USAID
OD AMERIČKOG NARODA

Inicijativa
Digitalna Srbija

UVOD U BLOKČEJN

Autor:
Aleksandar Matanović

SADRŽAJ

Izrada ovog vodiča omogućena je uz podršku američkog naroda putem Američke agencije za međunarodni razvoj (USAID).
Sadržaj ovog istraživanja je isključivo odgovornost Inicijative „Digitalna Srbija“ i ne predstavlja nužno stavove USAID-a ili Vlade SAD.

UVOD

ŠTA JE BLOKČEJN?

Najkraće rečeno, Blokčejn je inovativan protokol za razmenu i skladištenje informacija. Ne zvuči baš spektakularno, ali zapravo jeste. Da bismo razumeli kako se ti podaci šalju i skladište, možda je najbolje da setimo pojave **tabela na Google drive-u**. Ono što je tu tabelu razlikovalo od obične Excel tabele iz tog vremena, koju ste imali na svom računaru, pre svega je mogućnost da više ljudi čita, menja i unosi podatke. Iz ugla administriranja tabele, to je deljena baza podataka. Ipak, iz ugla skladištenja podataka, ona je centralizovana jer se nalazi sa na Google-ovim serverima.

U međuvremenu je i Microsoft napredovao, pa sada i Excel ima mogućnost da čuvate tabelu na svom računaru, ali da je ona istovremeno i deljena sa drugim ljudima. Dakle, kad god bih ja u svojoj kopiji te Excel tabele nešto uneo, odmah bi svi ostali videli taj unos u svojoj kopiji te tabele, jer se tabele automatski sinhronizuju međusobno pri svakom upisu. Na ovaj način nije samo administriranje distribuirano, već i skladištenje tabele, jer svako ima svoju kopiju na svom računaru. Zamislimo sada i da pri svakom unosu, svi drugi učesnici imaju zadatak da provere validnost tog unosa (da li uneti podatak ispunjava određena, unapred zadata, pravila) i da tek po proveri validnosti uneti podatak trajno postaje deo te zajedničke tabele. Ako dodamo još i pravilo da jednom uneti podatak ne može da se obriše ili izmeni, ta baza podataka postaje vrlo slična **Blokčejnu**. Ostalo je još nekoliko sitnica.

> Blokčejn je inovativan protokol za razmenu i skladištenje informacija.

> Podaci se pakuju u blokove, a ti blokovi se kriptografski međusobno povezuju u lanac. Upravo to čini promenu unetih podataka nemogućom.

Dodatna razlika između Blokčejna i obične tabele je sam format u kojem se podaci skladište. Kako samo ime kaže, **Blokčejn je lanac blokova**. Dakle, podaci se pakuju u blokove, a ti blokovi se kriptografski međusobno povezuju u lanac. Upravo to čini promenu unetih podataka nemogućom. Na kraju, ono što smo postigli u odnosu na deljenu tabelu na Google drive-u je da su i administriranje i čuvanje podataka distribuirani među učesnicima tako da nijedan pojedinačni učesnik nema mogućnost da ugrozi bazu ili bilo šta u njoj izmeni bez širokog konsenzusa ostalih učesnika.

ŠTA ZAPRAVO ZNAČI PEER-TO-PEER?

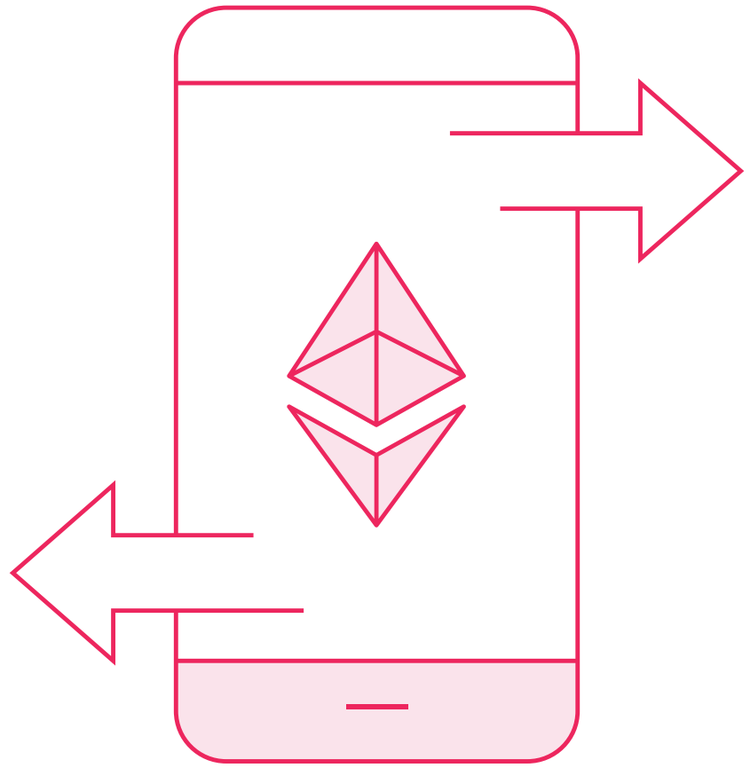
Kod deljene tabele na Google drive-u, tok informacija je takav da se svaki učesnik povezuje na Google-ov server i tako upisuje informacije i čita informacije koje su drugi upisali. Iako je to vrlo praktičan način zajedničkog administriranja baze podataka, centralizovan pristup ima i neke nedostatke. Na primer, eventualni problemi sa Google serverima bi doveli do toga da je baza svima nedostupna. Takođe, Google ima mogućnost da tu bazu izmeni ili čak ukloni bez pristanka učesnika ako bi zbog nekih svojih pravila doneli takvu

odluku. U Blokčejn sistemu se ne komunicira preko centralnog entiteta, već učesnici komuniciraju direktno između sebe putem peer-to-peer mreže. Sam naziv ukazuje na to da u komunikaciji između učesnika ne postoji posrednik. Da bi ta komunikacija bila moguća, potrebno da je budu online i da imaju instaliran odgovarajući softver. Pomoću tog softvera kopije zajedničke baze podataka se međusobno sinhronizuju. Kada kažemo da učesnici direktno između sebe komuniciraju, to ne znači da je svaki učesnik direktno povezan sa svakim drugim učesnikom, jer bi takva struktura bila nepotrebno kompleksna. Umesto toga, svaki učesnik je direktno povezan sa svega nekoliko drugih učesnika, a sa ostalima je povezan indirektno.

Zamislimo jednu tenisku ili odbojkašku mrežu. Svaki čvor na toj mreži bi bio učesnik, a parče konopca između 2 čvora bi bila direktna veza između 2 učesnika. Svaki čvor je direktno povezan sa samo nekoliko drugih (na primeru mreže taj broj je 4), ali je indirektno povezan sa svim drugim čvorovima. Kroz takvu mrežu, svaka nova informacija lako dođe do svih čvorova (učesnika) odakle god da je ta informacija krenula.

Sjajna osobina ovakve strukture je što informacija uvek lako nađe put do svih, čak i kad nisu svi učesnici online, kao što i teniska mreža i dalje vrši svoju funckiju čak i ako se pokida na par mesta. Ipak, peer-to-peer mreža ima i jednu korisnu osobinu koju teniska mreža nema.

