

Potencijal veći od rudarenja Bitcoina



Piše:
Branko Pavlović,
predsednik
Udruženja aktuara
Srbije

■ **Primena Blockchain tehnologije u osiguranju u budućnosti obezbediće osiguranicima jednostavnost, mobilnost, sigurnost i unapređenje korisničkog iskustva. Osiguravajuće kompanije će proširiti znanje o osiguranicima, poboljšati kontakt sa klijentima i biti u mogućnosti da na osnovu podataka o ponašanju klijenta u prošlosti individualizuju ponude za osiguranje**

Glavni razlog popularnosti Blockchaina su kriptovalute koje se zasnivaju na toj tehnologiji. Najpoznatija kriptovaluta je Bitcoin, čija vrednost je krajem 2017. godine dostigla oko 20.000 američkih dolara, a ubrzo zatim pala na ispod 10.000 dolara. Trenutno, u maju 2018. godine postoji oko 1.600 kriptovaluta i njihov broj se povećava. Mogućnosti primene Blockchain tehnologije daleko prevazilaze kriptovalute. Ovaj rad će biti posvećen predstavljanju Blockchain tehnologije i rudarenja kriptovaluta, sa posebnim naglaskom na primenu u oblasti osiguranja.

Transferi bez posrednika

Koncept Blockchain tehnologije je razvijen 2008. godine u originalnom dokumentu nepoznatog autora koji se potpisao kao Satoshi Nakamoto, što svemu daje izvesnu dozu misterioznosti. Autor je dokazao da se tzv. problem "duple potrošnje" digitalnih dobara može rešiti bez posrednika u koga obe strane imaju poverenja, najjednostavnije rečeno za prebacivanje digitalnog novca sa računara jednog korisnika na račun drugog korisnika nije neophodno posredovanje banke.

Blockchain je javna decentralizovana baza podataka u kojoj se transakcije izvršavaju i potvrđuju anonimno. Pored funkcija baze podataka Blockchain sada ima i mogućnost izvršavanja programa, što predstavlja veliki potencijal za biznis.

Najveće svetske osiguravajuće kompanije: Allianz, Generali, Liberty Mutual, itd. i najmoćnije reosiguravajuće kompanije Munich Re i Swiss Re zajedno su

se angažovale s ciljem da uvedu Blockchain tehnologiju u delatnost osiguranja i reosiguranja, kroz inicijativu B3i. Reosiguranje je po svojoj prirodi mnogo bliže filozofiji Blockchaina, jer puno reosiguravača i retrocesionara deli jedan rizik. Osiguravačima bi mogla da se obezbedi veća transparentnost njihovih reosiguravajućih ugovora. U slučaju transfera rizika iz osiguravajuće kompanije reosiguravaču, Blockchain može da pomogne da se sagleda koliko retrocesionara i na koji način su dalje podelili rizik sa reosiguravačem. Takođe, olakšao bi razmenu informacija o likvidiranim, a naročito rezervisanim štetama, između svih navedenih učesnika u preuzimanju rizika, što bi poboljšalo njihovu adekvatnost tehničkih rezervi. Osiguravač bi dobio brzo i lako potrebne informacije o svim retrocesionarima, koje su neophodne za poboljšanje kapitalne efikasnosti i ispunjenje zahteva za kapitalnu adekvatnost.

Pored reosiguranja, postoji veliki potencijal za primenu Blockchain tehnologije u raznim oblastima osiguranja, o čemu će detaljnije biti pisano u radu.

Privatne i javne Blockchain mreže

Javne Blockchain mreže su dostupne široj javnosti. Svako može da vidi šta je zapisano o izvršenim transakcijama, da pošalje zahtev za transakciju i ako je ispravan ta transakcija će biti uključena u lanac blokova i svako može da se uključi u proces validacije transakcija.

Privatne Blockchain¹ mreže dozvoljavaju uključivanje u mrežu samo pozvanim članovima, tako da ne postoji anonimnost

učesnika, kao kod javnih mreža. Prava postavljanja zahteva za transakcijama su omogućena samo članovima privatne organizacije. Za validiranje je nadležan osnivač privatne mreže ili se validacija radi po pravilima koje on odredi. Prava pristupa izvršenim transakcijama mogu biti omogućena svima ili ograničena na neki način.

Postoji i Konzorcijumska Blockchain mreža, u kojoj samo manji broj unapred određenih čvorova ima prava da vrši validiranje transakcija. Prava postavljanja zahteva za transakcijama i prava pristupa izvršenim transakcijama mogu biti omogućena svima ili ograničena na neki način.

Sve Blockchain mreže imaju puno sličnosti. Decentralizovane su i svaki učesnik je ravnopravan i može po potrebi imati ulogu klijenta ili servera. Svaki član mreže čuva kopiju cele evidencije o svim izvršenim transakcijama. Kopije se sinhronizuju kroz postizanje konsenzusa. U Tabeli 1 su prikazane glavne razlike javnih i privatnih Blockchain mreža.

Ključni izazov sa kojim se sreće javna Blockchain mreža je kako doneti konsenzus članova mreže o tome šta je ispravna transakcija, što je u teoriji igara poznato pod nazivom problem vizantijskih generala. Konsenzus je dinamički način postizanja dogovora unutar grupe. Dok glasanje pogoduje samo interesima većine, konsenzus obezbeđuje poštovanje interesa svih članova grupe.

