SVEUČILIŠTE U ZAGREBU

**FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA**

Računalna forenzika

**SEMINAR**

# Blockchain u računalnoj forenzici

*Karlo Siladi*

Voditelj: *doc. dr. sc. Predrag Pale*

Zagreb, siječanj, 2019.

## Sadržaj

# 1. Uvod

Blockchain je jedna od najznačajnijih inovacija današnjice. Doslovan prijevod engleskog termina *blockchain* na hrvatski jezik bio bi “lanac blokova”. Kako se može naslutiti iz imena riječ je o podatkovnim blokovima povezanim u jednosmjerni lanac u kojem svaka karika tj. blok ovisi o vrijednosti prethodne karike. Zbog sigurnosti i privatnosti povezivanje blokova u lanac temeljeno je na kriptografiji. Tako nam ova tehnologija daje veliku razinu pouzdanosti u spremljene podatke.

Primjene *blockchaina* su gotovo neograničene, primjerice može se koristiit kod spremanja medicinskih zapisa, digitalnih bilješki, prikupljanja poreza te mnoge druge.

## 2. Blockchain tehnologija

Ideja o spremanju informacija kao niza podatkovnih zapisa javila se 1991. godine gdje je grupa istraživača željela spremiti digitalne dokumente s vremenskom oznakom (engl. *timestamp*) kako bi ih ne bi bilo moguće antidatirati (engl. *backdate*) ili ih izmijeniti.

*Blockchain* je distribuirani dnevnik (engl. *distributed ledger*) koji je dostupan svima u mreži. Blokovi u dnevniku imaju vrlo važno svojstvo. Jednom kada su podaci zapisani u *blockchain* jako ih je teško izmijeniti. Svaki blok se sastoji od tri dijela: podataka, sažetka podataka (engl. *hash*) te sažetka prethodnog bloka. Primjerice podaci kod *Bitcoina* su detalji o transakciji (pošiljatelj, primatelj i iznos). Sažetak možemo usporediti s otiskom prsta. Jedinstven je za svaki blok te pomoću njega možemo razlikovati blokove, baš kao što je slučaj s otiskom prsta kod ljudi. Sažetak se izračunava prilikom stvaranja bloka na temelju podataka. Promjena podataka unutar bloka zahtjeva promjenu sažetka. Iz ovog se jasno vidi kako su sažeci vrlo korisni ako želimo detektirati promjenu podataka unutar bloka. Ako se sažetak (otisak) bloka promijeni to više nije isti blok. Treći element je sažetak prethodnog bloka. Pomoću njega se stvara lanac blokova jer pomoću sažetka prethodnog bloka možemo jedinstveno odrediti blok koji prethodi u lancu. Prvi blok u lancu nema svog prethodnika te se on naziva *genesis block*. Ako dođe do promjene podataka unutar bloka, mijenja mu se sažetak. Samim time sljedeći blok u lancu više ne pokazuje na ispravan blok te samim time on i svi sljedeći blokovi postaju neispravni. Ipak, sažeci nam ne predstavljaju savršeni mehanizam detekcije izmjene bloka jer su današnja računala vrlo brza te bi mogla izračunati i promijeniti sažetke svih blokova u lancu te se bi se izmjena mogla sakriti. Kako bi se smanjila mogućnost izmjena *blockchain* uvodi mehanizam zvan *proof-of-work* koji usporava stvaranje novih blokova. u slučaju *bitcoina* potrebno je oko 10 minuta da bi se dodao novi blok u lanac. Ovaj mehanizam znatno otežava izmjenu blokova jer bi se kod izmjene jednog bloka morali izmijeniti svi sljedeći blokovi u lancu što je zbog *proof-of-work* mehanizma zahtjeva puno vremena. Uz sažetke i *proof-of-work* mehanizam blockchain ima još jedan mehanizam kojim povećava sigurnost tako da je distribuiran. Umjesto da se

