OSNOVE KRIPTOVALUTA I BLOKČEIN TEHNOLOGIJE

Aleksandar Matanović, MSc in Digital Currency

Sadržaj

1. Uvod u Bitkoin

1.1. Osnovne funkcije novca

- **Novac kao sredstvo razmene** - Novac služi kao posrednik između proizvoda ili usluga kojima ljudi žele da trguju pri čemu se vremenski i prostorno odvajaju proizvoda ili usluga kojima ljudi žele da trguju pri čemu se vremenski i prostorno odvajaju prodaja i k upovina robe i ukida međusobna vremenskoprostorna zavisnost. Dobro sredstvo razmene ima nekoliko kvaliteta:
    a. Trajnost (Novac ne menja svojstva tokom vremena)
    b. Prenosivost (Lako se prenosi)
    c. Deljivost (Deljiv na dovoljno sitne delove da može bilo koja količina nečega da se plati tim novcem)
    d. Fungibilnost (Jedinice novca izgledaju jednako i međusobno su zamenljive)
    e. Nemogućnost falsifikovanja (Otporan na falsifikovanje)

- **Novac kao mera vrednosti** - U njoj novac predstavlja standardnu meru vrednosti robe, usluga, ekonomskih aktivnosti, imovine i obaveza. Ova uloga novca nam omogućava upoređivanje vrednosti, rezultata i veličina. Kako je svaka roba rezultat određene količine ljudskog rada, postoji element uporedivosti i samerljivosti. Da bi novac bio mera vrednosti drugih roba, nije neophodno fizičko prisustvo, stoga je najčešće novčana vrednost robe izražena u vidu cene. Ključna karakteristika koju valuta mora posedovati da bi služila kao jedinica vrednosti jeste stabilnost. U nekim slučajevima, mera vrednosti nije ista kao sredstvo razmene (mnoge zemlje imaju zvanične valute, ali izražavaju cene u drugoj valuti, na pr. cene automobila i nekretnina u Srbiji).

- **Novac kao blago (čuvar vrednosti)** - Novac ovde predstavlja mehanizam kojim se vrednost može sačuvati i povratiti u budućnosti uz određeni stepen predvidivosti buduće vrednosti. Skladištenje i očuvanje vrednosti nije funkcija isključivo valuta, već imovine uopšte (zlato, dijamanti, srebro, rezervne valute, obveznice, akcije, nekretnine itd.). Obzirom da buduće vrednosti bilo koje aktive imaju veći ili manji stepen nepredvidivosti, ne postoji savršeni čuvar vrednosti. U savremenim uslovima blago predstavlja novac povučen iz opticaja i čuvan kao oličenje vrednosti, bogatstva i društvene moći.

1.2. Evolucija novca

- **Trampa** - Jednostavno i direktno trgovanje robe ili usluga, bez posrednika. Trampa je dominirala na malim lokalnim seoskim tržištima i u plemenima. Danas nema veliku praktičnu primenu pre svega zbog globalizacije i problema "duple potražnje" (Ribar će ribu trampiti za žito samo ako njemu lično treba žito ili ako veruje da ga može brzo i lako trampiti sa nekim drugim za nešto što mu zaista treba).

- **Primitivni novac** - Primitivni novac je bio jedina forma novca do početka upotrebe novčića u 7. veku pre Nove ere. On predstavlja nadgradnju na sistem trampe jer su neki predmeti i namirnice postali opšte prihvaćeni kao vredni i lako zamenjivi za bilo šta drugo. Osnovnu funkciju sličnu današnjoj funkciji novca u to vreme imala je stoka, školjke, krzno, žito, kakao... Čak i stari latinski naziv za novac pecunia je izveden od reči pecus – govedo. U današnje vreme, primitivni novac se koristi samo u specijalnim uslovima ili izolovanim tržištima.

- **Metalni novac** - Moderne kovanice su prvobitno nastale u drevnoj Kini ili Grčkoj, u zavisnosti od metodologije poimanja prelaska iz primitivnog novca u moderne kovanice. 1200 godina pre Nove ere u Kini su se kovale prve metalne školjke koje se mogu smatrati prvim standardizovanim oblikom primitivnog novca ili ranim modernim kovanicama. Prvi zvanični metalni novčići proizvedeni su u Lidiji u antičkoj Grčkoj u 7 veku pre Nove ere u vidu štampanih kovanica elektruma (mešavine srebra i zlata). Mada je i pre lidijanskih novčića bilo sličnih primera u Kapadokiji i na Kritu, oni se smatraju prvim modernim kovanicama zbog svog oblika i obeležavanja koji su napravili veliki korak u standardizaciji, institucionalizaciji i prenosivosti kovanica. Iako su kovanice ostale dominantni novac u zapadnom svetu sve do 17 i 18 veka, izdavaoci kovanica bili su u konstantnom iskušenju da smanje količinu dragocenih metala u kovanicama dok su korisnici novčića bili u iskušenju da pretope kovanice i prodaju metal. Metalne kovanice su takođe imale problem da održe stabilnu vrednost tokom vremena. Promene u cenama osnovnih metala od kojih su se kovanice izrađivale menjala je konstantno efektivnu vrednost kovanica u odnosu na početnu vrednost, što je otežavalo poređenja vrednosti tokom vremena.

- **Papirni novac** - Papirni novac je korišćen još od 11 veka u Kini, ali je prvu javnu i masovnu upotrebu u zapadnom svetu dobio nakon osnivanja prve javne banke u Amsterdamu 1609. godine. Iako su depozitarne potvrde za plemenite metale postojale u južnoj Evropi vekovima pre, Banka u Amsterdamu je prva prihvatala lokalne, strane i oštećene kovanice i vrednovala ih po postavljenim standardima, te davala kredite u vidu računa u zajedničkoj vrednosti (bankarskom novcu) i izdavala priznanice. Za to je banka naplaćivala administrativnu nadoknadu. Standardizacija je smanjila potrebu za pretapanjem kovanica i bila je značajan korak ka većoj funkcionalnosti evropskih valuta. Banka je takođe uvela preteče nekoliko savremenih koncepata banaka i centralnih banaka uključujući državne garancije, oblik pravne prisile, kreditno poslovanje itd. Na početku Banka je delovala isključivo kao depozitna institucija, bazirana 100% na postojećoj rezervi (nisu davali zajmove koji nisu imali pokriće). Međutim, počeli su sa kratkoročnim pozajmicama novca iz depozita drugih za potrebe Dutch East India kompanije. Nažalost, kompanija je propala i nije izmirila obaveze prema Banci Amsterdama te je Banka postala prva žrtva preterano optimističnog kreditiranja, što će se ponavljati mnogim bankama kasnije.

- **Nacionalne valute** - Banka Engleske, osnovana 1694. godine, funkcionalna i danas, postala je preteča svih savremenih centralnih banaka i vekovima je bila najvažnija Centralna banka sveta, pogotovo tokom perioda kada je funta bila rezervna svetska valuta. Banka Engleske je nacionalizovana Zakonom o banci Engleske 1946. godine. Do 20. veka, američki dolar (USD) zamenio je funtu (GBP) kao najvažnija rezervna svetska valuta i posledično su Federalne Rezerve postale ključna centralna banka na svetu. Danas je američki dolar 100% dekretna valuta bez potpore u bilo kojoj robi, i njime upravljaju Federalne Rezerve, Centralna banka SAD, finansijska institucija u privatnom vlasništvu. Američki dolar se poput mnogih dekretnih valuta vodi blago inflatornom politikom (ciljna inflacija se kreće u intervalu od 2-3% godišnje) kako bi se sprečilo gomilanje novca van novčanih tokova i stimulisala ekonomska aktivnost uz održavanje visoke stope zaposlenosti.
  "Permit me to issue and control the money of a nation, and I care not who makes its laws! - *Mayer Amschel Rothschild*"

- **Privatne valute** - Uz razvoj interneta nastao je veliki broj privatnih valuta. Većinom postoje da bi se izbegli efekti inflacije (vezivanjem za određenu robu), da bi se ubrzao protok novca, da bi se olakšao pristup i trgovina itd. Pre Bitkoina, privatne valute su imale centralnog izdavača čime je vrednost upotrebe ograničena na određeni geografski region ili internet okruženje. Centralizacija je takođe učinila privatne valute izloženijim regulatornim pritiscima. Primeri su krediti za Fejsbuk, Linden dolari za upotrebu u igrici Drugi život, pa čak i Dizni novčići koji se mogu zameniti u standardne valute u parkovima. Servisi koji su pokušali da stvore valute koje imaju potporu u robi poput Liberty Reserve i eGold naleteli su na ozbiljne regulatorne poteškoće koje su dovele do ukidanja valute ili čak i kriminalnih optužbi za izdavače valute.

- **Kriptovalute** - Kriptovaluta je sredstvo razmene koje koristi kriptografiju za sigurnost transakcija i kontrolisanje stvaranja dodatnih jedinica valute. Smatra se podvrstom alternativnih valuta, preciznije digitalnih valuta. Ono što je kod kriptovaluta posebno zanimljivo je da njih niti izdaje niti kontroliše centralna banka niti bilo koja druga institucija. Kriptovalute uglavnom kreiraju njihovi korisnici kroz proces koji je poznat kao "rudarenje". Bitkoin je postao prva decentralizovana kriptovaluta u 2009. Od tada su se pojavile brojne kriptovalute, podatak iz Maja 2018. pokazuje da se na berzama trguje sa preko 1600 kriptovaluta.

