utjecaju bitcoin rudarenja objavljenom u časopisu Joule (2019) Stoll, Klaaßen i Gallersdörfer izračunato je da godišnja potrošnja električne energije potrebne za rudarenje iznosi 45.8 teravatsati, dok emisija CO_2 iznosi 22.00 do 22.9 mega tona.

U svrhu istraživanja je korišten tehničko-ekonomski model za određivanje potrošnje električne energije u svrhu procijene emisije CO_2. Da bi odredili geografski utjecaj na okoliš istraživači su razvili tri scenarija bazirana na IP adresi bazena rudara, IP adresi uređaja i IP adresi čvorišta. Na kraju su izračunali emisije CO_2 na osnovu podataka o načinu proizvodnje električne energije na području gdje se rudari bitcoin. Iznosi emisija odgovaraju ukupnoj emisiji $C0_2$ Jordana i Šri Lanke. Prema navedenim podacima o emisijama bitcoin je ekvivalent državama koje se nalaze na 82 i 83 mjestu po razini emisije CO_2.

[27]



Slika 12: Potrošnja energije za rudarenje bitcoina

Izvor: https://digiconomist.net/bitcoin-energy-consumption

[27]Stoll et al., The Carbon Footprint of Bitcoin, Joule (2019), https://doi.org/10.1016/j.joule.2019.05.012 (pristupljeno 21.06.2019.)

3.4. Blockchain u Republici Hrvatskoj

Prema podacima stranice coinatmradar.com u Hrvatskoj je trenutačno dostupno ukupno šest bitcoin bankomata. [28] Uz bitcoin bankomate na području Hrvatske posluje i nekoliko mjenjačnica virtualnih valuta. Osim virtualnih valuta, u Hrvatskoj se javljaju i prve naznake ostalih implementiranja blockchain tehnologije.

U okvirnoj strategiji pametnog Grada Zagreba (2018), Grad Zagreb planira izraditi posebnu strategiju za upotrebu blockchain tehnologije tj. mogućnost izrade distribuiranih aplikacija i novih sustava baziranih na blockchain tehnologiji. U strategiji se navode moguće primjene u ugovaranju, zaštiti intelektualnog vlasništva, internetu stvari i slično. Buduća strategija primjene blockchain tehnologije treba proučiti mogućnosti implementacije u hrvatski pravni sustav te predložiti nove e-usluge u Zagrebu.[29]

Osim navedenih primjera, u Hrvatskoj se održavaju i konferencije vezane za blockchain poput BlockSplit konferencije.

[28] https://coinatmradar.com/country/54/bitcoin-atm-croatia/ (pristupljeno 21.06.2019.)
[29] Grad Zagreb (2018): Okvirna strategija pametnog Grada Zagreba, str.39

4. POTENCIJALNE PRIMJENE BLOCKCHAIN TEHNOLOGIJE

4.1. Financijski sektor

Blockchain tehnologija ima potencijal za povećanje efikasnosti u financijskom sektoru. Uz sve prednosti koje donosi ova tehnologija dolaze i izazovi koje tek treba riješiti kako bi zaživjela primjena u realnosti.

Jedan od mogućih primjena tehnologije je svakako u području transformacije fizičke imovine u digitalnu formu radi vođenja evidencije o transakcijama. Današnji procesi zahtijevaju mnogo vremena da bi se transakcija izvršila, a u slučaju primjene blockchaina digitalizirana imovina bi se zapravo ponašala kao digitalni financijski instrumenti koji mijenjaju vlasnika čim se doda novi zapis na blockchain.

Prednost blockchaina se ogleda i kod revizijskih postupaka jer se u samom blockchainu nalaze zapisi o svim transakcijama i o sudionicima tih transakcija. Blockchain baza podataka sadrži zapise koji su nepromjenjivi i lako dostupni svim zainteresiranim stranama. [30]

Pametni ugovori također spadaju u kategoriju mogućnosti primjene blockchaina, no o njima detaljnije u nastavku rada.

U upotrebi blockchaina u financijskom sektoru javljaju se dvije osnovne prednosti:

- smanjenje vremena potrebnog za implementaciju dogovora nakon trgovine
- brža plaćanja

Period implementacije (engl. settlement period) se definira kao vrijeme potrebno da se izvrši i administrativno provede transakcijski nalog. To vrijeme se može uvelike smanjiti upotrebom blockchain tehnologije. Trenutno se većinom financijske imovine može samo upravljati za vrijeme radnog vremena financijskih institucija. U slučaju dva blockchaina, jednog koji bi sadržavao zapise o vlasništvu nad vrijednosnicama i drugom sa zapisom o raspoloživom novcu, bilo bi moguće provoditi trgovanje na financijskim tržištima bilo kada i bilo gdje u sam nekoliko sekundi.

Druga bitna prednost kod blockchaina je brzina plaćanja. Naime, međunarodni platni sustavu zahtijevaju višestruke regulatorne provjere što znatno produljuje sami proces prijenosa novca.

