

JEDINSTVENA DIGITALNA VRIJEDNOST

Balikić, Marko-Stjepan

Undergraduate thesis / Završni rad

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Economics in Osijek / Sveučilište Josipa Jurja Strossmayera u Osijeku, Ekonomski fakultet u Osijeku**

Permanent link / Trajna poveznica: <https://um.nsk.hr/um:nbn:hr:145:051705>

Rights / Prava: [In copyright](#)/[Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-08-25**



Repository / Repozitorij:

[EFOS REPOSITORY - Repository of the Faculty of Economics in Osijek](#)



Sveučilište Josipa Jurja Strossmayera u Osijeku
Ekonomski fakultet u Osijeku
Preddiplomski studij Poslovna informatika

Marko-Stjepan Balikić

JEDINSTVENA DIGITALNA VRIJEDNOST

Završni rad

Osijek, 2021.

Sveučilište Josipa Jurja Strossmayera u Osijeku

Ekonomski fakultet u Osijeku

Preddiplomski studij Poslovna informatika

Marko-Stjepan Balikić

JEDINSTVENA DIGITALNA VRIJEDNOST

Završni rad

Kolegij: Upravljanje informacijskim resursima

JMBAG: 0165056809

e-mail: mbalikic@efos.hr

Mentor: Prof. dr. sc. Josip Mesarić

Osijek, 2021.

Josip Juraj Strossmayer University of Osijek
Faculty of Economics in Osijek
Undergraduate Study Business Informatics

Marko-Stjepan Balikić


UNIQUE DIGITAL VALUE

Final paper

Osijek, 2021

IZJAVA

O AKADEMSKOJ ČESTITOSTI, PRAVU PRIJENOSA INTELKTUALNOG VLASNIŠTVA, SUGLASNOSTI ZA OBJAVU U INSTITUCIJSKIM REPOZITORIJIMA I ISTOVJETNOSTI DIGITALNE I TISKANE VERZIJE RADA

1. Kojom izjavljujem i svojim potpisom potvrđujem da je završni
(navesti vrstu rada: završni / diplomski / specijalistički / doktorski) rad isključivo rezultat osobnoga rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu. Potvrđujem poštivanje nepovredivosti autorstva te točno citiranje radova drugih autora i referiranje na njih.
2. Kojom izjavljujem da je Ekonomski fakultet u Osijeku, bez naknade u vremenski i teritorijalno neograničenom opsegu, nositelj svih prava intelektualnoga vlasništva u odnosu na navedeni rad pod licencom *Creative Commons Imenovanje – Nekomercijalno – Dijeli pod istim uvjetima 3.0 Hrvatska*. 
3. Kojom izjavljujem da sam suglasan/suglasna da se trajno pohrani i objavi moj rad u institucijskom digitalnom repozitoriju Ekonomskoga fakulteta u Osijeku, repozitoriju Sveučilišta Josipa Jurja Strossmayera u Osijeku te javno dostupnom repozitoriju Nacionalne i sveučilišne knjižnice u Zagrebu (u skladu s odredbama Zakona o znanstvenoj djelatnosti i visokom obrazovanju, NN br. 123/03, 198/03, 105/04, 174/04, 02/07, 46/07, 45/09, 63/11, 94/13, 139/13, 101/14, 60/15).
4. izjavljujem da sam autor/autorica predanog rada i da je sadržaj predane elektroničke datoteke u potpunosti istovjetan sa dovršenom tiskanom verzijom rada predanom u svrhu obrane istog.

Ime i prezime studenta/studentice: Marko-Stjepan Balikić

JMBAG: 0165056809

OIB: 82888141877

e-mail za kontakt: msbalikic@gmail.com

Naziv studija: Poslovna informatika

Naslov rada: Jedinствена digitalna vrijednost

Mentor/mentorica diplomskog rada: Prof. dr. sc. Josip Mesarić

U Osijeku, 14. rujna 2021. godine

Potpis Balikić

Jedinstvena digitalna vrijednost

SAŽETAK

Razvojem informatičke industrije i interneta, danas nastaje novi resurs kojim se ta grana industrije služi, a to je digitalni resurs. Korištenjem digitalnih resursa korisnici svakodnevno stvaraju nove vrste digitalne imovine, poput audio zapisa, video zapisa ili slika. Razvoj tehnologije omogućio je dostupnost takve vrste imovine svima i to gotovo trenutačno. Dostupnost raznih platforma, kao što su Youtube, Instagram, Spotify, pruža mogućnost svakoj osobi da bude autor novih digitalnih sadržaja. Isto tako, jednostavna je manipulacija tuđim digitalnim imovinama te je moguće napraviti bezbroj identičnih kopija. Problem koji se danas javlja je kako očuvati vjerodostojnost i integritet digitalnih resursa, a time i imovine. Rješenje tog problema mogao bi biti jedan od najbrže rastućih trendova današnjice - blockchain tehnologija. Blockchain je od svoje pojave prošao kroz razne faze razvoja. Najpoznatija primjena blockchaina je digitalna valuta Bitcoin, nakon koje slijede razni drugi projekti temeljeni na toj tehnologiji te razvoj cjelokupne blockchain strukture. Pojavom novih generacija blockchaina, poput Etheruma, javlja se mogućnost stvaranja decentraliziranih aplikacija, pametnih ugovora i tokena. Danas primjena blockchaina ne uključuje samo kriptovalute, već ima daleko veći potencijal. Blockchain svojom tehnologijom pruža mogućnost očuvanja integriteta podataka te stvaranje jedinstvene digitalne vrijednosti. Predmet istraživanja ovog rada bit će blockchain tehnologija te jedinstvena digitalna vrijednost. Za razumijevanje jedinstvene digitalne vrijednosti i njenog potencijala, završni će rad objasniti što je blockchain i način na koji funkcionira blockchain tehnologija.

Ključne riječi: Jedinstvena digitalna vrijednost, Blockchain, Digitalni resurs, Internet, Digitalna imovina

Unique digital value

ABSTRACT

Development of the IT industry and internet enabled the making of a new resource, the digital resource. By using digital resources daily, users create new types of digital assets like audio recordings, video recordings or images. The expansion of said technology made owning digital assets available to everyone almost instantly. The availability of different platforms such as YouTube, Instagram, Spotify offers every individual to be the author of digital content. On the other hand, it is very easy to manipulate other people's digital assets and make countless identical copies of it. The issue that arises in present time is how to maintain authenticity and integrity of digital resources and thereby digital assets themselves. Potential solution of the problem might lie in the biggest, fastest growing trend of today- blockchain technology. Blockchain went through various stages of development. The best-known implementation is a cryptocurrency named Bitcoin, later came other projects like it, as well as development of the blockchain structure. Emergence of next generation blockchains like Ethereum, facilitated the creation of decentralized applications, smart contracts, and tokens. But the implementation potential of the blockchain technology is much greater than just cryptocurrencies.

Blockchain technology has the ability to conserve data integrity and create a unique digital value. This paper will discuss blockchain technology and unique digital value. To understand unique digital value and its potential, it's necessary to provide the explanation of blockchain and how it works.

Key words: Unique digital value, Blockchain, digital resource, internet, digital asset

SADRŽAJ

1. Uvod	1
2. Metodologija rada	2
3. Digitalna imovina (eng. Digital asset)	3
3.1. Vrste digitalnih imovine	4
3.2. Digitalna imovina kao vrijednost	5
3.3. Problemi upravljanja digitalnom imovinom	7
4. Blockchain	9
4.1 Vrste blockchaina	10
4.1.1 Javna blockchain arhitektura	10
4.1.2 Privatna blockchain arhitektura	13
4.1.3 Hibridna blockchain arhitektura	14
4.2 Prijenos i verifikacija informacija	15
4.3. Algoritmi verifikacije informacija	16
4.3.1. Dokaz o radu (eng. Proof of Work- PoW)	16
4.3.2. Dokaz o udjelu (eng. Proof of Stake- PoS)	19
4.4 Problem bizantskih generala i kako je riješen blokchainom?	20
4.5 Pametni ugovori	22
5. Jedinstvena digitalna vrijednost	23
5.1 Nezamjenjiva digitalna imovina(eng. non-fungible token -NFT)	24
5.2 Zamjenjiva digitalna imovina	25
5.3 Tokenizacija	26
5.4 Tokenomija	27
6. Primjena blockchaina	29
6.1 Automobilska industrija	29
6.2 Tržište digitalnih kartica	30
7. Blockchain informacijski sustavi	32
7.1 Uloga pametnih ugovora u poslovnim sustavima	33
8. Zaključak	34
9. Literatura	35
10. Popis slika	37

1.Uvod

Digitalni resursi danas su neizbježan pojam u razvoju interneta i informatičke industrije. Gotovo svaka informacija kojom se manipulira elektroničkim putem oblik je digitalnog resursa. Korištenjem i obradom digitalnih resursa svakodnevno se stvaraju novi oblici digitalne imovine. Danas je dostupnost takvih resursa normalna pojava te je svaka osoba bar jednom preuzela neki oblik digitalnog resursa, odnosno, imovine putem interneta. Postavlja se pitanje što ako želimo imati neki oblik jedinstvene digitalne imovine koja bi predstavljala vrijednost neke informacije ili materijalnog objekta. Današnji način upravljanja takvim vrstama imovina ostavlja prostor za umnožavanje i neovlašteno kopiranje istih, a samim time digitalna imovina gubi na svojoj vrijednosti. Pojavom blockchain tehnologije potencijalno se nudi rješenje kako digitalnu imovinu očuvati, kako joj dodijeliti vrijednost te kako ju učiniti jedinstvenom. Tijekom gospodarske krize u 2009. godini, nepoznata osoba ili organizacija pod nazivom Satoshi Nakamoto objavljuje dokument pod nazivom „Bitcoin: A Peer-to-Peer Electronic Cash System“ (eng. Bitcoin- peer to peer elektronički novac) te pokreće revoluciju u svijetu digitalnih resursa, odnosno, imovine. Bitcoin kripto valuta samo je jedan način kako se koristi blockchain tehnologija. Danas postoji preko 1000 javno dostupnih blockchaina, a sve se više pojavljuju i zatvoreni blockchain sustavi za privatna poslovanja. Vodeće svjetske kompanije danas istražuju blockchain tehnologiju i već postoji stvarna primjena te tehnologije u poslovanju. Sve to ide u prilog tezi kako je potencijal blockchain tehnologije puno širi od kreacije elektroničkog novca. Možda je blockchain tehnologija savršen alat za stvaranje jedinstvene digitalne vrijednosti imovine i očuvanja njenog integriteta. Cilj je završnoga rada pobliže objasniti blockchain tehnologiju i njene elemente te na koji način blockchain tehnologija pridonosi razvoju jedinstvenih digitalnih vrijednosti.