Naime, ako bi neko presekao tenisku mrežu na pola, ona više ne bi bila funkcionalna. Međutim, čak i ako bi neko uspeo da "pokida" **peer-to-peer** mrežu tako što bi prekinuo sve moguće veze između 2 dela mreže, mreža bi se sama brzo ponovo povezala, jer softver svakog učesnika funkcioniše tako da čim se jedna veza prekine (recimo kad neki od učesnika ode offline), on automatski traži drugog učesnika sa kojim će direktno da se poveže.



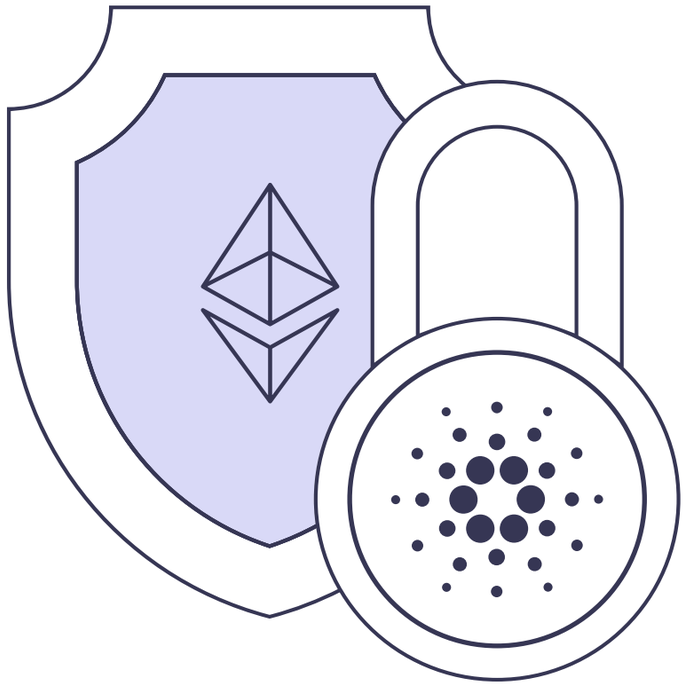
OSNOVNI PRINCIPI BLOKČEJNA

Karakteristike koje su do sada navedene čine Blokčejn strukturom sa prilično jedinstvenom kombinacijom osobina. Zbog peer-to-peer arhitekture mreže, struktura nema **SPOF (Single Point Of Failure)**. Savršeno dobro funkcioniše bez obzira na to koji broj učesnika je online ili offline. Pošto svaki učesnik ima svoju kopiju baze podataka koja se automatski sinhronizuje sa drugim kopijama, sa aspekta čuvanja podataka ovakva struktura je neuporedivo sigurnija od bilo čega što smo ikada imali. Kad nam je neka baza podataka bitna, dobro je povremeno raditi backup. Što je bitnija baza, to češće treba raditi backup i treba imati više kopija. Zamislite da imate bazu podataka sa 10.000 kopija koje se automatski ažuriraju u realnom vremenu. Blokčejn omogućuje upravo to.

Zbog peer-to-peer arhitekture mreže, struktura nema SPOF (Single Point Of Failure). Savršeno dobro funkcioniše bez obzira na to koji broj učesnika je online ili offline.

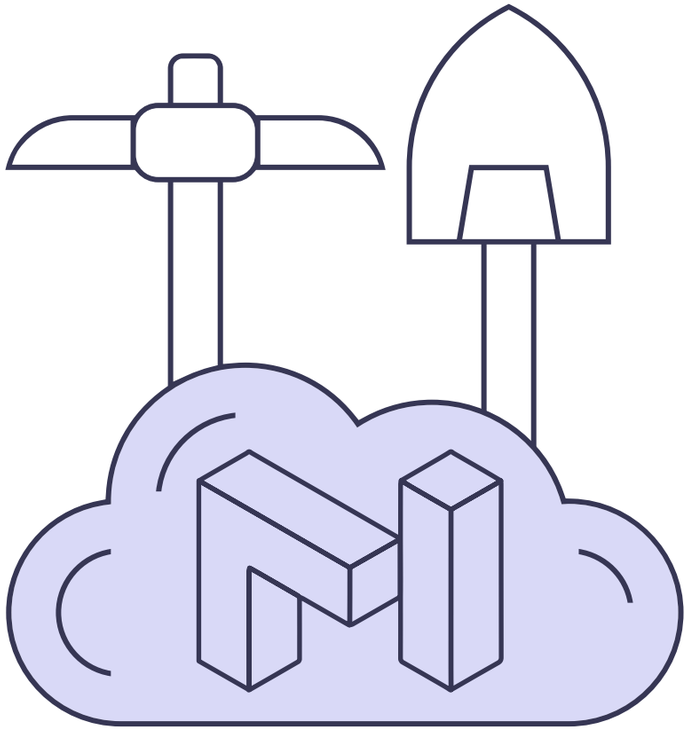
Ne samo da imamo u svakom trenutku veliki broj kopija baze, već su i podaci u toj bazi nepromenljivi, što je veliki korak napred kad je u pitanju **verodostojnost podataka**. To je omogućeno strukturom baze, to jest činjenicom da se podaci pakuju u blokove podataka koji su međusobno kriptografski povezani. Inače, kriptografija se u Blokčejn sistemima prilično intenzivno koristi, otuda ono “kripto” u kriptovalutama.

Ne samo da imamo u svakom trenutku veliki broj kopija baze, već su i podaci u toj bazi nepromenljivi, što je veliki korak napred kad je u pitanju **verodostojnost podataka**.



KLASIFIKACIJA BLOKČEJNA

Hronološki gledano, javni Blokčejn je starija vrsta Blokčejna od privatnog. Mnogi kripto i Blokčejn entuzijasti će reći da je javni Blokčejn jedini pravi Blokčejn i da privatni zapravo ne manifestuje osnovne vrednosti koje Blokčejn tehnologija nudi. Iako "javni vs. privatni Blokčejn" nije nešto što može da se posmatra crno-belo, jer ima puno Blokčejn rešenja koja su negde između (ni potpuno javni, ni potpuno privatni), pomenućemo koje su osnovne razlike između ove 2 vrste pristupa Blokčejn tehnologiji.



Javni Blokčejn je potpuno otvoren. Svako na svetu ima pravo da čita podatke upisane u Blokčejn, da validira unose drugih učesnika, da pakuje podatke u blokove i dodaje te blokove na već postojeću bazu podataka (što je inače poznato kao "rudarenje"), da predlaže izmenu softvera radi unapređenja funkcionisanja Blokčejna i da učestvuje u odlučivanju vezano za izmene softvera. Što je najbitnije, ne samo da svako ima ova prava, nego su i svima ta prava jednaka.

> Mnogi kripto i Blokčejn entuzijasti će reći da je javni Blokčejn jedini pravi Blokčejn i da privatni zapravo ne manifestuje osnovne vrednosti koje Blokčejn tehnologija nudi.

Sa druge strane, privatni Blokčejn nije otvoren za sve, već samo za one kojima je kreator Blokčejna namenio da imaju pristup. Isto važi i za sva druga prava. Kreator Blokčejna odlučuje ko ima pravo da unosi podatke, ko ima pravo da validira unose drugih učesnika, ko kreira blokove i ko učestvuje u izmenama na softveru. Ovde nisu svi učesnici ravnopravni, već različiti učesnici mogu imati različita prava.