1.3. Šta je bitkoin i kada je nastao?

Bitkoin (*Bitcoin*) je digitalna imovina i platni sistem koji je predstavio anonimni programer pod pseudonimom Satoši Nakamoto. Prvi put se kao ideja pojavljuje 31. Oktobra 2008., a kao otvoreni softver se pojavio u januaru 2009, kad je i počela emisija bitkoina. U pitanju je decentralizovana, distribuirana, pseudo-anonimna platna peer-to-peer mreža koja funkcioniše pomoću kompleksnog algoritma, a ujedno i valuta koju ta mreža koristi. Transakcije su verifikovane pomoću mrežnih čvorova i zapisane su u glavnu knjigu transakcija koja se zove blokčejn (*Blockchain*).

Bitkoin je prva decentralizovana digitalna valuta i ujedno najveća kriptovaluta po totalnoj tržišnoj vrednosti. Novi bitkoini su nagrada za obradu transakcija korisnicima uključenim u aktivnosti održavanja bitkoin mreže (proces poznat kao rudarenje). Bitkoini se osim rudarenjem mogu kupiti novcem na za to predviđenim berzama i menjačnicama ili se mogu dobiti u zamenu za robu i usluge. Bitkoin se uz neznatnu naknadu može poslati digitalnim putem pomoću softvera poznatog kao "novčanik" (*wallet*) koji se može nalaziti na računaru, mobilnom uređaju ili internetu.

Bitkoin je privatna decentralizovana digitalna kriptovaluta.

- **Privatna** - Ne izdaje je nijedna institucija.
- **Decentralizovana** - Ne postoji centralitozovani izdavač, jedinice valute se decentralizovano dodeljuju putem algoritma.
- **Digitalna** - Potpuno elektronska valuta, bez neophodne fizičke manifestacije ni vezivanja za određenu robu.
- **Kriptovaluta** - Kriptografija se koristi za verifikaciju transakcija i kontrolu generisanja novih jedinica valute.

1.4. Bitkoin kao novac

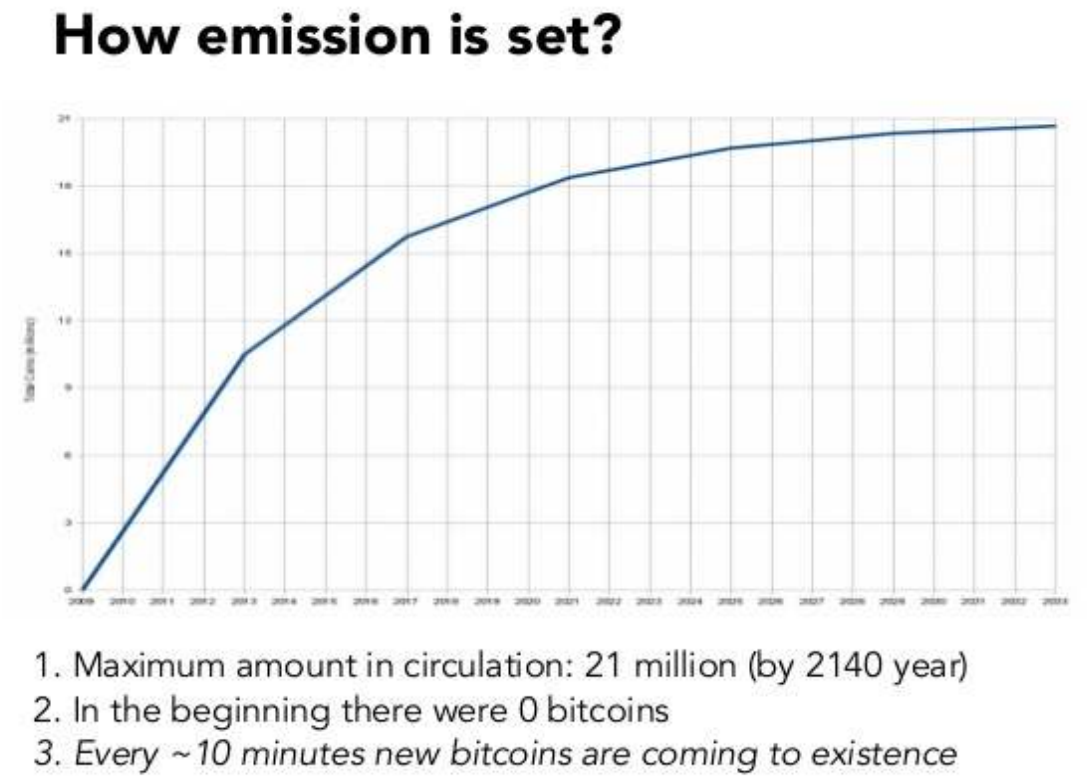
- **Bitkoin kao mera vrednosti** - Gledano iz perspektive bitkoina kao novca, teško je reći da bi bitkoin bio dobra mera vrednosti. Cena bitkoina se formira na otvorenom tržištu ponude i potražnje i iako je u osnovi deflatorna valuta, vrednost je od nastanka bila veoma volatilna i vremensko poređenje vrednosti robe i usluga sa bitkoinom bi bilo veoma teška, ako ne i nemoguće. Očekuje se da u budućnosti bolja regulacija ekonomskih okvira u kojima bitkoin postoji (regulacija berzi, menjačnica, biznisa, statusa bitkoina kao valute) pozitivno uticati i na stabilnost cene samog bitkoina.

- **Bitkoin kao čuvar vrednosti** - Bitkoin se do danas pokazao kao odličan čuvar vrednosti. Obzirom da je ponuda bitkoina predvidiva i bazirana na matematičkoj formuli, potražnja je faktor koji formira cenu, a očekuje se povećanje potražnje svakom daljnom implementacijom bitkoina i tehnologije na kojoj je baziran. Ipak, treba imati u vidu da je bitkoin još uvek mlad i da treba da preživi test vremena da bi se zaista nametnuo kao dobar i pouzdan čuvar vrednosti.

- **Bitkoin kao sredstvo razmene** - Bitkoin poseduje mnoge osobine koje bi trebalo da poseduje dobro sredstvo razmene.
    a) **Visoka izdržljivost**: Ne postoji način da se bitkoin degradira obzirom da je reč o kodu i da je ceo blokčejn sačuvan na brojim računarima širom sveta.
    b) **Lako prenosiv**: Bitkoin se može preneti bez posrednika širom sveta sa obaveštenjem u roku od nekoliko sekundi, inicijalnom potvrdom u roku od 10 minuta i nepovratnošću transakcije u roku od sat vremena. Bitkoin se može preneti na bilo koju tačku planete samo uz pomoć digitalnog zapisa ili zapamćene šifre.
    c) **Visok stepen jednakosti**: Bitkoin protokol tretira na isti način svaku jedinicu i podjedinicu.
    d) **Visok stepen deljivosti**: Svaki bitkoin se može podeliti na 100 miliona jedinica koje se zovu Satoši
    e) **Visoka otpornost na falsifikovanje**: Još uvek nije probijena kriptografija javnog i privatnog ključa koja je osnova sigurnosti bitkoina.

- **Monetarna politika bitkoina**
    a) **Fiksirana ponuda**: Novčana ponuda je regulisana protokolom i ograničava broj bitkoina na konačnih 21,000,000 (slika 1). Bitkoini se dodeljuju sve sporije i sporije (trenutno 12.5 BTC na svakih 10 minuta). Otprilike svake 4 godine prepolovljava se broj bitkoina koji se proizvedu u svakom bloku. Iako se očekuje da svi bitkoini budu u opticaju tek 2140, usled prepolovljavanja nagrade po bloku skoro svi bitkoini će biti izrudareni već 2030. godine.
    b) **Transparentna monetarna politika**: Bitkoin algoritam je otvoreni kod i samim time je dostupan na proveru svakome.
    c) **Vođen konsenzusom**: Svaki korisnik zauzima svoj stav o svakom ponuđenom rešenju ili promeni u sistemu. Takođe, svaki učesnik može da stvori mrežu po svojim pravilima, ali je ključno za svaku promenu da bude prihvaćena od većine učesnika u

sistemu (pravilo 51%). Trenutno se kompletan bitkoin protokol nalazi na preko 10000 računara što obezbeđuje pravičnost odluke o bilo kakvoj promeni u sistemu.