Ako velika vizantijska vojska koja se sastoji iz velikog broja armija iz različitih krajeva sveta opkoli jedan grad koji ima izuzetno snažnu odbranu, postavlja se pitanje kako generali tih armija da

¹ Jayachandran P. (2017), *The Difference between Public and Private Blockchain*, IBM

postignu konsenzus kada da izvedu koordinirani napad na grad, ako komuniciraju isključivo preko glasnika, a ne sastaju se nikad i nemaju vrhovnog komandanta na terenu. Postizanje konsenzusa je veoma bitno, jer u slučaju odsustva koordinacije i delimičnog napada jake odbrambene snage će sigurno pobediti. Situaciju komplikuju generali koji nisu odani vojski nego imaju svoje interese ili su u prijateljskim odnosom sa vojskom grada koga treba da osvoje. Takođe, glasnici ne mogu da obezbede potpuno pouzdanu razmenu informacija.

Drugim rečima, u pitanju je rešavanje postizanja konsenzusa u decentralizovanim sistemima u kojima ne postoji siguran protok informacija i postoje protivnici sistema.

Blockchain rešava ovaj problema tako što daje podsticaj i nagrađuje Bitcoinima dobro ponašanje, odnosno izvršavanje propisanog algoritma, a čini veoma skupim napad na mrežu uz malu verovatnoću uspeha napada. Satošijev algoritam garantuje da bez obzira šta urade neprijatelji sistema, lojalni članovi će uspeti da postignu konsenzus oko ispravnog rešenja. Sve dok je procesorska snaga lojalnih članova mreže veća od procesorske snage neprijatelja mreže, Blockchain funkcionise ispravno.

Postizanje konsenzusa u Blockchain tehnologiji

Blockchain tehnologija podržava ne samo distribuiranu bazu podataka nego i izvršavanje programskih procedura, tj. uključivanje biznis logike u bazu podataka. Blockchain sistem je vrlo robustan zbog svoje distribuiranosti i ne može se desiti da ceo sistem padne ako neki čvor ne radi ili bude napadnut. S obzirom da distribuirana baza nema centralni autoritet, konsenzus između čvorova mreže o validnosti transakcije je osnovni alat upravljanja sistemom. Postoji više načina postizanja konsenzusa u različitim realizacijama Blockchain sistema od kojih su u javnim Blockchain mrežama najpoznatiji sledeći²:

- Dokaz o radu (engl. Proof of Work) – prvi i najrasprostranjeniji način postizanja konsenzusa, koji se zasniva na rudarenju. Originalno je opisan u Satošijevom radu i na njemu su bazirane kriptovalute: Bitcoin, Litecoin, Bitcoin Cash, Ether, itd. Za validiranje transakcije svaki čvor mora da izvrši kompleksan matematički obračun. Zato uređaj troši određene resurse: električnu energiju i procesorsku snagu. S druge strane, za uspešno validiranje čvor (rudar) bude nagrađen određenom novčanom vrednošću u kriptovaluti.

	Javne mreže	Privatne mreže
Pristup	Prava čitanja i pisanja u bazi su omogućena svima	Prava čitanja i pisanja u bazi se deluju po određenim pravilima
Brzina	Spore	Brze
Bezbednost	Konsenzus se postiže metodama dokaz o radu ili dokaz o ulogu	Učesnici u mreži mogu biti samo oni čvorovi koji su pozvani
Identitet	Anonimni učesnici	Identiteti učesnika su poznati
Troškovi	Skupo	Jeftino

Tabela 1. Poređenje javnih i privatnih Blockchain mreža

Utrošak električne energije je garancija da rudari neće pokušavati da varaju sistem, jer je jedini način da prevara uspe da se raspolaže sa preko 50% procesorske snage celog sistema, odnosno da se potroši preko 50% ukupne električne energije koju sistem troši, što je preskupo. Čak ni tada se ne mogu menjati prethodne transakcije koje su zabeležene u bazi Blockchain, jer je ona nepromenljiva. Što više procesorske snage ima, čvor će brže završiti matematički obračun i dobiti nagradu brže, tj. zaradiće više.

- Dokaz o ulogu (engl. Proof of Stake) – ne podrazumeva rudarenje, jedni čvorovi validiraju transakcije, a drugi ih potvrđuju, ali svi drže deo svog novca u virtuelnom sefu i ko pokuša da prevari sistem, gubi novac; na njemu su bazirane kriptovalute: DASH, NEO, PIVX, itd.
- Delegirani dokaz o ulogu (engl. Delegated Proof of Stake) – takođe nema rudarenja, slično funkcionise kao prethodni, ali se uvode i čvorovi koji su delegati, čija je uloga da odnose odluke o pravilima rada, provizijama, itd. na njemu su bazirane kriptovalute: Steemit, BitShares i EOS.

U privatnim Blockchain mrežama najpopularniji način postizanja konsenzusa je PBFT (engl. Practical Byzantine Fault Tolerance). Ovde se lakše i brže postiže konsenzus, na uštrb anonimnosti, što i nije bitno u privatnim mrežama. Primer njegove realizacije je u sledećim Blockchain sistemima: Hyperledger i Ripple.