Princip otvorenosti kod javnih Blokčejna se manifestuje i kada je u pitanju softver. Naime, on je otvorenog koda (open source), dok kod privatnih Blokčejna to mahom nije slučaj. Zagovornici javnih Blokčejna smatraju da je open source pristup prirodno superioran, jer to što je izložen svakome da ga vidi omogućuje da se eventualne greške u softveru mnogo brže otkriju i koriguju.

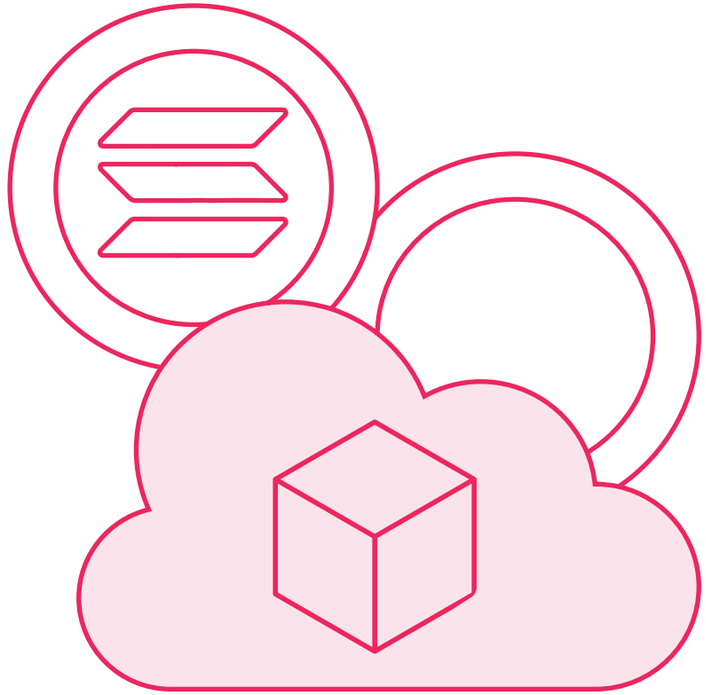
Posledice navedenih karakteristika su to da su javni Blokčejni bez dileme superiorni kad je u pitanju bezbednost i integritet podataka. Sa druge strane, privatni često prednjače kad su u pitanju performanse (količina podataka koja se može skladištiti, brzina upisa novih podataka i skalabilnost generalno). Takođe su fleksibilniji jer sve odluke donosi značajno manji broj učesnika, pa se naravno odluke mogu brže doneti. Samim tim, nameće se zaključak da je javni Blokčejn sjajan u situacijama kad imamo podatke velike vrednosti čija nam je verodostojnost i bezbedno čuvanje izuzetno bitno, a ti podaci nisu preterano veliki (mereno u bajtovima) niti postoji preterano veliki broj upisa u jedinici vremena. Nasuprot tome, kada treba brzo obraditi veliku količinu podataka, a vrednost tih podataka nije velika, onda je verovatno privatni Blokčejn bolji izbor, mada se u mnogim situacijama može postaviti pitanje zašto uopšte koristiti Blokčejn ako imamo alternativu u nekom potpuno centralizovanom sistemu, koji ima još bolje performanse.

Ipak, u praksi se često dešava da postoji potreba za kombinovanjem osobina javnih i privatnih Blokčejnova, pa između **potpuno javnih i potpuno privatnih** Blokčejna postoji čitav spektar onih koji su negde između.

Pravi balans između bezbednosti i performansi se neretko pokušava postići korišćenjem **Sidechain-ova.** Naravno da veliki javni Blokčejn (poput Etereuma) teško može da zadovolji potrebe svih korisnika istovremeno, delom zbog kapaciteta, delom i zbog činjenice da su za različite aplikacije potrebne različite karakteristike da bi mogle optimalno da funkcionišu. Sidechain-ovi taj problem rešavaju time što su dizajnirani baš specifično za neku određenu funkcionalnost, a povezani su sa glavnim Blokčejnom uglavnom da bi one najbitnije podatke upisivali na njega.

Pravi balans između bezbednosti i performansi se neretko pokušava postići korišćenjem Sidechain-ova.

Razlog za to je ranije pomenut visok nivo verodostojnosti podataka koji se nalaze na velikim javnim Blokčejnima. Iako paralela nije do kraja adekvatna, možda bi se odnos glavnog Blokčejna i njegovih sidechain-ova mogao opisati kao odnos Windows-a, kao operativnog sistema i raznih programa koje koristimo na računaru, a kojima je neophodan operativni sistem da bi mogli da se koriste.



RAZUMEVANJE EKONOMIJE BLOKČEJNA

PROOF OF WORK (POW) VS. PROOF OF STAKE (POS)

U svojoj suštini, Blokčejn je zapravo softver. Ono što je neophodno da bi neki softver funkcionisao je hardver na kojem će taj softver da bude instaliran i na kojem da radi. Uzmimo neki primer iz sveta tradicinalnih finansija, recimo banku. Banka ima vrlo kompleksan softver kako bi mogla da vrši obradu transakcija, kao i da čuva podatke o računima korisnika. Uz to joj je neophodna i sofisticirana hardverska infrastruktura kako bi taj softver mogao neprestano da radi na način na koji je predviđen da radi. Bitkoin mreža takođe radi obradu transakcija i čuva informacije o tome koliko Bitkoina ko poseduje. Sve te poslove radi sofverski kod koji stoji iza Bitkoina, ali se postavlja pitanje na kojem hardveru se taj kod izvršava ako znamo da je Bitkoin decentralizovan i da iza njega ne stoji nikakva kompanija ili pojedinac. Bitkoin funkcioniše zahvaljujući posebnim učesnicima koji su svoje hardverske resurse stavili na raspolaganje celoj mreži ostalih učesnika u Bitkoin ekosistemu. Ti posebni učesnici se zovu rudari i oni za taj doprinos bivaju nagrađeni novogenerisanim jedinacama Bitkoina.

Bitkoin funkcioniše zahvaljujući posebnim učesnicima koji su svoje hardverske resurse stavili na raspolaganje celoj mreži ostalih učesnika u Bitkoin ekosistemu.
Ti posebni učesnici se zovu rudari i oni za taj doprinos bivaju nagrađeni novogenerisanim jedinacama Bitkoina.

Nagrada je srazmerna snazi hardvera koji su stavili na raspolaganje mreži. Snagu hardvera dokazuju time što obavljaju veliki broj računskih operacija koje doprinose povećanju bezbednosti sistema i zbog toga se taj koncept naziva **Proof-of-Work (PoW)**. Ovde je snaga hardvera bitna iz 2 razloga.