Slika 1: Emisiona kriva bitkoina (izvor: www.slideshare.net)

2. Uvod u Blokčein

2.1. Posrednici

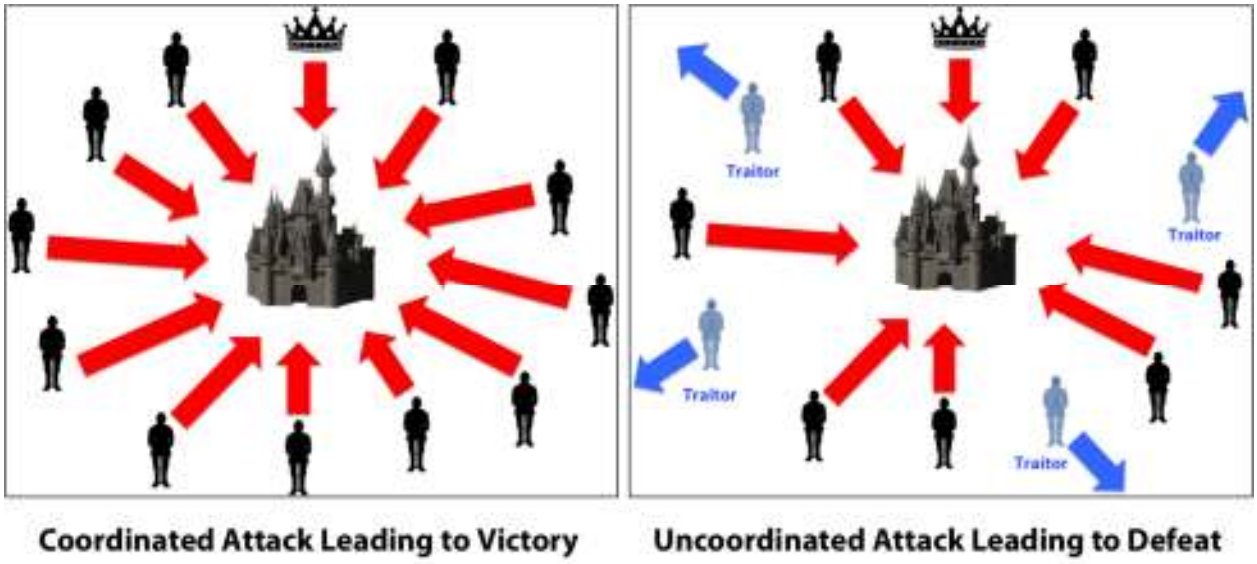
Posrednike koristimo svakodnevno, toliko često da uglavnom i ne razmišljamo o tome. Kada god imamo potrebu da nešto pošaljemo nekome ko nije na istoj lokaciji kao mi, moramo da koristimo posrednika ili više njih. Ako se radi o poruci koju šaljemo putem mobilnog telefona, posrednik može biti na pr. Telenor, MTS ili VIP (ako šaljemo SMS). Takođe, može biti Viber, Whatsapp, Telegram... mogu biti društvene mreže kao što je Facebook, Twitter ili Linkedin. Opcija za slanje poruke ima mnogo, ali sve one imaju jednu zajedničku stvar - uvek nam treba posrednik. Isto je kad šaljemo e-mail. Tada posrednik može biti Gmail, Yahoo, Hotmail ili bilo koji drugi e-mail provajder. Poruku možemo poslati i pismom, u tom slučaju posrednik je Pošta. Ako šaljemo paket, opet imamo puno opcija - Pošta, DHL, Fedex i razne druge kurirske službe. Oni koji bi da uštede na troškovima slanja ponekad koriste vozače autobusa kao posrednike, ali tad imaju veoma ograničen broj lokacija na koje mogu da pošalju. Slanje novca je posebno zanimljiva tema imajući u vidu da se na ovom kursu bavimo kriptovalutama. Mogućnosti su brojne - u lokalu možemo koristiti banke, PostNet ili ponovo vozače autobusa. Za slanje van zemlje opet imamo banke, Western Union, PayPal itd. Uglavnom, samo kada se fizički nalazimo na istom mestu kao i osoba kojoj nešto želimo da damo, možemo to uraditi samostalno. U svakom drugom slučaju neophodan nam je posrednik ili često više njih (Obično kada šaljemo nešto u inostranstvo imamo više posrednika uključenih u proces - više banaka, više mobilnih operatera...).

Posrednici nisu savršeni, njih koristimo uglavnom zato što moramo, a ne zato što želimo Posrednici su veoma važni jer nam omogućuju interakciju sa ljudima sa kojima se ne nalazimo na istoj lokaciji. Međutim, pored toga što su neophodni, posrednici često mogu biti i problem.

- **Trošak**: Usluge posrednika uglavnom nisu besplatne (izuzetak je komunikacija putem interneta - Skype, Viber, e-mail, WhatsApp...). Cene tih usluga mogu biti simbolične, a mogu biti i prilično velike - tolike da cena ponekad postaje dominantan faktor pri izboru posrednika.
- **Kašnjenje**: Posrednici uglavnom unose neko kašnjenje u proces slanja. Ponovo je izuzetak komunikacija putem interneta gde se to kašnjenje najčešće meri delovima sekunde. Primer situacije gde to kašnjenje može biti značajno je slanje novca u drugu zemlju preko bankovnog računa. Na tome dosta profitiraju servisi kao što su Western Union i Moneygram koji brzinom transfera (neuporedivo brži od banke) opravdavaju izuzetno visoke provizije.
- **Poverenje**: Da li možemo verovati posredniku da će za nas uraditi ono što nam potrebno? U većini slučajeva poverenje se podrazumeva i u većini slučajeva posrednik opravda to poverenje. Desi se ponekad da se paket izgubi ili da novčana transakcija značajno kasni zbog propusta posrednika, ali su ovakvi slučajevi ipak relativno retki.
- **Privatnost**: Ovo se nekako nadovezuje na poverenje. Posrednik često raspolaže privatnim podacima svojih klijenata. Postoji opravdan strah da bi posrednik te podatke mogao da zloupotrebi. Takođe, potencijalno može biti veliki problem ako posrednik te podatke ne čuva na dovoljno bezbedan način. U tom slučaju do njih mogu doći hakeri i zloupotrebiti ih.

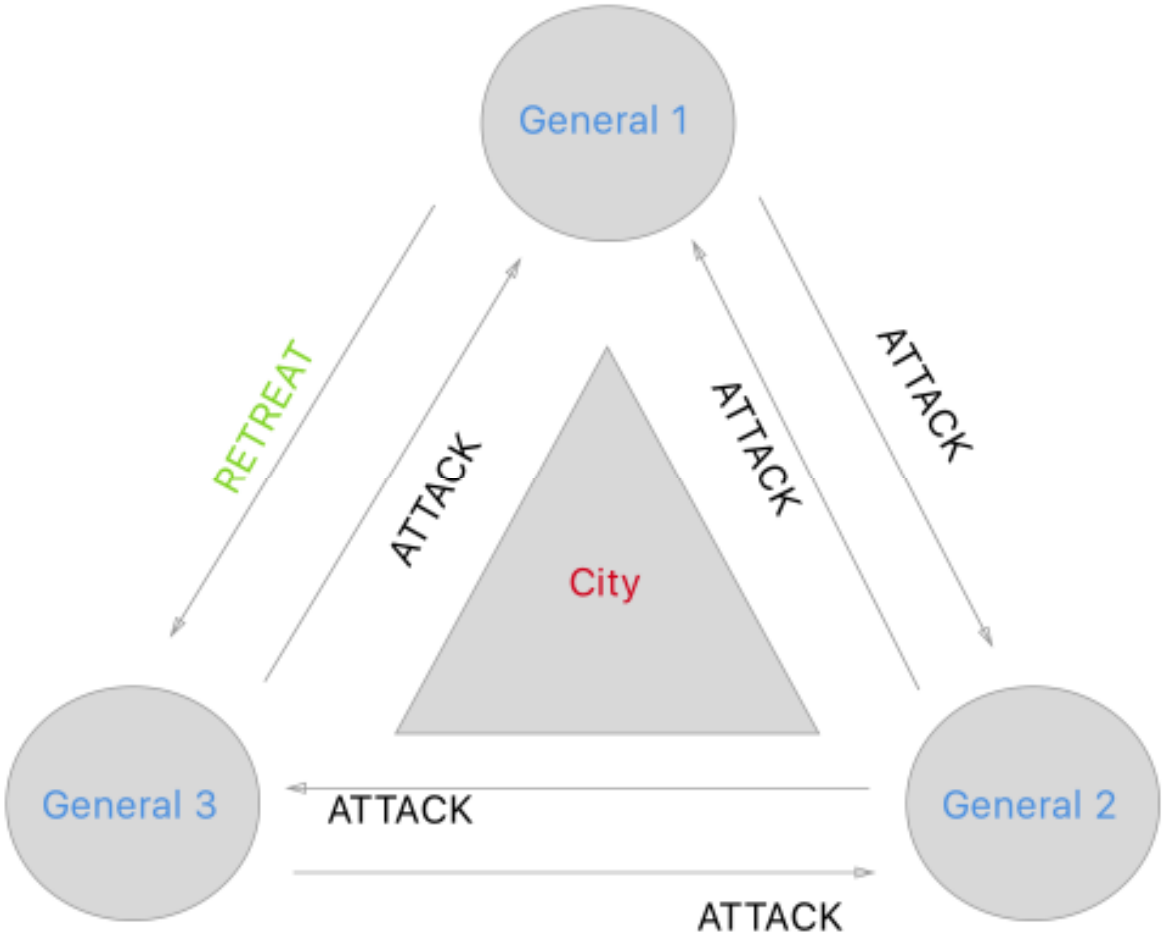
2.2. Problem vizantijskih generala

Problem vizantijskih generala je definisan još davne 1982 godine i ilustruje problematiku komunikacije preko posrednika koji nisu pouzdani. Zamislimo da vizantijski generali opsedaju neprijateljski grad i da treba da se dogovore oko zajedničkog plana akcije (Slika 2). Da bi napad uspeo, potrebno je da svi napadnu u isto vreme. Ako neki od generala ne izvrše napad u dogovoreno vreme, veoma je verovatno da napad neće uspeti.



