Sigurnost komunikacije korištenjem blockchain tehnologije u IoT sustavima

Smontara, Bruno

Sigurnost komunikacije korištenjem blockchain tehnologije u IoT sustavima

Smontara, Bruno

Veleučilište u Karlovcu

Strojarski odjel

Stručni studij mehatronike

Bruno Smontara

SIGURNOST KOMUNIKACIJE KORIŠTENJEM BLOCKCHAIN TEHNOLOGIJE U IoT-u

ZAVRŠNI RAD

Karlovac, 2019. godina

Karlovac University of Applied Science
Mechanical Engineering Department
Professional undergraduate study of Mechatronics

Bruno Smontara

SECURITY OF COMMUNICATION USING BLOCKCHAIN TECHNOLOGY IN IOT

Final paper

Karlovac, 2019.

Veleučilište u Karlovcu

Strojarski odjel

Stručni studij mehatronike

Bruno Smontara

SIGURNOST KOMUNIKACIJE KORIŠTENJEM BLOCKCHAIN TEHNOLOGIJE U IoT-u

ZAVRŠNI RAD

Mentor: dr. sc. Adam Stančić, viši predavač

Karlovac, 2019. godina

PREDGOVOR

Izjavljujem da sam završni rad na temu „Sigurnost komunikacije korištenjem Blockchain tehnologije u IoT-u“ izradio samostalno koristeći navedenu literaturu i stečeno znanje tijekom studija, uz pomoć mentora dr.sc. Adama Stančića, kojem se ovim putem zahvaljujem.

Bruno Smontara

SAŽETAK

Mogućnosti Interneta stvari (IoT) povećavaju se iz dana u dan zahvaljujući napretku informacijsko-komunikacijske tehnologije. U budućnosti sve što će se moći povezati bit će povezano i dostupno bilo kada i bilo gdje. Zbog toga javlja se problem sigurnosti podataka na Internetu.

Prilikom slanja podataka između dviju osoba koriste se centralizirani serveri kao posrednici u njihovoj komunikaciji koji pohranjuju podatke i prosljeđuju ih osobi kojoj su namijenjeni. Blockchain tehnologija umjesto centraliziranih servera koristi decentraliziranu mrežu nepoznatih računala koja potvrđuju informacije na bazi specifičnog algoritma bez posrednika. Prilikom potvrđivanja informacija, Blockchain tehnologija koristi hash-funkcije kojima nije moguće izmijeniti prvotnu informaciju bez posljedica koje se očituju u hash-u (šifriranoj poruci).

U ovom radu bit će prikazani Bitcoin i Elastos kao primjeri praktične implementacije Blockchain tehnologije koji svojim sigurnosnim metodama mogu dati kvalitetnu podlogu u rješavanju pitanja sigurnosti Interneta stvari.

Ključne riječi: Internet stvari, Blockchain tehnologija, funkcija sažetka, sigurnost

SUMMARY

The capabilities of the Internet of Things (IoT) are increasing day by day thanks to advances in information and communication technology. In the future, everything that will be able to be connected will be connected and available anytime, anywhere. Therefore, there is a problem of data security on the Internet. When sending data between two parties, centralized servers are used as intermediaries in their communication, which store the data and pass it on to the person for whom it is intended. Blockchain technology uses a decentralized network of unknown computers instead of centralized servers that validate information based on a specific algorithm without need for middleman. When validating information, Blockchain technology uses hash functions that cannot modify the original information without the consequences of different hash (encrypted message). This paper will show Bitcoin and Elastos as examples of the practical implementation of Blockchain technology that can assure security of Internet of things applying its safety methods.

Key words: Internet of Things, Blockchain technology, hash

SADRŽAJ

1. UVOD

Internet stvari predstavlja globalnu mrežnu infrastrukturu koju čine uređaji s mogućnošću povezivanja na Internet. Mreža povezanih uređaja omogućila je jednostavnije nadziranje i kontrolu uređaja na daljinu, ali i komunikaciju uređaja s ostalim uređajima u mreži. Sve veća uporaba uređaja povezanih na Internet dovela je u pitanje sigurnost komunikacije i privatnost podataka korisnika koji su podložni zlouporabi. Kao prijedlog rješavanju problema zlouporabe Interneta stvari objašnjen je koncept temeljen na Blockchain tehnologiji kojim se osigurava privatnost komunikacije te provjera integriteta podataka pohranjenih na Internetu. U radu je provedeno testiranje kriptografskih funkcija sažetka koje se koriste u dokazivanju vjerodostojnosti pohranjenih podataka te je kreiran blokovni lanac sačinjen od pet povezanih blokova. Rad se sastoji od nekoliko poglavlja u kojima je povezana tematika Interneta stvari i Blockchain tehnologije. U drugom poglavlju opisan je Internet stvari te je navedeno područje primjene u svakodnevnom životu. U trećem poglavlju opisane su opasnosti prilikom korištenja Interneta stvari provođenjem napada koji dovode u opasnost sigurnost podataka na Internetu. U četvrtom poglavlju opisana je Blockchain tehnologija kao temelj nastanka kriptovaluta od kojih je najpoznatija Bitcoin. Opisane su kriptografske funkcije sažetka koje su glavna značajka Blockchain tehnologije te opisani sustavi Bitcoin i Elastos kao mogućnosti rješavanja sigurnosti komunikacije sustava Interneta stvari. U posljednjem poglavlju provedena su testiranja nekoliko vrsta različitih kriptografskih funkcija sažetka na više tipova datoteka sa ciljem dokazivanja integriteta podataka prilikom promjena njihovih sadržaja. Kreiran je i blokovni lanac od pet blokova u kojima su pohranjene poruke nepromjenjivog sadržaja. Blokovi su povezani na način da se svaki novi blok referencira na svog prethodnika te tako osigurava nepromjenjivost sadržaja lanca.

2. INTERNET STVARI

Internet stvari (engl. Internet of Things, IoT) je globalna mrežna infrastruktura samokonfigurirajućih sposobnosti. Zasniva se na standardima i komunikacijskim protokolima gdje vlastite identitete imaju fizičke i virtualne stvari. Sastoji se od uređaja koji imaju jedinstvene identitete te su povezani na Internet [1].

Mnogi uređaji kao pametni telefoni te osobna računala već sada posjeduju svoje jedinstvene identitete te su povezani na Internet. Također, pod pojmom IoT-a promatraju se stvari nad kojima se vrši nadziranje i upravljanje, a koje nisu uobičajeno povezane s Internetom.

U 2019. godini najveća perspektiva Interneta stvari može se uočiti u medicini gdje postoje ideje kako bi recimo pametne narukvice, koje se koriste za očitanje otkucaja srca, mogle u hitnim slučajevima predati podatke o otkucaju srca medicinskoj ustanovi. Također, Internet stvari koristi se kod unaprjeđivanja uobičajenih kućanskih aparata, razvoja još veće sigurnosti automobila pa sve do pametnih gradova [2].

Slika 1.: Mogućnosti primjene Interneta stvari [2]

Broj pametnih uređaja u kućanstvu povećava se iz dana u dan. Uređaje kao televizori, hladnjaci, audio sustavi, strojevi za pranje rublja ili posuđa bilo bi izrazito

teško koristiti ukoliko bi svaki od navedenih zahtijevao vlastiti daljinski upravljač. Povezanost kućanskih uređaja na Internet omogućuje korištenje mobilne aplikacije kojom korisnik može upravljati uređajima na daljinu te nadzirati stanja uređaja i okoline pomoću senzora kojima su opremljena.

Pametni strojevi za pranje ili sušenje rublja omogućili bi korisniku uključivanje u rad kada on to želi te ga obavijestili o kraju ciklusa.

Pametni termostati korisniku bi olakšali kontrolu temperature kućanstva na daljinu. Tako bi korisnik ljeti ili zimi mogao doći u već predodređenu ambijentalnu temperaturu. Uređaji poput električnih grijalica, plinskih bojlera, sustava za centralno grijanje te rashladnih klima uređaja autonomno bi radili na održavanju željene temperature.

Pametni hladnjaci mogli bi pratiti stanja napunjenosti te obavijestiti korisnika ukoliko je namjernice potrebno kupiti ili pak voditi brigu o isteku roka valjanosti proizvoda.

Pametna rasvjeta u kućanstvu može pridonijeti smanjenju potrošnje električne energije prilagođavajući se uvjetima u prostoru. Rasvjeta se može uključivati i isključivati te prilagođavati jakost svjetla u ovisnosti o količini svijetlosti koje dolazi izvan prostorije.

Pametan video nadzor mogao bi korisnika obavijestiti u slučaju provale u kućanstvo te mu pružiti uvid na temelju poslane fotografije ili videozapisa. Također, servisi u oblaku mogli bi o događaju obavijestiti susjede ili policiju.

Pametni detektori dima i plinova imali bi ulogu obavijestiti korisnika ili vatrogasce o opasnosti te po potrebi kontrolirati druge uređaje na mreži kako bi izbjegli još veće posljedice. Npr. ukoliko dođe do istjecanja zapaljivih plinova, automatski bi se isključili ostali pametni uređaji u kućanstvu koji bi mogli uzrokovati iskrenje i otvoreni plamen.

Migracije stanovništva, klimatske promjene te industrijski i ekonomski razvoj mogu uzrokovati rast potreba za električnom energijom. Ona može dovesti do opterećenja električne mreže koja ima velik utjecaj na korisnike i infrastrukturu. Pametna električna mreža pružila bi mogućnost dvosmjerne komunikacije između

proizvođača električne energije i potrošača. Time bi se jednostavnije mogle predvidjeti nagle promjene u potrošnji električne energije te bi u slučaju kvara distributer imao povratnu informaciju bez potrebe prijave kvara od strane korisnika. Mrežu na mjestu nastanka kvara bilo bi moguće premostiti te ju izolirati od ostalih korisnika. Osim toga, pomoću pametnih brojila električne energije korisnici su u mogućnosti nadzirati potrošnju u svome kućanstvu ili poslovnim subjektima na daljinu [3].

Pametna parkirna mjesta pružala bi vozačima informacije o slobodnim parkirnim mjestima te smanjila zastoje na prometnicama. U sklopu IoT sustava svako parkirno mjesto senzorima bi detektiralo prisutnost automobila. Vozačima bi takve informacije bile dostupne putem pametnog telefona, tableta ili ugrađenog navigacijskog sustava.

Pametne prometnice pružale bi informacije vozačima o stanju na cestama. U slučaju zastoja ili prometnih nezgoda distribuirana mreža senzora i kamera postavljenih uz prometnice obavijestila bi vozača kako bi mogao pravovremeno reagirati ili promijeniti rutu. Na taj način bi se povećala sigurnost u prometu i smanjili nepotrebni zastoji.

Komunikacija svih uređaja na mreži u IoT infrastrukturi pretvorila bi gradove u živući organizam te smanjila potrebe ljudske intervencije ili ih olakšala pravovremeno intervenirajući i pružajući vjerodostojne informacije. Krajnji cilj Interneta stvari je olakšati korisnicima svakodnevni život, smanjiti potrošnju električne energije te povećati razinu sigurnosti na način da se eliminira faktor ljudske pogreške.

2. 1. Karakteristike IoT sustava

IoT sustav specifičan je po svojim karakteristikama. One zajedno omogućuju ostvarenje osnovne ideje ovog koncepta, a to je omogućavanje bežičnog povezivanja sustava uz korištenje različitih tehnologija što stvari oko nas čini sveprisutnima.

Karakteristike IoT sustava su [1]:

1. Dinamičnost i samoprilagodba: IoT uređaji mogu imati sposobnost dinamičke prilagodbe u različitim uvjetima i vršiti operacije ovisno o njihovim operacijskim stanjima. Primjerice, nadzorne kamere mogu prilagoditi svoja stanja (u normalno ili infracrveno) ovisno o tome da li je dan ili noć. Također, one prilagođavaju rezoluciju kada detektiraju kretanje objekata te uključuju ostale kamere da naprave isto. U ovom slučaju video nadzor vrši samoprilagodbu ovisno o promjenama stanja.

2. Samokonfiguracija: IoT uređaji mogu imati sposobnost samokonfiguracije dozvoljavajući velikom broju uređaja da obavljaju radnje zajedno kako bi postale funkcionalne. Jedan od svakodnevnih primjera korištenja samokonfiguracije jest praćenje vremenskih prilika. Ukoliko uređaji služe za očitanje temperature u gradu oni moraju biti svjesni susjednih uređaja kako bi sudjelovali u mjerenju srednje vrijednosti koju očitavaju.