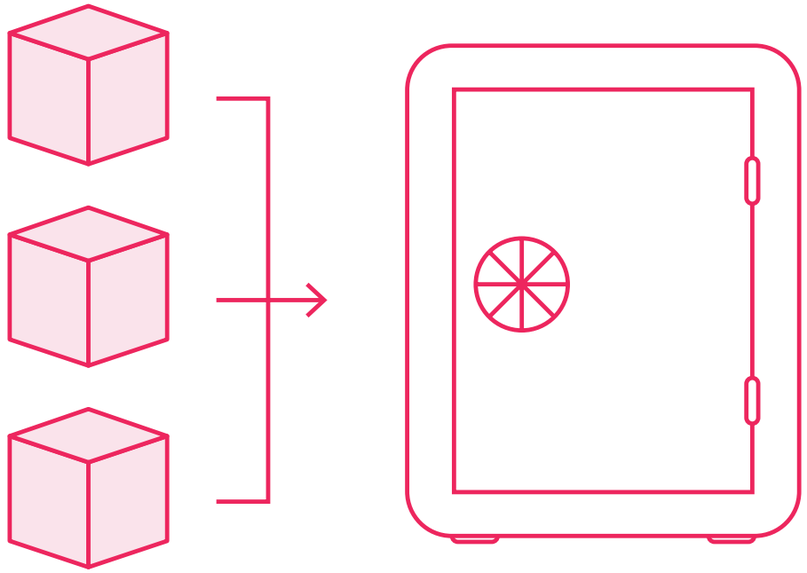
1.

Prvo, da bi softver uopšte mogao da funkcioniše (mada bi se to moglo postići i upotrebom neuporedivo slabijeg hardvera od onoga koji danas koriste Bitkoin ili Etereum).

2.

Drugo, da bi se eventualni napad na mrežu učinio što skupljim za potencijalnog napadača. Naime, da bi neko mogao da pokuša da ugrozi mrežu, morao bi da ima jači hardver od svih ostalih učesnika zajedno (takozvani “51% attack”). To napad na najveće Blokčejne čini ekstremno skupim, što u kombinaciji sa vrlo ograničenom štetom koja se može napraviti, napad čini prilično besmislenim.

Trenutno glavnu alternativu PoW konceptu predstavlja **Proof-of-Stake (PoS)**. I tu postoji određena hardverska infrastruktura, koja prosto mora da postoji da bi softver imao gde da radi, ali je ona ovde neuporedivo slabija jer postoji isključivo da bi obezbedila funkcionisanje softvera. Kod PoS se obeshrabrivanje napada na mrežu ne postiže jakim hardverom već time što oni koji rade obradu transakcija moraju da zaključaju (Stake-uju) određenu količinu kriptovaluta kao garanciju da će posao obrade transakcija obavljati u skladu sa pravilima. Oni su neka vrsta rudara u PoS sistemu. PoW rudari, koji su puno novca uložili u hardver, imaju jak motiv da transakcije obrađuju u skladu sa pravilima kako bi kroz nagrade koje dobijaju za taj posao isplatili investiciju i nešto zaradili. PoS rudarima su, sa druge strane, zaključane kriptovalute motiv da se ponašaju pošteno. Kod PoW rudara, nagrada je srazmerna snazi hardvera, a kod PoS rudara količini zaključanih kriptovaluta.



PREDNOSTI BLOKČEJN U ODNOSU NA TRADICIONALNE FIN. INSTITUCIJE

Ako bi prednost Blokčejna u odnosu na tradicionalne finansije trebalo da se svede na jednu reč, ta reč bi bila - sloboda. Postoje različiti nivoi slobode o kojima ovde govorimo, a krenućemo od slobode iz ugla krajnjeg korisnika. Blokčejn nam po prvi put u istoriji čovečanstva daje slobodu da svojom imovinom (ovde se misli na kriptovalute i razne vrste tokena) potpuno slobodno raspolažemo. Možemo izabrati način na koji ćemo tu imovinu čuvati, a ono što je posebno revolucionarno je što je možemo poslati kome god hoćemo, gde god da se taj neko nalazi, bez mogućnosti da taj prenos digitalne imovine bilo ko spreči. Dakle, po prvi put imamo tehnologiju koja omogućuje potpuno slobodan protok vrednosti. Zatim, korisnici mogu da izaberu bilo koju kriptovalutu ili token u skladu sa željama i potrebama koje imaju. Ta sloboda u svetu tradicionalnih finansija ne postoji, jer je izbor valute određen lokacijom na kojoj se neko nalazi. U Srbiji ne možemo plaćati u forintama, kao što se ni u Mađarskoj ne može plaćati dinarima. Mogućnost izbora tera kreatore kriptovaluta i tokena da naprave bolji proizvod koji će na slobodnom tržištu pobediti konkurenciju, jer nemaju način da bilo kome nametnu korišćenje onoga što prave. Tako zdrava konkurencija neminovno gura celu industriju ubrzano napred.

> Blokčejn nam po prvi put u istoriji čovečanstva daje slobodu da svojom imovinom potpuno slobodno raspolažemo.

Onima koji rade na proizvodima i uslugama baziranim na Blokčejn tehnologiji je opet sloboda ogromna prednost u odnosu na "konkurenciju" u svetu tradicionalnih finansija, gde je prostor za inovacije značajno ograničen regulativom. Svaka finansijska institucija je u obavezi da ispuni stroge regulatorne zahteve, što posebno komplikuje situaciju ako posluje u više država, jer svaka država ima svoja pravila koja se moraju poštovati. Usklađivanje sa regulativom značajno poskupljuje poslovanje finansijskih institucija i guši kreativnost. S druge strane, na primer Bitkoin je potpuno imun na regulativu jer ne postoji pravni entitet koji stoji iza njega, niti jurisdikcija gde je registrovan. Samim tim, programeri koji rade na daljem razvoju Bitkoina ni na koji način nisu sputani regulativom jer je ona prosto neprimenljiva na softverski kod koji oni pišu. Isto važi i za mnoge druge kriptovalute. To "borbu" čini prilično neravnopravnom, jer sa jedne strane postoji čitav niz prepreka da se inovira, a sa druge potpuna sloboda.

> Ako bi prednost Blokčejna u odnosu na tradicionalne finansije trebalo da se svede na jednu reč, ta reč bi bila - sloboda.

KOJE SU MANE I OGRANIČENJA BLOKČEJNA?

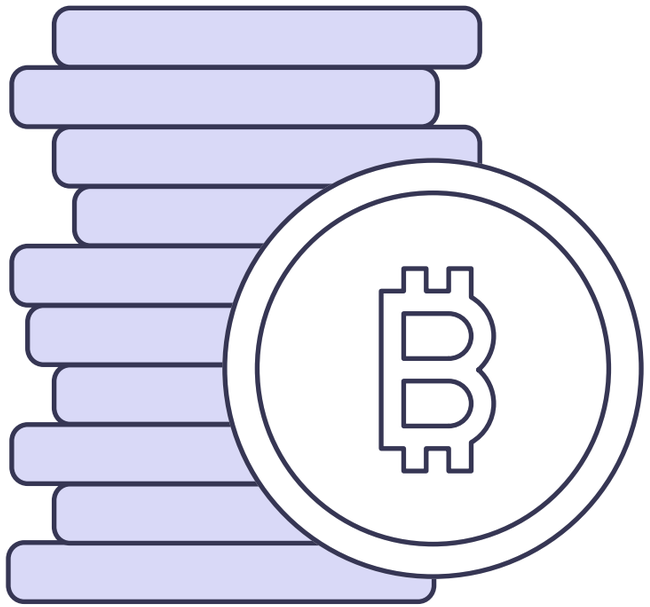
Iako je sloboda da se inovira bez sputavanja od strane regulative u neku ruku velika prednost, neusklađenost sa regulativom koja iz toga proističe često ume da komplikuje krajnjim korisnicima upotrebu digitalne imovine. Sve funkcioniše sjajno dok se krećete unutar "Blokčejn sveta", ali ima dosta frikcije na granici između tog sveta i sveta tradicionalnih finansija. Na primer, ako nekome nešto plaćate u kriptovalutama, korisničko iskustvo je uglavnom fantastično - brza transakcija, bez mogućnosti cenzure, uz minimalne troškove. Ipak, ako je onaj ko prihvata uplatu u zakonskoj obavezi da je primi u fiat novcu, u transakciju se uključuje i posrednik, transakcija postaje sporija, skuplja, a postoji i mogučnost da bude i cenzurisana od strane posrednika. Pored toga, za većinu ljudi kripto svet je i dalje relativno kompleksan. Neke to odbija u startu, a neki bivaju lake žrtve prevara ili hakova. Konačnost i nepovratnost kripto transakcija ume da bude sjajna stvar, ali neiskusne korisnike i one koji su tehnički malo slabije potkovani ta osobina neretko može skupo da košta.