2. Metodologija rada

U ovom završnom radu koristit će se sljedeće metode:

Metodom deskripcije opisat će se pojave koje se istražuju. „Svako istraživanje bi trebalo započeti s deskripcijom svih temeljnih pojmova ili pojava. U znanstvenom radu velika pozornost posvećuje se detaljnom opisivanju činjenica, pojava ili podataka kako bi se povećala objektivnost i točnost. No, za znanstveno - istraživački rad ključno je, osim točnog opisivanja pojava, odgovoriti i na pitanja „Kako?“ i „Zašto?“, tj. potrebno je istražiti i prikazati uzroke neke pojave“ (Žugaj i dr., 2006). Prema istom autoru: „deskripcija kao znanstvena metoda podrazumijeva postupak opisivanja pojava i predmeta kao i njihovih veza i odnosa, ali bez znanstvenog objašnjavanja i tumačenja.“ Metoda će se koristiti za opis funkcionalnosti blockchain tehnologije i njenih elemenata koji uključuju pametne ugovore, zamjenjive i nezamjenjive imovine.“

„Povijesna metoda postupak kojim se na temelju raznih dokumenata i dokaznog materijala može saznati sve što se u prošlosti dogodilo te kako i zašto se dogodilo, u znanstvenoistraživačkom radu. Kronologija, razvoj i uzročno-posljedične veze karakteristike su koje se koriste u ovoj metodi. Metoda se uglavnom primjenjuje u kombinaciji s drugim znanstvenim metodama zbog potrebe za ispitivanjem podrijetla, razvoja, uzroka, odnosa i sl. u društvu iako se može koristiti i samostalno.“ (Zelenika, R., 1998). Navedena metoda koristit će se za opis nastanka i razvoja blockchain infrastruktura.

3. Digitalna imovina (eng. Digital asset)

Digitalna vrijednost vezana je uz digitalnu imovinu te nije moguće razdvajati digitalnu imovinu od njene vrijednosti. Za razumijevanje digitalnih vrijednosti, prije svega, potrebno je definirati digitalnu imovinu. „Digitalna je imovina sva ona imovina koja egzistira u binarnoj formi, a podrazumijeva glazbu, slike, video i računalni software“ (Babeanu, Valerica i Gavrića, 2009:318). Međunarodni računovodstveni standard (MRS 38) digitalnu imovinu svrstava pod pojam nematerijalne imovine. „Nematerijalna imovina je imovina koja nema materijalnu supstanciju, ali ima vrijednost (value) utemeljenu na pravno reguliranom ovlaštenju vlasnika, npr. goodwill (goodwill), patent (patent), zaštitni znak (trade mark), autorsko pravo (copyright), software (software), pronalasci, dizajnerska uobličjenja, tj. sve vrste intelektualne imovine (intellectual property) (usp. Tangible property). Nematerijalna se imovina obično otuđuje licenciranim (licensing) ugovorima, a isplate za pravo njezina korištenja obavljaju se u obliku dohotka od autorskih prava (royalties) što ga ostvaruje osoba koja takvu imovinu otuđuje.“ (<https://www.moj-bankar.hr/Kazalo/N/Nematerijalna-imovina>, 2021.)

Uvrštavanjem digitalne imovine u nematerijalnu imovinu jasno je kako takva vrsta imovine ima i svoju vrijednost. Primjerice, u današnjem poslovanju vrijednost poduzeća ne uvjetuje isključivo materijalna imovina koju kompanija posjeduje, već i digitalna imovina poput računalnih programa. Vrijednost je širok pojam te su tijekom povijesti zabilježene razne definicije vrijednosti. Definicija vrijednosti u ekonomskom smislu najbliže objašnjava potencijal vrijednosti koju može imati digitalna imovina. Ona podrazumijeva „korisnost, poželjnost; prikladnost određene stvari, aktivnosti i sposobnosti da, pri danom stanju raspoloživosti, svojim fizičkim, kemijskim, estetskim, intelektualnim i drugim svojstvima može zadovoljiti ljudske potrebe i želje ili može biti razmijenjena za druge korisne i poželjne stvari ili aktivnosti“ (<https://enciklopedija.hr/Natuknica.aspx?ID=65496>, 2021).

Visinu takve vrijednosti definiraju ponuda i potražnja za istima s jedne strane, odnosno, stupanj korisnosti s druge strane.

Tržište digitalne imovine nije nova pojava. Prodaja knjiga, slika te glazbe putem raznih internet platformi već je ustaljena praksa. Međutim, tek pojavom blockchain tehnologije tržište digitalne imovine počinje eksponencijalno rasti. Blockchain mogućnosti da digitalne imovine učini

jedinstvenima i ograničenima i da spriječi neovlaštenu distribuciju digitalnih sadržaja, omogućila je mjesto digitalnoj imovini na tržištu te da se putem sila ponude i potražnje definira njena vrijednost.

3.1. Vrste digitalnih imovine

Digitalnu imovina može se podijeliti na više skupina: (<https://digitalassetmanagementnews.org/features/defining-digital-assets/>, 2021.)

- Digitalni sadržaji poput slika, videa, dokumenata
- Paketi podataka, odnosno Veliki podaci (eng. Big data)
- Digitalni modeli
- Digitalna dobra
- Internet domene i internet infrastruktura
- Korisnički računi

Pojavom blockchaina pojavile su se i nove vrste digitalnih vrijednosti te se danas razlikuju digitalne vrijednosti temeljene na blockchain strukturi.

Kriptovaluta – „digitalna ili virtualna valuta koja je osigurana kriptografskim algoritmima baziranim na blockchain decentraliziranom sustavu“ (<https://www.investopedia.com/terms/c/cryptocurrency.asp>, 2021.).

Tokeni - „Tokeni predstavljaju zamjenjivu i nezamjenjivu imovinu ili uslugu pogodnu za trgovanje i nalaze se na vlastitom blockchainu. Oni se uglavnom koriste za prikupljanje novčanih sredstava putem crowdsalea (online događaj na kojem sudionici mogu kupiti tokene u kriptovalutama), ali se mogu koristiti i kao zamjene za druge stvari. Tokeni ove vrste u pravilu su kreirani, distribuirani, prodani i raspodijeljeni putem procesa inicijalne ponude kriptovaluta (eng. Initial Coin Offering – ICO) koji uključuje skupno financiranje (eng. crowdfunding) za financiranje razvoja projekta“ (<https://www.investopedia.com/terms/c/crypto-token.asp>, 2021.).

3.2. Digitalna imovina kao vrijednost

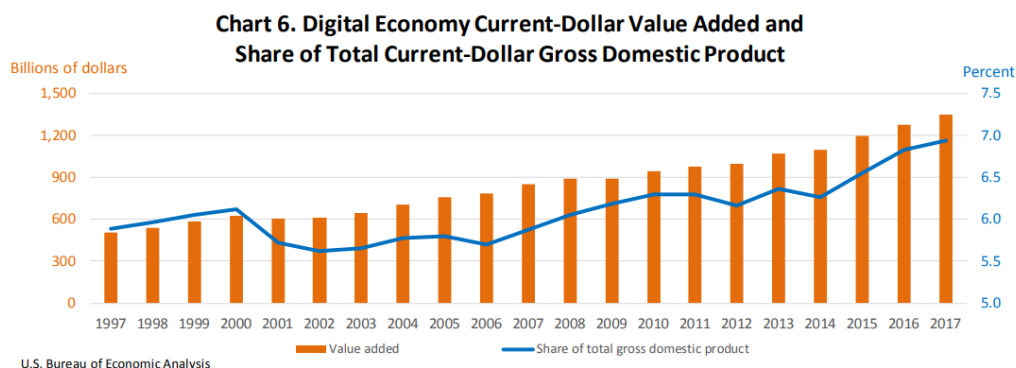
Pojavom digitalne imovine, tržište je počelo cijeniti takvu vrstu digitalnog resursa. Razvojem i pojavom raznih oblika digitalne imovine, oblikuje se i njihova vrijednost.

Digitalna imovina bila je prepoznata kao vrijednost i prije popularizacije blockchaina, što navodi i istraživanje McAfee iz 2013 koje procjenjuje da prosječni korisnik na svom uređaju ima pohranjene digitalne imovine u vrijednosti većoj od \$35,000 (<https://www.mcafee.com/blogs/consumer/digital-assets/>, 2021).

U vrijednost takve digitalne imovine uključene su osobne fotografije, videozapisi, glazba te poslovne informacije pohranjene na uređajima korisnika.

Pojava blockchaina pokrenula je još veće zanimanje za digitalnim vrstama imovine pa je tako vidljivo da pojavom te tehnologije tržište digitalne imovine kontinuirano raste. Danas se može reći kako je digitalna imovina jedan od vodećih trendova u svijetu.

„Od 1997. do 2017. digitalna ekonomija bruto dodane vrijednosti čini u prosjeku 6.1 posto bruto domaćeg proizvoda Sjedinjenih Američkih Država. Udio digitalne ekonomije u BDP-u je u porastu i 2017. godine činio je 6.9 posto ukupne ekonomije države, najveći udio u dosada promatranom vremenskom razdoblju. 2017. godine bruto dodana vrijednost digitalne ekonomije iznosila je 1351.3 milijarde američkih dolara“ (<https://apps.bea.gov/scb/2019/05-may/0519-digital-economy.htm>, 2019.). Vrijednost digitalne ekonomije prikazana je na Slici 1.