3. Povezivanje komunikacijskih protokola: IoT uređaji mogu podržavati više komunikacijskih protokola te komunicirati s ostalim uređajima i infrastrukturom.

4. Jedinstveni identiteti: Svaki IoT uređaj posjeduje svoj jedinstveni identitet. IoT sustavi mogu imati inteligentna sučelja koja se prilagođavaju ovisno o kontekstu, dozvoljavajući komunikaciju s korisnikom koji može zatražiti informacije od uređaja, nadgledati njegova stanja te vršiti kontrolu na daljinu.

5. Integracija u informacijsku mrežu: IoT uređaji su većinom integrirani u informacijsku mrežu koja omogućuje komunikaciju i izmjenjivanje informacija s ostalim uređajima i sustavima. Takvi uređaji mogu biti prepoznati od strane mreže ili drugih uređaja te imati sposobnost predstavljanja sebe i svojih karakteristika drugim uređajima i aplikacijama. Primjerice, jedan čvor u mreži za praćenje vremenskih prilika može poslati svoja stanja drugom aktivnom čvoru u mreži kako bi komunicirali i izmjenjivali informacije.

Daljnjim razvojem ovih karakteristika omogućuje se prepoznavanje daljnjih primjena IoT sustava u različitim sektorima i područjima znanosti.

2. 2. Povijesni pregled IoT sustava

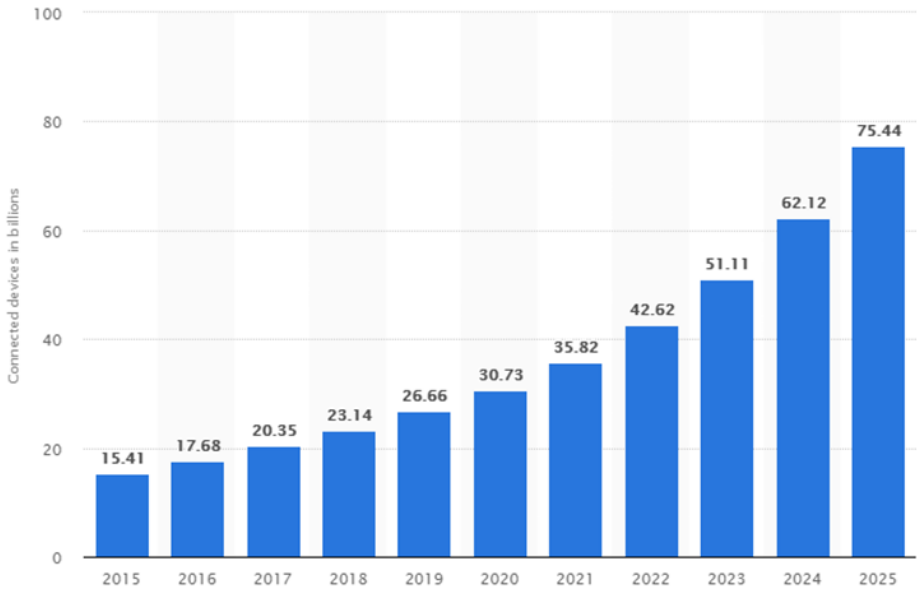
Internet kao značajna komponenta IoT-a pokrenut je od strane Ministarstva obrane SAD-a odgovornog za razvoj novih tehnologija za vojsku SAD-a pod nazivom DARPA (engl. Defense Advanced Research Projects Agency) 1962. godine te se razvio u ARPANET (engl. Advanced Research Projects Agency Network) 1969. godine. Tek 1980. godine reklamni servisi počeli su javnosti pružati podršku uporabe ARPANET-a.

Internet stvari kao koncept nije bio javno imenovan sve do 1999. godine, a jedan od prvih primjera IoT-a bio je aparat za Coca-Colu smješten u sveučilištu Carnegie Melon. Lokalni programeri spajali su se preko Interneta na aparat kako bi provjerili stanje napunjenosti pićima te jesu li ohlađena prije no što bi došli u inspekciju [4].

2003. godine pojam IoT-a počinje se pojavljivati u člancima i knjigama te je na taj način svrha razvoja IoT-a postala općepoznata. Smatra se da je pravo rođenje IoT-a bilo tijekom 2008. i 2009. godine kada je broj stvari ili objekata povezanih na Internet bio veći od broja ljudi na cijelom svijetu.

Tvrtka Gartner godišnje objavljuje izvješće vezano uz tehnologije koje dolaze, odnosno njihov *"hype"* ciklus. Svaka tehnologija u Gartnerovom izvještaju prolazi kroz nekoliko faza; faza "okidanja tehnologije", faza "vrhunca prenapuhanih očekivanja", a zatim faza "razočaranja" do faze "nagiba prosvjetljenja" sve dok ne stigne do "platoa produktivnosti" [5]. 2011. godine termin Internet stvari je dodan u godišnji Gartner Hype ciklus, a 2014. godine došao je do faze "vrhunca prenapuhanih očekivanja" [6].

O Internetu stvari se u Hrvatskoj prvi puta javno raspravljalo 2016. godine na prvoj IoT konferenciji gdje su posjetitelji mogli saznati od hrvatskih i europskih stručnjaka što je to IoT, odakle mu naziv te na koji način i gdje se može primijeniti [7]. Također, od 2011. godine održava se Tjedan Interneta stvari (engl. IoT week), godišnji europski tjedan novih saznanja na području IoT-a. Prema podacima Statista research development-a očekuje se da će do 2025. godine 75.44 milijardi uređaja biti povezani na Internet [8].



Slika 2.: Prikaz porasta broja uređaja spojenih na Internet u razdoblju od 2015. do 2025. godine [8]

3. SIGURNOST INTERNETA STVARI

Cilj Interneta stvari je čovjeku olakšati svakodnevni život. Pretpostavlja se da će kućni uređaji poput hladnjaka, pećnica, zvona za vrata, klima uređaja, kamera, ulaznih i garažnih električnih vrata biti dio Interneta stvari u puno većoj mjeri nego danas. Većina tih uređaja sposobna je prikupljati informacije iz okoline kao npr. zvuk, sliku, video, temperaturu, vlažnost zraka itd. Nezaobilazan problem koji se javlja kod naglog povećanja broja pametnih uređaja oko nas je sigurnost informacija koje se bilježe pa time dovode u pitanje čovjekovu privatnost. Ukoliko bi takvi uređaji bili kompromitirani, čovjek se više ne bi osjećao sigurno u vlastitom domu. Može se samo zamisliti kakav bi život bio uz strepnju hoće li netko imati uvid u stvari koje korisnik u svom domu radi, što govori te je li uopće kod kuće.

Istraživačka tvrtka The Economist Intelligence Unit iz Velike Britanije provela je istraživanje u osam zemalja uključujući Australiju, Kinu, Francusku, Njemačku, Japan, Južnu Koreju, Veliku Britaniju i SAD, a istraživalo se u kojoj su mjeri građani zabrinuti za privatnost osobnih podataka korištenjem IoT-a [9]. Velik dio ispitanika iskazao je najveću zabrinutost oko prikupljanja i prijenosa osobnih podataka kao i krađe identiteta te kreiranja potrošačkih obrazaca ponašanja na temelju istih. 92% ispitanika želi imati kontrolu nad informacijama koje se prikupljaju, a 57% unutar te skupine zahtjeva svoje pravo na brisanje podataka prema Općoj uredbi o zaštiti podataka (GDPR - General Data Protection Regulation). Nedostatak transparentnosti tvrtki i kontrole potrošača nad vlastitim informacijama samo produbljuju zabrinutost o privatnosti i sigurnosti.

Kao jedan od novijih primjera za zabrinutost o osobnim podacima iz 2019. godine može se navesti vodeća Crypto platforma Coinbase koja je obavijestila 3420 korisnika o nenamjernom spremanju nezaštićenih podataka za registraciju koji su pohranjeni kao običan tekst na njihovom serveru [10].

Na temelju ovih primjera vidi se da informacije na Internetu nisu sigurne u mjeri koliko bi njegovi korisnici to željeli. Stoga je važno upoznati se s novim mogućnostima rješavanja navedenih problema koji su lako rješivi korištenjem novih tehnologija poput

Blockchaina. Prije opisa Blockchain tehnologije valja se upoznati s vrstama napada na Internetu te mogućim rješenjima kako izbjeći pojedine napade i zaštititi vlastite podatke.

3. 1. Vrste napada na Internetu

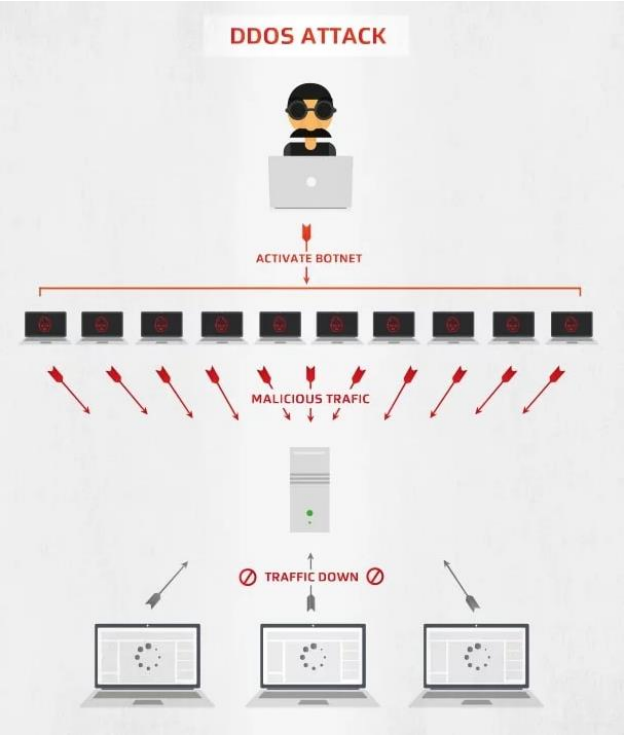
U slijedećim poglavljima navedeni su neki od učestalih vrsta napada s kojima se korisnik može susresti na Internetu, a koje ozbiljno dovode u opasnost osobne podatke svakodnevnim korištenjem Interneta stvari.

3. 1. 1. DDoS tip napada

Napad distribuiranog odbijanja usluge (engl. Distributed Denial of Service ili DDoS attack) je vrsta napada koja preplavljuje resurse sustava kako ne bi mogli odgovarati servisnim zahtjevima. DDoS napad pokreće se s velikog broja *host* uređaja koja su zaražena zlonamjernim softverom. Napadač šalje zlonamjerni softver na računala u mreži putem kontrolera. Ukoliko ga korisnik nenamjerno pokrene, njegovo računalo postaje dio *botneta* (mreža zaraženih računala) kontroliranim od strane napadača. Za razliku od napada koji služe napadaču da ostvari ili poveća pristup, DDoS ne omogućava direktnu korist napadaču. Za neke je dovoljno zadovoljstvo odbijanje usluge. Međutim, ako napadnuti resursi pripadaju poslovnom konkurentu, onda korist napadaču može biti zaista velika. Druga svrha ovoga napada može biti korištena u svrhu isključivanja sustava kako bi druga vrsta napada mogla biti izvedena [11].

DDoS je moguće zamisliti kao čekanje u prometu na prometnici s jednim trakom. Inače na toj prometnici nikada nema više od jednog ili dva automobila. Prometnica ne može podnijeti toliku količinu prometa i kao rezultat toga nastaje zastoj u kojem nema druge opcije nego čekati. U suštini, to se događa web stranici prilikom DDoS napada. Ako je web stranica preplavljena većom količinom prometa no što je namijenjeno, preopteretit će se server web stranice te ona neće moći pružati sadržaj posjetiteljima koji joj pokušavaju pristupiti. Ovu vrstu napada može biti još teže savladati zbog napadača koji se pojavljuje sa više različitih IP adresa (engl. Internet

Protocol address) diljem svijeta u isto vrijeme, što otežava određivanje izvora napada mrežnim administratorima [12].