Rudarenje bitcoina

Bitcoin

Bitcoin je potpuno digitalna valuta, nije baziran na zlatnoj podlozi, nema zemlju porekla i iza njega ne stoji nijedna državna centralna banka. Nastaje u procesu koji se zove rudarenje, izvršavanjem specifičnih algoritama uz poštovanje striktnih pravila, koja obezbeđuju automatski kriptografski sistemi i Bitcoin zajednica. Rudarenje je automatski proces koji računar obavlja kontinuirano. Od brzine obavljanja

matematičkih proračuna, odnosno procesorske snage računarskog sistema, zavise brzina i efikasnost rudarenja. Tokom rudarenja kriptovalute aplikacija za rudarenje pokušava da pogodi hash kôd novog bloka³. To je 64-cifreni heksadecimalni broj, koji je manji ili jednak traženom hash kôdu bloka koga određuje Blockchain mreža kriptovalute. Računar isprobava jedan za drugim "nonce" (engl. Number Only Created Once) koji je ključ u generisanju hash kôdova. Računar mora da isproba mnogo kombinacija pre nego što pogodi traženi hash kôd. Problem je u tome što ne pogoda hash kôd samo jedan računar. Nagradu dobija aplikacija koja prva pogodi traženi hash kôd. To znači da je moguće rudariti kriptovalute određeni vremenski period, a da se ništa ne zaradi ukoliko računar ima malu procesorsku snagu.

Nagrada za rudarenje, odnosno izradu Bitcoin bloka je 12.5 Bitcoina, što sredinom 2018. godine iznosi oko 100.000 američkih dolara. Blok se formira u proseku na svakih 10 minuta. Vrednost Bitcoina je vrlo promenljiva, krajem 2017. godine je dostigla čak 20.000 dolara. S obzirom da je Bitcoin virtuelan teško je razumeti kako je moguće da vredi toliko mnogo. Ipak treba se setiti da ni papirni novac ne vredi ništa sam po sebi, jer je odavno napušten sistem zlatne podloge novca. Vrednost papirnog novca nastaje zahvaljujući percepciji ljudi da on nešto vredi i podršci centralne banke države koja izdaje novac.

Najperspektivnija zamena za rudarenje Bitcoina je Litecoin, koji je postao popularan zato što je dostigao kritični broj ljudi koji ga rudare, i tako postao relevantan za menjačnice, ali je istovremeno isplativ za samostalno rudarenje, što za Bitcoin zbog velikog broja rudara već odavno nije moguće.

Rudarenje korak po korak

1. Nabavka mašine za rudarenje

Postoje na tržištu već gotove specijalizovane mašine za rudarenje ili se može koristiti kompjuter sa kvalitetnom grafičkom karticom koja ima jak procesor.

² Milinković N. (2017), Uvod u Blockchain – kako se postiže konsenzus u decentralizovanom sistemu?, www.startit.rs

³ Šta je Bitcoin i šta su kriptovalute? Kako rudariti Bitcoin i ostale kriptovalute?, www.balkanandroid.com

Prilikom odabira hardvera važno je obratiti pažnju na:

- Stopu hasha – To je broj operacija koje hardver može odraditi svake sekunde kada pokušava da reši matematički problem. Stopa se meri u hash u sekundi (H/s). Što je veća stopa hasha veće su šanse za rešavanje transakcijskog bloka.
- Potrošnju električne energije⁴ – Rad svakog računara troši energiju, a to naravno košta. Pravilnim izborom računarskih komponenti, važno je podesiti potrošnju električne energije mašine za rudarenje tako da ne troši više energije nego što će zaraditi rudarenjem. Snaga električne energija se izražava u vatima (w). Kvalitet uređaja je srazmerno količini hasheva koje može proizvesti po jednom vatu, odnosno količniku stope hasha i potrošnje struje. Uređaj koji ostvaruje 3 giga hasha u sekundi po vatu je bolji od onog koji ostvaruje 2 GH/s/w.

Može se koristiti i procesor klasičnog računara za rudarenje Bitcoina, ali u praksi ono nema smisla jer je jako sporo. Stopa hasha se može pojačati dodavanjem grafičkih kartica. Idealno bi bilo imati nekoliko grafičkih kartica u kompjuteru. Grafičke kartice su dizajnirane za teške matematičke probleme što ih čini posebno dobrim u rešavanju algoritma za rudarenje pri formiranju transakcijskog bloka. Procesor grafičke kartice daje 50-100 puta veću stopu hasha u odnosu na prosečni procesor klasičnog računara. Grafičke kartice se mogu uspešno koristiti i za rudarenje drugih kriptovaluta kao npr. *Litecoin*.

2. Otvaranje digitalnog novčanika za Bitcoine (engl. Wallet)

Za posedovanje Bitcoina potreban je virtuelni digitalni novčanik. Kada se kreira novčanik, dobijaju se privatna adresa i javna adresa. Privatna adresa je jedini dokaz o posedovanju Bitcoina, odnosno može se uporediti sa ključem kojim se otključava sef u kom su Bitcoini. Javna adresa služi da na nju drugi šalju Bitcoine. Iz javne adrese se ne može rekonstruisati privatna adresa.

3. Uključivanje u "mining pool"

Optimalno rešenje za uspešno rudarenje je priključenje grupi koja zajedno rudari Bitcoine, koja se na engleskom jeziku naziva mining pool. Verovatnoća uspeha pri pokušaju samostalnog rudarenja Bitcoina je jako mala. Pojedinaac sa bilo kakvom mašinom nema dovoljnu procesorsku snagu za takmičenje sa drugim grupama rudara. Pridruživanje grupi rudara značajno povećava verovatnoću uspeha u zavisnosti koliko je veliki mining pool.

Kada se rudarenje uspešno završi, nagrada se pravilno podeli među rudarima u zavisnosti od toga koliko je ko doprineo uspehu. Jedna od najvažnijih odluka pri počinjanju rudarenja je pravilan izbor mining poola. Potrebno je dobro proučiti koje pool je odgovarajući za koga, kako se deli nagrada, koliko je lako prebaciti novac na lični račun itd.