Slika 2: Vizantijski generali opsedaju grad (izvor: www.medium.com/@DebrajG)

Pošto se generali nalaze na različitim lokacijama oko grada, ne mogu se uživo dogovarati, već komuniciraju preko kurira. Ovde imamo dva potencijalna problema. Prvi problem je ako su neki od generala izdajnici. Oni će namerno sabotirati dogovor i preko svojih kurira slati informacije tako da i među poštenim generalima izazovu konfuziju. U jednostavnijem scenariju, svi generali su pošteni, ali nisu svi kuriri pošteni. Da još dodatno pojednostavimo slučaj, zamislimo da imamo 3 generala i svaki general po 2 kurira, pri čemu svaki šalje po jednog kurira svakom od svojih kolega. U ovom primeru, jedan od kurira prvog generala je izdajnik i on namerno trećem generalu prenosi pogrešnu poruku (Slika 3). Prvi i drugi general misle da je dogovor postignut i kreću u napad. Treći general dobija drugačije poruke od svojih kolega i zbog toga ne napada jer smatra da nije postignut dogovor. Umesto cele vojske, u napad kreće 2/3 vojske i to znatno umanjuje šanse za pobedu.



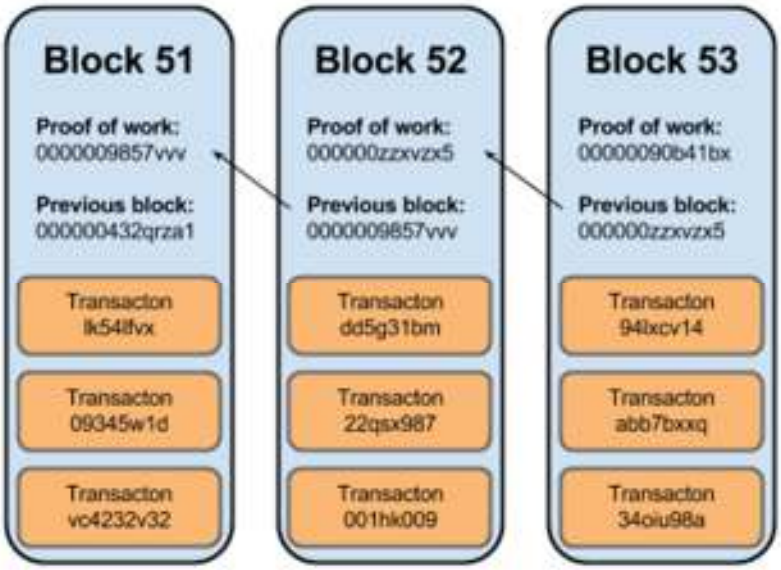
Slika 3: Kurir izdajnik (izvor: www.medium.com/@sardorislomov)

Na ovom jednostavnom primeru smo videli da je dovoljno da je samo 1 od 6 kurira izdajnik da bi šanse za uspeh napada značajno smanjile. U većim i kompleksnijim sistemima, broj učesnika (a često i broj izdajnika) ja značajno veći, što samo dodatno komplikuje situaciju. Ovaj problem posebno je izražen u sistemima koji nisu centralizovani i gde je broj učesnika prevelik da bi svako sa svakim direktno komunicirao. Bitkoin predstavlja upravo jedan takav sistem - veliki i decentralizovan. Kod centralizovanih sistema, gde problem komunikacije ne postoji, svi primaju informacije direktno sa vrha i do svih stižu iste informacije. Kod takvih sistema postoji druga vrsta problema - šta ako onaj koji je na vrhu donosi pogrešne odluke? Ipak, taj problem nije zanimljiv iz ugla ovog kursa, pa se nećemo na njemu duže zadržavati.

2.3. Blokčein kao rešenje problema vizantijskih generala

Priču o kriptovalutama smo počeli bitkoinom, pa ćemo i priču o blokčeinu početi bitkoinovim blokčeinom. Blokčein je registar svih transakcija koje su se ikad desile u bitkoinovom sistemu. To samo po sebi nije ništa spektakularno, jer svaki sistem u kojem se vrše neka plaćanja vodi evidenciju o tim transakcijama i čuva ih kao neku bazu podataka. Ono što je kod blokčeina velika inovacija je način na koji se informacije o transakcijama šalju i skladište.

Pođimo od samog imena. "*Blockchain*" je sastavljen od reči "*Block*" (blok) i "*chain*" (lanac). Dakle, bukvalno prevedeno, blokčein je lanac blokova. Naime, kod bitkoina se transakcije pakuju u blokove, a blokovi se vezuju u lanac (Slika 4). Za vezivanje blokova koristi se kriptografija, preciznije HEŠ (*HASH*) funkcija, na način da je nemoguće promeniti sadržaj jednog bloka, a da se ne promeni sadržaj svih blokova koji idu nakon njega. Ovo je izuzetno bitno svojstvo blokčeina jer obezbeđuje nepromenjivost podataka koji su upisani u blokčein.



Slika 4: Lanac blokova (izvor: www.dataconomy.com)

Kao što već znamo, bitkoin je decentralizovan, što znači da ne postoji centralni server ili bilo šta slično, na šta se korisnici povezuju. Svi korisnici bitkoina su povezani u *peer-to-peer* mrežu i svaki korisnik predstavlja jedno čvorište (*node*) te mreže (Slika 5). Pošto je *peer-to-peer* mreža takva da svaki korisnik može biti direktno povezan samo sa nekoliko drugih korisnika, to znači da je sa svima ostalima povezan indirektno. Informacija kroz *peer-to-peer* mrežu putuje tako što svaki učesnik šalje poruku samo onima sa kojima je direktno povezan, zatim svaki od njih tu poruku dalje šalje onima sa kojima je direktno povezan i tako sve dok poruka ne dođe do svih učesnika u mreži. Dakle, ovde imamo primer slanja informacija preko velikog broj posrednika i sjajan primer problema vizantijskih generala, samo mnogo komplikovaniji primer od onog kojeg smo prethodno razmatrali.

Slika 5: *Peer-to-peer* mreža (izvor: www.thenextweb.com)

Da bismo shvatili kako bitkoin rešava problem vizantijskih generala, bitno je da napomenemo još jednu bitnu osobinu bitkoina. Naime, neka od čvorišta (takva čvorišta se nazivaju "*full node*") u mreži imaju na svom hard disku kompletan blokčein (bazu svih transakcija koje su se ikada desile) i takvih čvorišta je na hiljade. Pošto svi oni stalno međusobno komuniciraju, uvek proveravaju da li se njihova kopija blokčeina slaže sa ostalima. Ako se ne slaže, oni automatski ažuriraju svoju verziju tako da se slaže sa ostatkom mreže. Zamislite to kao bazu podataka koja je replicirana na hiljadama računara i koja se na svim tim računarima ažurira u realnom vremenu. Koliko je teško izmeniti neki podatak u takvoj bazi?

Svaki korisnik bitkoina ima privatni ključ, javni ključ i bitkoin adresu. Javni ključ se kreira od privatnog ključa, ali na način da je nemoguće uraditi obrnut proces, to jest, od javnog ključa napraviti privatni. Zatim se od javnog ključa kreira bitkoin adresa na koju se primaju bitkoini i njega nema potrebe kriti. Sa druge strane, vrlo je važno da se dobro čuva privatni ključ. Privatnim ključem se potpisuju transakcije sa bitkoin adrese koja je za taj ključ vezana. Zamislite da je bitkoin adresa vaš broj bankovnog računa, a privatni ključ vaš pin kojim verifikujete plaćanja sa tog računa. Otprilike tako funkcioniše, uz jednu vrlo bitno razliku: Ako izgubite pin kojim verifikujete transakcije sa bankovnog računa, banka će vam izdati novi. Ako izgubite privatni ključ, izgubili ste zauvek bitkoine na adresi za koju je taj privatni ključ vezan. Ti bitkoini i dalje postoje, ali im niko ne može pristupiti bez privatnog ključa.

Kada želim da pošaljem bitkoine nekome, moram da unesem bitkoin adresu primaoca, iznos koji želim da pošaljem i da transakciju potpišem mojim privatnim ključem. Zatim informaciju o toj transakciji šaljem učesnicima sa kojima sam direktno povezan u *peer-to-peer* mreži, da bi je oni dalje prosledili sve do primaoca. Možda ste čuli da se kod bitkoina transakcije šalju bez posrednika? Ovo je zapravo vrlo netačno. Nema posrednika u onom klasičnom smislu u kojem doživljavamo posrednika - neko ko šalje našu transakciju i koji za to uzima novac i unosi kašnjenje, ali ima i pravo da tu transakciju ne odbije, zamrzne, odloži... Ipak, pri slanju bitkoin transakcije ima posrednika, čak hiljade njih, samo je njihova uloga malo drugačija.

Svako čvorište u bitkoin mreži je zapravo posrednik koji transakciju proveri i prosledi dalje sve dok ona ne dođe do svih čvorišta u mreži. Kad su je svi proverili i transakcija je došla do svih u mreži, ona ispunjava uslov da se ubaci u blok i time postane deo blokčeina (o procesu formiranja blokova transakcija ćemo više pričati malo kasnije). Šta svi ti posrednici zapravo proveravaju?

- Da li pošiljalac ima na svojoj bitkoin adresi dovoljno bitkoina da bi mogao da izvrši transakciju?
- Da li je adresa primaoca validna?
- Da li je potpis pošiljaoca validan?