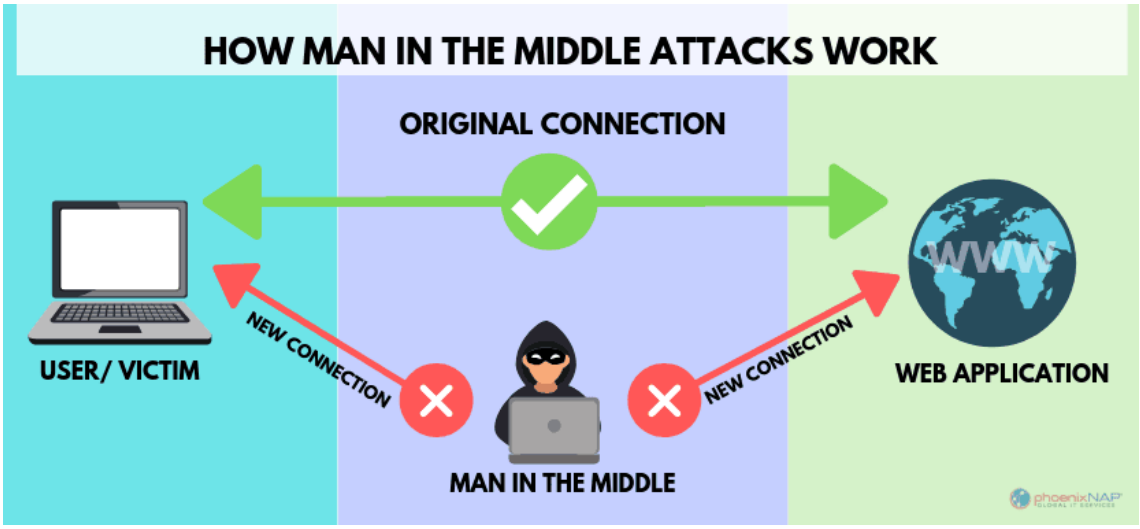


Slika 3.:Prikaz DDoS napada [13]

3. 1. 2. *Man-in-the-middle* tip napada

Napad posrednika (engl. Man-in-the-middle-attack) događa se kada zlonamjerni korisnik presretne komunikaciju između klijenta i servera. Na primjer, korisnik dobije e-mail koji izgleda kao da ga je poslala banka tražeći ga da se prijavi na svoj račun kako bi potvrdio osobne podatke. Prilikom otvaranja poveznice u e-mailu čini se kao da je pristupio web stranici banke, no zapravo osobni podaci koje korisnik upisuje završe u rukama napadača.

Man-in-the-middle napadi dolaze u dva oblika, jedan koji uključuje fizičku blizinu ciljane mete, dok drugi uključuje zlonamjeran softver (engl. malware) koji je naveden u primjeru s e-mailom te se još naziva *Man-in-the-browser* napad. Zlonamjerni korisnici obično izvršavaju ovakvu vrstu napada u dvije faze, presretanjem i dešifriranjem [14].



Slika 4.: Prikaz upada u komunikaciju između korisnika i servera [15]

3. 1. 2. 1. *Close to you* tip napada

Uobičajenim *Man-in-the-middle* napadom zlonamjerni korisnici moraju pristupiti nezaštićenom ili slabo zaštićenom usmjerivaču (engl. router). Te vrste povezivanja obično se nalaze na javnim mjestima s besplatnim pristupnim točkama bežične mreže (Wi-Fi), ali i u domovima korisnika ako nisu zaštitili svoju mrežu. Napadači mogu skenirati usmjerivač tražeći određene slabe točke kao slabe zaporke. Nakon što napadači pronađu slabo zaštićen usmjerivač, mogu se koristiti alatima za presretanje i čitanje prenesenih podataka. Uspješan *Man-in-the-middle* napad ne završava presretanjem podataka. Žrtvin kriptirani sadržaj mora biti dekriptiran kako bi napadač imao od njega koristi [14].

3. 1. 2. 2. *Man-in-the-browser* tip napada

S *Man-in-the-browser* napadom napadač traži način kako unijeti zlonamjeran softver u žrtvino računalo ili pametni telefon. Jedan od načina izvođenja ovoga napada je *phishing*. *Phishing* je aktivnost kada prevarant pošalje e-mail ili tekstualnu poruku korisniku za koju se čini da potiče iz pouzdanog izvora. Odabirom poveznice iz privitka elektroničke pošte korisnik nenamjerno učitava zlonamjerni softver na svoj uređaj. Zlonamjerni softver se zatim instalira na preglednik bez znanja korisnika. Zlonamjerni

softver bilježi podatke poslane između žrtve i ciljanih web stranica te ih šalje napadaču [14].

3. 1. 3. Načini provođenja *Man-in-the-middle* napada

Napad posrednika ostvaruje se prilikom presretanja komunikacije između klijenta i servera koju provodi zlonamjerni korisnik. Ovom vrstom napada zlonamjerni korisnik ostvaruje kontrolu nad korisnikovim uređajem na više različitih načina podvala (engl. spoof).

1. IP *spoofing*: Svaki uređaj sa mogućnošću spajanja na Internet koristi TCP/IP (engl. Transmission Control Protocol/Internet Protocol) skup protokola i ima IP adresu koja je slična kućnoj adresi korisnika. Podvalom IP adrese, napadač može prevariti korisnika tako da misli da komunicira sa željenom web stranicom koja to zapravo nije, možda dajući napadaču pristup informacijama koje inače ne bi dijelio.

2. DNS *spoofing*: DNS (engl. Domain Name System) spoofing podvala je tehnika koja navodi korisnika na lažnu web stranicu, umjesto stvarne koju namjerava posjetiti. Prilikom pretraživanja u pregledniku, korisniku može biti ponuđena stranica istoga izgleda, ali se njena IP adresa razlikuje od originalne. Žrtva DNS podvale može misliti da posjećuje sigurnu stranicu iako zapravo komunicira sa zlonamjernim korisnikom. Cilj počinitelja je preusmjeravanje prometa sa stvarne stranice ili krađa korisnikovih informacija za prijavu.

3. HTTPS *spoofing*: HTTPS (engl. Hypertext Transfer Protocol Secure) je oznaka da je web stranica sigurna tj. da je komunikacija s tom stranicom kriptirana, za razliku od HTTP (engl. Hypertext Transfer Protocol) koja nije kriptirana. Zlonamjerni korisnik može prevariti preglednik kako bi korisnik vjerovao da se radi o kriptiranoj komunikaciji, preusmjeravajući preglednik korisnika na stranicu čija komunikacija nije kriptirana. Također, on može pratiti komunikaciju te otuđiti osobne informacije koje korisnik dijeli.

4. Wi-Fi *eavesdropping*: Zlonamjerni korisnici mogu postaviti bežičnu mrežu s imenima sličnim tvrtkama koje se nalaze u blizini. Kada se korisnik poveže na takvu

mrežu, napadač može pratiti korisnikove aktivnosti te presretati osobne informacije za prijavu, informacije kartičnih plaćanja itd.

5. *Stealing browser cookies*: Kolačići (engl. cookies) u pregledniku su podaci koje web stranica pohranjuje na računalu korisnika. Na primjer, internet trgovac može pohraniti osobne informacije koje korisnik unese te stavke u košarici tako da ih ne treba poslije ponovo unositi. Zlonamjerni korisnici mogu otuđiti takve podatke. Budući da se u kolačićima pohranjuju podaci korisnikovih pregledavanja, napadač može dobiti pristup zaporkama, adresama i ostalim osjetljivim informacijama korisnika [14].

3. 2. Mogućnosti izbjegavanja napada

Kao jedno od rješenja izbjegavanja DDoS napada, gdje napadač glumeći identitete drugih korisnika preplavljuje resurse sustava, mogu se koristiti izolirana okruženja za pokretanje decentraliziranih aplikacija. Provođenje DDoS napada korištenjem tuđih uređaja zahtjevalo bi instalaciju zlonamjernog softvera koji nije u mogućnosti napustiti virtualni stroj korisnika kako bi uspješno zarazio resurse sustava korisnika. Na taj način nije moguće kreirati zahtjeve korištenjem uređaja drugih korisnika.

Kako bi izbjegli *Man-in-the-middle* napade potrebno je osigurati identitete aplikacija kako korisnici ne bi mogli biti prevareni u slučaju da naiđu na lažnu aplikaciju kojom bi zatim preuzeli zlonamjerni softver. Ukoliko do toga i dođe, aplikacije moraju biti pokretane u izoliranom okruženju bez izravnog povezivanja na Internet te bi zlonamjeran softver bio automatski izbrisan prekidom rada aplikacije prije no što bi mogao doći do resursa sustava pametnog uređaja. Navedena rješenja bit će detaljnije objašnjena u tehnologiji Elastosa [16].

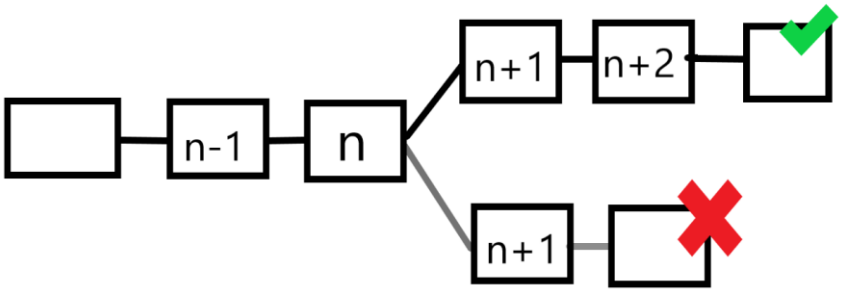
4. BLOCKCHAIN

Blockchain je vremenski označen niz nepromjenjivih zapisa kojim upravlja mreža računala, a koja nisu u vlasništvu samo jedne osobe te nema centraliziranog nadzora [17]. Termin *blockchain* jednostavno se može prevesti kao lanac blokova. U ovom slučaju, pojam blokova odnosi se na podatkovne blokove koji su povezani u jednosmjerni lanac. Struktura blokovnih podataka je uređeni zapis blokova transakcija. Blokovi su povezani unatrag tako da se svaki odnosi na onaj prethodni blok u lancu. Povezivanje blokova u lanac temeljeno je na kriptografiji [18].

Blockchain se može vizualizirati kao vertikalni niz blokova smještenih jedan preko drugoga tako da prvi blok služi kao temelj toga niza. Tako vizualizirani blokovi su rezultirali izrazom *height* ili visinom bloka, a odnosi se na udaljenost od prvoga bloka i *top* što označava najnoviji dodani blok.

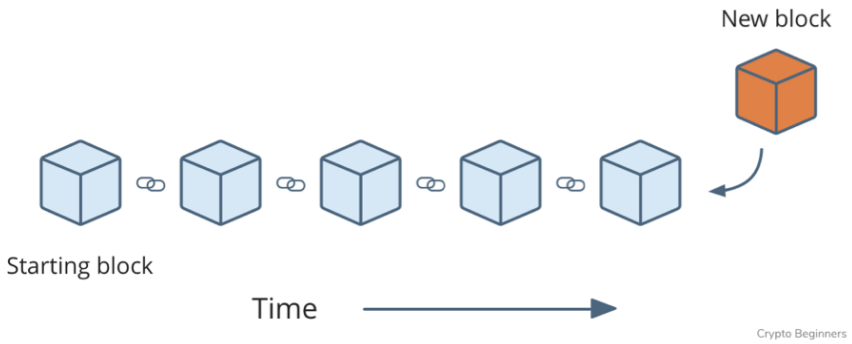
Svaki blok u blockchainu identificiran je pomoću hash vrijednosti (vrijednost funkcije sažetka) generirane korištenjem SHA-256 kriptografske funkcije sažetka na zaglavlju bloka. Također, svaki blok referencira prethodni blok poznatiji kao *parent block* pomoću prethodne hash vrijednosti bloka smještene u zaglavlju bloka. Drugim riječima, svaki blok sadrži hash vrijednost svoga *parent* bloka unutar svoga zaglavlja. Ta sekvenca hash vrijednosti koja povezuje svaki blok sa svojim *parent* blokom čini lanac koji seže sve do prvoga bloka ikad napravljenog, poznatog kao *genesis block*. Naime, blok ima samo jednog roditelja (engl. parent block), ali na trenutak može imati više „djece“. Svako dijete odnosi se na isti blok kao i roditelj te posjeduje istu roditeljsku hash vrijednost u polju koje sadrži hash vrijednost prethodnog bloka.

Ukoliko više rudara otkrije različite blokove u isto vrijeme, lanac se dijeli na dva različita dijela na način da se sastoji od jednoga lanca do trenutka dijeljenja a nakon toga se dijeli u dva lanca izgledom podsjećajući na vilicu. Stoga se takva situacija naziva *fork*. Na kraju samo jedan dječji blok postaje dio lanca i *fork* je riješen. Ako se na roditeljskom bloku dogodi neka promjena, mijenja se hash vrijednost roditeljskog bloka.