[30] Lewis, R., McPartland, J., Ranjan. R,. (2019): SPECIAL FEATURE: Cutting-Edge Innovation in the Cryptosphere, J.P. Morgan Center for Commodities at the University of Colorado Denver Business School, Denver, str. 12-15

Uz pomoć blockchain tehnologije vrijem potrebno da se izvrši međunarodna transakcija bi bilo uvelike reducirano.

Uz sve prednosti blockchain nosi i izazove kod same primjene, a najznačajniji od njih su:

- standardizacija
- interoperabilnost
- skalabilnost
- nemogućnost promijene zapisa
- pravna nesigurnost

Problem kod blockchaina je i manjak standardizacije kod raznih vrsta dizajna same mreže. Nedostatak standardizacije može prouzrokovati poteškoće prilikom implementacije tehnologije u same tvrtke. Mnoge nacionalne i međunarodne organizacije pokušavaju uspostaviti opće prihvaćene tehničke standarde. Vezano uz standardizaciju javlja se i pitanje interoperabilnosti između blockchain platformi kako sa već postojećim internim sustavima tako i eksterno između tvrtki. Idući jako značajan izazov blockchaina je skalabilnost, posebno kod mreža gdje je potrebno riješiti neki problem da bi se potvrdila transakcija. Samo rješavanje problema iziskuje procesorsku snagu i ograničava brzinu potvrde transakcije. Također blockchain kao tehnologija zahtjeva velike količine prostora za pohranu podataka jer svaki član mreže posjeduje i održava potpunu kopiju cijelog blockchaina.

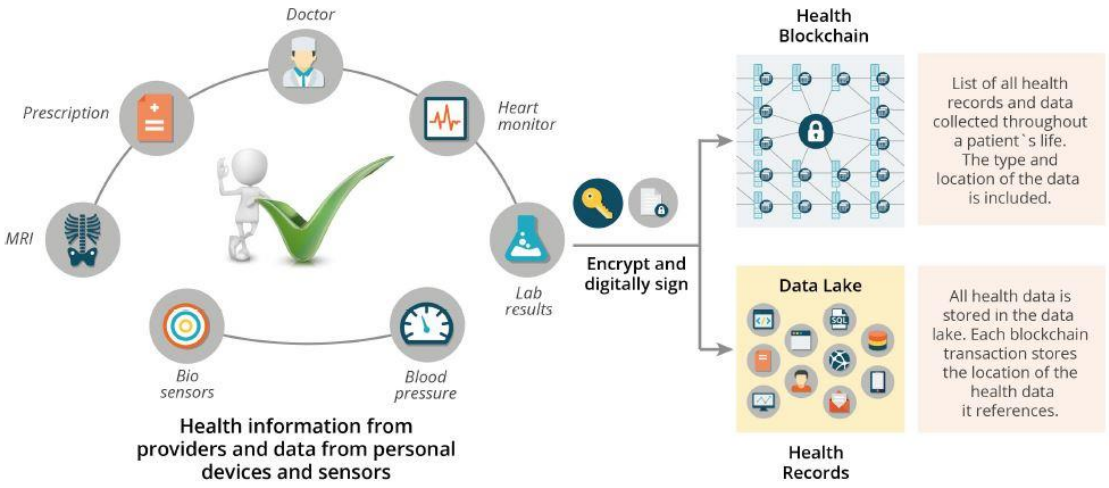
Iako nemogućnost izmjene jednom upisanog zapisa na blockchain donosi mnoge prednosti, postavlja se pitanje što ako regulator zatraži opoziv određene transakcije. Kod blockchaina za razliku od tradicionalnih baza podataka jedina mogućnost za „ispravak“ je protutranskacija koja bi poništila vrijednost već upisane transakcije.

Pravna nesigurnost ili bolje reći nejasnost spada u još jedna od izazova blockchaina. Tvrtke nemaju jasan pravni okvir koji bi se trebao primijeniti u slučaju prijevare ili nekih drugih neželjenih scenarija kod blockchaina. Ovo se posebno odnosi na tvrtke koje posluju u više pravnih sustava.[31]

[31] Lewis, R., McPartland, J., Ranjan. R,. (2019): SPECIAL FEATURE: Cutting-Edge Innovation in the Cryptosphere, J.P. Morgan Center for Commodities at the University of Colorado Denver Business School, Denver, str. 12-15