Kako oni mogu sve to da provere? Setimo se da postoje čvorišta koja na svom hard disku imaju kompletan blokčein (sve transakcije koje su se ikad desile). Baš zbog toga, oni u svakom trenutku znaju tačno na kojoj adresi koliko bitkoina ima i koje su adrese validne, a koje nisu. Ako transakcija prođe sve 3 provere, ona se prosleđuje dalje kroz peer-to-peer mrežu dok ne dođe do svih. Iako sve ovo deluje kao veoma kompleksan proces, u praksi je bitkoin transakciji potrebno manje od 1 sekunde da dođe do svih čvorišta u bitkoin mreži.

Za kraj ovog dela, vratimo se na problem vizantijskih generala. Šta ako su posrednici nepouzdani? Bitkoin je ovaj problem rešio na veoma zanimljiv način - povećao je broj posrednika! Ako ne možeš da veruješ jednom posredniku - koristi na hiljade njih! Deluje neverovatno, ali zaista funkcioniše. Hajde da razmislimo šta bi se desilo ako bi neki od učesnika u bitkoin mreži pokušao da promeni transakciju koju je primio, pre nego je prosledi dalje. Ne bi se desilo ništa, zbog načina na koji mreža funkcioniše. Učesnici u mreži konstanto komuniciraju i porede svoje kopije baze sa drugima. Ako primete da se njihova kopija razlikuje od drugih, oni svoju kopiju prilagode tako da bude ista. Međutim, svaki od učesnika je povezan direktno sa nekoliko drugih. Ako od jednog od njih dobija jednu informaciju, a od svih ostalih drugu, on će tog jednog učesnika jednostavno ignorisati, tako da izmenjena informacija ne može da propagira kroz mrežu.

U mreži od nekoliko hiljada učesnika jedan "izdajnik" ne može da učini nikakvu štetu, što je nekako i logično. Međutim, šta ako imamo više "izdajnika"? Dok god je njihov broj ispod 50%, cela mreža je bezbedna, jer su čvorišta programirana tako da stav većine prihvataju kao tačan. Dakle, da bi se mreža ugrozila, potrebno je pošteni članovi mreže budu u manjini, ali to nije jedini uslov, što napad na mrežu čini još težim. Da bi napad uspeo, neophodno je da napadači budu u većini i da budu savršeno sinhronizovani. Sinhronizacija hiljada učesnika je sama po sebi dovoljno teška, a napad čini još težim to što bi oni morali da deluju istovremeno i trenutno čim se pojavi transakcija koju žele da izmene. Problem je što vrlo teško mogu unapred da znaju kada će se tačno transakcija desiti i kako će izgledati. Napad na bitkoin mrežu je teoretski moguć, ali se u praksi pokazao kao nemoguć punih 9 godina.

Ovde vidimo zašto je bitkoin mnogo više od internet novca - on je rešio problem poverenja u decentralizovanoj mreži učesnika koji se međusobno ne poznaju, što je zapravo problem vizantijskih generala (koji je do pojave bitkoina bio nerešiv punih 26 godina). Možemo slati novac (ili bilo koji elektronski zapis) pomoću posrednika koje ne poznajemo i kojima ne verujemo, a opet biti potpuno sigurni da će novac stići tačno onome kome treba i tačno u iznosu koji je poslat.

2.4. Javni blokčein

Do sada smo se bavili isključivo bitkoinovim blokčeinom. Blokčeinova je puno, jer skoro svaka kriptovaluta ima svoj blokčein, mada su neke od bitnih karakteristika svima njima zajedničke i praktično preuzete od bitkoinovog blokčeina.

Većina kriptovaluta (među njima i bitkoin) ima javni blokčein, koji ima sledeće karakteristike:

- Svako mu može pristupiti, to jest videti sve transakcije koje se na blokčeinu dešavaju. Postoji puno servisa koji omogućuju pregled blokčeinova (poznati kao *Block Explorer*-i), a najpoznatiji je blockchain.info na kojem se može pratiti bitkoinov blokčein.
- Svako može da vrši transakcije. Dovoljno je da preuzme mobilni ili desktop novčanik (*Wallet*) ili koristi neki od onlajn novčanika i može slobodno da vrši transakcije.
- Svako može da učestvuje u kreiranju blokova i samim tim u deobi nagrade koja se za dodavanje blokova dobija. Drugim rečima, svako može da bude "rudar".
- Svako može da ima udela u odlučivanju o izmenama i dopunama protokola koji upravlja kriptovalutom. Kod nekih kriptovaluta odluke donose rudari, ali postoje i kriptovalute kod kojih udeo u upravljanju imaju i drugi učesnici.
- Protokol koji upravlja sistemom je u formi otvorenog koda. Svako može taj kod pregledati, ali svako može i predložiti izmene i dopune tog koda. Ukoliko većina prihvati predložene promene, te promene postaju sastavni deo protokola. Takođe je vrlo čest slučaj da se uzme kod jedne kriptovalute, malo se izmeni i lansira kao nova kriptovaluta. Taj proces se naziva "forkovanje".

Iz potpune otvorenosti javnih blokčeinova proizilaze i neke od njihovih prednosti i mana. Glavne **prednosti** javnih blokčeinova su:

- Blokčein je otporan na potencijalne napade. Zbog činjenice da svako može da bude čvorište u peer-to-peer mreži, broj tih čvorišta je veoma veliki i samim tim je teže da broj "nepoštenih igrača" bude preko 50%. Trenutno je kod bitkoina broj tih čvorišta oko 13 12.000. Ako bi neko hteo da poremeti normalan protok informacija kroz bitkoin mrežu, morao bi da ima preko 12.000 savršeno sinhronizovanih čvorišta. Čak i tada, šteta koju bi mogli da načine je vrlo mala ako nemaju podršku preko 50% "rudara", što je izuzetno skupo.
- Baza podataka je nepromenjiva. Ovo ponovo proizilazi iz toga što je celokupna baza transakcija replicirana na hiljadama računara širom sveta. Takođe, blokčein održava mreža rudara sa veoma velikom zbirnom procesorskom snagom. Istorija se može promeniti dobrovoljno - tako što se većina učesnika složi da se promena izvrši. Ovo je u praksi malo verovatno, jer bi većina morala da se složi oko nečega što ugrožava integritet mreže i samim tim obara cenu kriptovalute vezane za taj blokčein. Istorija se može promeniti i nasilno, pri čemu je potrebno da napadač kontroliše više od 50% procesorske snage celog sistema tokom dužeg vremenskog perioda. Ovo bi bio izuzetno skup poduhvat i ne postoji način da se tolika investicija finansijski isplati napadaču.

Glavne **mane** javnih blokčeinova su:

- Kapacitet blokčeina je vrlo ograničen, kako po broju transakcija koji može da se obradi u jedinici vremena tako i po količini podataka koja u blokčeinu može da se skladišti. Da bi što više ljudi moglo da učestvuje u održavanju mreže, zahtevi moraju biti relativno skromni, kako u količini prostora na hard disku koji blokčein zauzima, tako i u brzini internet konekcije. Bitkoin mreža trenutno može da obradi svega nekoliko transakcija u sekundi. Poređenja radi, Visa može da obradi desetine hiljada transakcija u sekundi.
- Način upravljanja je neefikasan. Da bi se izvršila bilo kakva, čak i najsitnija, promena u sistemu, potrebno je da se većina oko te promene složi. To bi otprilike bilo kao kada bi se za svaku pojedinačnu odluku u državi organizovao referendum. Jasno je da ovakav princip otežava upravljanje i smanjuje fleksibilnost sistema. Čak ni za dobre predloge nije lako obezbediti većinu, a često nije baš lako odrediti koji je predlog dobar, a koji nije. Odličan primer za ovaj problem je ono što se u bitkoin mreži dešava već 2 godine. Naime, još od 2015-te postoje različiti predlozi kako da se unapredi protokol kako bi se povećao kapacitet bitkoin mreže, ali nikako da se mreža usaglasi oko jednog od tih predloga.

2.5. Privatni blokčein

Tokom prvih nekoliko godina svog postojanja, bitkoin i blokčein tehnologija uopšte, su privlačili vrlo malo pažnje i retko ko im je davao ozbiljnu šansu. Pre 5 godina je situacija polako počela da se menja i sve više institucija i kompanija je počelo da pokazuje interesovanje za blokčein tehnologiju. Svakako ih je privukao njen vrlo inovativan način slanja i skladištenja podataka, kao i način na koji rešava problem poverenja u sistemu koji ima više učesnika. Međutim, ono što im se nije svidelo je transparentnost i to što je sistem svima dostupan. Ta svojstva im uglavnom ne odgovaraju za većinu potencijalnih poslovnih primena. Zato se pojavila ideja o privatnom blokčeinu koji bi zadržao većinu prednosti javnog blokčeina, ali i otklonio ono što takve organizacije vide kao nedostatke.