Slika 5.: Prikaz dijeljenja blokovnog lanca (engl. fork) [19]

Promjena hash vrijednosti roditeljskog bloka zahtjeva promjenu pokazivača prethodnog bloka hash vrijednosti njegovog djeteta. To zauzvrat rezultira promjenom hash vrijednosti djeteta koje zahtjeva promjenu pokazivača na unuka koje naposlijetku mijenja hash vrijednost unuka i tako dalje. Ovaj kaskadni efekt osigurava da kada blok ima više generacija koje ga slijede, ne može biti promijenjen bez prisile na ponovnu rekalkulaciju svih slijedećih blokova. Budući da rekalkulacija zahtjeva veliku računalnu snagu, postojanje dugog lanca blokova čini blockchainovu dugu povijest nepromjenjivom, a to je i ključna karakteristika sigurnosti Bitcoina, jedne od decentraliziranih mreža koja koristi Blockchain tehnologiju [20]. U nastavku teksta bit će prikazane osnovne funkcionalnosti blockchaina kroz primjere njegovog iskorištavanja u Bitcoinu i Elastosu.



Slika 6.: Vizualni prikaz spajanja blokova u lanac blokova [21]

4. 1. Razvoj Bitcoina

Prva spomen digitalnih valuta seže u 1998. godinu; više od desetljeća prije nastanka Bitcoina. Tada je koncept digitalne valute predstavio računalni inženjer Wei Dai pod nazivom B-money [22]. Iste godine pojavljuje se projekt pod nazivom Bit Gold predstavljen od strane jednog od prvih začetnika Blockchain tehnologije, kriptografa Nicka Szabe [22]. Iako navedeni projekti nikada nisu ugledali svijetlo dana, zasigurno su poslužili kao dobar temelj nastanku Bitcoina.

Bitcoin je 2008. godine pod nazivom Bitcoin: A peer-to-peer Electronic Cash System predstavljen javnosti od strane pojedinca ili skupine ljudi pod pseudo imenom Satoshi Nakamoto [23]. U objavi je predstavljen opis decentraliziranog elektroničkog novca koji kao glavnu značajku ističe distribuirani konsenzus dokaz rada (engl. Proof-Of-Work) čime je prvi puta riješen problem dvostrukog trošenja istoga iznosa bez potrebe za središnjim nadzorom.

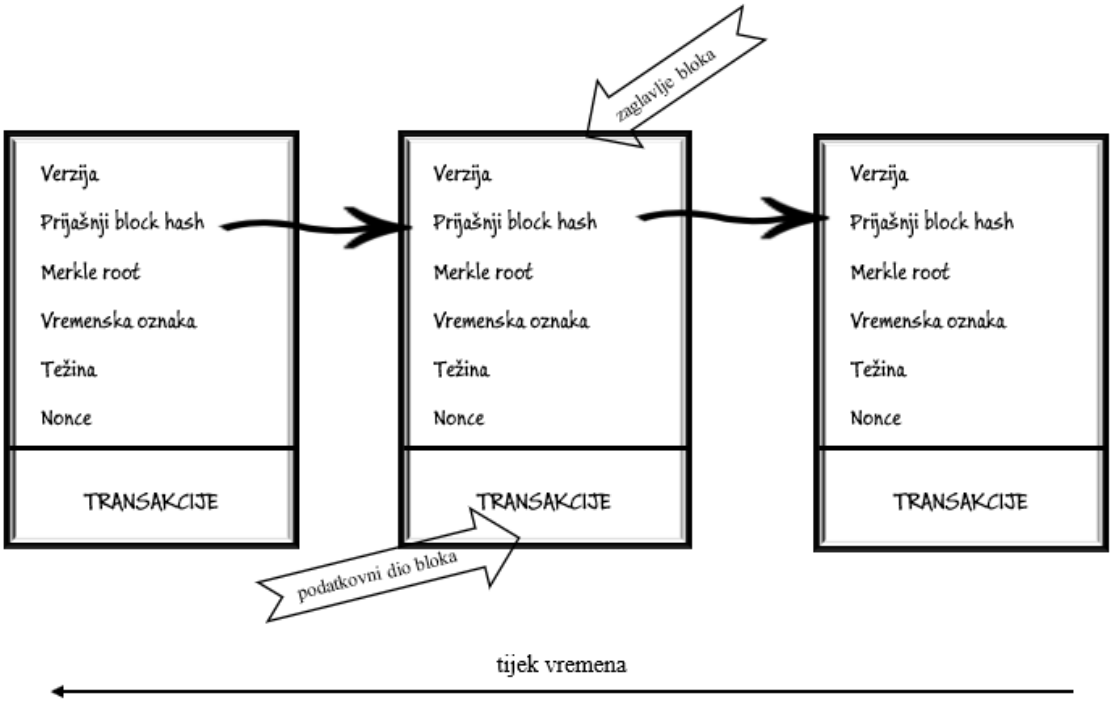
Softver je prvi puta pokrenut 2009. godine te je započeto rudarenje Bitcoina kreiranjem prvog bloka pod nazivom Genesis block. 2011. godine misteriozni se kreator Bitcoina povukao iz javnosti te mu se tada gubi svaki trag. Budući da je kôd javno dostupan, odgovornost razvoja mreže ostavljena je u rukama dobrovoljaca kao još jedan pokazatelj decentralizirane karakteristike cijelog sustava [23].

4. 2. Proces rudarenja

Održivost digitalne valute Bitcoin temelji se na radu mreže računala pod nazivom rudarenje. Rudarenje je postupak u kojem se kreiraju novi Bitcoini svakim pronađenim blokom. Također, potvrđuje se valjanost transakcija na mreži. Što je više rudara uključeno u proces rudarenja, to će mreža biti sigurnija na način da zlonamjernim korisnicima otežava ostvarivanje većine ukupne procesorske snage mreže. Ona bi morala iznositi više od 50% kako bi zlonamjerni korisnici ostvarili prednost u brzini rekalkulacije blokova, čime bi bili u mogućnosti kreirati dvostruko trošenje istog novca.

Blok u Bitcoin mreži sastoji se od podatkovnog dijela i zaglavlja te pokazivača koji uvijek pokazuje prethodni blok. Čvor koji rudari mora vrijednost funkcije sažetka prethodnog izrudarenog bloka pohraniti u zaglavlje bloka kao *Previous block hash*. Unutar podatkovnog dijela nalaze se sve transakcije iz određenog vremenskog perioda koje tek trebaju biti potvrđene kao valjane. Transakcije iz podatkovnog dijela pohranjuju se u zaglavlje računajući vrijednost funkcije sažetka *Merkle tree* metodom koja osigurava učinkovitu i sigurnu verifikaciju velikih struktura podataka. *Merkle tree* izgleda kao naopako okrenuto drvo s korijenom prema gore, a granama prema dolje na čijim se krajevima nalazi lišće. Svakoj transakciji zasebno se računa vrijednost funkcije sažetka i ona postaje dio lisnog čvora. Svakom susjednom paru lisnih čvorova zajedno se računa vrijednost funkcije sažetka te pohranjuje kat iznad kao novi čvor i tako redom prema vrhu drveta u ovom slučaju korijena. Posljednja hash vrijednost naziva se čvor korijena te predstavlja rješenje zvano *Merkle root* i pohranjuje se u zaglavlje bloka. U zaglavlju bloka se još nalaze vrijeme (engl. time-stamp), težina bloka (engl. difficulty target) koja označava kompleksnost rješavanja bloka, verzije softvera za rudarenje, te na kraju broja *nonce* koji je postavljen na nulu. Broj *nonce* predstavlja jedinu nepoznanicu u zaglavlju bloka te nije javno obznanjen u mreži. Čvor koji rudari mijenja parametar *nonce* tako da kreće od nule uvećavajući svakim pokušajem broj za jedan. Rudarenje novog bloka traje sve dok se dobivena hash vrijednost zaglavlja ne poklopi sa hash vrijednošću koja predstavlja rješenje toga bloka. Upravo ta radnja ukazuje na kompleksnost rješavanja blokova te zahtijeva velike količine električne energije utrošene na njen rad. Prosječno vrijeme pronalaska bloka u Bitcoin mreži iznosi 10 minuta. Zbog svojstva hash funkcije njeno rješenje nikako nije moguće pretpostaviti niti

naći brži put do cilja nego nasumično pogađati vrijednost *nonce*. To ujedno čini Bitcoin mrežu sigurnom od zlonamjerne upotrebe prisiljavajući zlonamjerne korisnike na utrošak električne energije koji je najčešće neisplativ [20].



Slika 7.: Izgled bloka prilikom rudarenja

Rudarenje Bitcoina obavlja se uređajima zvanim „ASIC Miners" što označava integrirane krugove posebne namjene (engl. Application Specific Integrated Circuits) u ovom slučaju za rudarenje algoritma SHA-256.

Slika 8.: Prikaz najnovijeg uređaja tvrtke Antminer S17 PRO, 50TH/s što označava sposobnost uređaja na izvršavanje hash funkcije 50 bilijuna puta u sekundi [24]

4. 3. SHA-256

Kriptografske funkcije sažetka matematičke su funkcije korištene u kriptografiji koje jednostavno izračunavaju vrijednosti funkcije sažetka od dobivene ulazne poruke, ali jako ne mogu reproducirati ulaznu poruku na temelju već generirane vrijednosti funkcije sažetka [25]. Takve funkcije ulazne vrijednosti različitih duljina pretvaraju u izlazne vrijednosti fiksne duljine. Funkcije sažetka mogu biti korištene za više različitih aktivnosti od dokazivanja autentičnosti informacija te integriteta podataka do nasumičnog generiranja brojeva [26].

Također, koriste se u svrhu spremanja zaporki. Ukoliko se zaporka sprema u običnom tekstualnom zapisu mogla bi se lako otuđiti, stoga se računaju vrijednosti funkcije sažetka zaporke te se spremaju umjesto samih zaporki. Prilikom upisivanja zaporke njena vrijednost funkcije sažetka se uspoređuje sa pohranjenom vrijednosti. U slučaju poklapanja vrijednosti korisnik dobiva dozvolu za pristup. Na taj način se

onemogućava napadačima pristup zaporkama jer čak i kada bi se domogli vrijednosti funkcije sažetka ne bi im bile od nikakve koristi [27]. Postoje više vrsta kriptografskih hash funkcija a jedne najpoznatijih su MD5, SHA-1, SHA-2, SHA-3, RIPEMD-160.

SHA ili "Secure Hash Algorithm" predstavljena je od strane američke nacionalne sigurnosne agencije (engl. National Security Agency, NSA). SHA-256 je kriptografska hash funkcija koja ulaz nasumične veličine pretvara u izlaz fiksne veličine od 32 bytea [28]. Hash funkcije su snažne zato što su jednosmjerne. To znači da je moguće koristiti funkciju sažetka za dobivanje izlazne vrijednosti, ali nije moguće koristiti izlaznu vrijednost kako bi se od nje ponovno dobila ulazna. Upravo ta značajka SHA-256 funkcije ju čini idealnom za primjenu u Bitcoin mreži.

Slika 9.:Prikaz promjene ulazne poruke u vrijednost funkcije sažetka

4. 4. Svojstva kriptografske hash funkcije

Kriptografska funkcija sažetka posebna je vrsta funkcija čija svojstva ju čine idealnom za primjenu u kriptografiji. Postoje određena svojstva koja kriptografska funkcija mora posjedovati kako bi se smatrala sigurnom.

Kako bi kriptografska funkcija sažetka bila korisna, ona mora biti [29]:

1. Iskoristivost raspoloživih računalnih resursa (engl. Computationally Efficient): Računala moraju biti u mogućnosti matematički izvesti funkciju sažetka u jako kratkom vremenskom periodu. Ukoliko bi računalu trebalo nekoliko minuta za izvođenje funkcije to ne bi bilo praktično.

U stvarnosti ovo nije toliko velik problem kao što je bio prije 40 ili 50 godina. Današnja prosječna osobna računala mogu procesuirati zahtjevne funkcije sažetka u malom djeliću sekunde.

2. Deterministič nost (engl. Deterministic): Kako bi kriptografska funkcija bila deterministička ona mora za svaku ulaznu poruku uvijek dati istu vrijednost funkcije sažetka. Ako se računa vrijednost funkcije sažetka iste ulazne poruke deset milijuna puta, ona mora apsolutno svaki put proizvesti istu vrijednost. Ako bi kriptografska funkcija za isti ulaz proizvela različite izlazne vrijednosti, hash vrijednost bi bila nasumična i stoga beskorisna.