4. Bitcoin klijent

Bitcoin klijent povezuje računar na Blockchain mrežu, omogućava interakciju sa drugim Bitcoin klijentima, prosleđuje transakcije i prati lanac blokova. Da bi mogao početi rudarenje potrebno je

S obzirom na veliki broj ljudi koji se bave rudarenjem, očigledno je da je u ovom trenutku rudarenje uglavnom profitabilan posao. Pošto postoji veliki broj kriptovaluta koje se dobijaju rudarenjem i sa razvojem primene Blockchain tehnologije ih je svakim danom sve više, postoji izuzetno veliki potencijal za zaradu od ovog posla i u bliskoj budućnosti

duže vreme da klijent skine sa mreže ceo Blockchain lanac. Bitcoin klijent automatski sinhronizuje informacije između rudara i mreže.

5. Aplikacija za rudarenje

Softver za rudarenje daje instrukcije hardveru o prolasku kroz transakcijske blokove kako bi ih rešio. Ne postoji univerzalni softver za rudarenje. Izbor aplikacije zavisi od mašine za rudarenje. Postoji veliki broj raspoloživih rudarskih aplikacija. Mnogi mining poolovi imaju svoju aplikaciju koju šalju novom rudaru kada im se pridruži. Aplikacija služi za upravljanje mašinom za rudarenje i omogućava uvid da li se nešto izrudarilo i kolika je nagrada dobijena za to.

6. Početak rudarenja

Pri puštanju u rad celog sistema za rudarenje, često se otkriju neusklađenosti u podešavanju softvera i hardvera. Tek kada sve najzad proradi i delovi Bitcoina počnu da pristižu na javnu adresu virtuelnog novčanika, vidi se da li se ulaganje u hardver i

potrošnja struje i ostalih resursa isplatila.

U praksi se sada rudarenje pomoću grafičkih kartica koristiti uglavnom na drugim kriptovalutama. Otkad su se pojavili specijalno dizajnirani uređaji za rudarenje Bitcoina ASIC (engl. Application Specific Integrated Circuits), kompleksnost rudarenja Bitcoina je toliko porasla, da se grafičke kartice ne mogu takmičiti sa njima.

Profitabilnost rudarenja

Pre bilo kakvog ulaganja u hardver, trebalo bi izračunati mogući profit koji se može ostvariti rudarenjem. Potrebno je proveriti različite scenarije pri rudarenju različitih kriptovaluta. Postoji veliki broj kalkulatora profitabilnosti na Internetu. U kalkulator se unose sledeći parametri: cena hardvera, stopa hasha, potrošnja energije, trenutne cena kriptovalute koja se rudari, zahtevnost mreže tj. koliko je teško rešiti transakcijski blok, itd.

S obzirom na veliki broj ljudi koji se bave rudarenjem, očigledno je da je u ovom trenutku rudarenje uglavnom profitabilan posao. Pošto postoji veliki broj kriptovaluta koje se dobijaju rudarenjem i sa razvojem primene Blockchain tehnologije ih je svakim danom sve više, postoji izuzetno veliki potencijal za zaradu od ovog posla i u bliskoj budućnosti.

Ipak potrebno je biti oprezan. Istraživanje objavljeno na sajtu bitcoin.com⁵, tvrdi da je 46% od 902 kriptovalute ponuđene putem inicijalne javne ponude (engl. Initial Coin Offering = ICO) propalo u 2017. godini. Od toga, 146 nisu uspele skupiti dovoljno novca u ICO fazi, a 276 su ili pale na vrednost nula ili su bile prevara kako bi se neko preko noći obogatio. Većina propalih kriptovaluta nisu imale realnu primenu. Ponuđene su kriptovalute za zubare, vozače kamiona, agente za nekretnine itd, ali ciljne grupe od njih nisu imale nikakve koristi i samim tim nije bilo dovoljno potražnje za njima, pa su propale.

Potencijalna primena blockchain tehnologije u osiguranju u budućnosti

Iako je koncept Blockchain tehnologije objavljen pre deset godina, ne računajući Bitcoin, prve primene se tek sada mogu sresti u finansijskoj industriji. Očekuje se da će ova tehnologija ostvariti svoj pun potencijal tek za pet godina.

U oblasti osiguranja postoje velike mogućnosti za primenu ove napredne tehnologije. Najveći potencijal za razvoj se nalazi u sledećem:

1. mikroosiguranje – Blockchain tehnologija omogućava da se poštuje imperativ malih troškova administracije ugovora o mikroosiguranju, jeftinim obezbeđivanjem pouzdanog registra za polise

⁴ Kako postati rudar, www.crobotcoin.com

⁵ Sedgwick K. (2018) 46% of Last Year's ICOs failed already, news.bitcoin.com

2. isplata šteta – korišćenjem Blockchain infrastrukture za plaćanje moguća je brža i jeftinija isplata šteta, naročito u inostranstvu, npr. po zelenoj karti ili klinikama koje pružaju usluge za putno osiguranje
3. borba protiv prevara – zahvaljujući Blockchain tehnologiji moguće je dobiti znatno više informacija o osiguranim slučajevima, npr. o saobraćajnoj nesreći, iz različitih izvora, i na taj način sprečiti pokušaje prevara u osiguranju. Takođe, mreža uspešno otkriva lažne identitete potencijalnih prevaranata i sprečava višestruko plaćanje iste štete u jednoj osiguravajućoj kompaniji, kao i isplatu jedne štete u više osiguravajućih kompanija.
4. reosiguranje – znatno se olakšava i ubrzava razmena informacija o riziku i šteta između osiguravača, reosiguravača i daljih retrocesionara
5. pametni ugovori – moguća je automatizacija plaćanja šteta kod ove vrste ugovora o osiguranju, pošto Blockchain tehnologija omogućava ispitivanje da li su ispunjeni uslovi za isplatu
6. preuzimanje specifičnih rizika – pojednostavljuje se osiguranje specifične imovine kojoj je teško odrediti vrednost, npr. umetničkih dela, dijamanta itd, pošto Blockchain tehnologija omogućava čuvanje i pronalaženje podataka o poreklu i prethodnim kupoprodajama takvih predmeta
7. preuzimanje standardnih rizika – lakim pristupanjem javnim podacima o prethodnoj istoriji i ponašanju potencijalnog osiguranika, npr. u kasko osiguranju, koje obezbeđuje Blockchain tehnologija može se značajno unaprediti proces preuzimanja rizika.