> Iako je sloboda da se inovira bez sputavanja od strane regulative u neku ruku velika prednost, neusklađenost sa regulativom koja iz toga proističe često ume da komplikuje krajnjim korisnicima upotrebu digitalne imovine.

Često se kaže da u Blokčejn svetu **klasična regulativa** nije potrebna jer je softverski kod zakon koji bez izuzetka važi za svakoga. Ipak, u tom kodu se ponekad nalaze i greške, pa i to ume biti uzrok raznih vrsta gubitaka za korisnike. Umesto klasične regulative, odnose u Blokčejn svetu uglavnom regulišu takozvani "pametni ugovori", ali za sada ne postoji kompatibilnost između njih i regulative, pa se eventualni problemi nastali korišćenjem pametnih ugovora teško mogu rešiti unutar pravnog sistema.

KAKO INVESTIRATI U BLOKČEJN TEHNOLOGIJU?

Konačnost i nepovratnost kripto transakcija ume da bude sjajna stvar, ali neiskusne korisnike i one koji su tehnički malo slabije potkovani ta osobina neretko može skupo da košta.



U Blokčejn tehnologiju se može investirati na 2 osnovna načina.

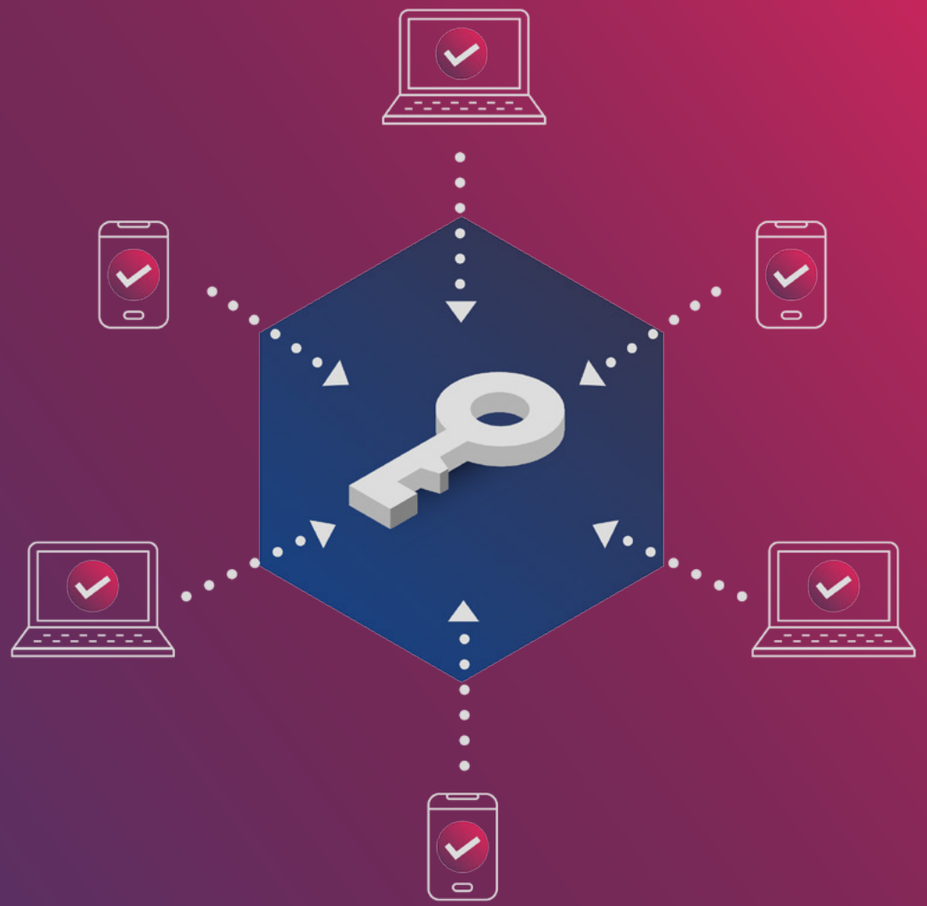
1.

Prvi način je investiranje u decentralizovane Blokčejn platforme kroz kupovinu kriptovaluta/tokena koje su za taj Blokčejn vezane. Pošto iza pravih javnih Blokčejn platformi ne stoje kompanije, nemoguće je investirati u njih, pa je kupovina kriptovaluta/tokena jedini način da se investira u projekat, uz očekivanje (koje nikako nije bez osnova) da će cena kriptovalute/tokena pratiti popularnost Blokčejn platforme za koju je vezana.

2.

Drugi način je tradicionalan, kupovinom udela u kompaniji koja se bavi Blokčejn tehnologijom ili kupovinom investicionih jedinica u fondovima koji ulažu u kriptovalute ili Blokčejn kompanije. Zbog regulative, institucionalnim investitorima je često samo ovaj način invesiranja i dozvoljen, dok je direktna kupovina kriptovaluta/tokena svakako primamljiviji način investiranja fizičkim licima.

TEHNOLOGIJA
BLOKČEJNA



KRATKA ISTORIJA BITKOIN BLOKČEJNA

Blokčejn nastaje početkom 2009-te godine, istovremeno sa prvom kriptovalutom - Bitkoinom. Zapravo Bitkoin je prva implementacija Blokčejn tehnologije. Kod Bitkoina, ta "Blokčejn baza podataka" je zapravo baza Bitkoin transakcija. Osim što je kriptovaluta, **Bitkoin** je istovremeno i decentralizovana finansijska infrastruktura. Korišćenje Blokčejn tehnologije omogućuje da korisnici međusobno razmenjuju vrednost (digitalnu imovinu) bez posrednika kao što su banke ili druge tradicionalne finansijske institucije.

U godinama nakon nastanka Bitkoina, pojavljivale su se nove kriptovalute, takođe bazirane na Blokčejn tehnologiji, ali se nisu suštinski razlikovale od njega, niti su imale zapažen uspeh. Naredni veliki iskorak u razvoju Blokčejna dešava se pojavom **Etereuma**. Dok su se mnoga druga Blokčejn rešenja fokusirala na povećanje kapaciteta, brzine generisanja blokova i dodavanje novih funkcionalnosti, Bitkoin se nije vremenom mnogo menjao, već je akcenat bio na jednostavnosti i superiornoj bezbednosti, pa se nije eksperimentisalo ni sa čim što bi tu bezbednost moglo da ugrozi.