4.2. Zdravstveni sektor

Blockchain koji sadrži medicinske podatke, bilo tekst ili slike, zahtijeva određeni prostor za pohranu. Ako bi se medicinski blockchain zasnivao na bitcoin modelu, svaki član zdravstvenog sustava bi imao sve zdravstvene podatke svih drugih korisnika. Naravno iz praktičnih razloga ovaj model nema smisla. Linn i Koo (2016) nude prijedlog modela za primjenu blockchaina u zdravstvu. Naime, predlažu da se blockchain ponaša kao zapisnik adresa na kojim se mogu pronaći medicinski podaci. Ovdje bi se blockchain mogao usporediti sa katalogom u knjižnici koji sadrži osnovne podatke o knjigama te lokaciju gdje se knjiga nalazi. Na taj način zapisi u blockchainu bi sadržavali osnovne podatke o medicinskoj dokumentaciji te o vrsti dokumentacije. Lanac bi sadržavao kompletnu povijest upisa pojedine medicinske dokumentacije te podatke sa uređaja kao pametni satovi koji mjere razne medicinski relevantne pokazatelje. Svi medicinski podaci bi zapravo bili spremljeni u skladište podataka(engl. Data Lake). Zajedničke podatke u skladištu podataka bi se onda moglo koristiti za razna istraživanja u svrhu poboljšanja medicinske usluge. Svaki put kada je informacija spremljena u skladište podataka, adresa tih podataka se zapisuje na blockchain. Uz to pacijent bi bio obaviješten svaki put kada bi se dodao novi zapis te bi on sam mogao dodavati podatke sa mobilnih aplikacija i ostalih uređaja uz pomoć digitalnog potpisa i enkripcije.[32]



Slika 13: Blockchain u zdravstvu

Izvor: https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf

[32] Linn L, Koo M (2016): Blockchain for health data and its potential use in health IT and health care related research. https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf (pristupljeno 22.06.2019.)

4.3. Javna uprava

Mogućnosti primjene blockchain tehnologije u javnom sektoru su mnogobrojne. Ovdje će se objasniti neke od njih.

4.3.1. Evidencija digitalnih identiteta pravnih i fizičkih osoba

Blockchain se može koristiti za uspostavljanje digitalnog registra identiteta pravnih i fizičkih osoba te raznih institucija države. Sva pravna dokumentacija poput potvrde o rođenju, o sklapanju braka, putnih isprava se mogu spremati u blockchain bazu podataka. Svi identiteti se mogu povezati i sa osobnim podacima građana poput zdravstvenih i financijskih podataka kako bi se postigla što veća razina interoperabilnosti. Naravno, sve ove primjene podrazumijevaju i zaštitu osobnih podataka građana. Država mora osigurati da građani posjeduju podatke i da s njima mogu upravljati.

4.3.2. Katastar

Katastarskim zapisima se također može upravljati putem blockchaina na način da se vlasnici čestica zajedno sa detaljima relevantnim za prodaju čestice kronološki upisuju u katastar. Pošto su transakcije na blockchainu trajno zapisane, bilo bi moguće provjeriti cjelokupnu povijest vlasništva nad nekom česticom te sve relevantne informacije kroz vrijeme. To bi minimiziralo potrebu za trećom stranom prilikom transakcije i smanjilo vrijeme potrebno za procesuiranje same transakcije.

4.3.3. Nadzor lanca opskrbe

Slično kao kod katastra uz pomoć blockchain moguće je pratiti robu i imovinu. Na ovaj način se može dobiti uvid u cjelokupan proces od proizvodnje preko transporta do kupnje i potrošnje nekog proizvoda. Na ovaj način se povećava razina povjerenja u određenu imovinu ili konkretno neke proizvode.

Potencijalni primjeri upotrebe su u praćenju hrane, lijekova te prirodnih resursa kao što su dijamanti. [33]

[33]Berryhill, J., Bourgery, T., Hanson, A. (2018): https://www.oecd-ilibrary.org/governance/blockchains-unchained_3c32c429-en (pristupljeno 22.06.2019.)

5. PAMETNI UGOVORI – POJAM, KARAKTERISTIKE, ZNAČAJ I MOGUĆNOSTI PRIMJENE

5.1. Pojam pametnog ugovora

Model pametnih ugovora je predložio Nick Szabo još 1997. godine. Ideja pametnog ugovora leži u tome da bi se on trebao samostalno aktivirati tj. da nije potreban posrednik u samom izvršenju ugovora. Da bi se to ostvarilo potrebno je da se pravila kodiraju u nekom programskom jeziku te nakon toga smještaju na blockchain. Smještanjem na blockchain, naknada izmjena odredbi ugovora nije moguća. Kada dođe do ostvarivanja uvjeta za izvršenje ugovora, odrednice ugovora se automatski izvrše.

Nakon što je uočeno da se blockchain tehnologija može koristiti na puno područja došlo je i do kreiranja prvih platformi za razvoj. Prva platforma je bila Ethereum, koju je inicirao Vitalik Buterin 2013. godine koja je realizirana 2015. godine. [34]

Sam naziv ugovori dolazi od izvođenja uvjetnih novčanih transakcija. Na primjer, u slučaju ispunjenja uvjeta X, dolazi do novčane transakcije Y. Ono što blockchain kao takav dodaje konceptu pametnih ugovora je to da jednom upisan kod u blok nije moguće promijeniti što oslobađa sudionike u ugovoru od uvjeta međusobnog povjerenja. Nakon dogovora o pametnom ugovoru, tj. programskom kodu, sudionicima ne treba nikakva treća strana da bi se ugovor izvršio.