koristi središnji entitet koji upravlja lancem, *blockchain* koristi *peer-to-peer* mrežu kojoj se svatko može pridružiti. Prilikom pridruživanja svaki član dobiva cijelu kopiju lanca. Kod stvaranja novog bloka isti se šalje svim čvorovima u mreži. Svaki čvor ga zatim validira kako bi bio siguran da blok nije izmijenjen. Ako je provjera uspješna svaki čvor dodaje blok u vlastitu kopiju lanca. Čvorovi u mreži postižu konsenzus o tome je li blok valjan te hoće li da dodati u lanac. Dakle, u teoriji se može izmijeniti *blockchain* tako da se izmjene svi blokovi u lancu, odradi *proof-of-work* za svaki blok i preuzme kontrola na više od 50% mreže. Samo tako bi se mogao izmijeniti lanac.

Jedan od novijih mogućnosti *blockchaina* jesu pametni ugovori (engl. *smart contracts*). Pametni ugovori su jednostavni programi koji su spremljeni na *blockchainu* te mogu automatski razmjenjivati kovanice na temelju određenih uvjeta.

# 3. Primjena blockchain tehnologije

## 3.1 Financijski sustav

*Blockchain*, tj. njegova implementacija u financijski sustav je opisana 2008. godine u radu pod imenom "*Bitcoin: A Peer-to-Peer Electronic Cash System*" čiji autor je Satoshi Nakamoto na web stranici *bitcoin.org* koja uvodi novu kriptovalutu *bitcoin*. To je bio prvi primjer korištenja *blockchaina* u praksi. U kriptovalutama *blockchain* rješava problem stvaranja distribuirane baze podataka, bez potrebe za korištenjem posebnog entiteta koji će nadzirati transakcije.

## 3.2 Zdravstveni sustav

Trenutno je zdravstveni sustav vrlo nepovezan. Primjerice kada obavite neku pretragu u jednoj zdravstvenoj ustanovi morate osobno otići po nalaze i u fizičkom obliku ih odnijeti u drugu zdravstvenu ustanovu.. Razlog tome je taj da su medicinski zapisi vrlo povjerljivi te svaka ustanova drži zapise u svojoj bazi zbog nedostatka povjerenja u ostale. Nedavno je taj sustav digitaliziran, ali se javlja veliki sigurnosni problem. Zapisi se drže u jednoj centraliziranoj bazi. Ukoliko bi se zapisi držali u *blockchain* distribuiranoj bazi zapise bi bilo gotovo nemoguće izmijeniti, a korištenjem kriptografije bi se zapisi zaštitili od nedozvoljenog pristupa.

## 3.3 Farmaceutska industrija

Farmaceutska industrija je od kritične važnosti za očuvanje zdravlja i života u današnjem društvu. Upravo je iz tog razloga ona među najprofitabilnijim industrijama u svijetu. Ono što predstavlja veliki problem je to što je velik broj konzumiranih lijekova zapravo lažan. Prema podacima svjetske zdravstvene organizacije (engl. *World Health Organization, WHO*) u nerazvijenim zemljama 1 od 10 lijekova je lažan. Ovaj problem mogao bi se umanjiti tako da postoji sigurniji i pouzdaniji način praćenja lijekova od proizvodnje do polica u ljekarnama. Upravo bi *blockchain* tehnologija u kombinaciji s barkodovima mogla riješiti navedeni problem. Naime, već

je ranije objašnjeno da je *blockchain* zapravo niz (lanac) podataka (blokova) koje je gotovo nemoguće izmijeniti. Ako prilikom proizvodnje, skladištenja, transporta i distribucije proizvođač, dobavljač i distributer unose podatke o trenutnoj fazi (lokaciji i statusu) lijeka svatko može dobiti podatke o cijelom proizvodnom ciklus od tvornice do police u ljekarni s točnim lokacijama i vremenom, a koji imaju veliku razinu povjerenja zbog distribuirane baze podataka na kojoj je zasnovan *blockchain*.