3. Skrivenost izvorne poruke (engl. Pre-image resistant): Izlazna vrijednost hash funkcije ne smije otkriti nikakve informacije o ulaznoj poruci. Potrebno je istaknuti da kriptografski hash algoritam može primiti bilo kakav podatak u digitalnom obliku bez obzira na njegov sadržaj ili format. Neovisno veličini ulazne poruke, izlazna hash vrijednost uvijek će biti iste duljine. Ukoliko bi duža ulazna poruka davala dužu vrijednost funkcije sažetka to bi napadačima uvelike pomoglo pri pokušaju otkrivanja nečije ulazne poruke.

4. Mogućnost pojave kolizije (engl. Collision resistant): Ovaj pojam označava svojstvo da mora biti izuzetno malo vjerojatno; drugim riječima praktički nemoguće da dvije različite ulazne poruke daju istu vrijednost funkcije sažetka. Budući da je broj ulaza zapravo beskonačan, ali broj izlaza uvijek određen konačan broj, postoji matematička mogućnost da više od jednog ulaza proizvede isti izlaz. Cilj je da mogućnost pronalaska dva ulaza koji daju isti izlaz bude izrazito mala, kako ne bi predstavljala rizik. Kriptografske hash funkcije MD5 te SHA-1 teoretski i praktično su probijene, što znači da je moguće na temelju dobivene hash vrijednosti izračunati više različitih ulaznih poruka s istom hash vrijednosti [30].

4. 5. Asimetrična enkripcija

Za potrebe dokaza o vlasništvu na Bitcoin mreži koristi se asimetrična enkripcija. U slučaju simetrične enkripcije korišten je isti ključ za enkripciju i dekripciju, što znači da ga istovremeno moraju posjedovati pošiljatelj i primatelj. Takva vrsta enkripcije nije pogodna za korištenje u blockchainu, jer ne postoji dovoljno siguran način razmjene tajnog ključa između dvije osobe. Za razliku od simetrične,

asimetrična enkripcija koristi 2 ključa od kojih je jedan javan i svima dostupan, a drugi privatan.

Kreiranje privatnog ključa započinje generiranjem nasumičnog niza nula i jedinica (256 bitova) čija vrijednost ne smije biti veća od broja 2^{256}. Od dobivenog privatnog ključa dobiva se javni ključ kriptografskom funkcijom eliptične krivulje na način da se vrijednost privatnog ključa pomnoži sa unaprijed određenom točkom krivulje što rezultira drugom točkom koja čini javni ključ. Sa dobivenim javnim ključem generira se Bitcoin adresa tako što se računa vrijednost funkcije sažetka javnog ključa korištenjem SHA-256 funkcije, a zatim koristeći RIPEMD160 funkciju [20].

Za ispisivanje dobivene vrijednosti u kraćem obliku koristi se "Base-58 Encoding" čija abeceda je sastavljena od brojeva, velikih i malih slova te triju znakova (123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz+/\).
Kako ne bi dolazilo do pogrešno upisanih adresa ljudskom rukom koristi se "Base58Check Encoding" na način da se na početak dodaje prefiks "0x00" te se vrši SHA-256 funkcija dva puta zaredom. Prva četiri znaka funkcije dodaju se na kraju adrese te služe provjeri točnosti unesene adrese korisnika.

Kako bi korisnik koji želi poslati određenu količinu Bitcoina mogao kreirati transakciju, mora svojim privatnim ključem dokazati da je vlasnik navedenog ključa te vrijednosti koju želi poslati. Na temelju pošiljateljevog javnog ključa, lako je provjeriti vjerodostojnost informacija. Također, transakcija sadrži javno dostupan ključ primatelja koji će svojim privatnim ključem dokazati da je novi vlasnik poslanog Bitcoina. Budući da je Bitcoin valuta bez fizičkog oblika, dijele se samo prava na daljnje korištenje valute s osobe na osobu [18].

4. 6. Pametni ugovori

Godine 1994. američki kriptograf Nick Szabo prvi puta je predstavio "Smart contracts" ili pametne ugovore [31]. Pametni ugovori su kôd računalnog programa s mogućnosti samostalnog izvršavanja, a predstavljaju dogovor između više stranaka bez posrednika. Ugovori se automatski izvršavaju kada su ispunjeni dogovoreni uvjet [31].

Popularnost su stekli tek pojavom decentralizirane platforme Ethereum koju je 2014. godine predstavio rusko-kanadski programer Vitalik Buterin [32]. Cilj je bio napraviti decentraliziranu platformu kao podlogu za izgradnju decentraliziranih aplikacija što nije bilo moguće na tadašnjim blockchain sustavima bez izrade novog vlastitog blockchaina. Problem Bitcoina bio je nedostatak programskog jezika s alatima koji bi omogućili izradu aplikacija [32].

Bitcoin skripte su lista pohranjenih uputa sa svakom transakcijom koje opisuju pravo na slanje valute korištenjem javnih i privatnih ključeva. Kao takve nisu u mogućnosti izvoditi petlje potrebne za rad pametnog ugovora. Stoga je za potrebe Ethereuma osmišljen programski jezik Solidity koji omogućuje kreiranje pametnih ugovora [33].

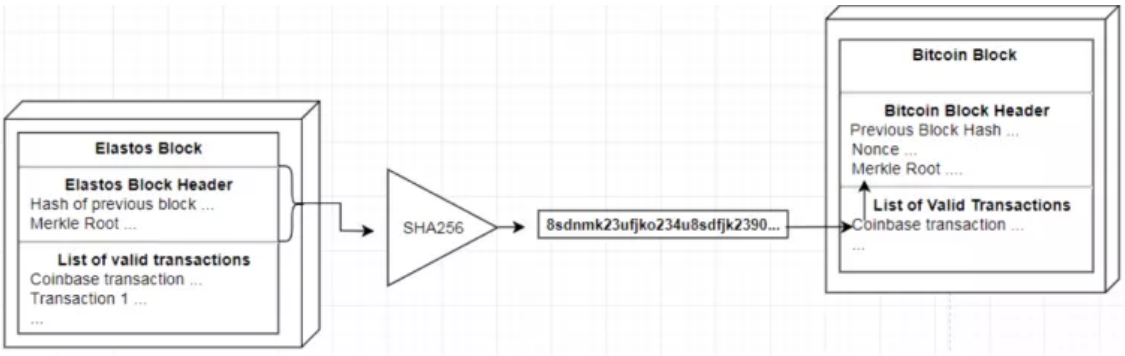
Za procesuiranje ugovora odgovoran je "Ethereum virtualni stroj", izolirani sustav za pametne ugovore na Ethereumu čiji je cilj izvođenje procesa u sigurnom okruženju bez pristupa Internetu [34]. Pametni ugovori mogli bi biti od velike važnosti u funkcioniranju Interneta stvari. Npr. spomenuti pametni sustav parkirnih mjesta mogao bi komunicirati sa pametnim uređajem automobila te kreirati pametni ugovor u kojem bi u ovisnosti o trajanju korištenja parkirnog mjesta automatski izvršio isplatu sredstava prilikom odlaska korisnika.

4. 7. Elastos

Elastos je decentralizirani ekosustav te platforma za izgradnju decentraliziranih aplikacija zasnovana na Blockchain tehnologiji [35]. Projekt je službeno pokrenut 2018. godine od strane programskog inženjera Rong Chena te suosnivača Dr. Feng Han-a. Tehnologije na kojima počivaju Bitcoin i Ethereum uvelike su doprinijele njegovom razvoju [36]. Elastosov glavni blokovni lanac koristi udruženo rudarenje s Bitcoinom što znači da je konsenzus postignut na oba lanca istovremeno umjesto korištenja vlastitog *proof of work* konsenzusa. Prednost ovakvog pristupa je korištenje sigurnosti Bitcoinove mreže te ušteda električne energije.

Kako bi se omogućilo udruženo rudarenje, Bitcoin rudar mora nadograditi svoj program za rudarenje pritom ne žrtvujući potrošnju električne energije niti brzine

rudarenja Bitcoina [37]. Trenutni odaziv Bitcoin rudara na nadogradnju programa kojim se omogućuje rudarenje Elastosa iznosi čak 50% svih Bitcoin rudara u mreži, što ju čini jednom od trenutno najsigurnijih [38].



Slika 10.: Istovremeno rudarenje oba blokovna lanca [37]

Fizički entiteti poput uređaja te virtualni entiteti poput aplikacija u IoT-u moraju imati vlastite identitete koji se mogu pohraniti na blockchainu. Ovakav blokovni lanac koristi se za pohranu decentraliziranih identiteta korisnika, uređaja i aplikacija te nisu kontrolirani od strane centraliziranih tvrtki poput Google-a ili Amazon-a. Na taj se način korištenjem Interneta stvari osigurava pravo korisnika na dostupnost sadržaja te autentikaciju upotrebom privatnih i javnih ključeva na blockchainu [39].

Korištenjem aplikacija kojima se pristupa uređajima Interneta stvari dovodi se pitanje privatnost komunikacije između klijenta i servera, spomenute u *Man-In-The-Middle* vrsti napada, stoga se za pokretanje aplikacija koristi izolirano okruženje zvano Runtime. Ono se može opisati kao virtualno računalo koje koristi resurse uređaja kako bi se kreiralo sigurno okruženje u kojem je aplikacija izolirana od direktnog pristupa Internetu i ostalih procesa uređaja te čak i od operacijskog sustava uređaja. Komunikacija s uređajem odvija se preko najnižeg programskog sloja tj. kernela te tako nema curenja podataka. Ukoliko se nekim slučajem preuzme zlonamjerni softver on će biti izbrisan nakon prestanka korištenja aplikacije tj. gašenja virtualnog računala te neće moći zaraziti korisnikove resurse sustava [40].

Daljnja komunikacija između IoT uređaja odvija se pomoću decentralizirane peer-to-peer Carrier mreže bez servera koja ima ulogu enkripcije i usmjeravanja

prometa na mreži [41]. Svaki IoT uređaj povezan na Carrier mrežu istovremeno postaje čvor mreže sa zadaćom usmjeravanja prometa te izvršavanja pametnih ugovora. Svi paketi na mreži usmjeravaju se nasumično između čvorova te nije moguće predvidjeti put podataka od izvora do odredišta [42].

Kako bi korisnici zaista mogli posjedovati svoje digitalne resurse i osigurati im privatnost, oni nisu pohranjeni na centralizirane servise kojima upravljaju privatne tvrtke. Tehnologija takve pohrane podataka temelji se na IPFS (engl. InterPlanetary File System) protokolu kojim se omogućava distribuirana pohrana na način da se dijelovi kriptiranih podataka nalaze na puno različitih izvora umjesto na jednom centraliziranom serveru. Također, pruža se mogućnost korisniku na ne samo primanje već i pružanje sadržaja iznajmljivanjem svojeg slobodnog prostora na disku. Time ne postoji centralna točka napada kojom bi bilo moguće onemogućiti korisnicima pristup podacima [43].

Upotrebom ovakvog sustava pri korištenju Interneta stvari osigurala bi se privatnost komunikacije te prava na pristup pohranjenom sadržaju, eliminirajući presretanje komunikacije MITM napadima te distribuirano odbijanje usluge DDoS napadima.

5. TESTIRANJE VRIJEDNOSTI FUNKCIJE SAŽETKA

Izrazito bitno obilježje funkcija sažetka zahtjeva da najmanja promjena ulazne poruke rezultira drastičnom promjenom vrijednosti funkcije sažetka. Ukoliko bi se izmijenio mali dio iz skupine ulaznih podataka bilo bi lako na temelju dobivene vrijednosti funkcije sažetka zaključiti da se izgubila autentičnost izvora. U sljedećim primjerima bit će testirane četiri različite funkcije sažetka na četiri različite vrste datoteka sa ciljem uspoređivanja vrijednosti funkcije sažetka prilikom najmanje promjene sadržaja datoteke, promjene imena datoteke te promjene veličine datoteke kako bi se usporedila duljina vrijednosti funkcije sažetka. Za primjer testiranja korišten je Hashem all! online kalkulator [44].

5. 1. Testiranje vrijednosti SHA-256 funkcije sažetka na Word datoteci

U prvom primjeru korištena je SHA-256 funkcija sažetka na Word datoteci koja sadrži poruku „Veleučilište u Karlovcu“. Zatim je napravljena izmjena sadržaja datoteke na način da se glas „č“ promijenio u „c“ te poruka glasi „Veleucilište u Karlovcu“. Na temelju izračuna vrijednosti funkcije sažetka prije te nakon izmjene poruke vidljivo je da se vrijednost funkcije sažetka drastično promijenila.