Evo po čemu se privatni blokčeinovi razlikuju od javnih:

- Blokčein nije svima vidljiv. Blokčein je vidljiv samo onima koji imaju dozvolu. Dozvolu najčešće izdaje kreator ili vlasnik blokčeina, s tim da postoji mogućnost da se izdaju različite kategorije dozvola kod kojih je i količina vidljivih podataka različita.
- Ne može svako da vrši transakcije. I transakcije su omogućene samo onima sa dozvolom. Dozvolu mogu dozvolu može da izdaje vlasnik blokčeina, ali i neka od organizacija koje učestvuje u sistemu, pri čemu se krajnji korisnici preko tih organizacija vezuju za blokčein.
- Ne može svako da kreira blokove, već samo oni koji su za to "ovlašćeni" od strane vlasnika blokčeina. Za razliku od većine javnih blokčeinova, ovde kreiranje blokova najčešće ne podrazumeva angažovanje snažnog i skupog hardvera koji rudari.
- Ne učestvuje svako u odlukama. O svim izmenama u protokolu odlučuju samo oni koji su za to delegirani od strane vlasnika blokčeina
- Kod nije javno dostupan. Ponekad nije dostupan čak ni svim učesnicima u sistemu. Ne može bilo ko da predloži izmenu koda, već postoji tim koji se bavi razvojem protokola.

- Privatni blokčein ne mora da ima kriptovalutu. Kod javnih blokčeinova, kriptovaluta služi da motiviše rudare da pomognu u održavanju sistema. Ovde sistem najčešće održavaju organizacije koje su deo sistema i kojima je sama mogućnost korišćenja sistema "nagrada" za njihov doprinos u njegovom održavanju. Vrednost blokčeina raste sa njegovim brojem korisnika, kako kod javnih, tako i kod privatnih blokčeinova. Zbog toga su veoma česti primeri grupa kompanija koje zajednički rade na razvoja nekog blokčein projekta koji bi kasnije zajedno koristili. Projekti koji okupljaju najveći broj kompanija su: Hyperledger, Enterprise Ethereum Alliance i R3.

Glavne **prednosti** privatnih blokčeinova su:

- Kapacitet ovakvog blokčeina može biti izuzetno veliki. Pošto su kod privatnih blokčeinova učesnici sistema uglavnom kompanije, njima nije preterani problem da obezbede veliki skladišteni prostor gde bi se blokčein čuvao, kao i dovoljno brzu internet konekciju koja bi mogla da podrži veliki broj transakcija. Samim tim, ovakav blokčein može biti značajno veći i brži od javnog.
- Upravljanje je efikasnije. Za razliku od javnih blokčeinova gde hiljade ljudi učestvuje u donošenju odluke, kod privatnih blokčeinova su najčešće u pitanju desetine kompanija, a ponekad i svega nekoliko. Zbog ovoga je znatno lakše postići konsenzus oko svake odluke pa se i izmena protokola može lakše i brže implementirati. Ipak, to što je broj učesnika manji, ne znači da će se uvek lako složiti oko svega. Primera radi, nekoliko kompanije ja napustilo R3 konzorcijum jer se nisu slagale sa pravcem razvoja blokčeina koji je većina nametnula.

Glavne **mane** privatnih blokčeinova su:

- Previše moći u rukama malog broja kompanija. I kod privatnih blokčeinova se uglavnom odluke donose konsenzusom. Međutim, ovde je potreban značajno manji brojučesnika da bi se obezbedila većina koja može da preuzme kontrolu nad sistemom. Često je broj onih koji kontrolišu sistem još manji nego što na prvi pogled deluje. Naime, pošto se sistemu pristupa sa dozvolom, neko mora tu dozvolu da izdaje. Broj onih koji izdaju dozvolu je često osetno manji od ukupnog broja korisnika. Oni koji izdaju dozvolu zapravo kontrolišu sistem jer mogu ukinuti dozvolu onima koji su neposlušni, a umesto njih ubaciti poslušne i tako obezbediti većinu. Postoje još neki načini na koje većina može manipulisati sistemom, a da se to i ne primeti, ali to prevazilazi okvire ovog kursa.
- Nova vrsta napada na sistem. Javni blokčeinovi su transparentni i nema svrhe hakovati ih da bi se došlo do poverljivih podataka, jer ti poverljivi podaci kod njih ne postoje. Međutim, privatni blokčeinovi su privatni pre svega zbog toga da bi podaci koji se u blokčeinu nalaze bili dostupni samo učesnicima u sistemu. Ti podaci za njih imaju veliku vrednost, samim tim postaju vrlo zanimljiva meta hakerima koji bi dolaženjem do tih podataka mogli da ugroze učesnike u sistemu ili da ih ucenjuju.

2.6. Potencijal za primenu blokčein tehnologije

- **Kriptovalute** - Prva primena blokčein tehnologije su kriptovalute, to jest bitkoin. Mogućnost da se u decentralizovanoj mreži uspostavi poverenje dozvoljava da se transakcije vrše na brz, jeftin i bezbedan način, bez ikakvih ograničenja.
- **Čuvanje podataka** - Kada nam je neki fajl veoma bitan, mi uradimo bekap. Blokčein može da ima hiljade ažurnih kopija kompletne baze podataka u svakom trenutku. Ipak, videli smo da javni blokčeinovi imaju ograničen kapacitet što se tiče količine podataka koju mogu da skladište, dok privatni možda nisu dovoljno pouzdani za to.
- **Integritet podataka** - Kao što smo naučili, podatke u blokčeinu je skoro nemoguće izmeniti. Kad god nam je bitno da budemo sigurni da će neki podatak biti sačuvan baš onakakav kakav jeste i da niko neće moći, blokčein bi mogao biti rešenje.
- **Kontrola potrošnje** - Sve transakcije koje su se ikada desile su vidljive na blokčeinu, pa nam to može omogućiti da pratimo da li su se određena sredstva potrošila baš na način na koji je bilo planirano.
- **Određivanje vremena** - Uz svaku transakciju zapisanu u blokčeinu, zapisano je i vreme kad se ona dogodila, tako da se uvek može precizno utvrditi tok događaja.

Spisak se ovde ne završava, ali je za sada dovoljno da se pomene ovih 5 primena.

3. Rudarenje

3.1. Heš funkcija i Proof-of-Work algoritam

3.1.1. Slanje transakcija

Da bismo deo o rudarenju bolje razumeli, nije loše da se podsetimo prethodne dela i nekih stvari koje smo tu obradili:

- Bitkoinima na određenoj bitkoin adresi se može pristupiti samo uz pomoć privatnog ključa koji je za tu adresu vezan.
- Vlasnik privatnog ključa, kada želi da pošalje bitkoine, unosi bitkoin adresu primaoca, iznos koji šalje i na kraju transakciju potpisuje svojim privatnim ključem (to "potpisivanje" se iz ugla korisnika zapravo vrši jednim klikom. Nakon tog klika, softver koji upravlja bitkoin novčanikom kreira digitalni potpis primenom kriptografskih funkcija).
- Kada je transakcija potpisana, ona se šalje kroz *peer-to-peer* mrežu, kako bi stigla do svih čvorišta u mreži i kako bi svi korisnici znali da se transakcija dogodila.
- Tokom propagiranja transakcije kroz mrežu, svako od čvorišta proverava validnost transakcije i tek nakon provere šalje transakcije dalje kroz mrežu. Time se sprečava da transakcija koja nije validna propagira kroz mrežu.
- Čvorišta mogu da provere validnost transakcije jer poseduju svoju kopiju baze svih transakcija koje su se ikada desile, pa samim tim znaju koje su adrese validne i koliko na kojoj adresi ima bitkoina.

3.1.2. Heš funkcija

Heš funkcija je kriptografska funkcija koja podatke proizvoljne dužine konvertuje u podatke fiksne dužine. Bitkoin koristi SHA256 heš funkciju. SHA256 funkcija za podatak proizvoljne dužine daje rezultat dužine tačno 256 bita ili 64 karaktera u heksadecimalnom sistemu (heksadecimalni sistem je sistem sa bazom 16 u kojem se zapis sastoji iz svih deset cifara - 0,1,2,3,4,5,6,7,8,9 i prvih 6 slova abecede - A,B,C,D,E,F).

Heš funkcija ima dve vrlo korisne osobine za rudarenje bitkoina:

- Na osnovu rezultata je nemoguće izračunati ulazni podatak.
- Svaka promena ulaznog podatka, čak i najmanja, potpuno menja rezultat.

3.1.3. Kreiranje blokova

Ako čvorišta verifikuju transakcije, šta onda rade rudari? Posao rudara je da transakcije, koje su prethodno verifikovane od strane čvorišta, pakuju u blokove. Kod kreiranja blokova postoje određena pravila:

- Svi rudari na svetu se takmiče u kreiranju blokova.
- Blok ne sme biti veći od 1MB, tako da je broj transakcija koje mogu da stanu u blok ograničen.
- Kada neko predloži pobednički blok on ga šalje ostalima u peer-to-peer mreži na proveru. Ako čvorišta utvrde da je blok validan, dodaju ga u blokčein.
- Pobednik dobija 12.5 bitkoina + provizije na sve transakcije koje su ušle u taj blok (provizije se plaćaju zbog toga što je broj transakcija koje su kandidati da uđu u blok veći od kapaciteta bloka, pa rudari biraju transakcije sa većim provizijama kako bi više zaradili).
- Čim se doda novi blok, trka ponovo počinje i svi pokušavaju da prvi kreiraju naredni validan blok.
- Pobednik je onaj koji prvi kreira blok čiji HešŠ je manji od zadatog broja. Taj zadati broj je u direktnoj vezi sa težinom rudarenja (*mining difficulty*). Što je veći broj rudara i njihova zbirna procesorska snaga - to je težina veća, a zadati broj manji.
- Taj zadati broj se automatski podešava tako da se blokovi kreiraju u proseku na svakih 10 minuta. Podešavanje se vrši na svakih 2016 blokova, što je u proseku 2 nedelje. Ako je u prethodnih 2016 blokova procesorska snaga mreže porasla, taj broj će se smanjiti. Ako se procesorska snaga povećala, taj zadati broj će se povećati.
- Na svake 4 godine se nagrada za rudare prepolovljava. U prve 4 godine, nagrada je bila 50 bitkoina po bloku, zatim je pala na 25 bitkoina po bloku, a trenutno iznosi 12.5 bitkoina po bloku.