ŠTA JE ETEREUM MREŽA?

Etereum mreža je lansirana u julu 2015-te godine, čitavih 6 i po godina nakon Bitkoina. Za razliku od Bitkoinovog Blokčejna, čija je jedina funkcija da obrađuje i skladišti podatke o Bitkoin transakcijama, Etereum otvara vrata za čitav spektar novih proizvoda i usluga baziranih na Blokčejn tehnologiji. Ako za Bitkoin možemo reći da je decentralizovana finansijska infrastruktura, za Etereum bismo mogli reći da je decentralizovani svetski kompjuter. Pored obrade transakcija, Etereum omogućuje da na njegovoj mreži "instaliramo" decentralizovane aplikacije koje mogu obavljati praktično bilo koju funkciju. Jedina granica je mašta kreatora i kapacitet mreže.

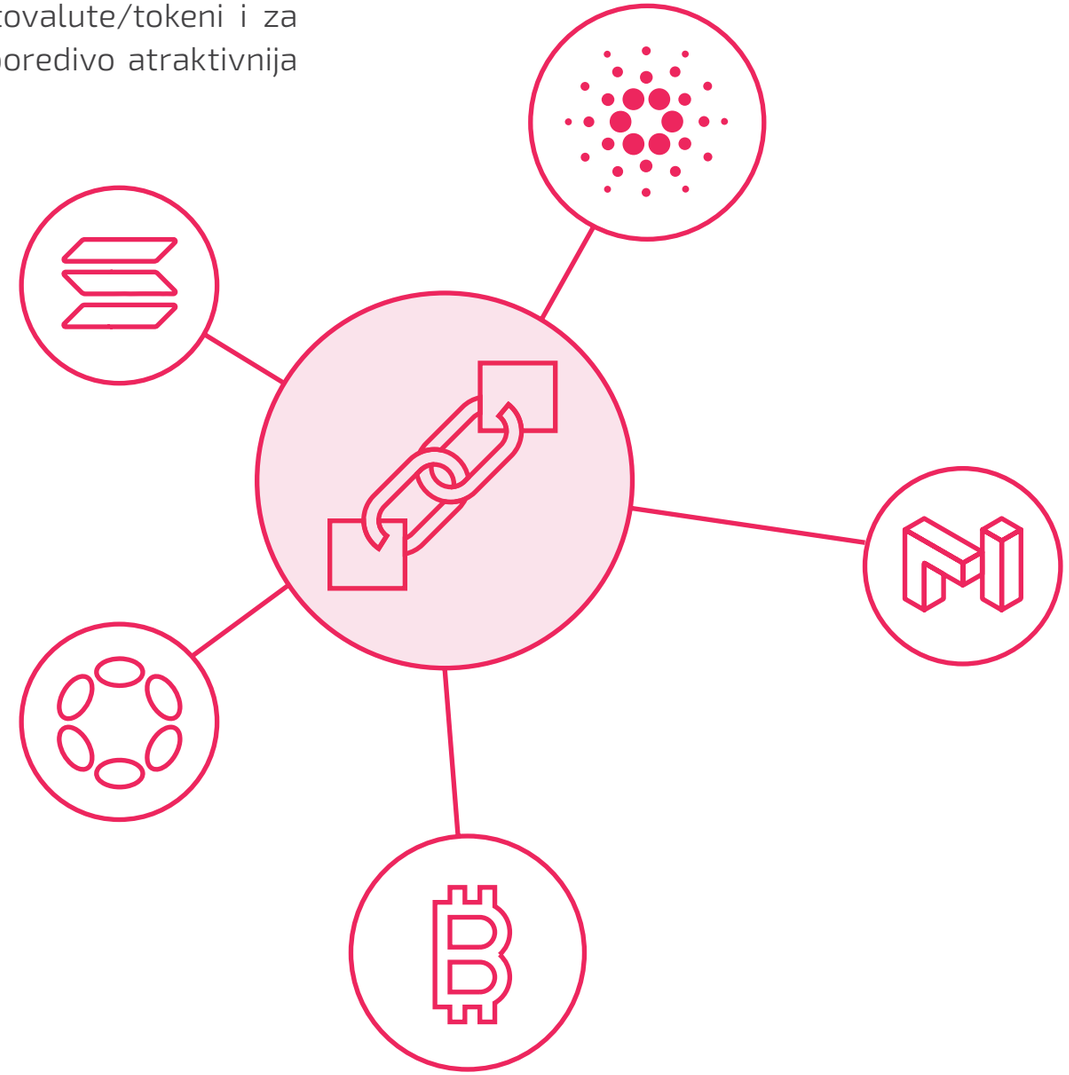
> Etereum otvara vrata za čitav spektar novih proizvoda i usluga baziranih na Blokčejn tehnologiji. Ako za Bitkoin možemo reći da je decentralizovana finansijska infrastruktura, za Etereum bismo mogli reći da je decentralizovani svetski kompjuter.

Ovo drugo uopšte nije trivijalno ograničenje, jer čak i relativno jednostavne aplikacije mogu prilično da "zaguše" Etereum mrežu ako se često koriste. Naime, kao i kod Bitkoina, postoji ograničeni broj transakcija koji Etereum mreža može da obradi u jedinici vremena. Svako korišćenje bilo koje decentralizovane aplikacije na Etereum mreži sa sobom povlači i transakciju Ethera (kriptovalute koja je vezana za Etereum Blokčejn). Što je više onih koji žele da izvrše transakciju, veća je konkurencija za ograničen broj transkcija koji može da stane u blok, pa cene izvršavanja transakcija rastu, često na desetine dolara po transakciji, a mogu ići i da nekoliko stotina dolara. Upravo problem sa kapacitetom je glavni razlog što Etereum Blokčejn planira prelazak sa PoW rudarenja na PoS.

Iako je potencijal za primenu Blokčejna poput Etereuma praktično neograničen, ipak vredi pomenuti neke od trenutno najčešćih primena.

Etereum omogućuje kreiranje različitih vrsta digitalnih tokena koji imaju neku specifičnu funkciju, dodeljenu od strane kreatora, a koji nemaju svoj Blokčejn već koriste infrastrukturu Etereuma. Ti tokeni mogu biti korisnički, kada uglavnom služe za plaćanja u određenom zatvorenom sistemu (sjajan primer su online igrice). Mogu biti i investicioni tokeni, koji prilično liče na deonice u kompaniji. Korisniku daju različita prava, kao što je pravo na učestvovanje u odlučivanju o budućnosti projekta ili pravo na učešće u raspodeli dobiti. Za kraj, tu su i **NFT (Non-Fungible Tokens)** tokeni, koji omogućuju kreiranje unikatnog digitalnog sadržaja (gde postoji način da se utvrdi šta je original, a šta kopija) ili digitalnog reprezenta nekog realnog objekta.