Slika 1. Vrijednost digitalne ekonomije

(Izvor: <https://apps.bea.gov/scb/2019/05-may/0519-digital-economy.htm>)

„Nematerijalna imovina trenutno čini **90%** ukupne imovine američkih sastavnica indeksa S&P 500, a materijalna samo 10 posto dok je prije pola stoljeća ovaj omjer bio obrnuto proporcionalan, što govori kako je tehnologija postala dominantna u poslovanju, ali i u životu. Iako je često teško procijeniti nematerijalnu imovinu zbog određenih računovodstvenih praksi, nematerijalna ulaganja danas vrijede više od 21 bilijuna američkih dolara. Vrijednost nematerijalne imovine porasla je sa **122 milijarde dolara 1975. godine, na čak 21,3 bilijuna u 2018. godini.** Najveća promjena u imovini dogodila se krajem osamdesetih i početkom devedesetih godina kada tehnologija polako počinje kucati na vrata i kada društvo polako kreće prema eri nove tehnologije. Upravo u to vrijeme nematerijalna imovina počinje dobivati većinski status u tvrtkama.“ (<https://lider.media/poslovna-scena/svijet/infografika-rastuca-vrijednost-nematerijalne-imovine-136315>, 2021.).

3.3. Problemi upravljanja digitalnom imovinom

Pojavom digitalne imovine postavljaju se novi zahtjevi prilikom upravljanja takvom imovinom. Posjedovanje sve većeg broja i različitih oblika digitalne imovine predstavlja izazov njihove pohrane. Pohrana takve vrste informacije na fizičkim medijima više nije praktična. Kapaciteti fizičkih medija, koji omogućavaju pohranu informacija, ne mogu pratiti sve veći broj digitalnih informacija u svakodnevnom okruženju pa samim time danas više nisu praktično sredstvo za pohranu, kako informacija tako i digitalne imovine. Alternativa fizičkoj pohrani danas su servisi bazirani na oblaku, poput Dropboxa. Takvi su servisi prvotno uspjeli proširiti kapacitete pohrane, međutim, veća količina pohrane donosi probleme poput organizacije digitalne imovine, ali i njihove preglednosti. Upravljanje u takvim uvjetima opterećuje mrežu što otežava brzi pristup imovini. Vrijednim digitalnim imovinama danas je potrebna adekvatna zaštita. Pristup takvoj vrsti imovina, primjerice u poslovnom okruženju, mora biti ograničen i kontroliran. Sprječavanje neovlaštenog pristupa imovini, kao i njena sigurnost, danas su jedan od najčešćih zahtjeva koje korisnici postavljaju prilikom upravljanja digitalnom imovinom.

Ključni je problem koji se javlja prilikom upravljanja digitalnim imovinom sprječavanje neovlaštenog kopiranja i umnožavanja takve vrste imovine. Danas postoje sustavi koji služe za zaštitu i kontrolu kršenja digitalnog sadržaja. Jedan od takvih sustava je i sustav za upravljanje digitalnim pravima (eng. Digital Rights Management - DRM).

„Upravljanje digitalnim pravima (eng. Digital Rights Management - DRM) zajednički je naziv za čitav niz tehnologija koje se koriste za zaštitu i kontrolu korištenja digitalnog sadržaja. Koriste ih izdavači i drugi vlasnici autorskih prava kako bi ograničili pristup digitalnim uređajima i multimedijalnim sadržajima te spriječili njihovo neovlašteno umnožavanje i pretvorbu u druge formate. Premda sam pojam ima sličnosti sa zaštitom od kopiranja (eng. copy protection), u osnovi se više koristi kada se govori o zaštiti kreativnih sadržaja. Zaštita od kopiranja najčešće se odnosi isključivo na programsku podršku (eng. software)“ (Laboratorij za sustave i signale , 2011:4).

Razvoj tehnologije i interneta pridonosi i sve većoj prisutnosti neovlaštenog korištenja autorskih prava i ilegalne distribucije digitalnih sadržaja. Gotovo pa nema digitalnog medija koji nije pogođen tim problemom. Sukladno tome, razvijane su i tehnologije poput AAC3 (eng. Advanced

Access Content System), odnosno, standarda putem kojeg se sprječava neovlašteno umnažanje sadržaja.

„Riječ je o standardu za distribuciju digitalnih sadržaja i upravljanje pravima njihova korištenja namijenjenom ograničenju pristupa i onemogućavanju neovlaštenog umnažanja sadržaja pohranjenog na optičkim diskovima nove generacije. Specifikacija standarda objavljena je u travnju 2005. godine i prihvaćena od strane proizvođača kao osnova zaštite HD DVD i Blu-ray diskova“ (Laboratorij za sustave i signale, 2011:4).

Takve tehnologije možda su djelomično usporile razvoj ilegalnih tržišta digitalnih sadržaja, međutim, danas se sve manje koriste fizički mediji poput CD-a ili DVD-a, a sve više mediji pohranjeni direktno na internetu u digitalnom obliku. Takav način čuvanja digitalnih zapisa dovodi do pojava ilegalnih streaming servisa i platformi za neovlašteno skidanje digitalnih sadržaja.

„Procjenjuje se da je u Hrvatskoj stopa piratizacije filmskih djela iznosi približno 65%-70% od ukupne konzumacije tih djela, iz čega je očito da su gubici za ovu gospodarsku granu vrlo značajni. Kada je riječ o glazbenim djelima, stopa piratizacije u Hrvatskoj putem interneta prelazi 90%, dok se ona koja se odnosi na klasično crno piratstvo kreće oko 25%. Procijenjeni financijski gubici za glazbenu industriju, autore i izvođače veći su od 150 milijuna kuna godišnje. Osim toga, često se zanemaruju i gubici koji nastaju u sferi tzv. sivog piratstva, odnosno, zbog korištenje djela bez odobrenja, a koji se također broje u milijunima kuna. Visoke stope piratstva u Hrvatskoj, osim što donose novčane gubitke stvarateljima djela i popratnoj djelatnosti, ujedno i koče dolazak internacionalnih servisa za legalno korištenje (*download*) autorskih sadržaja“ (<http://www.stop-krivotvorinama-i-piratstvu.hr/hr/krivotvorenje-i-piratstvo/osobito-pogodeni-ind-sektori/zabavni-sadrzaji-i-softver/>, 2021.).

4. Blockchain

Prema Oxfordovom rječniku blockchain se definira kao „sustav u kojem se evidencija transakcija izvršenih u bitcoinu ili drugoj kriptovaluti održava na nekoliko računala koja su povezana u peer-to-peer mrežu“ (<https://www.lexico.com/definition/blockchain>, 2021.). Međutim, blockchain kao skup zapisa transakcija puno je složeniji i kompleksniji. W Viriyasitavat i D. Hoonsopon u svom radu, pod nazivom „Blockchain Characteristics and Consensus in Modern Business Processes“, proširuju definiciju blockchaina te blockchain definiraju kao “tehnologiju koja omogućuje nepromjenjivost i cjelovitost podataka čiji je zapis podataka stvoren i održavan kroz sustav različitih distribuiranih čvorova koji su povezani u peer- to-peer mrežu“ (D. Viriyasitavat i D. Hoonsopon, 2018:3).

Blockchain u direktnom prijevodu znači lanac blokova, odnosno, decentralizirana baza podataka koja međudjelovanjem svih komponenti u sustavu potvrđuje integritet podataka. Komponente koje čine blockchain ovise o samoj vrsti blockchain infrastrukture. Prva je primjena blockchain infrastrukture kriptovaluta Bitcoin. Krajem 2009. godine osoba ili organizacija pod nazivom Satoshi Nakamoto objavljuje rad „Bitcoin: A Peer-to-Peer Electronic Cash System“ (eng. Bitcoin-peer to peer elektronički novac). Unazad 10 godina, na tržištu se javljaju razni projekti koji svoj sustav temelje na takvoj blockchain tehnologiji. Nove verzije blockchaina pružaju i novi način korištenja takvih struktura. Blockchain danas nije isključivo rezerviran za kriptovalute, već je savršen alat za očuvanje vrijednosti i integriteta informacija.

4.1 Vrste blockchajna

4.1.1 Javna blockchain arhitektura

Javni je blockchain decentralizirana baza podataka otvorenog koda dostupna neograničenom broju korisnika. Sve transakcije u javnom blockchainu vidljive su svim korisnicima. Javni blockchain, pomoću svoje decentralizirane baze podataka, omogućava transparentnost transakcija. Primjerice, transakcije na bitcoin blockchainu vidljive su putem takozvanog bitcoin pretraživača (Slika 2).

Latest Transactions

The most recently published unconfirmed transactions

Hash	Time	Amount (BTC)	Amount (USD)
c299bc37c36de54edb7b...	14:55	0.08142540 BTC	\$2,747.31
59ff275b2a0cc2c97f3136...	14:55	34.71882415 BTC	\$1,171,419.03
893f02b5e647c79031321...	14:55	0.01574800 BTC	\$531.34
cde033b3606833708d67...	14:55	0.00306620 BTC	\$103.45
bda08394edaccd9b7116c...	14:55	0.05382577 BTC	\$1,816.09
2c019199309a1bd59b424...	14:55	0.58391607 BTC	\$19,701.43

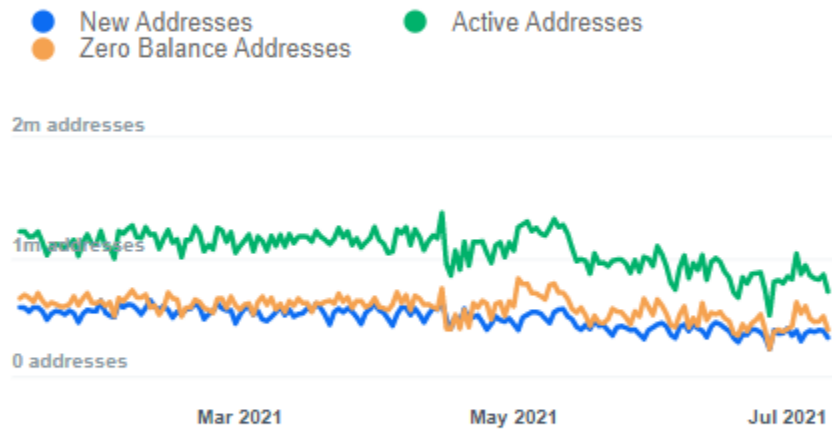
Slika 2. Transakcije na bitcoin blockchainu

(Izvor: <https://www.blockchain.com/explorer>)

Zahvaljujući transparentnosti na blockchainu, moguće je statistički pregledavati sve transakcije koje se odvijaju putem takve otvorene blockchain mreže.