## 3.4 Industrija

Jedan proizvodni proces se sastoji od nabave resursa, korištenja tih resursa u svrhu stvaranja proizvoda te prodaja proizvoda. Ako se radi o velikim tvornicama nerijetko se događaju razne prevare od prodaje resursa lošije kvalitete do podmetanja lažnih proizvoda. *Blockchainom* bi se mogao riješiti taj problem jer bi se s velikom razinom pouzdanosti mogla utvrditi autentičnost svake pošiljke te, ako bi u teoriji kupac mogao saznati od kojeg materijala je izrađen kupljeni proizvod te bi mogao potvrditi njegovu autentičnost.

## 3.5 Glazbena industrija

U glazbenoj industriji uobičajeno je da se glazbenici fokusiraju na stvaranje glazbe i njeno izvođenje dok prodaju i administrativne poslove odrađuju menadžeri i popratno osoblje. Kroz povijest smo vidjeli mnoge slučajeve gdje su menadžeri i glazbenici završili na sudu zbog problema raspodjele novca prilikom prodaje albuma. Ovaj problem bi se također mogao riješiti *blockchain* tehnologijom tako da se svaka kupnja albuma zabilježi zapisom u *blockchain*, a pomoću pametnog ugovora udjeli se automatski izračunavaju i šalju glazbenicima i menadžerima.

## 3.6 Izborni sustav - glasanje

Prevare prilikom izbora su česta tema gotovo kod svih izbora. Prilikom prebrojavanja listića tj glasova imamo jednu centraliziranu državnu agenciju koja vrši taj posao. Ako je netko unutar agencije korumpiran dolazi do prevara koje je vrlo teško uočiti i dokazati. Kada bi se glasanje obavljalo pomoću blockchain tehnologije gdje bi se

listići tj glasovi čuvali u distribuiranoj bazi te bi postupak glasanja postao pravedniji te bi bilo vrlo teško utjecati na ishod.

# 4. Blockchain u računalnoj forenzici

U svakoj istrazi u današnje vrijeme digitalni dokazi imaju vrlo važnu ulogu u slučajevima računalnog kriminala (engl. cyber crime investigation). Oni nam omogućuju da povežemo osobu s kriminalnim radnjama. Od velike važnosti je mogućnost garancije integriteta, autentičnosti i provjerljivost digitalnog dokaza tijekom cijele istrage. *Blockchain* tehnologija ima svojstvo cjelovitog prikaza transakcija (zapisa) sve do izvora koja joj daje veliku razinu povjerenja. Korištenje *blockchaina* u forenzici ima višestruke prednosti. Poboljšava efikasnost transakcijama zbog povećanja povjerenja u ostale sudionike, uvelike smanjuje mogućnost prevare i manipulacije transakcijama te smanjuje trošak spremanja jer više nije potrebna treća strana koja validira transakcije.

## 4.1 Pohrana digitalnih dokaza

Rješenja bazirana na *blockchainu* mogu se iskoristiti za održavanje i praćenje pohrane digitalnih dokaza. *Blockchain* je struktura podataka koja nam omogućuje stvaranje digitalnog dnevnika zapisa i pohranu transakcija (događaja, zapisa) koja je distribuirana među svim sudionicima u mreži. *Blockchain* pomoću kriptografije štiti proces zapisivanja i pohrane zapisa unutar mreže nepobitan revizijski trag. Kako bi se povećala sigurnost izračunava se sažetak digitalnog dokaza i sprema se na *blockchain* preko pametnog ugovora. Ostali detalji kao što su lokacija, vrijeme i datum o mjestu zločina također se zapisuju na *blockchain*. Tijekom istrage svaki prijenos dokaza automatski se zapisuje na *blockchain* pomoću pametnog ugovora, bilježeći podatke kao što su adresa i podaci tko preuzima dokaz, trenutno stanje dokaza, dozvole pristupa, vrijeme i datum i sl. Nadalje, svaki pristup digitalnom dokazu također se zapisuje na *blockchain* pomoću pametnog ugovora potaknutog od strane forenzičara koji dokaz koristi.