Zatim je ime datoteke „Word datoteka“ izmijenjeno u „Word datoteka 1“ bez promjene sadržaja datoteke. Na temelju izračuna vrijednosti funkcije sažetka prije te nakon izmjene imena datoteke vidljivo je da se vrijednost funkcije sažetka nije promijenila.

Zatim je višestruko uvećana veličina datoteke kako bi se testiralo ima li memorijsko zauzeće datoteke utjecaja na duljinu vrijednosti funkcije sažetka. Dobivena vrijednost funkcije sažetka iste je duljine što dokazuje da memorijsko zauzeće datoteke nema utjecaja na duljinu vrijednosti funkcije sažetka.

Tablica 1.: Testiranje SHA-256 funkcije sažetka na Word datoteci

	SHA-256	Trajanje
Original tekst. datoteke	EE10FF7B5731853EB318B03B19D520CC649763D2E144B13542D2B823732AFE08	4ms
Izmijenjen tekst. datoteke	633AD3A7E36741B0768489061C0F7151303CFFD36929ABB43958474CC4E5DDF1	4ms
Promjena naziva izmjenjenog teksta. datoteke	633AD3A7E36741B0768489061C0F7151303CFFD36929ABB43958474CC4E5DDF1	4ms
Izmjena veličine dat.	461D4B2918A41ED0D45C98847DECAFB85D1D5510DF4D2AFB5891A44A401EFA62	15ms

5. 2. Testiranje vrijednosti MD5 funkcije sažetka na fotografiji

U drugom primjeru korištena je MD5 funkcija sažetka na fotografiji. Za primjer fotografije odabran je logotip Veleučilišta u Karlovcu.

Slika 11.: Logotip Veleučilišta u Karlovcu [45]

Zatim je napravljena izmjena na fotografiji. Na originalnu fotografiju dodan je jedan piksel plave boje na vanjskoj kružnici logotipa koji ljudskim okom nije uočljiv bez uvećanja. Izmjena boje samo jednog piksela logotipa rezultirala je drastičnom promjenom vrijednosti funkcije sažetka.

Slika 12.: Uvećan prikaz dijela logotipa na kojem je napravljena izmjena

Zatim je ime originalne datoteke „VUKA“ izmijenjeno u „VUK“ brisanjem zadnjeg glasa „A“ u imenu bez promjene sadržaja prvotne datoteke. Na temelju izračuna vrijednosti funkcije sažetka prije te nakon izmjene imena datoteke vidljivo je da se vrijednost funkcije sažetka nije promijenila.

U zadnjem koraku višestruko je uvećana veličina datoteke kako bi se testiralo ima li memorijsko zauzeće datoteke utjecaja na duljinu vrijednosti funkcije sažetka. Dobivena vrijednost funkcije sažetka iste je duljine što dokazuje da memorijsko zauzeće datoteke nema utjecaja na duljinu vrijednosti funkcije sažetka.

Tablica 2.: Testiranje MD5 funkcije sažetka na slikovnoj datoteci

	MD5	Trajanje
Original slikovna dat.	EA08155121C429E63D6536A6AEAD47F5	5ms
Izmijenjena slikovna dat.	2DA5869C137D51DA2B114237501600AC	7ms
Promjena naziva originala slikovne dat.	2DA5869C137D51DA2B114237501600AC	5ms
Izmjena veličine dat.	06C38BC6BEA7B7D8F603976912E060EF	81ms

5. 3. Testiranje vrijednosti SHA-1 funkcije sažetka na zvukovnom zapisu

U trećem primjeru korištena je SHA-1 funkcija sažetka na zvukovnom zapisu snimljenom pametnim telefonom. Kod prve izmjene napravljena je izmjena na zvukovnom zapisu na način da je vrijeme trajanja skraćeno za jednu sekundu. Izmjena zvukovnog zapisa kojim je skraćeno vrijeme trajanja za samo jednu sekundu rezultirala je drastičnom promjenom vrijednosti funkcije sažetka.

Zatim je ime datoteke „zvuk1“ izmijenjeno u „zvuk2“ . Na temelju izračuna vrijednosti funkcije sažetka prije te nakon izmjene imena datoteke vidljivo je da se vrijednost funkcije sažetka nije promijenila.

U zadnjoj izmjeni veličina datoteke je umanjena kako bi se testiralo ima li memorijsko zauzeće datoteke utjecaja na duljinu vrijednosti funkcije sažetka. Dobivena vrijednost funkcije sažetka iste je duljine što dokazuje da memorijsko zauzeće datoteke nema utjecaja na duljinu vrijednosti funkcije sažetka.

Tablica 3.: Testiranje SHA-1 funkcije sažetka na mp3 datoteci

	SHA-1	Trajanje
Original mp3 dat.	21E86A46983A7149261E51A4AEAEBF4C56226095	6ms
Izmijenjena mp3 dat.	C7423386CD9C9B8905E28AE0984356C427030571	5ms
Promjena naziva mp3 dat.	C7423386CD9C9B8905E28AE0984356C427030571	7ms
Izmjena veličine dat.	EE839FF02021EDFEC4C5D1DDA58F09717885494E	4ms

5. 4. Testiranje vrijednosti RIPEMD-160 funkcija sažetka na komprimiranoj datoteci

U četvrtom primjeru korištena je RIPEMD-160 funkcija sažetka na komprimiranoj Word datoteci s porukom „testiranje kriptografske funkcije“. Zatim je napravljena izmjena sadržaja datoteke iz „testiranje kriptografske funkcije“ u „testiranje kriptografske funkcije RIPEMD-160“. Na temelju izračuna vrijednosti funkcije sažetka prije te nakon izmjene poruke vidljivo je da se vrijednost funkcije sažetka drastično promijenila.

U sljedećem koraku ime datoteke „Testiranje kriptografske funkcije“ izmijenjeno u „Kriptografija“. Na temelju izračuna vrijednosti funkcije sažetka prije te nakon izmjene imena datoteke vidljivo je da se vrijednost funkcije sažetka nije promijenila.

U zadnjoj izmjeni višestruko je izmijenjena veličina datoteke kako bi se testiralo ima li memorijsko zauzeće datoteke utjecaja na duljinu vrijednosti funkcije sažetka. Dobivena vrijednost funkcije sažetka iste je duljine što dokazuje da memorijsko zauzeće datoteke nema utjecaja na duljinu vrijednosti funkcije sažetka.

Tablica 4.: Testiranje RIPEMD-160 funkcije sažetka na zip datoteci

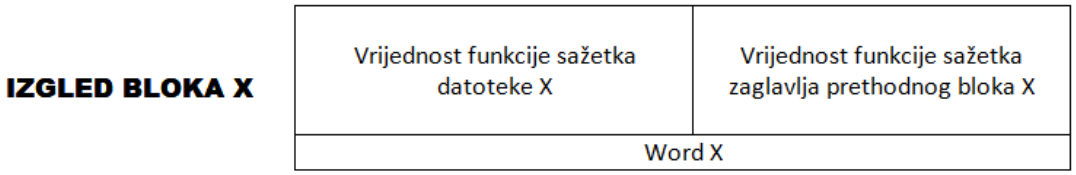
	RIPEMD-160	Trajanje
Original zip dat.	E4C26E9CABDEA2FDA221FAAB9DCE1263E78E0299	3ms
Izmijenjena zip dat.	1D1108E82FBD380BD5FB354951CD31C6C923F818	4ms
Promjena naziva zip dat.	1D1108E82FBD380BD5FB354951CD31C6C923F818	5ms
Izmjena veličine dat.	F61E9177BFE6494AF9F4849F614AF4C39EE97DDD	11ms

Ovim primjerima dokazano je da bez obzira na odabir kriptografske funkcije sažetka i bez obzira na vrstu datoteke, njihove vrijednosti funkcije sažetka i dalje

odgovaraju svojstvima koje kriptografska funkcija mora zadovoljavati. Male izmjene u sadržaju datoteka rezultirale su promjenom vrijednosti funkcije sažetka dok promjena imena datoteke nije rezultirala promjenom vrijednosti funkcije sažetka. Također je dokazano da veličine datoteke nije povezana s duljinom vrijednosti funkcije sažetka koja ostaje iste duljine, ali je utjecala na trajanje izračuna vrijednosti funkcije sažetka.

5. 5. Izrada blokovnog lanca

U nastavku će biti prezentirana izrada blokovnog lanca u kojem će biti objašnjeno pohranjivanje podataka u blokove računanjem vrijednosti funkcije sažetka datoteke te povezivanje blokova pohranom podatka prethodnog bloka. Blok se sastoji od podatkovnog dijela u kojem se nalazi Word datoteka te zaglavlja u kojem se nalazi vrijednost funkcije sažetka Word datoteke i vrijednost funkcije sažetka zaglavlja prethodnog bloka.



Slika 13.: Prikaz sheme bloka x

Vrijednost funkcije sažetka zaglavlja prethodnog bloka dobivena je spajanjem vrijednosti funkcije sažetka Word datoteke iz prethodnog bloka te vrijednosti funkcije sažetka zaglavlja bloka prije prethodnog bloka, od čega se zajedno računa vrijednost funkcije sažetka. Na taj način svaki noviji blok sadrži informaciju o prethodnom bloku te ih povezuje. Nulti blok neće imati vrijednost funkcije sažetka zaglavlja prethodnog bloka iz razloga što je prvi kreiran te će se vrijednost funkcije sažetka zaglavlja u bloku 1 sastojati samo od vrijednosti funkcije sažetka datoteke 0. Kao primjeri teksta unutar Word datoteka odabrani su neki od planeta iz sunčevog sustava.

Blok 0:

U podatkovnom dijelu bloka 0 nalazi se Word datoteka 0 koja sadrži tekst sa imenom planeta “Merkur”. Izračunom vrijednosti funkcije sažetka datoteke 0 dobiva se vrijednost:
8EC7542C2D8D39C0998412379217D6EBF66FB9E1F45F0AD3B7E6F812D252C90D

Slika 14.: Vrijednost funkcije sažetka datoteke 0 [44]

Vrijednost funkcije sažetka datoteke 0 pohranjuje se u zaglavlje bloka 0 na odgovarajuće mjesto.

Blok 1:

U podatkovnom dijelu bloka 1 nalazi se Word datoteka 1 koja sadrži tekst sa imenom planeta “Venera”. Izračunom vrijednosti funkcije sažetka datoteke 1 dobiva se vrijednost:
01C468C61182E30BD109E10B2D282CA2F8FB4DA7A5D47888C48955837D31AD5D

Slika 15.: Vrijednost funkcije sažetka datoteke 1 [44]

Vrijednost funkcije sažetka datoteke 1 pohranjuje se u zaglavlje bloka 1 na odgovarajuće mjesto. Blok 1 za razliku od bloka 0 ima prethodni blok stoga je potrebno izračunati vrijednost zaglavlja prethodnoga bloka 0 koje se sastoji samo od računanja vrijednosti funkcije sažetka od već dobivene vrijednosti funkcije sažetka datoteke 0.

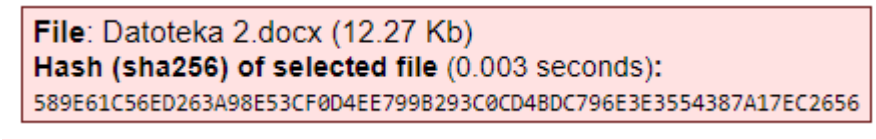
Izračunom vrijednosti funkcije sažetka zaglavlja bloka 0 dobiva se vrijednost: BCC3151C9C998641E02D5A95D83F7E3A33B757688BF6A520321D304C753F0BC7

Slika 16.: Vrijednost funkcije sažetka zaglavlja bloka 0 [44]

Dobivena vrijednost zaglavlja bloka 0 pohranjuje se zaglavlje bloka 1 na mjesto vrijednosti funkcije sažetka prethodnog bloka.

Blok 2:

U podatkovnom dijelu bloka 2 nalazi se Word datoteka 2 koja sadrži tekst sa imenom planeta "Zemlja". Izračunom vrijednosti funkcije sažetka datoteke 2 dobiva se vrijednost: 589E61C56ED263A98E53CF0D4EE799B293C0CD4BDC796E3E3554387A17EC2656



Slika 17.: Vrijednost funkcije sažetka datoteke 2 [44]

Vrijednost funkcije sažetka datoteke 2 pohranjuje se u zaglavlje bloka 2 na odgovarajuće mjesto.