Samo neki od primjera uključuju prikaz aktivnih adresa u jednom danu i prikaz ukupnog broja adresa u određenom vremenskom periodu što je prikazano na Slikama 3. i 4.

Daily Active Addresses ?

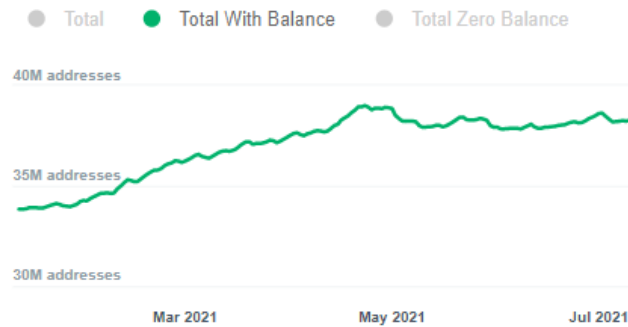


<u>7-Day NA Change</u>	<u>7-Day AA Change</u>	<u>7-Day ZBA Change</u>
-15.68%	-30.92%	-37.78%

Slika 3. Aktivne adrese

(Izvor: <https://www.blockchain.com/explorer>)

Total Addresses ?



Total With Balance

30-Day Average

38.17m addresses

30-Day High

38.62m addresses Jul 2 2021

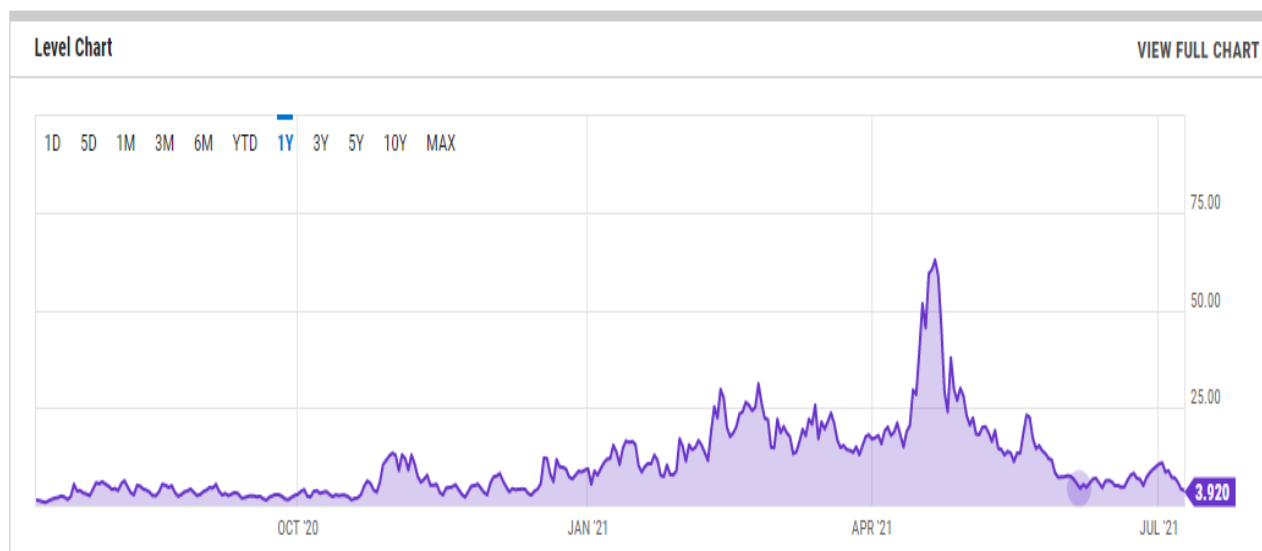
30-Day Low

37.87m addresses Jun 14 2021

Slika 4. Ukupan broj adresa

(Izvor: <https://www.blockchain.com/explorer>)

Bitcoin blockchain koristi sustav naknada. Prilikom generiranja svake transakcije, potrebno je platiti rad mreže. Plaćanje se izvršava u bitcoinu. Ukoliko korisnika zanima visina naknade u tom trenutku, postoje platforme koje u realnom vremenu izračunavaju trenutačnu naknadu. Pregled takvih informacija dostupan je putem web servisa kao što je Ycharts. Kretanje cijene naknade za bitcoin prikazano je na Slici 5.



Slika 5. Cijena Bitcoin naknade za transakciju

(Izvor: https://ycharts.com/indicators/bitcoin_average_transaction_fee)

4.1.2 Privatna blockchain arhitektura

Privatni blockchain namijenjen je za rad u zatvorenom sustavu. On sprječava neovlašten pristup mreži te samo korisnici koji imaju dodijeljene ovlasti imaju pravo pristupa. Takav način rada pogodan je za organizacije koje nemaju interes za dijeljenjem informacija s vanjskim korisnicima, ali imaju potrebu za korištenjem blockchain strukture unutar svog poslovanja. Privatni blockchain danas je najrasprostranjeniji u logističkom sektoru poduzeća. Tvrtka Everledger prepoznala je potencijal blockchaine. Everledger razvija privatnu blockchain infrastrukturu za praćenje porijekla dijamanta, od pronalaska dijamanata kao sirovine pa sve do njihove završne obrade.

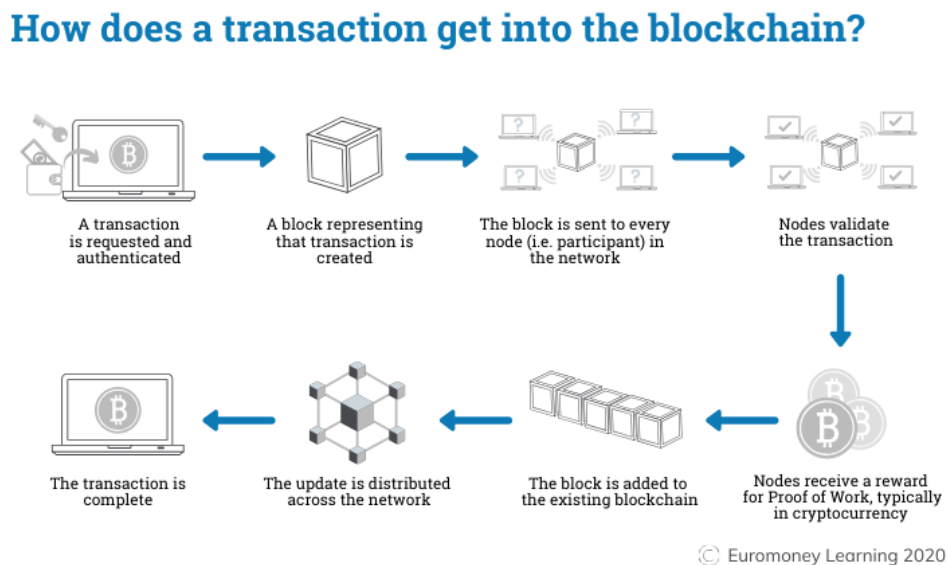
4.1.3 Hibridna blockchain arhitektura

Hibridni model blockchajna kombinira privatni i javni blockchain na način da korisnik može sam odlučiti želi li da njegova transakcija bude javno vidljiva ili želi obaviti isključivo privatnu transakciju vidljivu samo korisniku koji ju je odaslao i primatelju. Takav blockchain najčešće koristi višeslojnu arhitekturu koja se sastoji od privatnih slojeva na kojoj se odvijaju transakcije isključivo za autorizirane korisnike te javno dostupnih slojeva blockchajna na kojima pristup imaju svi korisnici. Hibridne blockchain infrastrukture svoju primjenu mogle bi imati u području medicine. Primjerice, razmjena medicinske dokumentacije isključivo s liječnikom, a pri tome zaštita vlastite privatnosti od drugih korisnika.

4.2 Prijenos i verifikacija informacija

Prilikom transakcije putem blockchaina, privatnim ključem potpisuje se transakcija te potvrđuje da je istu poslao originalni vlasnik. Privatni ključ također sprječava manipulaciju ostalih korisnika mreže tom transakcijom. Nakon što je transakcija odaslana, potrebno je postići konsensus u sistemu, odnosno, transakcija mora dobiti potvrdu ostalih korisnika mreža da je valjana. Način validacije takvih transakcija, odnosno, postizanja konsensusa, ovisi o vrsti i arhitekturi samog blockchaina na kojoj je transakcija inicijalizirana.

Blockchain arhitekture koje koriste „Dokaz o radu“ algoritam, dokazuju istinitost transakcije putem rudara, odnosno, rudari predstavljaju računalnu snagu koja rješava matematičke dokaze u kriptografskim algoritmima same transakcije. Jednom potvrđena transakcija po kriptografskim pravilima ulazi u blok. Kako je blockchain, lanac blokova, tako svaki novonastali blok dolazi na kraj tog lanca te se na taj način sprječava modificiranje svih prethodnih blokova. Tijek transakcije u blockchainu (slika 6.).