Pametni ugovor kao takav pristupa samo podacima koji su upisani u Blockchain. Zbog toga je ponekad potrebno imati sustave koji će zapisivati podatke u blockchain kako bi pametni ugovori mogli izvršavati već programirane naredbe, tj. odredbe ugovora. Sustavi koji prenose informacije iz stvarnog svijeta u blockchain u svrhu mogućnosti donošenja odluka putem pametnih ugovora se nazivaju „oracles“.

Programski kod koji se koristi za pametne ugovore može se zapravo koristiti za bilo što. Jedino je bitno da da su podaci zapisani u samom blockchainu. Pametni ugovori se mogu koristiti i za primjene koji ne spadaju u domenu ugovora, poput standardizacije podataka, komunikacije te izračuna. [35]

---

[34] Minović, M. (2017): Blockchain tehnologija: mogućnosti upotrebe izvan kripto valuta, https://www.researchgate.net/publication/318722738_BLOCKCHAIN_TEHNOLOGIJA_MOGUCNOSTI_UPOTREBE_IZVAN_KRIPTO_VALUTA (pristupljeno 22.06.2019.)

[35] https://ubik.hr/2018/03/26/sto-su-pametni-ugovori-uvod/ (pristupljeno 22.06.2019.)

5.2. Karakteristike pametnih ugovora

U kontekstu blockchaina pametni ugovori označuju transakcije koje su kompliciranije od same prodaje i kupovine virtualnih valuta. Klasični ugovor bi se mogao definirati kao dogovor između dvije ili više strana da će nešto učiniti ili neće učiniti u zamjenu na nešto drugo. Pametni ugovori sadržavaju istu strukturu, samo što nemaju treće strane koja bi posredovala kod provedbe ugovora.
Prema Swan (2015) tri elementa po kojima se pametni ugovori razlikuju od klasičnih su:

- Autonomnost
- Samodostatnost
- Decentraliziranost

Autonomnost se odnosi na karakteristiku pametnih ugovora da jednom kada se iniciraju, agenti koji su ga inicirali ne trebaju više biti u kontaktu sa pametnim ugovorom. Drugi element se odnosi na samodostatnost u obliku upravljanja resursima. Putem skupljanja sredstava za obavljanje raznih usluga pametni ugovori mogu automatski podmirivati nastale troškove na osnovi korištenja raznih resursa potrebnih za rad. I treće što ih dijeli od tradicionalnih ugovora je decentraliziranost što znači da da ugovori nisu spremljeni na jednom centraliziranom serveru već su distribuirani po cijeloj mreži.
Klasična usporedba za pametne ugovore je prodajni aparat (engl. vending machine). Nasuprot ljudskom ponašanju, prodajni aparat se ponaša prema algoritmu. Kada se ubaci novac u aparat i odabere željeni proizvod, aparat taj proizvod isporuči. Ne postoji mogućnost da aparat ne želi izvršiti ugovor. Tako je slično i sa pametnim ugovorima, praktično „kod je zakon“. [36]

5.2.1. Ethereum platforma

Ethereum mreža je platforma za programiranje pametnih ugovora. Na mrežu je vezana i odgovarajuća virtualna valuta ether. Najednostavniji primjer pametnog ugovora na Ethereum platformi je da jedan korisnik želi drugom poslati 10 ethera na određeni datum. Ethereum platforma je počela sa radom sredinom 2015. godine. Samu platformu je predložio Vitalik Buterin u želji da ispravi nedostatke na bitcoin blockchainu. Osim za pametne ugovore Ethereum platforma je zamišljena i za druge primjene poput izgradnje decentraliziranih

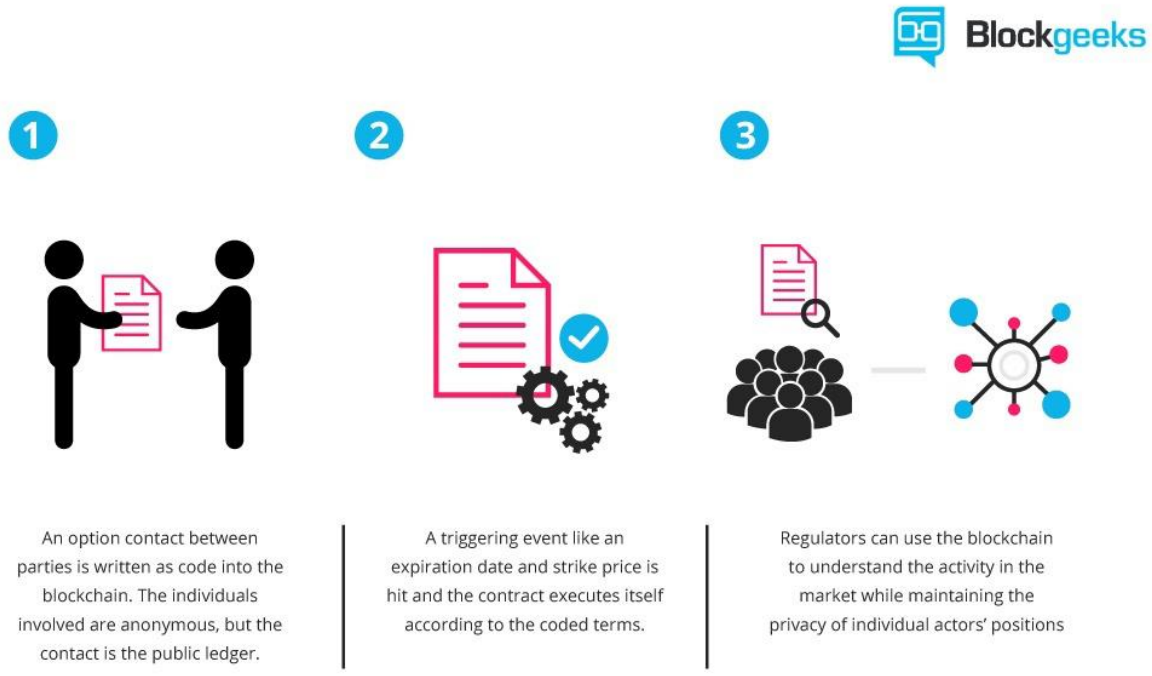
[36] Swan, M. (2015): Blockchain: Blueprint for a New Economy, O'Reilly Media, Sebastopol, str. 16.