3.1.4. Proof-of-work algoritam

Šta sve mora da sadrži jedan blok?

- Heš prethdnog bloka, kako bi blokovi bili povezani u lanac – blokčein.
- *Coinbase* transakciju - to je transakcija kojom rudar sam sebi dodeljuje novih 12.5 bitkoina, kao nagradu za to što je prvi kreirao validan blok. On tih 12.5 bitkoina ne uzima ni od koga, već ih kreira i jedino na taj način se novi bitkoini ubacuju u opticaj.
- Transakcije koje je rudar izabrao da spakuje u taj blok (najčešće ih ima oko 2500, ne može stati mnogo više zbog ograničenja veličine bloka na 1MB)
- *Nonce* - broj koji se vrti od 0 do 2^{32} u pokušaju da se nađe onaj za koji će heš bloka imati odgovarajuću vrednost (nižu od zadate).

Zbog osobina heš funkcije, rudari nemaju način da pretpostave kakvi su im ulazni podaci potrebni da bi dobili rezultat koji žele. Zato moraju da isprobavaju redom različite vrednosti *Nonce* broja, jednu po jednu, da bi dobili željeni rezultat. Pošto ne postoje prečice da se dođe do rezultata, nego se bukvalno

isprobava jedan po jedan broj dok se ne pogodi onaj pravi, ova metoda se naziva "potpuna pretraga" (*brute force*). Zbog ovoga je bitno imati jak hardver, jer on može više pokušaja da napravi za kraće vreme i time povećava šansu da baš on bude taj koji će prvi kreirati validan blok. Da bi se našli potrebni ulazni podaci koji daju odgovarajući rezultat neophodan je izuzetno veliki broj pokušaja, a da bi se taj veliki broj pokušaja odradio za kratko vreme, neophodna je velika procesorska snaga i velika količina rada. Zbog toga se ovaj algoritam za rudarenje naziva *Proof-of-Work*, jer je rudar morao da uloži veliku količinu rada da bi došao do rezultata.

Kod ovog algoritma je dobra stvar to što je nekom drugom potrebno veoma malo vremena i rada kako bi proverio validnost rezultata. Kada rudar kreira blok koji zadovoljava potrebne uslove, on ga šalje ostatku mreže na proveru. Oni vrlo lako i brzo provere da li se za ulazne podatke koje je on imao zaista dobija heš koji on tvrdi da je dobio i, ako se pokazalo da je bio u pravu, taj blok zvanično postaje sastavni deo blokčeina i on dobija svoju nagradu od 12.5 bitkoina + provizije. Ako blok nije validan, mreža će odbiti taj novi blok i potraga za "pobednikom" se nastavlja.

3.1.5. Orphan blokovi

Ponekad se desi da 2 rudara skoro u isto vreme nađu novi blok koji zadovoljava zadate uslove. Ako su oba validna, oba će biti prihvaćena od strane mreže, ali ne od cele mreže. Naime, u peer-to-peer mreži informacija putuje od čvorišta do čvorišta dok ne dođe do svih. Kada rudar nađe blok, on tu informaciju najpre pošalje čvorištima sa kojima je direktno povezan. Ako je drugi rudar našao novi blok u skoro isto vreme, do njega još nije došla informacija da je neko drugi kreirao blok i on takođe šalje informaciju o svom novom bloku čvorištima sa kojima je direktno povezan.

Praktično sa 2 različite strane mreže u isto vreme kreću kroz mrežu 2 različita bloka, od kojih je svaki validan. Svako od čvorišta će prihvatiti onaj blok koji do njega prvi dođe, a drugi će odbaciti. Kad se propagacija završi, situacija će biti takva da će deo mreže imati jedan blok kao poslednji, a deo mreže će imati drugi blok kao poslednji (svi ostali blokovi su im isti). Kako se ovaj problem rešava? U ovom trenutku postoje dve verzije blokčeina, deo mreže ima jednu verziju, a deo mreže drugu, razlikuju se po poslednjem bloku. Prvi deo ne priznaje transakcije koje se nalaze u poslednjem bloku drugog dela mreže i obrnuto (iako se verovatno neke transakcije poklapaju). Rudari u prvom delu mreže pokušavaju da nadograde novi blok na njihovu verziju blokčeina, dok rudari u drugom delu mreže pokušavaju da nadograde blok na njihovu verziju blokčeina. Koja god grupa da prva uspe u tome, ona će svoju verziju blokčeina nametnuti celoj mreži.

Setimo se, čvorišta stalno međusobno komuniciraju i upoređuju svoj blokčein sa "komšijama". Ako primete da neko ima blokčein sa većim brojem blokova, pretpostaviće da iza njega stoji većinski deo mreže i preuzeće tu verziju blokčeina. U tom slučaju, oni će svoj poslednji blok praktično odbaciti kao nevažeći, zajedno sa svim transakcijama u njemu. Zato se taj blok naziva "*Orphan*" (siroče). Teoretski je moguće da se 2 puta za redom dogodi da 2 rudara u isto vreme kreiraju novi blok, ali su šanse za to izuzetno male. Šanse da se to desi 3 puta za redom su zanemarljivo male, pa većina smatra da je bitkoin transakcija konačna ako su od trenutka slanja te transakcije dodata 3 nova bloka (s tim da ta transakcija mora da bude u prvom od ta 3). Oni konzervativniji čekaju 6 blokova.

3.2. Rudarski pulovi

Broj rudara u svetu je veliki i u stalnom porastu. Šansa za svakog pojedinačnog rudara da prvi kreira sledeći blok je izuzetno mala. Srećom, blokovi se pojavljuju u proseku na svaki 10 minuta. Međutim, često ni to nije dovoljno brzo. Uzmimo primer rudara čija procesorska snaga predstavlja 0.01% ukupne rudarske procesorske snage u svetu (što je, uzgred budi rečeno, vrlo ozbiljan rudar). Statistički gledano, na 10.000 blokova jedan je njegov, što znači da bi u proseku na svakih 70 dana on kreirao po jedan blok i zaradio 12.5 bitkoin + provizije. Ali to je samo statistika, to nikako nije zagarantovano.

U praksi, takav rudar može da kreira 2 bloka u jednom danu, ali može i da 2 godine ne kreira nijedan blok. Pošto rudari imaju fiksne troškove, bitno im je i da imaju predvidive prihode. Zato postoje rudarska udruženja, poznatija kao pulovi. Ona okupljaju veći broj rudara koji imaju dogovor da, ko god unutar pula kreira blok, nagradu dele svi, srazmerno snazi koju su dali pulu na raspolaganje. Vlasnik pula uzima za ovo određenu proviziju, koja je obično nekoliko procenata. Ako je pul veći, on će svakodnevno kreirati blokove pa će i svi rudari u pulu imati dnevne isplate, koliko god male one bile. Time su sebi obezbedili redovne prihode i ne zavise od svoje sreće u pokušavanju kreiranja bloka pre svih ostalih.

3.3. Cloud mining

Rudarenje zahteva odgovarajući prostor, sa dobrim električnim instalacijama, dobrom ventilacijom/sistemom za hlađenje i zvučnom izolacijom. Neki odustaju od rudarenja baš zbog tih komplikacija. Kao rešenje za te probleme nastao je "*Cloud Mining*". Tu je ideja da čovek umesto kupovine rudarske opreme praktično plati najam nečije postojeće rudarske opreme. Na taj način učestvuje u rudarenju iako fizički ne poseduje hardver, pa samim tim ne mora da brine oko struje, hlađenja, buke, obezbeđenja i sličnih stvari koje rudarima zadaju glavobolje.

Iako *Cloud Mining* zvuči sjajno u teoriji, u praksi je to sve samo ne sjajno. Problem je što mi ne možemo znati da smo zaista zakupili neki hardver i da li on radi za nas. Veoma visok procenat kompanija koje nude Cloud Mining servis su zapravo prevaranti. Oni nemaju nikakvu opremu ili imaju vrlo malo i uopšte ne rudare. Naime, oni od novca novih investitora isplaćuju stare. Iz ugla investitora, sve funkcioniše jer dobijaju redovne isplate. Međutim, taj sistem funkcioniše sve dok redovne isplate ne premaše količinu novca koji se dobija od novih investitora. Kada se to desi, oni prestaju da isplaćuju. Neki to urade pod izgovorom da su hakovani, neki se pravdaju privremenim "tehničkim problemima", a neki samo ugase sajt i nestanu. Legitimne kompanije koje se bave *Cloud Mining*-om su nažalost veoma retke.

3.4. Evolucija hardvera za rudarenje

Kada je u januaru 2009-te bitkoin počeo da se rudari, nije bila potrebna nikakva posebna oprema za to. Rudarenje su vršili procesori (CPU rudarenje). Bitkoin ništa nije vredeo, pa niko nije ni video interes u tome da rudarenje optimizuje i učini ga efikasnijim.