Poslednjih godina, čitav novi svet decentralizovanih finansija se pojavio, pre svega baš na Etereum mreži. Ovde pod "decentralizovanim finansijama" ne smatramo samo mogućnost da putem kriptovaluta pošaljemo novac na decentralizovan način, već se misli na čitav niz finansijksih usluga koje su do skoro postojale samo u svetu tradicinalnih finansija. Može se menjati jedna kriptovaluta/token za drugu na potpuno decentralizovan način (van kripto berzi i menjačnica), mogu se uzimati "krediti" u kriptovaluti/tokenu uz davanje kolaterala, u nekoj drugoj kriptovaluti/tokenu ili se mogu deponovati kriptovalute/tokeni i za to dobiti kamata (često neuporedivo atraktivnija nego u bankama).

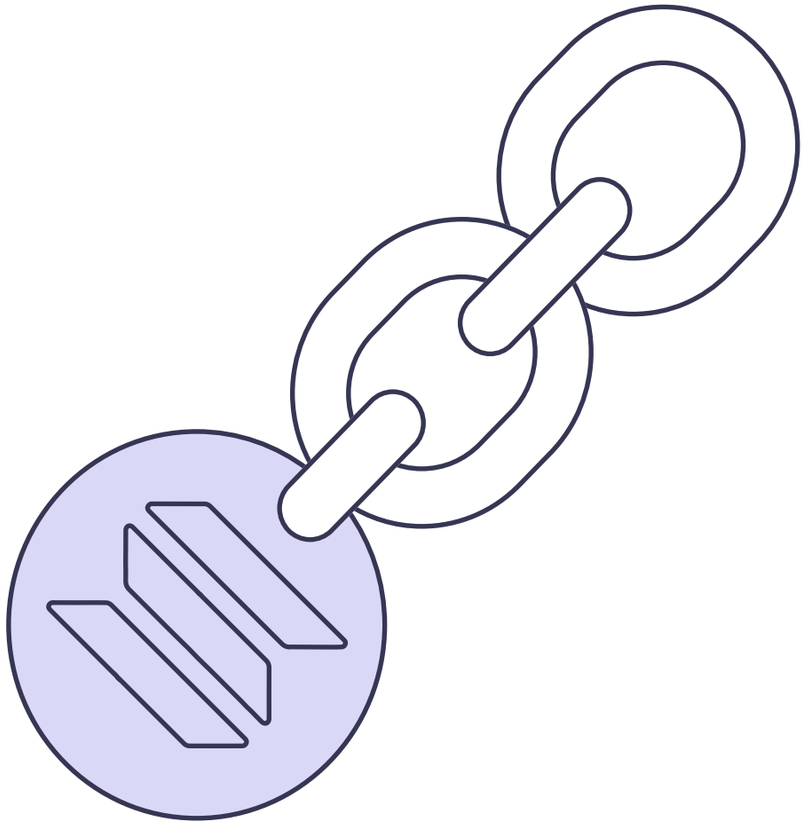


DALJI RAZVOJ BLOKČEJN TEHNOLOGIJE

Čini se da smo još daleko od konsenzusa oko toga kako tehnologija treba dalje da se razvija. Postoje takozvani "maksimalisti", kojih najviše ima u Bitkoin taboru, mada ih ima i kod Etereuma, koji smatraju da treba da postoji samo jedan glavni Blokčejn i da sve drugo bude, direktno ili indirektno, vezano za njega. Sa druge strane imamo hiljade različitih Blokčejna, bez sumnje, mnogo više nego što nam realno treba. Konačno rešenje je verovatno negde između jednog i hiljada Blokčejna, ali je korisno eksperimentisanje sa hiljadama jer ćemo kroz puno neuspelih eksperimenata na kraju doći do najboljih rešenja.

S jedne strane, postoje jaki razlozi za centralizaciju, kako zbog network effect-a, tako i zbog činjenice da su veći Blokčejni po pravilu bezbedniji, a prirodno je da želimo da budemo vezani za najbezbedniji Blokčejn. S druge strane, zbog veoma širokog spektra primene koji se Blokčejn tehnologiji predviđa, verovatno da nije realno očekivati da jedan Blokčejn (pa makar i sa svojim sidechain-ovima) bude rešenje za sve te očekivane primene.

Ono što se definitivno vidi kao trend je **zaokret ka PoS konceptu**. Praktično sve kriptovalute (i njihovi Blokčejni) koje su nastale u prvim godinama nakon Bitkoina su bile bazirane na PoW konceptu. Problem kod tog pristupa je što često istim hardverom može da se rudari više kriptovaluta. Samim tim, one manje su vrlo osetiljve na potencijalne 51% napade što ih čini nebezbednim. Kod PoS-a, "rudari" jedne kriptovalute ne mogu na ovaj način ugroziti drugu, pa je iz bezbednosnih razloga tranzicija na PoS logična, iako bezbednost svakako nije jedini razlog. Pošto Bitkoin ima ubedljivo najjaču hardversku infrastrukturu, rudari drugih kriptovaluta ga ne mogu ugroziti, pa je sasvim realan scenario da na kraju Bitkoin ostane jedini bitan PoW Blokčejn, dok će ostali preći na PoS.



BUDUĆNOST
BLOKČEJNA

NOVE PRIMENE BLOKČEJN TEHNOLOGIJE

Nema sumnje da je Blokčejn tehnologija prvo “napala” finansijsku industriju i da je i dalje tu ubedljivo najprisutnija. Ipak, svi se slažu da se na tome neće završiti. Osobine Blokčejn tehnologije mogu biti veoma korisne u **mnogim drugim industrijama**. Obzirom na to da su bezbednost i integritet podataka među najbitnijim karakteristikama Blokčejn tehnologije, logično je da prvo razmišljamo o primeni baš tamo gde su te karakteristike izuzetno bitne.

Već godinama neke države eksperimentišu sa prebacivanjem katastra na Blokčejn. To ima puno smisla, jer se tu čuvaju podaci vrlo visoke vrednosti (jer su same nekretnine uglavnom veoma vredne), pa je vrlo bitno da se čuvaju bezbedno i da se podacima ne može manipulisati. S druge strane, promena vlasništva nekretnina je nešto što se relativno retko dešava, pa problemi sa skalabilnošću Blokčejn tehnologije ovde zapravo nisu prepreka. Ovakvo rešenje bi omogućilo potpunu automatizaciju i tržišta nekretnina, gde bi se kompletan promet mogao obavljati online, sa notarima koji digitalno overavaju ugovore prethodno (takođe digitalno) potpisane od strane kupca i prodavca, gde se nakon tih potpisa i transakcije izmena automatski izvrši u katastru.

Obzirom na to da su bezbednost i integritet podataka među najbitnijim karakteristikama Blokčejn tehnologije, logično je da prvo razmišljamo o primeni baš tamo gde su te karakteristike izuzetno bitne.