aplikacija. Tako razvijene aplikacije imaju razne prednosti poput toga da su kriptografski sigurne, funkcioniraju na temelju konsenzusa i imaju „zero downtime“ što znači da rade neprekidno.

Ethereum pametni ugovori imaju mogućnost da :

- Upravljaju dogovorom između dvije ili više strana
- Funkcioniraju kao „računi s više potpisa“ tj. virtualna valuta se isplaćuje samo kada se određen broj ljudi složi
- Koriste druge ugovore
- Spremaju podatke npr. registar članova

Iako je i bitcoin blockchain jednostavna vrsta pametnog ugovora koja omogućuje prijenos vrijednosti od jednog korisnika prema drugom, Ethereum nudi mogućnost programerima da pišu vlastite programe. U praksi to znači da svatko može izraditi vlastiti pametni ugovor. [37]



Slika 14: Pametni ugovori

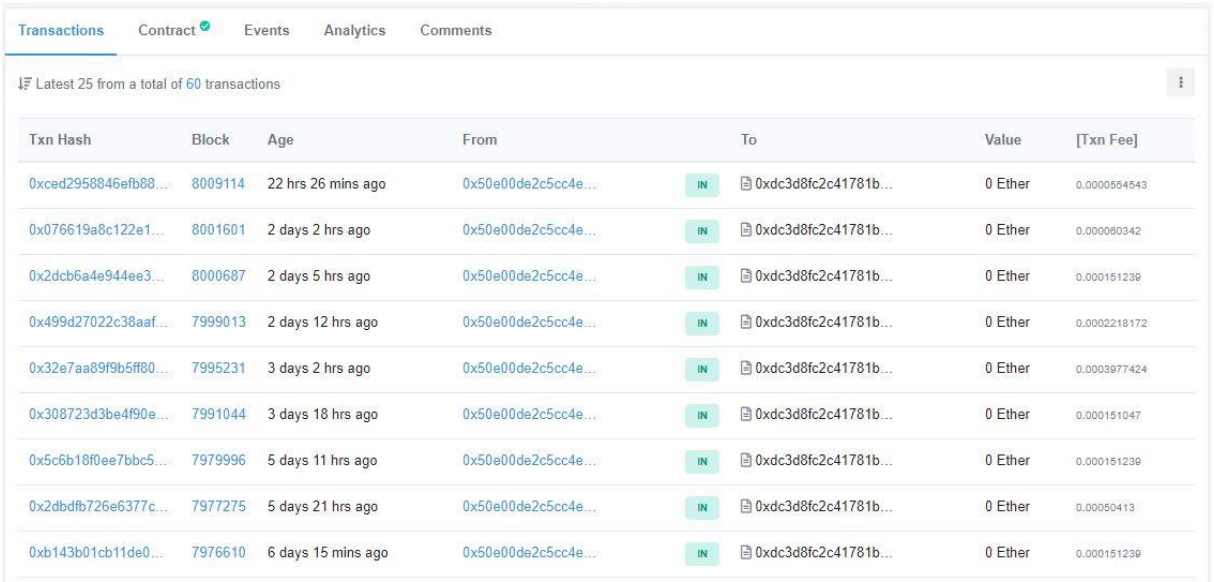
Izvor: https://www.elinext.com/industries/financial/trends/smart-vs-ricardian-contracts/

[37] https://bitcoinvodic.com/kako-funkcioniraju-ethereum-pametni-ugovori/ (pristupljeno 23.06.2019.)