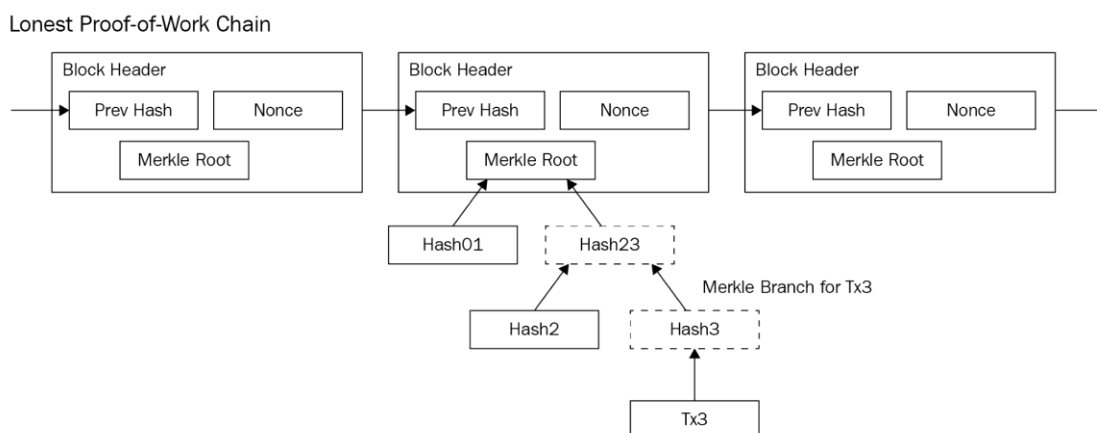
Slika 6. Tijek transakcije u blockchainu

(Izvor: <https://www.euromoney.com/learning/blockchain-explained/how-transactions-get-into-the-blockchain>)

4.3. Algoritmi verifikacije informacija

4.3.1. Dokaz o radu (eng. Proof of Work- PoW)

Dokaz o radu kriptografski je algoritam koji zahtjeva rad procesorske snage u računalima za verifikaciju transakcija. Prilikom stvaranja novog bloka, potrebno je riješiti kriptografsku zagonetku, odnosno, pronaći odgovarajuću vrijednost bloka koja je zaštićena hash funkcijom. Proces verifikacije takvih kompleksnih matematičkih problema u takvom sustavu naziva se rudarenje odnosno (eng. mining). Bitcoin blockchain sastoji se od blokova povezanih u beskonačni lanac. Jednom kada računalo izrudari, odnosno, izračuna ispravnu vrijednost hash funkcije odgovarajućeg bloka, u lanac se dodaje novi blok. Takav algoritam u kojem se dokazuje rad računala, odnosno, rudara za stvaranje novih blokova te verifikaciju postojećih blokova naziva se Dokaz o radu. Cilj je kriptografskog algoritma spriječiti dvostruku transakciju na mreži (eng. double spending). Iako je koncept kriptografskog algoritma, temeljenog na Dokazu o radu predstavljen od strane Cynthia Dwork i Moni Naor 1993. godine, tek pojavom bitcoina populariziran. Danas termin dokaz o radu najčešće vežemo uz kriptovalute. Bitcoin struktura blokova čija se istinitost potvrđuje dokazom o radu prikazana je putem Merkleovog stabla (Slika 7.).



Slika 7. Merkleovo stablo

(Izvor: <https://bitcoin.org/bitcoin.pdf>)

4.3.1.1. Hash funkcija

Za razumijevanje blockchain algoritma, potrebno je objasniti hash funkciju.

„Hash funkcija preuzima poruku kao input i stvara output u obliku hash koda, hash rezultata, hash vrijednosti ili jednostavno hash“. (A. Menezes, P. van Oorschot i S. Vanstone, 1996:321).

U bitcoin blockchainu verifikacija transakcije provodi se putem SHA-256 hash funkcije. Konverziju teksta u hash funkciju prikazat ćemo na sljedećem primjeru:

Ukoliko se riječ Auto kriptira putem hash-256, output te riječi glasit će:

Primjer inputa: Auto

SHA-256 Output:

929260ad9b9ea9fe0f3553dd964f4ff3deb5792efd031a2b90f573fe91f012bb








Promijeni li se samo jedno slovo u prvotnoj riječi koja je izabrana, dobit će se potpuno nova funkcija.

Primjer: Auti

SHA-256 Output:

6c6c11f72e4332c799b7cc78df8c5f3ebcbd786e92f6addec9cf6ad1bd6a11d2

Prilikom inicijalizacije transakcije, svaka transakcija ulazi u blok. Jednom kada se stvori novi blok s transakcijama, bloku se dodjeljuje hash broj prijašnjeg i hash broj sadašnjeg bloka. Istovremeno, blok sadrži i nonce broj (nasumično generiran broj). Rudari rudarenjem podataka traže nonce broj. Jednom kada je taj broj pronađen, transakcija je potvrđena. Na slici 8 prikazana je usporedba Pow algoritma za više različitih kriptovaluta.

#	Name	Algorithm	Block Time
1	 Bitcoin #1 BTC	SHA256	10 minutes
2	 Ethereum #2 ETH	Ethash	~14 seconds
3	 Dogecoin #7 DOGE	Scrypt	60 Seconds
4	 Bitcoin Cash #12 BCH	SHA256	10 minutes
5	 Litecoin #14 LTC	Scrypt	~2.5 minutes
6	 Ethereum Classic #19 ETC	Ethash	N/A
7	 Monero #28 XMR	CryptoNight	120 seconds
8	 Bitcoin SV #38 BSV	SHA256	10 minutes
9	 Decred #53 DCR	Blake (14r)	5 minutes
10	 Zcash #62 ZEC	Equihash	2.5 minutes

Slika 8. Pow algoritmi

(Izvor: <https://cryptoslate.com/cryptos/proof-of-work/>)

4.3.2. Dokaz o udjelu (eng. Proof of Stake- PoS)

Proof of stake algoritam uveden je drugom generacijom blockchaina i pojavom kriptovalute Ethereum. Za razliku od dokaza o radu, u kojem se računalne snage, odnosno, rudari međusobno natječu za verifikaciju transakcije, proof of stake algoritam verifikaciju transakcija raspoređuje korisnicima prema udjelu valuta koji korisnici posjeduju. Na taj način smanjuje se upotreba računalne snage te pruža efikasnije i jednostavnije održavanje blockchain arhitekture. Najpoznatiji algoritam proof of stake je Ethash.

4.3.2.1 Ethash

Značaj pojave Ethash algoritma na blockchain tehnologiju odrazio se pomoću njegove mogućnosti stvaranja decentraliziranih aplikacija i pametnih ugovora.

Karakteristike Ethas algoritma (<https://eth.wiki/en/concepts/ethash/ethash>, 2021)

- Veličina bloka iznosi 16 MB
- Ethas koristi predmemorije iz kojih se može generirati skup podataka veličine 1 GB
- Zahvaljujući predmemoriji rudarenje blokova moguće je izvršiti s umanjenom količinom računalne snage
- Ažuriranje blokova izvršava nakon svakih 30 000 blokova dodanih u lanac

4.4 Problem bizantskih generala i kako je riješen blockchainom?

Moderna informatika danas poznaje termin „Problem bizantskih generala“ čiji naziv potječe još od Bizantskog carstva, odnosno problema koji su imali bizantski generali za vrijeme svojih bitaka.

Za vrijeme bizantskog Carstva, generali koji su koordinirali napad imali su problem s koordinacijom napada iz više pravaca. Kako prenijeti informacija o vremenu napadanja svim nadređenima da počnu djelovati u isto vrijeme? Hoće li prilikom prijena informacije, informacija biti izmijenjena te mogu li generali imati međusobno povjerenje? Takva problematika danas je prisutna i u informatici. Pravovremeni prijenos informacije i pouzdanost svakodnevni je izazov informatičara.

„Pouzdan računalni sustav mora se nositi s neuspjehom jedne ili više komponenata. Komponenta koja je zakazala može demonstrirati ponašanje koje je često zanemareno te tada dolazi do slanja proturječnih informacija u različite dijelove sustava. Problem suočavanja s ovom vrstom neuspjeha izražen je apstraktno kao problem bizantskih generala“ (Lamport, Shostak i Pease, 1982: 382). Stvaranje informacijskih sustava koji će raditi bez greške te neće imat slabe točke, danas je gotovo pa mit. Činjenica je da, bez obzira na kvalitetu, stručnost, znanje prilikom stvaranja informacijskih sustava, nema garancije da će sustavi raditi besprijekorno. Na Slici 9. prikazan je problem bizantskih generala.

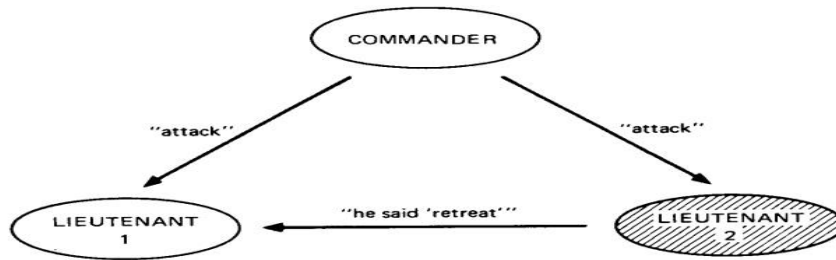


Fig. 1. Lieutenant 2 a traitor.

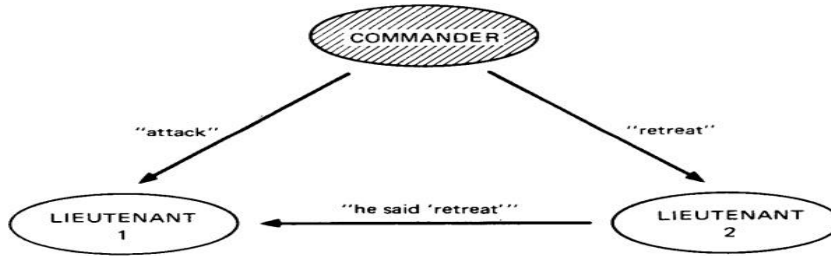


Fig. 2. The commander a traitor.

Slika 9. Problem bizantskih generala

(Izvor: (Lamport, Shostak, Pease, 1982: 382))

Pojavom blockchaina, odnosno decentralizirane baze podataka riješen je problem bizantskih generala.

Potvrđivanjem transakcija koje su zaštićene kriptografskim algoritmima stvara se beskonačni lanac blokova transakcija. Takovim način upravljanja informacijama kreira se beskonačni lanac blokova, u kojem su vidljive sve transakcije koje su generirane. Upravo takav pristup pohrane informacija stvara povjerenje i integritet informacija.

4.5 Pametni ugovori

Ugovor u tradicionalnom smislu potječe od latinske riječi „contractus, pravni posao, suglasno očitovanje volja dvaju ili više subjekata usmjereno na postizanje dopuštenih pravnih učinaka, a koji se sastoje u postanku, prestanku ili promjeni pravnog odnosa“ (<https://www.enciklopedija.hr/natuknica.aspx?id=63011>, 2021). Kako bi se ispunila ugovorna obveza, potrebno je obostrano povjerenje sudionika. Takvo povjerenje postiže se prisustvom treće strane. U tradicionalnom smislu treću stranu možemo definirati kao Javni bilježnik.