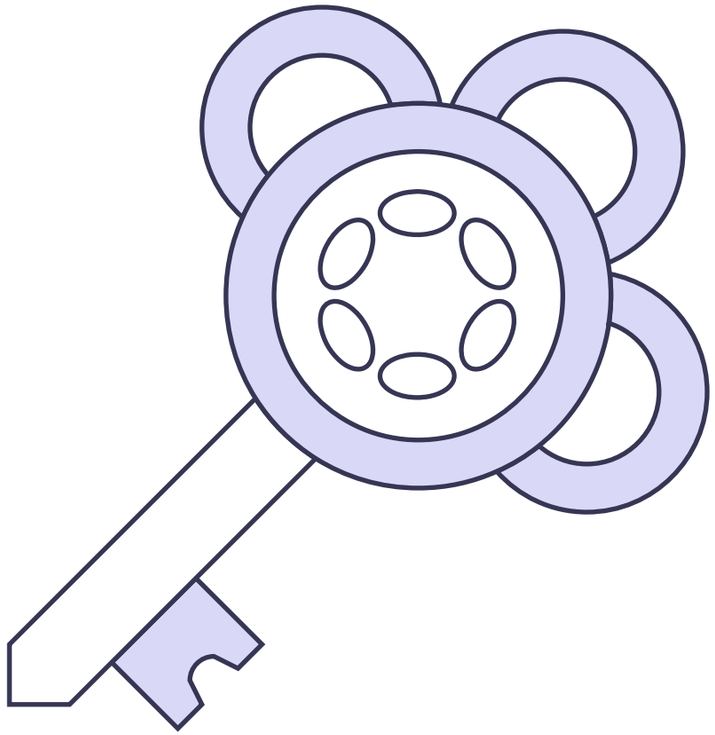
Pomenuti princip vođenja katastra i tržišta nekretnina bi se verovatno zasnivao na tome da svaka nekretnina ima svoj NFT koji je za nju vezan, jer je svaki NFT jedinstven, kao što je i svaka nekretnina jedinstvena. Slično se NFT-evi mogu koristiti za manje-više sve što je unikatno. Pored **digitalne umetnosti**, gde već vidimo rastuće prisustvo NFT-a, realno je očekivati sve više preplitanja Blokčejna sa umetnošću, kroz zaštitu autorskih prava, prodaju karata za razne događaje uz zaštitu od preprodaje i falsifikovanja. Koncerti u metaverzumu su već realnost, ali verovatno da smo i tu tek na početku.

Pored toga, bilo je nekoliko eksperimenata i vezano za glasanje na izborima putem Blokčejna. Široka primena takvog koncepta glasanja učinila bi izbore i referendume vrlo jeftinim i jednostavnim za organizaciju, a rezultati bi odmah nakon glasanja bili automatski dostupni. Ipak, treba rešiti još puno izazova pre nego što ovo postane realnost. Najpre, potreban je relativno visok nivo tehnološke pismenosti da bi se ovako nešto moglo primenjivati kao potpuna alternativa današnjem načinu glasanja. Takođe, ako bi se glasalo preko telefona, a ne na izbornim mestima, bilo bi još teže utvrditi da li je neko samostalno glasao ili uz nečiju sugestiju. Za kraj, neophodan je visok nivo pouzdanosti sistema, jer svaka eventulna greška može imati ozbiljne posledice.

KAKO ĆE BLOKČEJN UTICATI NA VAŠ ONLINE IDENTITET?

Sa pojavom Bitkoina, videli smo kako je dobro kada imamo potpunu kontrolu nad svojim novcem, a ostalima otkrivamo samo onoliko podataka koliko je neophodno za izvršenje transakcije, bez žrtvovanja čak i delića te kontrole. Bilo bi sjajno primeniti tako nešto i na online identitet uz očuvanje istog principa - jedino mi imamo potpunu kontrolu nad svojim podacima, a otkrivamo samo onoliko koliko je neophodno u određenoj situaciji. Tehnološki, ono što bi bilo bitno je dodatna zaštita anonimnosti, jer u nekim situacijama postoji potreba da ona bude potpuna. Već pomenuto glasanje pomoću Blokčejna je baš jedan takav primer. Na tome se radi već godinama, pre svega razvojem **ZKP (Zero Knowledge Proof)** rešenja. Inače, uprošćeno rečeno, ona se zasnivaju na pretpostavci da tačnost nekog podatka možemo potvrditi bez uvida u taj podatak.

Pored glasanja, online identitet na Blokčejnu može imati i mnoge druge zanimljive primene, praktično se može koristiti za skoro sve čemu online pristupamo, pa čak i kada ne pristupamo, a postoji potreba da o tome postoji zapis online. Kao dobar primer je primena u medicini, gde se može omogućiti deljenje medicinske istorije pacijenata bez otkrivanja identiteta. Ovo bi omogućilo lakše postavljanje dijagnoze i bolje lečenje, a naučnicima bi dalo mnogo više materijala koji bi mogli da koriste u istraživanjima i tako dođu do boljih terapija i lekova.



ŠTA JE SLEDEĆE U BLOKČEJNU?

Kao i kod mnogih drugih tehnologija, samo naša mašta je granica. Obzirom na principe decentralizovanosti i otvorene inovacije, ovde je to čak i tačnije nego u mnogim drugim industrijama. Međutim, različite tehnologije se često razvijaju zajedno jer su u određenoj meri zavisne jedne od drugih, to jest, tek međusobnom kombinacijom daju pravu vrednost. Kad je u pitanju Blokčejn, te "bratske" tehnogije su pre svih **AI *(Artificial Inteligence)*** i **IoT *(Internet of Things)***.

Povećanjem broja uređaja povezanih na internet (IoT) i njihova veća autonomija u odlučivanju (AI) dovešće polako do toga da će veći broj finansijskih transakcija vršiti mašine nego ljudi. Pošto su kriptovalute programabilan novac, logično je da mašine koriste novac koji im je nekako prirodan (koliko god reč "prirodan" zvučala čudno kad pričamo o mašinama).

Kroz istoriju nas je često brinula koncentracija prevelike moći u rukama malog broja ljudi. Uskoro možemo doći u situaciju da se više plašimo koncentracije prevelike moći u "rukama" malog broja mašina. To je dodatni razlog zbog kojeg je bitno da neki budući svet, u kojem će mašine imati mnogo bitniju ulogu nego danas, bude baziran na principima decentralizacije, a to se najbolje postiže upravo primenom Blokčejn tehnologije.

Kroz istoriju nas je često brinula koncentracija prevelike moći u rukama malog broja ljudi. Uskoro možemo doći u situaciju da se više plašimo koncentracije prevelike moći u "rukama" malog broja mašina. To je dodatni razlog zbog kojeg je bitno da neki budući svet, u kojem će mašine imati mnogo bitniju ulogu nego danas, bude baziran na principima decentralizacije, a to se najbolje postiže upravo primenom Blokčejn tehnologije.

www.preduzmi.rs

Naslov: Uvod u blokčejn

Autor: Aleksandar Matanović

Izdavač: Inicijativa „Digitalna Srbija“

Štampa: Inicijativa „Digitalna Srbija“, bulevar Milutina Milankovića 11a, Beograd

Tiraž: 10

Mesto izdavanja: Beograd

Godina izdavanja: 2024.

ISBN 978-86-82900-05-4

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

004.738.5.056(0.034.2)

МАТАНОВИЋ, Александар, 1979-
Uvod u blokčejn [Електронски извор] / autor Aleksandar Matanović. - Beograd : Inicijativa "Digitalna Srbija", 2024 (Beograd : Inicijativa "Digitalna Srbija"). - 1 USB fleš memorija ; 1 x 2 x 7 cm

Sistemski zahtevi: Nisu navedeni. - Nasl. sa naslovne strane dokumenta. - Tiraž 10.

ISBN 978-86-82900-05-4

a) Блокчејн технологија

COBISS.SR-ID 140774921