5.3. Značaj pametnih ugovora

Pametni ugovori imaju potencijal izmijeniti iz temelja industrije koje danas ispunjavaju funkcije poput verifikacija, raznih vrsta provjera, licenciranja itd. Također utjecati će i na klasične proizvodne i prodajne lance u raznim sektorima.[38]

Trenutno pametni ugovori nisu široko rasprostranjeni, no ipak je moguće naći projekte koji su zaživjeli. Jedan od njih je servis „fizzy" osiguravajuće kuće AXA. Naime radi se o servisu za ugovaranje osiguranja u slučaju kašnjenja leta. Korisnici sami biraju iznos premije osiguranja i sklapaju policu osiguranja, zapravo pametni ugovor između osiguranika i osiguravajuće kuće AXA. Pametni ugovor je povezan na baze podataka koje sadržavaju podatke o zračnom prometu te na taj način samostalno prepoznaje ako je došlo do ispunjenja uvjeta za izvršenje ugovora. Konkretno za ovaj proizvod uvjet za isplatu je da let kasni dva ili više sati. Nakon ispunjenja uvjeta ugovor automatizmom isplaćuje odgovarajuću naknadu osiguraniku. Na ovom primjeru se ogledaju prednosti koje primjena pametnog ugovora nosi u odnosu na klasični sustav osiguranja. Osiguranik ne mora podnositi zahtjev za isplatu štete, ne mora ići u poslovnicu osiguranja niti mora prikupljati dokumentaciju da bi dokazao pravo na obeštećenje.[39]



Slika 15: Pametni ugovori fizzy servisa na Ethereum platformi

Izvor: https://etherscan.io/address/0xdc3d8fc2c41781b0259175bdc19516f7da11cba7

[38] https://www.pwc.de/en/newsletter/it-security-news-en/blockchain-and-smart-contracts.html (pristupljeno 23.06.2019.)

[39] https://dzone.com/articles/what-is-smart-contracts-blockchain-and-its-use-cas-1 (pristupljeno 23.06.2019.)

5.4. Mogućnosti primjene pametnih ugovora

Pametni ugovori imaju mnogobrojne mogućnosti primjene samim time što bi trebali zamijeniti klasične ugovore s kojima se svakodnevno susrećemo. Mogućnosti primjene jako ovise i o industriji o kojoj se radi. Može se načelno zaključiti da industrije koju su već visoko digitalizirane biti prve koje će implementirati pametne ugovore u svoje poslovne procese. U nastavku će se objasniti implementacije pametnih ugovora koje bi najbrže mogle ugledati svjetlo dana.

5.4.1. Osiguranje

Pametni ugovori imaju potencijal da značajno smanje vrijeme čekanja na administriranje odštetnih zahtjeva te isplatu šteta. Ovdje bi došlo do automatizacije procesa samim time što bi neki događaji automatski aktivirali isplatu odšteta. Pametni ugovor može samostalno dohvaćati informacije o događajima koji mogu pokrenuti proces isplate odštete ili podatke mogu unijeti sami osiguranici ili zaposlenici osiguranja, na primjer u slučaju krađe osiguranog uređaja i slično.

5.4.2. Ugovori o radu

Korištenje pametnih ugovora kod ugovora o radu donosi mnoge prednosti u odnosu na klasične ugovore. Pri upotrebi pametnih ugovora jasnije se određuje što poslodavac očekuje od zaposlenika i obratno što može značajno pridonijeti boljem odnosu između poslodavca i posloprimca. Također sama isplata naknade za rad se automatizira i značajno ubrzava.[40]

5.4.3. Iznajmljivanje i kupoprodaja nekretnina

Uz pomoć pametnih ugovora je moguće dizajnirati ugovore o najmu kao i o kupoprodaji nekretnina. Uz najam i kupoprodaju biti će moguće i pratiti sve prošle zapise na blockchainu vezane uz određenu nekretninu. Bitno je napomenuti da su ove aplikacije još uvijek na teoretskoj razini i da je potrebno razvijati tehnologiju kako bi ušle u masovnu primjenu.[41]

[40] https://disruptionhub.com/smart-contract-uses/ (pristupljeno 23.06.2019.)
[41] https://www.pwc.at/en/digital-real-estate/blockchain-in-real-estate.html (pristupljeno 23.06.2019.)

6. ZAKLJUČAK

Široj javnosti pojam blockchain je poznat samo kao nešto što ima veze sa virtualnom valutom bitcoin. No, blockchain tehnologija je puno više od virtualnih valuta, iako su one zapravo učinile cijelu tehnologiju popularnom i potaknute brojna istraživanja na tu temu. Nakon bitcoin groznice krajem 2017. godine nije se mnogo pisalo ni o virtualnih valutama ni o blockchainu, no to ne znači da se tehnologija nije nastavila razvijati. Najbolji dokaz tome je najava Facebooka o lansiranju vlastite virtualne valute Libra koja bi bila donekle implementirana u sadašnji monetarni sustav.

Iako je bitcoin potpuno nepraktičan da ispunjava svrhu novca iz više razloga, ipak je pokazao da blockchain može funkcionirati u stvarnom svijetu.

Usprkos prednostima koje blockchain nosi bitno je istaći da postoje i nedostatci koje treba riješiti kako bi došlo do masovne primjene tehnologije. Uz blockchain se veže i pojam pametnih ugovora za koje sigurno ima prostora u industrijama koje su već visoko automatizirane i koji već ulaze u praktičnu primjenu kroz neke projekte.