Digitaliziranjem pametnih ugovora te automatiziranjem uvjeta po kojima se ugovori ispunjavaju, stvaraju se pametni ugovori. Pametne ugovore po prvi put spominje Nick Szabo 1997. te ih definira kao „računalno generirani transakcijski protokol koji automatizirano ispunjava uvjete ugovora“ (Szabo, 1997). Osnova je ideja pametnih ugovora automatiziranje tradicionalnih ugovora između dviju strana korištenjem programskog koda. Međutim, puni potencijal korištenja pametnih ugovora bilo je moguće ostvariti tek pojavom Ethereum blockchaine. Vitalik Buterin, 2014. godine, objavljuje dokumentaciju za Ethereum infrastrukturu.

Javno dostupan i vidljiv blockchain, putem kojeg korisnici mogu izrađivati aplikacije, stvarati vlastite tokene te pametne ugovore. Sva pravila tradicionalnih ugovora vrijede i za ugovore u digitalnom obliku, odnosno, za pametne ugovore. Pametni ugovori pokreću se na Ethereum platformi putem Ethereum Virtual Machine (Evm) softwarea. Pomoću programskog koda unaprijed se definiraju pravila i zahtjevi. Primjerice, ukoliko se određeni uvjet ispuni, isplatit će se definirani iznos Ethera. Jednom kada se ugovor implementira na Ethereum blockchain, ostaje zauvijek na njemu. Ukoliko se javi zahtjev da se ugovor nakon nekog vremena makne s Ethereum blockchaine, moguće je implementirati naredbu za samouništenje. Važno je napomenuti da sva pravila i uvjete koji će pametni ugovor sadržavati moraju biti implementirani prije nego što se ugovor postavi na blockchain. Naknadne promjene nisu moguće.

5. Jedinствena digitalna vrijednost

Jedinствena digitalna vrijednost produkt je blockchaina. Digitalna vrijednost sadržana je u jedinstvenoj digitalnoj imovini koja putem obrade, pomoću blockchaina, sadrži meta podatke poput vlasnika, vremena nastanka i povijest transakcija. Svi metapodaci upisani su u blockchain te time digitalni imovina postaje imovina sa svojim integritetom, odnosno postaje jedinstvena digitalna vrijednost.

Karakteristike koje digitalnoj imovini daju vrijednost:

- Vlasništvo nad informacijom
- Vrijednost informacije
- Povijest kretanja informacije
- Digitalna lokacija informacije
- Istinitost informacije

Danas je moguće pomoću blockchaina na različite načine potvrditi integritet samih podataka. Sam proces na koji način odabrati potvrdu informacija, ovisi i o vrsti arhitekture blockchaina koji se koristi prilikom takve obrade.

Na primjeru ethereum platforme i blockchaina, koji radi na Ethas algoritmu, vrijednost neke informacije moguće je pretvoriti u token. Traženi zahtjevi prilikom stvaranja takvih jedinstvenih informacijskih vrijednosti dovode do podjele imovine na zamjenjive i nezamjenjive.

5.1 Nezamjenjiva digitalna imovina(eng. *non-fungible token -NFT*)

Nezamjenjiva digitalna imovina, odnosno, nezamjenjivi token trenutno je jedna od najtraženijih digitalnih vrsta imovina na tržištu. Pohranom takve vrste imovine, pomoću blockchaina stvara se ujedno i digitalna vrijednost te imovine. Digitalna imovina koja je definirana i pohranjena putem blockchain tehnologije naziva se token.

Vrijednost koju posjeduje takva imovina očituje se kroz njegovu jedinstvenost, ograničenost na tržištu te kroz njenu potvrdu integriteta. Razvojem takve vrste tokena javlja se novi termin NFT.

„Engleska kratica NFT označava naziv non-fungible token, u prijevodu nezamjenjivi token. NFT je poseban kriptografski generirani token koji koristi blockchain tehnologiju za povezivanje s jedinstvenom imovinom koja se ne može replicirati. Jedinstveni token može biti bilo što (digitalna slika, rečenica, video zapis ili bilo koji podatak), no, za razliku od svega drugog digitalnog, NFT je jedinstvena imovina, a sve ostalo su kopije i reprodukcije“ (<https://www.iusinfo.hr/aktualno/u-sredistu/45492>, 07.05.2021).

Zahvaljujući blockchain tehnologiji danas se može materijalne stvari, kao što su umjetnine, glazba, kolekcionarski primjerci razne robe, pa čak i zemljišta, pretočiti u digitalnu informaciju, odnosno, nezamjenjivi token koji predstavlja digitalnu vrijednost neke materijalne stvari. Blockchain omogućava dodjelu jedinstvenog broja pomoću kriptografskih algoritama svakoj digitalnoj, a time i fizičkoj, imovini. Jednom kada se takvu imovinu definira i pohrani na blockchainu, blockchain tehnologija garantira sigurnost da je takva imovina jedinstvena i nezamjenjiva.

Stvaranje nezamjenjive imovine najviše se cijeni na tržištu glazbene, digitalne pa i filmske umjetnosti. Upravo ta tržišta su razvojem internet tehnologije najviše pogođena neovlaštenim dijeljenjem autorskih prava te im blockchain tehnologija može poslužiti kao savršen alat za zaštitu digitalne imovine.

5.2 Zamjenjiva digitalna imovina

Za razliku od nezamjenjive digitalne imovine koja je jedinstvena imovina bez mogućnosti replikacije, postoje i zamjenjive imovine.

Zamjenjive su imovine „vrste kriptografskih tokena koje su istovjetne jedna drugoj te se mogu mijenjati za ostale zamjenjive vrijednosti istog tipa. To su vrijednosti koje su usporedive sa stvarima koje koristimo svakodnevno te se mogu primjenjivati slično kao i digitalne vrijednosti“ (<https://www.blockchain-council.org/blockchain/a-quick-guide-to-fungible-vs-non-fungible-tokens/>, 2020.).

Prema Blockchain council kao primjer nezamjenjive vrijednosti navodi se Bitcoin. Vrijednost Bitcoina kao jedinice jednaka je svakom pojedinačnom Bitcoinu. Jedan Bitcoin uvijek vrijedi 1 Bitcoin. Takva jednakost čini Bitcoin zamjenjivim. Jednostavnijim rječnikom vrste kriptovaluta ili tokena koje su u svojoj osnovi jednake mogu se zamijeniti s drugim kriptovalutama ili tokenima iste vrste.

5.3 Tokenizacija

Tokenizacija je pojam koji se do sada koristio najviše u bankarstvu.

Prema definiciji tokenizacija je “proces pohrane kartičnih podataka na WSPay-u, odnosno na sigurnom PCI DSS L1 okruženju, uz prethodnu provjeru ispravnosti unesenih podataka i uz SCA (Strong Customer Autentikaciju) sa ciljem da se kupcima omogući brzo plaćanje, bez unosa kartičnih podataka, kod ponovne kupnje na online prodajnom mjestu.

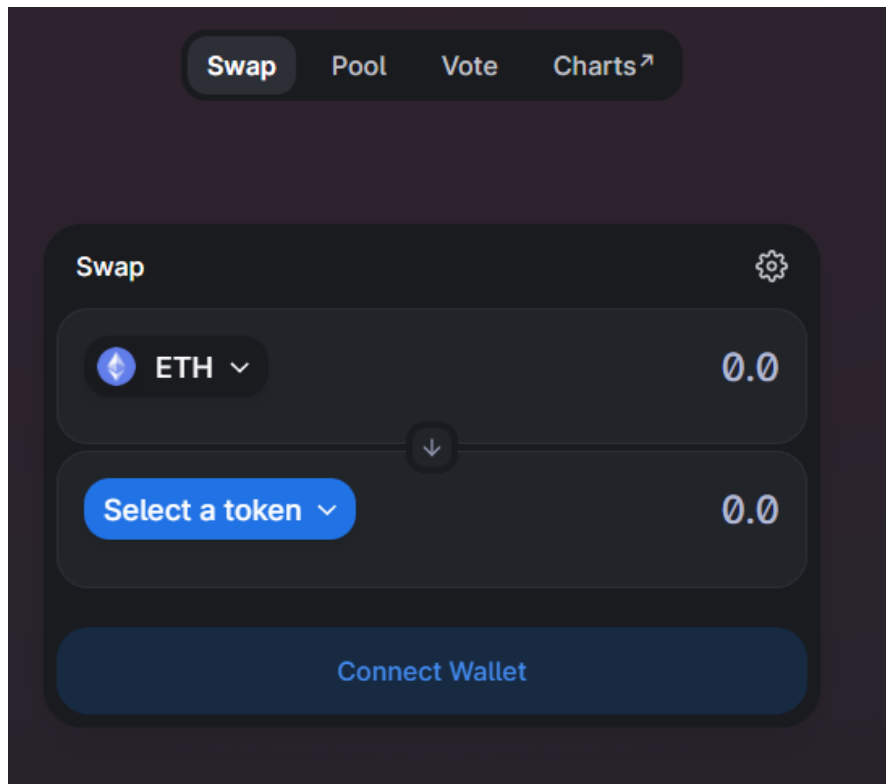
Rezultat Tokenizacije je TOKEN i Token number koji se koriste za provođenje brzih transakcija kod sljedećih plaćanja, a prema pravilima koja propisuje PSD2 regulativa i kartične sheme“ (<https://www.wspay.info/cd/137/tokenizirane-transakcije-transakcije-sa-spremljenim-karticnim-podacima>, 2021.).

Iako se za blockchain tehnologiju i stvaranje tokena koristi isti naziv tokenizacija, važno je navesti kako tokenizacija putem blockchaina nema poveznice s riječima token i tokenizacija koje se koriste u bankarstvu. Definicija tokenizacije putem blockchaina:

„Tokenizacija je proces pretvaranja dijela podataka koji je od posebnog značaja, kao što je broj računa, u nasumični niz znakova koji se zove token i koji nema nikakvu vrijednost ako dođe do povrede sigurnosti. Tokeni služe kao reference originalnim podacima, ali se ne mogu koristiti za nagađanje njihove vrijednosti. Za razliku od enkripcije, tokenizacija ne koristi matematičke procese za transformaciju podatka u token. Umjesto toga, tokenizacija koristi bazu podataka, koja se zove trezor tokena, u kojoj je pohranjena veza podataka i tokena. Na taj je način originalni podatak osiguran, često enkrijcijom“ (<https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/tokenization-vs-encryption.html>, 2021.).