Ključne prednosti primene Blockchain tehnologije u osiguranju su:

- smanjene troškova pribave, administracije i rešavanja šteta,
- povećanje transparentnosti i poverenja korišćenjem otvorenog distribuiranog sistema,
- povećanje efikasnosti operacija,
- automatsko uključivanje eksternih podataka u proces preuzimanja rizika i određivanja cena,
- povećanje brzine isplate šteta i
- smanjenje ukupnih isplaćenih iznosa za štete kroz efikasnije otkrivanje prevara.

U Tojoti smatraju da ova tehnologija može postići velike rezultate kada se primeni na automatizaciju vožnje i delatnost osiguranja na sledeći način: senzori u automobilu sakupljali bi podatke prilikom vožnje, čuvali ih u Blockchain lancu, a u slučaju saobraćajne nesreće ti podaci bi se slali osiguravajućoj kompaniji, koja bi na taj način mogla bolje da proceni štetu.

Mogu se zamisliti razni scenariji u kojima će se koristiti Blockchain tehnologija u osiguranju u situacijama koje u ovom trenutku nisu moguće, ali će u relativno bliskoj budućnosti postati realnost, između ostalog i zahvaljujući ovoj tehnologiji.

Scenario 1: Osiguranje od autoodgovornosti samo u periodu kada se automobil koristi

U savremenom svetu sve češća je kupovina različitih usluga samo u relativno kratkom vremenskom periodu, kada se one zaista koriste. Primer osiguranja budućnosti je da vozilo nije više osigurano od autoodgovornosti tokom cele godine, nego samo u vremenskom periodu kada se vozi. U osiguranju to će se najlakše postići korišćenjem mobilne aplikacije u kojoj se osiguravajuće pokriće kupuje samo za period kada je ono potrebno. Jedna od mogućih realizacija takvog osiguranja, korišćenjem Blockchain tehnologije, izgleda na sledeći način. Automobil šalje potrebne podatke o sebi aplikaciji osiguravajuće kompanije koja je instalirana na mobilnom uređaju klijenta, i kada klijent unese očekivani vremenski period putovanja, aplikacija osiguravajuće kompanije izračuna premiju osiguranja i prikaže klijentu ponudu. Ukoliko klijent prihvati ponudu šalje zahtev za osiguranjem u Blockchain mrežu. Čim mreža

Potrebno je biti oprezan. Istraživanje objavljeno na sajtu bitcoin.com, tvrdi da je 46% od 902 kriptovalute ponuđene putem inicijalne javne ponude propalo u 2017. godini

validira zahtev, podaci se upisuju u Blockchain evidenciju i osiguravajuće pokriće počinje da važi. Kada klijent posle nekog vremena odluči da se vrati kući, pošto je njegovo prethodno pokriće za isti put u suprotnom smeru već u Blockchain evidenciji, jednim klikom se aktivira osiguravajuće pokriće za povratno putovanje.

Scenario 2: Kasko osiguranje automobila bez vozača

Vozila bez vozača se već testiraju širom sveta i samo je pitanje trenutka kada će postati realnost na ulicama i ko će ih i kako osigurati. Kada autonomno, samoupravljujuće taksi vozilo završi sa vožnjom putnika, na najbližoj taksi stanici čeka sledeću mušteriju. Nekoliko vandala vidi da je prethodna mušterija zaboravila nešto na sedištu i razbiju prozor da to ukradu. Automobil automatski poziva policijske dronove koji doleću da snime lica i lokacije ovih osoba i plaća dronovima ovu uslugu. Nakon

toga se odveze do servisa gde mu zame-
ne staklo. Snimci drona i račun od mehaničara se šalju osiguravajućoj kompaniji i šteta se isplaćuje praktično odmah, što je značajno brže nego po trenutno važećoj proceduri. Automobil se relativno brzo vraća na posao.

Scenario 3: Rešavanje šteta

Proces rešavanja šteta je najpogodniji za implementaciju Blockchain tehnologije. Momenat rešavanja štete je trenutak istine za osiguravajuću kompaniju, jer od toga zavisi dalji odnos sa klijentom. U slučaju da ovaj proces ne ide glatko, neminovan je gubitak poverenja klijenta u kompaniju i prekid dalje saradnje. Najveći izazovi u ovom procesu su sledeći:

- ručno unošenje podataka u prijavu štete,
- previše birokratizovana i komplikovana procedura rešavanja šteta,
- skupi posrednici kod kojih se može prijaviti šteta,
- kašnjenje u rešavanju zbog ispitivanja da li je u pitanju prevara u osiguranju,
- veliki broj dokumenata koji je potrebno prikupiti za rešavanje štete,
- ručno pripremanje dokumentacije za isplatu i
- predugo čekanje na isplatu rešene štete.