Na kraju je bitno naglasiti da blockchain tehnologija nije čarobni štapić koji će riješiti sve probleme, ali svakako ima potencijal da znatno unaprijedi mnoge procese u društvu.

LITERATURA

KNJIGA:

1. Swan, M. (2015): Blockchain: Blueprint for a New Economy, O'Reilly Media, Sebastopol

PUBLIKACIJE:

1. D. Buterin, E. Ribarić, S. Savić (2015): Bitcoin– nova globalna valuta, investicijska prilika ili nešto treće, Zbornik Veleučilišta u Rijeci, Vol. 3 , No. 1, str. 148-149, str. 150-151, str. 154-155
2. Grad Zagreb (2018): Okvirna strategija pametnog Grada Zagreba, str.39
3. Kraft, D. (2015); Difficulty Control for Blockchain-Based Consensus Systems, University of Graz, Graz, str. 3
4. Lewis, R., McPartland, J., Ranjan. R,. (2019): SPECIAL FEATURE: Cutting-Edge Innovation in the Cryptosphere, J.P. Morgan Center for Commodities at the University of Colorado Denver Business School, Denver, str. 12-15

INTERNET IZVORI

1. Blockchain - Wikipedia https://en.wikipedia.org/wiki/Blockchain (pristupljeno 10.06.2019.)
2. Što je u stvari blockchain i kako radi? - Tehnologije @ bug.hr (2018) https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011 (pristupljeno 10.06.2019.)
3. A Very Brief History Of Blockchain Technology Everyone Should Read (2018) https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#1d8f7c157bc4 (pristupljeno 10.06.2019.)
4. Blockchain: Za razliku od ljudi, imun je na manipulaciju, korupciju... (2017) https://www.netokracija.com/sto-je-blockchain-132284 (pristupljeno 10.06.2019.)

5. Klasična kriptografija - Osnovni pojmovi https://web.math.pmf.unizg.hr/~duje/kript/osnovni.html (pristupljeno 10.06.2019.)
6. Blockchain: Za razliku od ljudi, imun je na manipulaciju, korupciju... (2017) https://www.netokracija.com/sto-je-blockchain-132284 (pristupljeno 13.06.2019.)
7. Blockchain: Za razliku od ljudi, imun je na manipulaciju, korupciju... (2017) https://www.netokracija.com/sto-je-blockchain-132284 (pristupljeno 14.06.2019.)
8. Što je u stvari blockchain i kako radi? - Tehnologije @ bug.hr (2018) https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011 (pristupljeno 14.06.2019.)
9. What is Hash Rate? 3 Things to Know (2019 Updated) (2019) https://www.buybitcoinworldwide.com/mining/hash-rate/ (pristupljeno 14.06.2019.)
10. Bitcoin Mining, Explained (2019) https://www.investopedia.com/terms/b/bitcoin-mining.asp (pristupljeno 14.06.2019.)
11. Što je u stvari blockchain i kako radi? - Tehnologije @ bug.hr (2018) https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011 (pristupljeno 14.06.2019.)
12. Blockchain security: What keeps your transaction data safe? - Blockchain Pulse: IBM Blockchain Blog (2017) https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/ (pristupljeno 14.06.2019.)
13. Private Key (2018) https://www.investopedia.com/terms/p/private-key.asp (pristupljeno 15.06.2019.)
14. Public Key (2018) https://www.investopedia.com/terms/p/public-key.asp (pristupljeno 14.06.2019.)
15. Što su virtualne valute? - Što su virtualne valute? - HNB? (2017) https://www.hnb.hr/-/sto-su-virtualne-valute- (pristupljeno 16.06.2019.)
16. Cryptocurrency Market Capitalizations | CoinMarketCap https://coinmarketcap.com/all/views/all/ (pristupljeno 20.06.2019.)
17. Blockchain: Top Cryptocurrency Market Information https://www.blockchain.com/prices (pristupljeno 20.06.2019.)
18. About Hyperledger https://www.hyperledger.org/about (pristupljeno 21.06.2019.)
19. The difference between public and private blockchain - Blockchain Pulse: IBM Blockchain Blog (2017) https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/ (pristupljeno 21.06.2019.)