5.4 Tokenomija

Tijekom povijesti se trguje različitim resursima koje imaju svoju vrijednost. Trgovanje digitalnim resursima novo je područje ekonomije koje se populariziralo zahvaljujući razvoju blockchaina. Pojavom jedinstvene digitalne imovine javlja se i tržište takvih vrijednosti. Blockchain podrška za stvaranje tokena omogućava trgovanje takvim digitalnim vrijednostima. Digitalne imovine na blockchainu relativno su novi pojam, iako je potencijal takve imovine prepoznat, tržište digitalne imovine je tek u razvoju, posljedično i primjena takve imovine još nije velika. Danas zahvaljujući tokenizaciji, koja omogućava pretvorbu bilo kojeg fizičkog objekta u token, razumljivo je da postoji široki spektar upotrebe takvih tokena kao i vrsta tokena koji mogu postojati. Tokeni egzistiraju isključivo na onom blockchainu na kojem su stvoreni, odnosno, svaki token reprezentira svoj ekosustav na tom blockchainu. U početku je postojao problem razmjene takvih vrijednosti. Međutim, pojavljuju se platforme koje pružaju mogućnost razmjene različitih tokena. Primjerice, uniswap platforma. Uniswap je decentralizirana mjenjačnica bazirana na Ethereum blockchainu putem koje je moguće razmjenjivati tokene. Uniswap pomoću Ethereum blockchaina radi na temelju pametnih ugovora. Takav način decentralizirane mjenjačnice dopušta korisnicima da sami mogu objavljivati tokene koje žele prodati (Slika 10).



Slika 10. Uniswap aplikacija

(Izvor: <https://app.uniswap.org/#/swap>)

Očigledno je da prilikom korištenja takvih platformi, u kojoj nema centralnih posrednika, postoji opasnost od krivotvorenja tokena. Prilikom kupovanja vrijednosti, bitno je provjeriti vjerodostojnost pametnog ugovora na kojem je imovina stvorena te na taj način verificirati ispravnost tokena.

6. Primjena blockchaina

6.1 Automobilska industrija

Često se prilikom kupovine automobila postavljaju pitanja poput koliko je vlasnika automobil imao, koliko kilometara je prešao, kada je rađen zadnji servis. Svi ti podaci uglavnom su dostupni tek kada se kupac zaputi do tehničke stanice ili ovlaštenog tijela koje posjeduje informacije o samom vozilu. U nekim slučajevima, poput provjere kilometraže na automobilu, teško je saznati istinitost informacija koje kupac u tom trenutku dobiva.

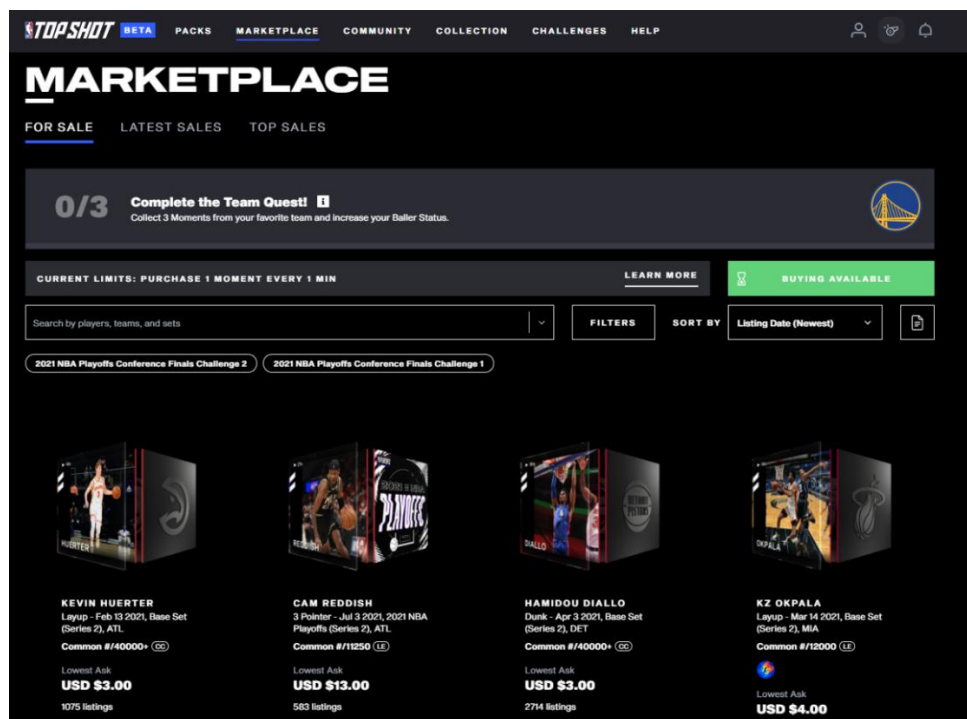
“Europske statistike su raznolike i u sferi procjene. U Njemačkoj, iz koje se u Hrvatsku uvozi veliki broj rabljenih automobila, policija procjenjuje kako je svako treće rabljeno vozilo prodano s lažnim brojem prijeđenih kilometara, a konzervativne procjene govore kako se prouzročena šteta u Luksemburgu, Francuskoj, Nizozemskoj i Njemačkoj kreće od 1,5 do 2,9 milijardi eura na godinu. Primjenom na cijelu Europsku uniju, riječ je o 5,6 do 9,6 milijardi eura godišnje” (<https://www.hak.hr/vijest/170/upozorenje-kupcima-rabljenih-vozila-prevare-s-vracanjem-kilometraze>).

Problem krivotvorenja kilometraže na automobilima, potaknulo je BMW na stvaranje blockchain sustava koji bi riješio problem krivotvorenja kilometraže. Sustav je zamišljen kao javni blockchain koji omogućava stvaranje digitalnog zapisa koji sadržava informacije o njihovim vozilima, poput prijeđenih kilometara, popravaka i broju vlasnika koji su posjedovali vozilo. Digitalni zapis implementiran je putem pametnih ugovora nazvanih “VerifyCar”. Sustav bi prikupljao, putem ugrađenog hardwarea u automobilima, u stvarnom vremenu informacije poput prijeđenih kilometara. Upravljanje tako prikupljenim podacima, koji su pohranjeni na blockchainu, bilo bi prepušteno vlasnicima automobila. Vlasnik odlučuje želi li proslijediti informacije o svom vozilu ovlaštenom servisu ili potencijalnom budućem kupcu. Primateelj informacija može usporediti dobivene informacije s informacijama pohranjenim na blockchainu, te ukoliko se informacije podudaraju, primatelj zna da je informacija o podacima vozila vjerodostojna. Takav pristup problemu riješio bi mogućnost manipulacija i krivotvorenja informacijama u automobilskoj industriji.

6.2 Tržište digitalnih kartica

Tržište digitalnim karticama trenutno je jedno od najpopularnijih tržišta kada su u pitanju digitalne imovine. Vrijednost takve imovine zbog njene rijetkosti često doseže velike iznose.

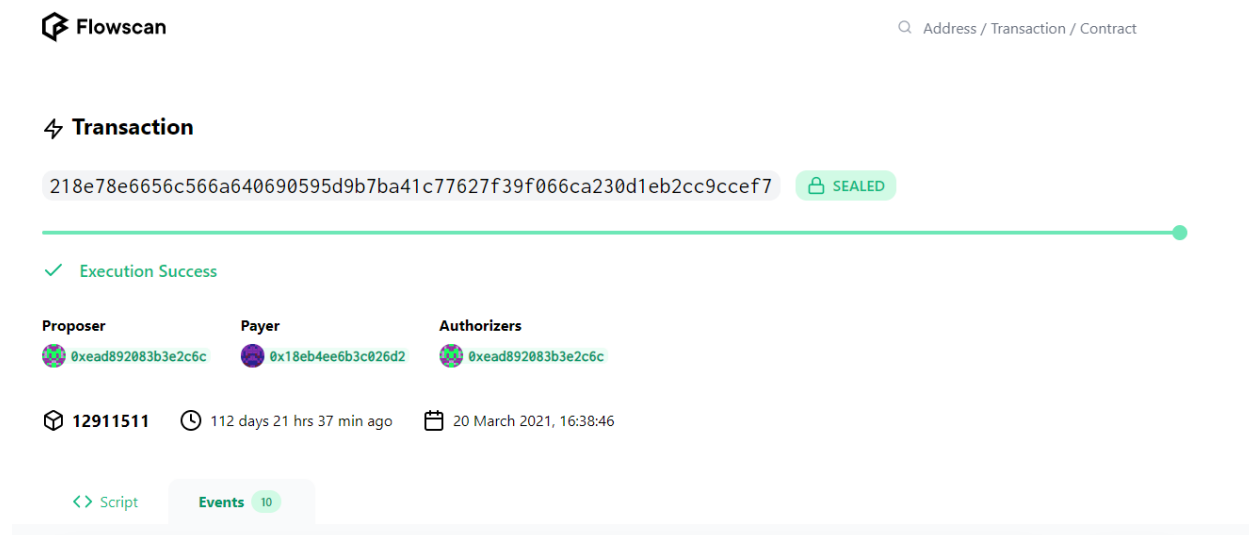
Nbatopshot platforma bazirana je na blockchainu koji nudi mogućnost skupljanja kolekcija takozvanih sportskih trenutaka. Svaki pojedinačni sportski trenutak u obliku kratkog videozapisa licenciran je službeno od strane američke košarkaške lige. Platforma radi na način da NBA izrezuje najbolje trenutke s utakmice u kratke videozapise te u suradnji s tvrtkom Dapper Labs odlučuje koliko takvih trenutaka pušta u opticaj. Svaka pojedinačna kartica unesena je na blockchain koji garantira jedinstvenost iste te nemogućnost kopiranja i manipulacije video zapisa. Postoji posebno tržište na kojem se takve digitalne vrijednosti mogu razmjenjivati. Vrijednost kartica određuje i broj tih kartica koje su puštene u opticaj, vrijednost samog trenutka u videozapisu, u sportskom smislu i slično. Početna stranica Topshot trgovine digitalnim karticama prikazana je na Slici 12.