Blok 2 ima svoj prethodni blok stoga je potrebno izračunati vrijednost funkcije sažetka zaglavlja prethodnoga bloka 1 koje se sastoji od računanja vrijednosti funkcije sažetka od već dobivene vrijednosti funkcije sažetka datoteke 1 na čiji kraj dodajemo vrijednost funkcije sažetka zaglavlja prethodnog bloka.

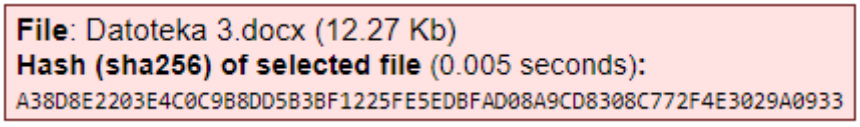
Izračunom vrijednosti funkcije sažetka dobiva se vrijednost: C4408927BE7BE70290C258357D3C10BD6263F9B7AFAF6335C7079FCDE846F486

Slika 18.: Vrijednost funkcije sažetka zaglavlja bloka 1 [44]

Dobivena vrijednost funkcije sažetka zaglavlja bloka 1 pohranjuje se u zaglavlje bloka 2 na mjesto vrijednosti funkcije sažetka prethodnog bloka.

Blok 3:

U podatkovnom dijelu bloka 3 nalazi se Word datoteka 3 koja sadrži tekst sa imenom planeta "Mars". Izračunom vrijednosti funkcije sažetka datoteke 3 dobiva se vrijednost: A38D8E2203E4C0C9B8DD5B3BF1225FE5EDBFAD08A9CD8308C772F4E3029A0933



Slika 19.: Vrijednost funkcije sažetka datoteke 3 [44]

Vrijednost funkcije sažetka datoteke 3 pohranjuje se u zaglavlje bloka 3 na odgovarajuće mjesto.

Blok 3 također ima svoj prethodni blok stoga je potrebno izračunati vrijednost funkcije sažetka zaglavlja prethodnoga bloka 2 koje se sastoji od računanja vrijednosti funkcije sažetka od već dobivene vrijednosti funkcije sažetka datoteke 2 na čiji kraj dodajemo vrijednost funkcije sažetka zaglavlja prethodnog bloka.

Izračunom vrijednosti funkcije sažetka dobiva se vrijednost: 9899BFAE364C5A30AF030E1FAF90895ED140A63F1ED67759D726A07947529E16

Slika 20.: Vrijednost funkcije sažetka zaglavlja bloka 2 [44]

Dobivena vrijednost funkcije sažetka zaglavlja bloka 2 pohranjuje se u zaglavlje bloka 3 na mjesto vrijednosti funkcije sažetka prethodnog bloka.

Blok 4:

U podatkovnom dijelu bloka 4 nalazi se Word datoteka 4 koja sadrži tekst sa imenom planeta "Jupiter". Izračunom vrijednosti funkcije sažetka datoteke 4 dobiva se vrijednost: C1DD6A118B20F37615BFCB5DC2E74FC26A1798D7EFC78F4A72C825F57BEF1889

Slika 21.: Vrijednost funkcije sažetka datoteke 4 [44]

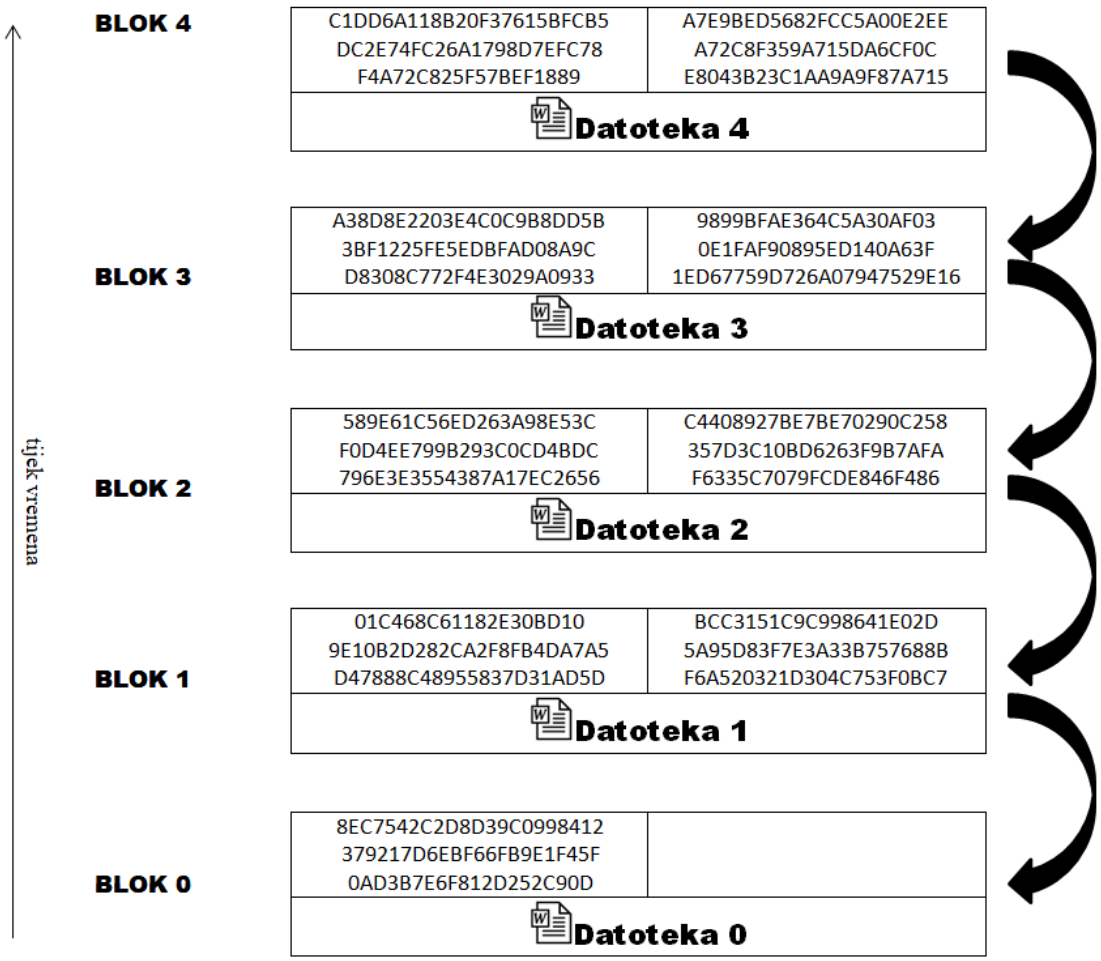
Vrijednost funkcije sažetka datoteke 4 pohranjuje se u zaglavlje bloka 4 na odgovarajuće mjesto.

Blok 4 također ima svoj prethodni blok stoga je potrebno izračunati vrijednost funkcije sažetka zaglavlja prethodnoga bloka 3 koje se sastoji od računanja vrijednosti funkcije sažetka od već dobivene vrijednosti funkcije sažetka datoteke 3 na čiji kraj dodajemo vrijednost funkcije sažetka zaglavlja prethodnog bloka. Izračunom vrijednosti funkcije sažetka dobiva se vrijednost:

A7E9BED5682FCC5A00E2EEA72C8F359A715DA6CF0CE8043B23C1AA9A
9F87A715

Slika 22.: Vrijednost funkcije sažetka zaglavlja bloka 3 [44]

Dobivena vrijednost funkcije sažetka zaglavlja bloka 3 pohranjuje se u zaglavlje bloka 4 na mjesto vrijednosti funkcije sažetka prethodnog bloka. Time je kreirani blokovni lanac od pet blokova dovršen te je svaki idući blok povezan sa svojim prethodnim blokom.



Slika 23.: Prikaz kreiranog blokovnog lanca

Kako bi se testirala posljedica promjene sadržaja u blokovnom lancu u slijedećem primjeru će Word datoteka 3 tekstualnog sadržaja “Mars” biti zamijenjena porukom “Mjesec”.

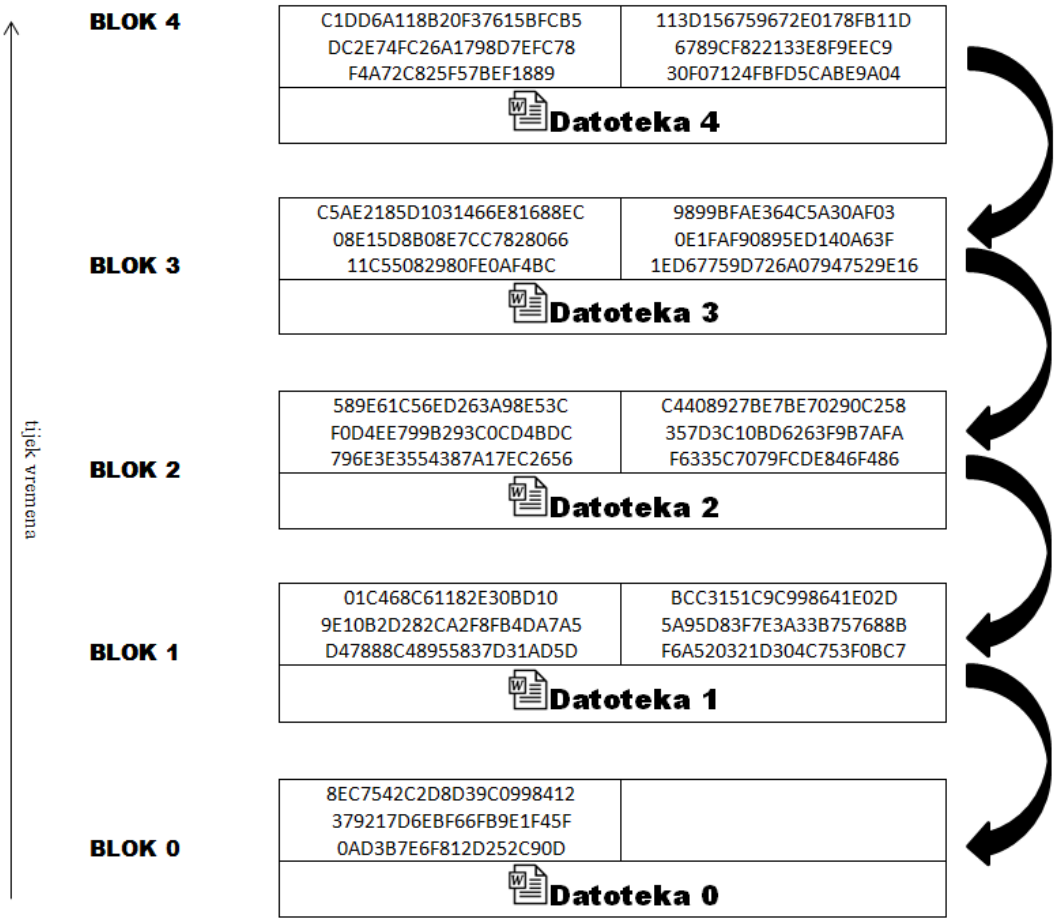
Računanjem vrijednosti funkcije sažetka datoteke 3 sa porukom “Mjesec” rezultirala je vrijednošću:

C5AE2185D1031466E81688EC08E15D8B08E7CC782806611C55082980FE0AF4BC

Slika 24.: Vrijednost funkcije sažetka datoteke 3 nakon promjene sadržaja [44]

Nova vrijednost funkcije sažetka datoteke 3 u bloku 3 rezultirala je promjenom vrijednosti funkcije zaglavlja koja se ne podudara sa vrijednosti u bloku 4, stoga noviji blok u ovom slučaju blok 4 nije validan bez ponovne rekalkulacije bloka. Nova vrijednost funkcije sažetka zaglavlja nakon rekalkulacije bloka iznosi: 113D156759672E0178FB11D6789CF822133E8F9EEC930F07124FBFD5CABE9A04

Slika 25.: Vrijednost funkcije sažetka zaglavlja bloka 4 [44]



Slika 26.: Prikaz kreiranog blokovnog lanca nakon rekalkulacije bloka

U blokovnom lancu povezanost blokova od ključne je važnosti. Promjena sadržaja poruke u bilo kojem bloku rezultirala bi promjenom zaglavlja u svim idućim blokovima do kraja blokovnog lanca. To bi rezultiralo prisiljavanjem zlonamjernog korisnika na ponovnu rekalkulaciju svih idućih blokova od bloka na kojem je napravljena izmjena pa sve do kraja lanca što bi bilo najčešće neisplativo u odnosu na korist koja se tim napadom može ostvariti. Visoka razina sigurnosti pohrane podataka kao transakcije i identiteti nad kojima nema centralizirane vlasti, prepoznata je kao jedna od metoda ostvarivanja sigurne komunikacije korištenjem uređaja Interneta stvari.