Blockchain tehnologija može pomoći u prevazilaženju većine navedenih izazova zahvaljujući tome što donosi transparentnost, a samim tim i poverenje, procesi su vrlo efikasni i sve se zasniva na postignutom konsenzusu.

Postojeći proces rešavanja šteta

Tradicionalne osiguravajuće kompanije često imaju procese obrade šteta organizovane na sledeći način:

1. Klijenti dostavljaju podatke o nastalim štetama osiguravajućim kompanijama. Vrlo često nedostaju pojedini podaci, a nekad se dešava i da su dostavljeni podaci nekonzistentni. Takođe, nekad su i falsifikovani, pošto američka statistika kaže da je oko 10% svih prijavljenih šteta u stvari pokušaj prevare u osiguranju.
2. Regulator delatnosti osiguranja ili udruženje osiguravača obično pokušava da uspostavi centralnu evidenciju o štetama. To je prilično veliki teret za njihovu administraciju, prvenstveno zbog raznorodnih informacionih sistema koje imaju osiguravači i njihove nemogućnosti da dostave potpuno ispravne podatke.
3. Podaci o štetama se dostavljaju u određenim slučajevima sudu, organizacijama za zaštitu prava potrošača i sličnim organizacijama. Ti procesi su potpuno netransparentni za klijenta.
4. Razmena podataka o rešenim i rezervisanim štetama sa reosiguravačem je spora i komplikovana, jer se najčešće vrši ručno.

Unapređeni proces rešavanja šteta⁶

Uvođenjem Blockchain distribuirane kriptovane evidencije čiji čvorovi mreže su osiguravajuće kompanije, regulator, udruženje i reosiguravači, proces se može prilično unaprediti. Procesi bi izgledali ovako:

1. Svi podaci o štetama su upisani u Blockchain evidenciji i njihova ispravnost je potpuna, jer je zasnovana na konsenzusu, npr. datum nastanka štete su potvrdili i klijent i osiguravajuća kompanija. Jednom upisani podaci se ne mogu menjati, što otežava falsifikovanje i praktično onemogućava pokušaj prevare u osiguranju.
2. Regulator i udruženje imaju podjednako lak i brz pristup podacima kao i osiguravajuće kompanije.
3. Sud i ostale zainteresovane strane, posle autorizacije od strane nadležnih čvorova mreže, takođe mogu podjednako efikasno pristupiti svim podacima za koje su ovlašćeni da vide.
4. Reosiguravači su deo mreže i imaju uvid u sve podatke o štetama u trenutku upisa kao i osiguravači.

Očigledno, proces je značajno unapređen na opštu korist svih zainteresovanih strana. Klijent dobija uvid i kontrolu nad upotrebom njegovih podataka, jeftiniju sledeću polisu ako ima dobru istoriju šteta i u slučaju šteta manje dokumenata mora da prikupi. Osiguravač se uspešnije bori protiv prevara u osiguranju, ima efikasnije interne procedure, pruža kvalitetniju uslugu klijentu pa samim tim ima i bolji odnos sa klijentom. Takođe, svaki osiguravač dobija pristup štetama za svakog potencijalnog klijenta, što mu omogućava bolje upravljanje rizikom portfelja. Reosiguravač ima automatizovan pristup i rad sa podacima o štetama osiguravača.

Primena blockchain tehnologije u osiguranju u 2018. godini

Moguće je dizajnirati zaista veliki broj primena Blockchain tehnologija u osiguranju, ali osim teorije i implementacija određenih rešenja je daleko odmakla. U daljem tekstu biće više reči o konkretnim primerima implementacije ove tehnologije u delatnosti osiguranja.

Konzorcijum B3i

Jedan od primera uspešne implementacije Blockchain tehnologije u osiguranju i retrocesiji je B3i konzorcijum, koji je obezbedio dokaz koncepta korišćenja distribuirane evidencije koja menja tradicionalnu infrastrukturu, u cilju povećanja brzine razmene informacija i smanjenja rizika. Ključne odrednice misije ove

Postojeći proces reosiguravanja	Proces reosiguravanja uz pomoć Blockchain tehnologije
• Ugovor se ručno definiše na papiru	• Ugovor se definiše digitalno na platformi B3i
• Pisano i usmeno pregovaranje o svakom ugovoru između više brokera i reosiguravača	• Pregovaranje između više brokera i reosiguravača je automatizovano
• Podatke ručno obrađuju svi učesnici za sebe	• Podaci se unose samo jednom, a obrađuju se automatski u Blockchain mreži
• Fature i potraživanja svako pravi za sebe, pa je neophodno usaglašavanje svih strana	• Fature i potraživanja generiše mreža, pa je usaglašavanje nepotrebno
• Komplikovano i dugotrajno usaglašavanje uzrokuje kašnjenja u prenosu novca	• Pošto nema usaglašavanja prenos novca je značajno ubrzan
• Kopije ugovora se čuvaju lokalno	• Ugovor se čuva u Blockchain mreži

Tabela 2. Poređenje postojećeg i budućeg procesa reosiguravanja

inicijative su: standardizacija, integracija i automatizacija. Osnivači konzorcijuma su među najvećim i najznačajnijim osiguravajućim i reosiguravajućim kompanijama u svetu⁷: Achmea, Aegon, Ageas, Allianz, Generali, Hannover Re, Liberty Mutual, Munich Re, RGA, SCOR, Sampo Japan Nipponkoa, Swiss Re, Tokio Marine, XL Catlin i Zurich.