20. Stoll et al., The Carbon Footprint of Bitcoin, Joule (2019), https://doi.org/10.1016/j.joule.2019.05.012 (pristupljeno 21.06.2019.)
21. Bitcoin ATM Croatia – find bitcoin machine locations https://coinatmradar.com/country/54/bitcoin-atm-croatia/ (pristupljeno 21.06.2019.)
22. Linn L, Koo M (2016): Blockchain for health data and its potential use in health IT and health care related research. https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf (pristupljeno 22.06.2019.)
23. Berryhill, J., Bourgery, T., Hanson, A. (2018): https://www.oecd-ilibrary.org/governance/blockchains-unchained_3c32c429-en (pristupljeno 22.06.2019.)
24. Minović, M. (2017): Blockchain tehnologija: mogućnosti upotrebe izvan kripto valuta, https://www.researchgate.net/publication/318722738_BLOCKCHAIN_TEHNOLOGIJA_MOGUCNOSTI_UPOTREBE_IZVAN_KRIPTO_VALUTA (pristupljeno 22.06.2019.)
25. Što su pametni ugovori – uvod – ubik.hr (2018) https://ubik.hr/2018/03/26/sto-su-pametni-ugovori-uvod/ (pristupljeno 22.06.2019.)
26. Ethereum pametni ugovori - kako funkcioniraju? - Bitcoin vodič (2018) https://bitcoinvodic.com/kako-funkcioniraju-ethereum-pametni-ugovori/ (pristupljeno 23.06.2019.)
27. Blockchain and smart contracts (2017) https://www.pwc.de/en/newsletter/it-security-news-en/blockchain-and-smart-contracts.html (pristupljeno 23.06.2019.)
28. What Is Smart Contracts Blockchain and Its Use Cases in Business - DZone Security (2018) https://dzone.com/articles/what-is-smart-contracts-blockchain-and-its-use-cas-1 (pristupljeno 23.06.2019.)
29. 5 Applications Of Smart Contracts - Disruption Hub (2018) https://disruptionhub.com/smart-contract-uses/ (pristupljeno 23.06.2019.)
30. Blockchain in Real Estate https://www.pwc.at/en/digital-real-estate/blockchain-in-real-estate.html (pristupljeno 23.06.2019.)

GRAFIČKI PRILOZI

Popis slika:

Slika 1: Rezultat hash funkcije 9
Slika 2: Rezultat hash funkcije nakon dodavanja zareza 9
Slika 3: Težina rudarenja na bitcoin blockchainu 11
Slika 4: Primjer privatnog ključa u bitcoin blockchainu 13
Slika 5: Javni ključ, privatni ključ i javna adresa 14
Slika 6: Javni ključ 14
Slika 7: Javna adresa 14
Slika 8: Broj transakcija na bitcoin blockchainu 15
Slika 9: Najpoznatije virtualne valute 16
Slika 10: Veličina bitcoin blockchaina 17
Slika 11: Kretanje cijene bitcoina 18
Slika 12: Potrošnja energije za rudarenje bitcoina 20
Slika 13: Blockchain u zdravstvu 24
Slika 14: Pametni ugovori 28
Slika 15: Pametni ugovori fizzy servisa na Ethereum platformi 29

SAŽETAK

Cilj ovoga rada je objasniti blockchain kao tehnologiju, njezina tehnička uporišta kao i ulogu koju trenutno igra u ekonomiji. Nadalje se raspravljaju trenutni primjeri tehnologije u vidu virtualnih valuta i projekta Hyperledger. Osim toga objašnjava se i ekološki aspekt same tehnologije i njezin utjecaj na okoliš.
U potencijalnim primjenama tehnologije raspravljaju se mogućnosti u financijskom sektoru te u zdravstvenom sektoru i javnoj upravi.
Dalje se objašnjava primjer upotrebe blockchain tehnologije na pametnim ugovorima.
Kod pametnih ugovora naglasak se stavlja na Ethereum platformu za razvoj te na već postojeću primjenu kod „fizzy“ usluge osiguravajuće kuće AXA uz koju je moguće realizirati ugovor o osiguranju uz pomoć pametnih ugovora. Također se objašnjavaju potencijale mogućnosti primjene pametnih ugovora u drugim industrijama.

Uz prednosti koje nosi blockchain tehnologija izlažu se i problemi i nedostatci koji sprječavaju masovnu upotrebu servisa na blockchainu. U ovom radu se raspravljaju problemi blockchaina poput utjecaja na okoliš, nedostatak standardizacije, skalabilnosti te pravne nesigurnosti.

Rezultat ovoga rada je da blockchain omogućava primjene koje zaista mogu biti značajne, ali i da postoje nedostatci koje treba riješiti.

Ključne riječi: blockchain, blockchain primjene, pametni ugovori

SUMMARY

Purpose of this paper is to explain blockchain as a technology, its technical background, and the current role that it plays in the economy.
The Hyperledger project as well as Crypto Currencies are also discussed.
Their ecological aspects are explained, as well as technology's environmental impact and it's possible uses in the finance sector, in health care, and in public administration.
The use of Blockchain technology via smart contracts, and its emphasis on the Ethereum platform for development are discussed, as well as the already existing "Fizzy" service that enables insurance contracting, powered by the AXA insurance company. The uses of smart contacts in other industries are explained as well.

Blockchain brings advantages as well as disadvantages, which stop the mass use of Blockchain's services, exemplified and discussed in this paper.
Disadvantages of blockchain include its negative environmental impact, lack of standardization, lack of scalability and the legal uncertainty that is brings.

In conclusion, Blockchain can be beneficial, but it also has shortcomings that need to be addressed.

Keywords: blockchain, blockchain applications, smart contracts