6. ZAKLJUČAK

Sve veća upotreba Interneta stvari rezultirala je jednostavnijim nadziranjem te upravljanjem uređaja povezanih na Internet. Uređaji koji nalaze primjenu u svakodnevnom životu prate stanja u okolini prikupljajući podatke poput temperature, tlaka, jakosti svjetla, kvalitete zraka, ali i puno intimnijih informacija poput fotografija te zvukovnih zapisa i videozapisa korisnika. Činjenica da uređaji postaju „sve pametniji“ te snimaju audio zapise visoke kvalitete i videozapise dovela je u pitanje privatnost korisnika te sigurnost osobnih podataka na Internetu. Korištenjem Interneta stvari nailazi se na ograničenja koja je potrebno otkloniti kako bi sustav mogao funkcionirati. Ograničeni procesni i energetski resursi uređaja ograničavali bi brzinu preuzimanja, pohrane, obrade i slanja podataka. Zbog toga je potrebno osigurati hardver uređaja sa sposobnošću obavljanja zahtjevnijih procesorskih radnji te smanjiti potrošnju električne energije zbog uštede baterija uređaja koji nemaju pristup gradskoj mreži. Ograničeni memorijski sustavi centraliziranih servisa na kojima se pohranjuju zabilježene informacije uređaja mogli bi biti zamijenjeni decentraliziranim sustavima što bi omogućilo veću sigurnost te dostupnost pohranjenih podataka te smanjenje troškova pohrane podataka. Potrebno je omogućiti i dostatnu brzinu pristupa Internetu kako bi se osigurao nesmetan prijenos podataka među uređajima. IoT sustav je neupotrebljiv u slučaju nedostupnosti internetske veze koja predstavlja ključan faktor u povezivanju uređaja na Internetu. Kao dva najznačajnija problema koji uzrokuju zabrinutost pri korištenju Interneta stvari navedeni su DDoS napadi koji uskraćuju uslugu korisnicima te MITM napadi kojima je moguće presretati komunikaciju između klijenta i servera te otuđiti osobne podatke. Upotrebom mehanizma digitalne kriptografije postalo je jednostavnije provjeravati integritet podataka i osigurati nepromjenjivost sadržaja što je i dokazano u radu testirajući različite vrste kriptografskih funkcija sažetka na više različitih vrsta datoteka. Blockchain tehnologija na kojoj počiva velik broj kriptovaluta među kojima je najpoznatija Bitcoin, omogućila je integritet decentraliziranih, javno dostupnih baza podataka koje sadrže povijesti transakcija korisnika. Također, omogućila je i pohranu jedinstvenih identiteta korisnika uz pomoć kojih nije moguće kreirati lažne zahtjeve, lažirajući identitete drugih korisnika bez posjedovanja privatnog kriptografskog ključa korisnika. U tehnologiji

Elastosa opisani su načini sigurnog pokretanja aplikacija pri korištenju Interneta stvari bez mogućnosti MITM napada kojim bi zlonamjerni softver mogao usmjeravati komunikaciju zlonamjernom korisniku. Također, komunikacija među svim pametnim uređajima Interneta stvari bila bi kriptirana te nasumično prosljeđivana čvorovima u mreži. Na posljetku sve informacije te osobni podaci korisnika bili bi pohranjeni na decentralizirane sustave za pohranu podataka eliminirajući probleme centraliziranih servisa osiguravajući dostupnost te sigurnost podataka. Iako još uvijek zabrinutost korisnika nije dosegla svoj vrhunac, daljnjom upotrebom Interneta stvari osobni podaci postat će najvrjednija imovina korisnika.

7. LITERATURA

[1] Bahga, A., Madisetti, V.: „Internet of Things: A Hands-on Approach“, https://books.google.hr/books?id=JPKGBAAAQBAJ&lpg=PA1&hl=hr&pg=PA2#v=onepage&q&f=true, pristupljeno 18. 9. 2019.

[2] Johnny: „The definition of Internet of Things: A simple explanation“ https://www.expressvpn.com/blog/what-is-the-internet-of-things-iot/, pristupljeno 18. 9. 2019.

[3] Office of Electricity: „Grid Modernization and the Smart Grid“, https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid, pristupljeno 18. 9. 2019.

[4] Foote K.: „A Brief History of the Internet of Things“, https://www.dataversity.net/brief-history-internet-things/, pristupljeno 18. 9. 2019.

[5] Brebrić, K.: „Gartnerov hype ciklus tehnologija“, http://www.bug.hr/vijesti/gartnerov-hype-ciklus-tehnologija/110441.aspx, pristupljeno 18. 9. 2019.

[6] Postscapes: „Internet of Things (IoT) History“, https://www.postscapes.com/internet-of-things-history/, pristupljeno 18. 9. 2019.

[7] PAR University: „Prva IoT konferencija u Hrvatskoj“, http://www.par.hr/prva-iot-konferencija-u-hrvatskoj/, pristupljeno 18. 9. 2019.

[8] Statista Research Department: „Internet of Things - number of connected devices worldwide 2015-2025“, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ , pristupljeno 18. 9. 2019.

[9] „Globalno istraživanje o sigurnosti IoT uređaja“, https://mreza.bug.hr/globalno-istrazivanje-o-sigurnosti-iot-uredaja/, pristupljeno 18. 9. 2019.

[10] Boddy, M.: „Coinbase Accidentally Saves Unencrypted Passwords of 3,420 Customers“, https://cointelegraph.com/news/coinbase-accidentally-saves-unencrypted-passwords-of-3-420-

customers?fbclid=IwAR3C207ViD7yBbbFRU2NKsmNqdTEa2tDfWZMjdGl7ESGxqsT3k66DvnbaI8, pristupljeno 18. 9. 2019.

[11] Melnick, J.: „Top 10 Most Common Types of Cyber Attacks“, https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/ , pristupljeno 18. 9. 2019.

[12] Rapid7: „Common Types of Cybersecurity Attacks“, https://www.rapid7.com/fundamentals/types-of-attacks/ , pristupljeno 18. 9. 2019.

[13] Regan, J.: „The Ultimate Guide to Denial of Service (DoS) Attacks“ https://www.avg.com/en/signal/what-is-ddos-attack, pristupljeno 18. 9. 2019.

[14] Symantec: „What is a man-in-the-middle attack?“, https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html , pristupljeno 18. 9. 2019.

[15] Dobran, B.: „What are Man in the Middle Attacks & How to Prevent MITM Attack With Examples“, https://phoenixnap.com/blog/man-in-the-middle-attacks-prevention , pristupljeno 18. 9. 2019.

[16] Elastos, https://www.elastos.org, pristupljeno 18. 9. 2019.

[17] Rosic, A.: „What is Blockchain Technology? A Step-by-Step Guide For Beginners“, https://blockgeeks.com/guides/what-is-blockchain-technology/, pristupljeno 18. 9. 2019.

[18] Arunović, D.: „Što je u stvari blockchain i kako radi?“ https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011, pristupljeno 18. 9. 2019.

[19] „Blockchain: why have permissionless blockchains to be slow?“, https://eric-diehl.com/blockchain-why-have-permissionless-blockchains-to-be-slow/, 18. 9. 2019.

[20] Antonopoulos, A.:“Mastering Bitcoin“, O’Reilly Media, California, (2014.), 978-1-449-37404-4

[21] Colorado State University: „Blockchain principles and applications“, http://www.cs.colostate.edu/~cs481a3/#/, pristupljeno 18. 9. 2019.

[22] Ledger: „How It All Began: A Brief History On Bitcoin & Cryptocurrencies“, https://www.ledger.com/how-it-all-began-a-brief-history-of-bitcoin-cryptocurrencies/, pristupljeno 18. 9. 2019.

[23] Marr, B.: „A Short History Of Bitcoin And Crypto Currency Everyone Should Read“, https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/#39ede1573f27, pristupljeno 18. 9. 2019.

[24] Bitmain: https://shop.bitmain.com/product/detail?pid=00020190813102515061 8stdgtjt0729, pristupljeno 18. 9. 2019.

[25] Edgar, T., Manz, D.: „Science and Cyber Security“, https://www.sciencedirect.com/topics/computer-science/hash-function, pristupljeno 18. 9. 2019.

[26] Denis, T., Johnson, S.: „Hash Functions“, https://www.sciencedirect.com/topics/computer-science/hash-function, pristupljeno 18. 9. 2019.

[27] Bobby: „What is Cryptographic Hashing? MD5, SHA, and More“, https://tiptopsecurity.com/what-is-cryptographic-hashing-md5-sha-and-more/, pristupljeno 18. 9. 2019.

[28] Asolo, B.: „What Is SHA-256 And How Is It Related to Bitcoin?“, https://www.mycryptopedia.com/sha-256-related-bitcoin/, pristupljeno 18. 9. 2019.

[29] Daniel: „Cryptographic Hash Functions Explained: A Beginner’s Guide“, https://komodoplatform.com/cryptographic-hash-function/, pristupljeno 18. 9. 2019.

[30] „Why are MD5 and SHA-1 still used for checksums and certificates if they are called broken?“, https://security.stackexchange.com/questions/87375/why-are-md5-and-sha-1-still-used-for-checksums-and-certificates-if-they-are-call, pristupljeno 18. 9. 2019.

[31] Petersson, D.: „How Smart Contracts Started And Where They Are Heading“, https://www.forbes.com/sites/davidpetersson/2018/10/24/how-smart-contracts-started-and-where-they-are-heading/#735ce1b637b6, pristupljeno 18. 9. 2019.

[32] Rosic, A.: „What is Ethereum? [The Most Comprehensive Step-by-Step-Guide!]“, https://blockgeeks.com/guides/ethereum/, pristupljeno 18. 9. 2019.

[33] „Differences/similarities of “Bitcoin script” and “Ethereum smart contract”?“, https://ethereum.stackexchange.com/questions/57660/differences-similarities-of-bitcoin-script-and-ethereum-smart-contract, pristupljeno 18. 9. 2019.

[34] „Smart Contracts/EVM FAQ“, https://counterparty.io/docs/faq-smartcontracts/#what-is-the-evm, pristupljeno 18. 9. 2019.

[35] Elastos foundation: „Elastos white paper“, https://elanews.net/wp-content/uploads/2018/04/elastos_whitepaper_en.pdf?189db0&189db0, pristupljeno 18. 9. 2019.

[36] Pachhai, K.: „Development History“, https://github.com/elastos/Elastos/wiki/Development-History , pristupljeno 18. 9. 2019.

[37] Pachhai, K.: „Elastos In A Nutshell – A Layman’s Perspective: Merged Mining Part 2/2“, https://blog.cyberrepublic.org/2018/12/10/elastos-in-a-nutshell-a-laymans-perspective-merged-mining-part-2-2/ , pristupljeno 18. 9. 2019.

[38] Elastos Network Statistics: „Statistics related to elastos infrastructure“, https://www.noderators.org/elastossummary/, pristupljeno 18. 9. 2019.

[39] Elastosacademy: „A Decentralized ID for Trust.“, https://elastos.academy/did/ , pristupljeno 18. 9. 2019.

[40] Reddit: „Sidechain limitations?“, https://www.reddit.com/r/Elastos/comments/9p2gw0/sidechain_limitations/, pristupljeno 18. 9. 2019.

[41] Elastosacademy: „CARRIER, A Decentralized Peer-to-Peer Network“, https://elastos.academy/carrier/, pristupljeno 18. 9. 2019.

[42] ElaNews: „Solving the Elastos Enigma“, https://elanews.net/2019/08/21/solving-the-elastos-enigma/, pristupljeno 18. 9. 2019.

[43] Curran, B.: „What is Interplanetary File System IPFS? Complete Beginner’s Guide“, https://blockonomi.com/interplanetary-file-system/, pristupljeno 18. 9. 2019.

[44] Hash'em all!, http://www.hashemall.com/, pristupljeno 18. 9. 2019.

[45] Leksikografski zavod Miroslav Krleža:“ Portal hrvatske tehničke baštine“, http://tehnika.lzmk.hr/veleuciliste-u-karlovcu/, pristupljeno 18. 9. 2019.

8. PRILOZI

8. 1. Popis slika

8. 2. Popis tablica