Slika 11. Nbatopshot tržište kartica

(Izvor: <https://nbatopshot.com/marketplace>)

Svaka digitalna kartica koja se prodaje putem Nbatopshota zabilježena je na blockchainu. Primjer kako izgleda digitalna kartica na blockchainu prikazan je na Slici 13.



Slika 12. Hash transakcija digitalne kartice

(Izvor: <https://flowscan.org/>)

7. Blockchain informacijski sustavi

Informacije su neizbježan dio svakog poslovanja. Svako poduzeće teži za što kvalitetnijim, preciznijim i bržim upravljanjem informacijama. Blockchain, arhitektura kao podloga za upravljanje informacijskim resursima, idealna je upravo zbog mogućnosti koje ta tehnologija nudi. Putem blockchaina moguće je gotovo istovremeno slati veliku količinu informacija, na način da su informacije javno dostupne svima kojima su namijenjene te je moguće pratiti cijeli tijek informacije od njenog nastanka. Informacijski sustavi temeljeni na blockchainu omogućili bi svim korisnicima u takvom sustavu da aktivno sudjeluju u upravljanju informacijama te bi svaka promjena informacija ostala trajno zapisana na sami blockchain. Uvođenjem blockchain tehnologije u poslovne sustave poduzeća, moguće je ubrzati tijek informacija između pojedinih funkcija i procesa u samom poduzeću. Svaki poslovni sustav danas sastoji se od određenih informacijskih tokova koji prosljeđuju informacije na razne funkcije. Pomoću blockchaina tijek informacija, ne samo da bi bio ubrzan, već se isti može raditi potpuno transparentno te se svaki događaj u poduzeću može retrospektivno pratiti.

7.1 Uloga pametnih ugovora u poslovnim sustavima

Svaki poslovni sustav ima određene radnje koje se nakon nekog vremena ponavljaju. U tom slučaju idealno rješenje za automatizaciju takvih radnji su pametni ugovori. Primjerice, ukoliko tvrtka ili poduzeće naručuje neku komponentu u istom vremenskom razmaku od dobavljača, moguće je putem pametnih ugovora automatizirati nabavku te komponente. Prilikom takvih operacija, putem pametnih ugovora, plaćanje takve nabavke isto bi bilo automatizirano. Svaki takav zahtjev poduzeća bi mogla sama definirati te implementirati u pametne ugovore. Korištenje pametnih ugovora u poslovanju moglo bi uštedjeti vrijeme koje je potrebno za procese koji inače zahtijevaju posrednike. Eliminacija posrednika učinila bi takav sustav i novčano efikasnijim. Ukoliko je sigurnost ili privatnost jedan od zahtjeva poslovnih sustava, pametni ugovori garantiraju kako će samo ovlaštene osobe imati pravo pristupa informacijama. Međutim, iako su pametni ugovori zanimljiv alat za provedbu određenih procesa u poslovanju, ljudski faktor pogreške i dalje je prisutan. Dovoljna je jedna pogreška prilikom postavljanja uvjeta u pametnim ugovorima zbog čega je narušena možda i najveća prednost takvih ugovora, automatizacija poslovanja.

8. Zaključak

Blockchain tehnologija, od svoje pojave 2009. godine, kontinuirano napreduje. Iako prvotno namijenjena digitalnoj valuti, vrijeme je pokazalo da se blockchain može primijeniti na gotovo sve procese koji danas koriste centralizirane sustave. Razvojem i pojavom novih generacija blockchain struktura te omogućavanje izvedbe decentraliziranih aplikacija i pametnih ugovora, otvaraju se vrata stvaranju jedinstvenih digitalnih vrijednosti. Blockchain je alat koji rješava problem s dokazivanjem integriteta informacija i općenito upravljanjem velikim volumenom informacija koje su danas u opticaju. Produkt takve tehnologije, koja kombinira blockchain, pametne ugovore, tokene i decentralizirane aplikacije, jedinstvena je digitalna imovina. Takva vrsta jedinstvene digitalne imovine ujedno je i jedinstvena digitalna vrijednost. Trajno je zapisana na blockchain infrastrukturi s vjerodostojnim informacijama te potvrdom integriteta. Prvotno samo ideja osobe ili organizacije pod pseudonimom Satoshi Nakamoto i njegovog peer to peer elektroničkog novca dovela je do razvoja potpuno nove informatičke industrije pa i ekonomije u digitalnom svijetu. Blockchain ne služi isključivo za stvaranje kriptovaluta, već svoj potencijal može primijeniti na sve grane tehnologije te donijeti revoluciju na području informatičke industrije, poput revolucije i značaja koju je donijela pojava interneta.

9. Literatura

1. Delia Babeanu D., Valerica M. , Gavrilă A. (2009), *STRATEGIC OUTLINES: BETWEEN VALUE AND DIGITAL ASSETS MANAGEMENT*. Bucharest, Bucharest Academy of Economic Studies dostupno na: https://www.researchgate.net/publication/46559484_STRATEGIC_OUTLINES_BETWEEN_VALUE_AND_DIGITAL_ASSETS_MANAGEMENT
2. Lamport L., Shostak R., and Pease M. , *The Byzantine Generals Problem*. (1982). SRI International, dostupno na: <https://lamport.azurewebsites.net/pubs/byz.pdf>
3. Menezes A., van Oorschot P, and Vanstone S., *Handbook of Applied Cryptography*. (1996). CRC Press; 1st edition , dostupno na: <https://cacr.uwaterloo.ca/hac/>
4. Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, (2008), dostupno na: <https://bitcoin.org/bitcoin.pdf>
5. Viriyasitavat W., Hoonsopon D., *Blockchain Characteristics and Consensus in Modern Business Processes*. (2018). Chulalongkorn, Chulalongkorn University, dostupno na: https://www.researchgate.net/publication/326680277_Blockchain_Characteristics_and_Consensus_in_Modern_Business_Processes
6. Zelenika R. *Metodologija i tehnologija izrade znanstvenog i stručnog djela*, (1998). Ekonomski fakultet Sveučilišta u Rijeci, Rijeka.
7. Žugaj M. *METODOLOGIJA ZNANSTVENOISTRAŽIVAČKOG RADA*, (1997). Fakultet organizacije i informatike, Varaždin, 1997. dostupno na: <https://hrcak.srce.hr/file/331356>

Internet izvori

8. Blockchain Council <https://www.blockchain-council.org/blockchain/a-quick-guide-to-fungible-vs-non-fungible-tokens/> [pristupljeno: 12. srpnja 2021].
9. Centar informacijske sigurnosti <https://www.cis.hr/files/dokumenti/CIS-DOC-2011-02-003.pdf> [pristupljeno: 2. srpnja 2021].

10. Centar koordinacijskih tijela za provedbu prava intelektualnog vlasništva u Republici Hrvatskoj. <http://www.stop-krivotvorinama-i-piratstvu.hr/hr/krivotvorenje-i-piratstvo/osobito-pogodeni-ind-sektori/zabavni-sadrzaji-i-softver/> [pristupljeno: 5. srpnja 2021].
11. Digital Asset Management News <https://digitalassetmanagementnews.org/features/defining-digital-assets/> [pristupljeno: 30. lipnja 2021].
12. Ethereum <https://eth.wiki/en/concepts/ethash/ethash> [pristupljeno: 10. srpnja 2021].
13. HAK(<https://www.hak.hr/vijest/170/upozorenje-kupcima-rabljenih-vozila-prevare-s-vracanjem-kilometraze>) [pristupljeno: 3. rujna 2021].
14. Investopedia <https://www.investopedia.com/terms/c/cryptocurrency.asp> [pristupljeno: 30. lipnja 2021].
15. Investopedia <https://www.investopedia.com/terms/c/crypto-token.asp> [pristupljeno: 30. lipnja 2021].
16. Lexico.com <https://www.lexico.com/definition/blockchain> [pristupljeno: 5. srpnja 2021].
17. McAfee <https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/tokenization-vs-encryption.html> [pristupljeno: 6. srpnja 2021].
18. Moj-bankar <https://www.moj-bankar.hr/Kazalo/N/Nematerijalna-imovina> [pristupljeno: 29. lipnja 2021].
19. Mrežno izdanje *Hrvatske enciklopedije* <https://enciklopedija.hr/Natuknica.aspx?ID=65496> [pristupljeno: 29. lipnja 2021].
20. Mrežno izdanje *Hrvatske enciklopedije* [pristupljeno: 10. srpnja 2021]. <https://www.enciklopedija.hr/natuknica.aspx?id=63011> [pristupljeno: 11. srpnja 2021].
21. Poslovni je tjednik *Lider*<https://lider.media/poslovna-scena/svijet/infografika-rastuca-vrijednost-nematerijalne-imovine-136315> [pristupljeno: 2. srpnja 2021].
22. Pravni i poslovni informacijski sustav <https://www.iusinfo.hr/aktualno/u-sredistu/45492> [pristupljeno: 11. srpnja 2021].
23. U.S. Bureau of Economic Analysis Izvor: <https://apps.bea.gov/scb/2019/05-may/0519-digital-economy.html> [pristupljeno: 2. srpnja 2021].
24. Web secure payment gateway <https://www.wspay.info/cd/137/tokenizirane-transakcije-transakcije-sa-spremljenim-karticama> [pristupljeno: 12. srpnja 2021].

10. Popis slika

Slika 1. Vrijednost digitalne ekonomije	5
Slika 2. Transakcije na bitcoin blockchainu	10
Slika 3. Aktivne adrese	11
Slika 4. Ukupan broj adresa	12
Slika 5. Cijena Bitcoin naknade za transakciju	13
Slika 6. Tijek transakcije u blockchainu	15
Slika 7. Merkleovo stablo	16
Slika 8. Pow algoritmi	18
Slika 9. Problem bizantskih generala	21
Slika 10. Uniswap aplikacija	28
Slika 12. Nbatopshot tržište kartica	30
Slika 13. Hash transakcija digitalne kartice	31