## 4.2 Evidencija noćenja u hotelima

Indijski startup Zebi je implementirao sigurnosno rješenje temeljeno na *blockchain* tehnologiji namijenjeno hotelima. Proizvod spaja *blockchain* i umjetnu inteligenciju (engl. *artificial intelligence, AI*) kako bi na siguran način pohranjivao podatke o gostima hotela kako bi spriječio kriminalne aktivnosti. Ista tehnologija je primjenjiva za pohranu zemljišnih knjiga, popisa zaposlenika, obrazovnih certifikata i sl. U Indiji je zakonom propisano da hoteli moraju na dnevnoj bazi policiji davati popis gostiju u čemu ih rješenje temeljeno na *blockchain* tehnologiji oslobađa administrativnog posla te pritom otklanja ljudsku pogrešku i povećava razinu sigurnosti podataka. Prikupljeni podaci se uspoređuju s bazama osoba povezanih s kriminalom i nestalih osoba olakšavajući rad policiji. Takav oblik digitalizacije već je prihvatio i Japan i Singapur.

## 4.3 Interpol

U današnje vrijeme policija se sve češće susreće s kibernetičkim kriminalom. Tako je Interpol otvorio novi odjel koji se isključivo bavi istragama i istraživanjima kibernetičkog kriminala *The Interpol Global Complex for Innovation, IGCI*. Pošto je korištenje kriptovaluta temeljeno na *blockchain* tehnologiji u stalnom porastu Interpol je razvio svoju kriptovalutu kako bi mogao simulirati napade i prevare na kriptovalute i pripremiti se na njih. Također, zanimljivo je da je MIT naglasio kako uvođenjem koncepta pametnih ugovora porasla mogućnost malverzacija kriptovalutama. Upravo je iz toga jasno zašto policija i ostale institucije moraju što prihvatiti *blockchain* tehnologiju i pripremiti se na potencijalne prevare i kibernetički kriminal s kriptovalutama i *blockchainom* općenito.

# 5. Zaključak

*Blockchain* je još uvijek tehnologija u povojima. Iako ima jako puno prednosti i može unaprijediti mnoge aspekte naših života trebat će još dosta vremena dok *blockchain* u potpunosti ne zaživi. Pozitivna stvar je ta da *blockchain* konstantno evoluira i unaprjeđuje se.

Potpuna transparentnost, provjerljivost i visoka razina povjerenja odlike su *blockchaina* koje imaju ogroman potencijal koji može koristiti agencijama za provedbu zakona.

# 6. Literatura


*[1] L. M. Cullell, "Digital Forensics and Blockchain" [Online]. Dostupno: https://medium.com/@blockxlabs/digital-forensics-and-blockchain-bf3af5e7153c. [Pristup: 18. Prosinac. 2018].*

*[2] S. Rothrie, „On the Frontline: How Blockchain Forensics Fight Crypto Crimes“ [Online]. Dostupno: https://coincentral.com/on-the-frontline-how-blockchain-forensics-fight-crypto-crimes/ [Pristup: 18. Prosinac. 2018].*

*[3] Chainanalysis, „Building trust in blockchains“, [Online]. Dostupno: https://www.chainalysis.com/, [Pristup: 18. Prosinac. 2018].*

*[4] J. Nylander, „Interpol Creates Digital Currency To Fight Bitcoin Crimes“, [Online]. Dostupno: https://www.forbes.com/sites/jnylander/2015/08/31/interpol-creates-digital-currency-to-fight-bitcoin-crimes/#6329b0d1195d, [Pristup 7. Siječanj. 2019].*