Savremeni proces reosiguravanja je prilično neefikasan i nije se mnogo menjao u poslednjih stotinak godina. Neefikasnost dovodi do kašnjenja u obradi ugovora o reosiguranju i šteta, što donosi reputacioni rizik za osiguravača i eventualne probleme sa tokovima gotovine, kao što je prikazano u Tabeli 2.

Distribuirana evidencija koju nudi Blockchain tehnologija može značajno da unapredi proces reosiguravanja⁸. Ukoliko bi se u Blockchain evidenciju uključili svi ugovori o reosiguranju, izgubila bi se potreba za usaglašavanjem jer bi se svi podaci nalazili na jednom mestu u jedinstvenoj distribuiranoj evidenciji čije kopije se nalaze kod svih osiguravača i reosiguravača. Postojao bi jedan standard za obradu podataka i jedna platforma koja bi se izvršavala automatski. Sve to bi ubrzalo proces, optimizovalo tokove gotovine i obezbedilo potpuno integrisani informacioni sistem.

U septembru 2017. godine članovi inicijative delatnosti osiguranja B3i su prvi put predstavili funkcionalnu beta verziju IT rešenja upravljanja ugovorima o imovinskom reosiguranju viška štete za slučaj katastrofa tipa smart contract, zasnovanog na Blockchain tehnologiji. Reosiguranje viška štete (engl. Excess of Loss) po katastrofalnom događaju je neproporcionalni ugovor o reosiguranju koji limitira

akumulirane štete koje mogu nastati ostvarenjem katastrofalnog događaja. Obično do određenog iznosa akumuliranih šteta reosiguravač ne plaća ništa, ali plaća sve štete preko tog iznosa.

Očekuje se da do kraja trećeg kvartala 2018. godine bude završeno testiranje beta verzije i lansirana unapređena aplikacija "Codex1 Property Cat XL Treaty" koja će se koristiti na tržištu reosiguranja. Osnovne funkcionalnosti aplikacije, koja bi trebalo da bude dostupna u celom svetu, su cediranje, preuzimanje i dalje trgovanje rizikom na tržištu reosiguranja. Blockchain tehnologija podrazumeva korišćenje jedne distribuirane evidencije o ugovorima o reosiguranju, koja omogućava sigurne, poverljive i efikasne transakcije. U budućnosti, ovo rešenje za reosiguranje će biti prošireno i na delatnost osiguranja.

Analizom slučaja⁹ utvrđeno je da ovo rešenje povećava produktivnost, odnosno smanjuje administrativne troškove za 30%, što bi dovelo do smanjenja kombinovanog racija oko 2 procentna poena. S obzirom da je ukupna godišnja premija ove vrste reosiguranja oko 60 milijardi USD, primenom ovog rešenja cela industrija osiguranja bi povećala profit za preko milijardu američkih dolara godišnje.

B3i rešenje se implementira u IBM-ovoj privatnoj Blockchain mreži, pod nazivom Hyperleder Fabric Network. Početkom 2018. godine, mreža je imala 117 čvorova koji se bave validiranjem transakcija, što je čini najvećom mrežom ovog tipa.

Osiguranje sezonskog skipassa

Parametarsko osiguranje je poznato od ranije, ali Blockchain tehnologija mu daje novu vrednost i obezbeđuje potpunu

⁶ Generali claims team (2017), *Blockchain Use Case: Claims Management*, Generali Blockchain Conference, Mogliano Veneto, Italy

⁷ www.b3i.tech

⁸ De Crom S. (2017), *Blockchain: the Potential to Drive Efficiencies across the Industry*, Aegon, Utrecht, Nederland

automatizaciju i transparentnost. Glavne karakteristike parametarskih proizvoda su:

- Štete se isplaćuju kada se izmere predefinisane vrednosti parametara rizika, npr. nivo vode u reci, broj dana bez kiše itd. Parametri moraju biti konzistentni, lako merljivi i stalno ažurni;
- Izvor informacija za parametre treba da bude automatski merljiv i potpuno nezavisan od uticaja osiguravača i osiguranika.

Navedeni tip osiguranja ima velike prednosti: brza i konzistentna isplata šteta, transparentnost proizvoda, maksimalno jednostavna administracija kod osiguravača, nemogućnost prevara u osiguranju, mala neizvesnost jer su parametri obično jednostavni rizici, mogućnost da se osiguraju rizici koji do sada nisu osiguravani, itd. Blockchain tehnologija može u potpunosti automatizovati rad sa parametarskim proizvodima osiguranja.

Generali u Italiji priprema inovativni proizvod osiguranja sezonskog skipassa u skijaškoj regiji Prato Nevoso¹⁰, koji će biti realizovan u Blockchain tehnologiji. Kupovinom ovog proizvoda skijaši koji imaju sezonski skipass mogu da refundiraju deo novca za dane kada uslovi za skijanje nisu bili prihvatljivi. Ukoliko su optimalni uslovi za skijanje, što znači da je radilo više od 70% staza na skijalištu u regiji Prato Nevoso, trajali manje od 20 dana refundira se 50% troškova dnevnog skipassa (17 EUR), za svaki dan kada uslovi nisu bili optimalni. Takođe, refundira se i 50% troškova dnevnog skipassa sa popustom (12,5 EUR), za svaki dodatni dan kad skijanje nije bilo moguće iz bilo kog razloga. Ova refundacija se vrši automatski na račun skijaša, čim se steknu uslovi, bez potrebe da se skijaši obraćaju Generaliju i prijavljuju štetu. Kupovinom ovog osiguranja, skijaši koji skijaju celu sezonu dobijaju novu vrednost, odnosno imaju komparativnu prednost skijanja u ovoj regiji u odnosu na ostale.

Svi pravni i aktuarski detalji ovog proizvoda su potvrđeni i izabran je agent koji će ga prodavati. Lansiranje proizvoda se očekuje tokom 2018. godine.

Oblasti primene bezbrojne

Posle samo deset godina od pojave Satošijevog rada kojim je promovisana Blockchain tehnologija, stekli su se uslovi za njenu masovniju primenu. Iako se očekuju značajniji efekti njene primene tek za pet godina, pored trgovine kriptovalutama, već sada ima zanimljivih i korisnih implementiranih projekata koji se

Ethereum i pametni ugovori

Ethereum¹¹ je javna mreža realizovana u Blockchain tehnologiji u kojoj su implementirani pametni ugovori i u kojoj je moguće izvršavati decentralizovane aplikacije. Tvorac Ehtereuma je Vitalik Buterin koji je 2013. godine u svom radu predložio unapređenje Satošijevog koncepta Bitcoina i na taj način omogućio realizaciju pametnih ugovora i izvršavanje decentralizovanih aplikacija. To je postigao pomoću Ethereum virtuelne mašine, odnosno softvera koji radi u Ethereum mreži i omogućava izvršavanje programskog koda bilo koje decentralizovane aplikacije. Pored naknade za validaciju transakcija, kao kod Bitcoina, rudari ovde bivaju nagrađeni kriptovalutom Ether i zato što izvršavaju servise na mreži.

Pametni ugovori omogućavaju implementaciju razmene novca, imovine, akcija i bilo čega drugog što ima vrednost na transparentan i beskonflikatan način bez posredovanja treće strane. Oni se automatski izvršavaju. Nastaju kada se klasični ugovori pretvore u programski kôd i čuvaju u Blockchain mreži, a zatim ih se svi čvorovi pridržavaju i izvršavaju ih. Ugovori definišu pravila i kazne u slučaju nepoštovanja i sprovode se automatski, i time umesto pravne sigurnosti klasičnih ugovora daju algoritamsku sigurnost, odnosno garanciju da će se sigurno realizovati.

Karakteristike pametnih ugovora koji imaju izuzetan potencijal u biznisu su:

- poverenje – podaci su zauvek nepromenljivi u Blockchain mreži,
- transparentnost – sve ugovorne strane su nedvosmisleno pristale na uslove iz ugovora,
- sigurnost – podaci su zaštićeni kriptovanjem,
- brzina – automatsko izvršavanje je višestruko brže od manualnog,
- autonomija – nema potrebe za advokatima ni drugim posrednicima i
- niže cene – svi posrednici su eliminisani, pa cena pada.

baziraju na ovoj tehnologiji. Oblasti primene ove tehnologije su bezbrojne, ali rad je bio posvećen primeni u delatnosti osiguranja.

Mogu se zamisliti razni scenariji u kojima će se koristiti Blockchain tehnologija u osiguranju u situacijama koje u ovom trenutku nisu moguće, ali će u relativno bliskoj budućnosti postati realnost

Primena Blockchain tehnologije u osiguranju u budućnosti obezbediće osiguranicima jednostavnost, mobilnost, sigurnost i unapređenje korisničkog iskustva. Osiguravajuće kompanije će proširiti znanje o osiguranicima, poboljšati kontakt sa klijentima i biti u mogućnosti da na osnovu podataka o ponašanju klijenta u prošlosti individualizuju ponude za osiguranje. Sve zainteresovane strane će dobiti pouzdane sisteme koji neće moći da padnu, dokaze o izvršenim transakcijama koji se ne mogu falsifikovati i kompletnu istoriju transakcija koja se može pratiti i koristiti po potrebi.

S obzirom na kratku istoriju korišćenja Blockchain tehnologije od samo nekoliko godina, nisu još uvek rešeni svi problemi što otežava da ova inovativna tehnologija ostvari svoj pun potencijal u praksi. Ne postoje standardni protokoli, kao npr. http protokol za Internet, niti jedinstveno rešenje za implementaciju Blockchain tehnologije. Određeni ekosistemi pokušavaju da nametnu svoju verziju kao standard (Hyperledger, Bitcoin, Ethereum, itd.) što je karakteristika ranog razvoja različitih tehnologija. Integritet podataka koji obezbeđuje Blockchain tehnologija u ovom trenutku ugrožavaju kvantni kompjuteri. Potrošnja električne energije za validiranje transakcija raste sa povećanjem mreže, tako se dovodi u pitanje buduća ekonomska opravdanost korišćenja ovog rešenja. Iako će proteći neko vreme dok se svi problemi ne reše, sada je pravi trenutak za eksperimentisanje i pilot projekte u cilju pronalaska odgovarajućeg poslovnog modela u delatnosti osiguranja. Konzorcijum najpoznatijih svetskih osiguravajućih i reosiguravajućih kompanija, B3i, prepoznao je ovaj trenutak i preduzeo korake koji će dovesti do prve značajne implementacije Blockchain tehnologije u delatnosti osiguranja, odnosno reosiguranja u 2018. godini. ■

⁹ Di Marzo A. (2017), *B3i Consortium: the Future of (Re)Insurance Transactions*, Generali Blockchain Conference, Mogliano Veneto, Italy

¹⁰ Group of authors (2017), *Parametric Insurance: a 100% Automatic and Transparent Solution*, Generali Blockchain Conference, Mogliano Veneto, Italy

¹¹ Milinković N. (2017), *Uvod u Blockchain – Ethereum i pametni ugovori*, www.startit.rs