Sredinom 2010-te godine počinje polako da se trguje bitkoinom, samim tim rudarenje polako postaje profitabilno i ljudi traže načine da rudare više. Rešenje je pronađeno u grafičkim karticama (GPU rudarenje) u julu 2010-te. Naime, došlo se do zaključka da, uz odgovarajući softver, grafičke kartice mogu značajno efikasnije da rudare od procesora. Tad je krenula trka koja traje i danas. Trebalo je naći što jaču grafičku karticu i time ostvariti prednost u odnosu na druge rudare. Zbog rudarenja već godinama traje velika nestašica jakih grafičkim kartica na svetskom nivou. Bitkoin se odavno rudari na drugi način, ali mnoge druge kriptovalute i dalje se oslanjaju na GPU rudarenje.

Grafičke kartice troše puno struje, prave veliku buku i generišu veliku količinu toplotne energije, tako da se intenzivno tragalo za alternativom. Alternativa su bile FPGA ploče koje su se pojavile u maju 2011-te. One nisu bile mnogo jake, ali su trošile neuporedivo manje električne energije od grafičkih kartica. Ipak, nikada nisu uspele da u potpunosti zamene grafičke kartice. Delom je to verovatno zbog toga što su bile relativno skupe (iako bi se to vremenom isplatilo), a delom što se pojavilo nešto mnogo bolje.

Krajem januara 2013-te su se pojavile ASIC mašine i to je bio početak kraja GPU i FPGA rudarenja, barem kada je bitkoin u pitanju. Grafička kartica je pravljena za nešto drugo i, mada može da rudari, ipak nije za to proizvedena i zbog toga su joj performanse ograničene. FPGA ploče su sastavljene od određenih komponenti koje su povezane baš tako da se napravi uređaj za rudarenje. Zbog toga su efikasnije od grafičkih kartica. Sa ASIC uređajima se otišlo korak dalje. To su uređaji koji se projektuju i već u fabrici izrađuju samo za jednu određenu funkciju - u ovom slučaju za rudarenje.

3.5. Drugi pristupi rudarenju

Često se velika potrošnja električne energije pominje kao ozbiljan problem bitkoin rudarenja. ***Proof-of-Work*** (PoW) algoritam je takav da rast mreže neminovno dovodi do rasta potrošnje električne energije. Bitkoin je najupečatljiviji primer, ali generalno sve kriptovalute čije se rudarenje bazira na proof-of-work algoritmu imaju isti problem. (Bitkoin je čak energetski efikasniji od mnogih jer ASIC rudari imaju značajno bolji odnos procesorske moći i potrošnje od GPU rudara). Druge zanimljive kriptovalute koje koriste PoW algoritam su Itirijum (*Ethereum*), Zkeš (*Zcash*) i Lajtkoin (*Litecoin*).

Najpopularniji alternativni algoritam za rudarenje je ***Proof-of-Stake*** (PoS). Kod tog modela, rudari dobijaju nagradu koja nije srazmerna snazi njihovog hardvera već količini kriptovalute koju već poseduju (narodski rečeno - para na paru ide). Najčešće je neophodan određeni minimalni iznos koji neko mora da ima kako bi mogao da rudari. Zbog dosta različitog pristupa, mnogi ljudi ovaj proces ne zovu "rudarenje" već "kovanje" (*minting*). Neki od primera PoS algoritma su kriptovalute Stratis i NEO. Čak i Itirijum ozbiljno planira prelazak na PoS model. Kod ovog modela ne postoji ogromna procesorska snaga koja štiti mrežu. Pravo odlučivanja je srazmerno količini kriptovalute koju neko ima i ovaj algoritam se vodi logikom da onaj ko ima puno neke kriptovalute neće donositi odluke koje su na štetu te kriptovalute. Ovo je slično modelu upravljanju kompanijom gde je "težina" nečijeg glasa direktno srazmerna broju akcija kompanije koji poseduje.

Varijacija ovog modela predstavlja ***Delegated Proof-of-Stake*** (DPoS) gde se određenom broju "delegata" poverava održavanje mreže - primer je Bitšers (*BitShares*). Postoje kriptovalute koje kombinuju PoW i PoS pa su na neki način hibridne. Pokušavaju da iskoriste prednosti svakog od pristupa pri tom. U

hibridnom sistemu deo nagrade od kreiranja novih blokova ide onima koji svojim hardverom doprinose održavanju mreže, a deo ide onima koji imaju određeni broj jedinica te kriptovalute. Primeri ovakvog rudarskog algoritma su Deš (*Dash*) i Pirkoin (*Peercoin*).

Iako su PoW i PoS najpopularniji algoritmi za rudarenje, postoje još neki. ***Proof-of-Burn*** je algoritam kod kojeg se koini "spaljuju", to jest šalju na adresu koja nikome nije dostupna i samim tim se nikako ne mogu dalje trošiti. To obično funkcioniše tako što se spaljuju jedinice jedne kriptovalute da bi se dobila druga. Kod kriptovalute Kaunterparti (*Counterparty*) se slanjem bitkoina na adrese koje nisu dostupne generišu jedinice te kriptovalute za onoga ko je te bitkoine "spalio".

Proof-of-Space ili ***Proof-of-Capacity*** je algoritam kod kojeg se umesto procesorske snage sistemu daje na raspolaganje skladišteni prostor na hard disku. Što više prostora neko da na raspolaganje mreži - to veću nagradu dobija u kriptovaluti koja se na taj način "rudari". Primer je Brstkoin (*Burstcoin*).

Pored svih navedenih, postoje još neki algoritmi koji se koriste u privatnim blokčeinovima kao što su ***Proof-of-Authority*** i ***Proof-of-Elapsed-Time***.

4. Altkoini

4.1. Fork

Naziv Altkoin se koristi da opiše kategoriju kriptovaluta, tj. bilo koju kriptovalutu koja je alternativa Bitkoinu. Kada je Bitkoin postao prva uspešna digitalna valuta, mnogo drugih je pokušalo da se nadoveže na njegov uspeh. Generalno gledano Altkoini pokušavaju da prevaziđu neka ograničenja koje Bitkoin kao takav ima, tj. da zamene ili unaprede bar jednu komponentu koju Bitkoin ima. Na primer, novi i moderniji Altkoini izlaze na tržište i pomeraju granice kao što su brzina transakcije, kapacitet, privatnost...

Prve alternative dodavale su samo malo više vrednosti nego što Bitkoin poseduje i u početku su pokušavale da kopiraju njegov uspeh. Štaviše, većina današnjih kriptovaluta su samo kopije Bitkoina sa malim, neprimetnim izmenama. Imaju manju rudarsku snagu iza sebe, imaju manje developera koji ih unapređuju i manje su korisne zbog malog efekta koji mreža stvara (mali broj učesnika).

Fork je događaj koji se javlja kada se blokčein podeli na dva dela. To može da se desi kada se ustanovi neko novo pravilo koje opisuje koja je transakcija validna. Korisnici blokčeina moraju da podrže predložene izmene protokola ili da ih odbace. Ako se korisnici ne slože oko podrške predloženim izmenama, mreža se deli na dva dela i stvaraju se dva različita blokčeina kroz proces poznat kao "forkovanje".

4.2. Bitkoin keš

Bitkoin (BTC) je doživeo *hard fork* (račvanje) i tako je nastao Bitkoin Keš (BCH). Do ovoga je došlo kada je broj transakcija na Bitkoinu porastao toliko da su korisnici morali da čekaju dugo na izvršenje svojih transakcija. To je stvorilo niz transakcija koje su se gomilale, čija je cena znatno veća od regularne i za obične korisnike prevelika za izvršavanje. Da bi se ovo prevazišlo bilo je potrebno smisliti novo rešenje. Protokol unapređenja Bitkoina (BIP) 148 je pokrenuo soft fork tako što je predložio novi protokol (SegWit) koji stvara više prostora u blokovima za više transakcija.

Za one koji nisu želeli da prihvate ovu promenu, Bitmain mreža je predstavila rešenje sa hard fork-om (UAHF) koje je imalo blok veličine 8 MB, bez Segwit-a i još tri načina da se originalan Bitkoin unapredi. Pošto je BCH rezultat hard fork-a, svako ko je posedovao BTC dobio je istu vrednost i u BCH tokenima. Bitkoin keš je od nastanka do sadašnjeg trenutka varirao sa vrednošću svojih tokena da bi trenutno bio četvrta kriptovaluta po ukupnoj tržišnoj vrednosti, posle Bitkoina, Itera i Ripla.

4.3. Lajtkoin

Lajtkoin (LTC) je zasnovan na Bitkoin *open-source* kodu, ali sa par tehnoloških razlika (ukupan broj novčića je 84 umesto 21 milion, prosečno vreme između 2 bloka je 2.5 minuta umesto 10, algoritam za

rudarenje je "scrypt" umesto "SHA-256", rudarenje je memorijski, a ne procesorski zahtevno). Lajtkoin nikad nije imao cilj da zameni Bitkoin, već da bude “srebro, pored Bitkoin “zlata”.

4.4. Zkeš

Zkeš (ZEC) je kripto valuta koja je nastala iz *Zerocoin* projekta. *Zerocoin* protokol koje je inicijalno trebalo da unapredi anonimnost korisnika na Bitkoinu, postao je *Zerocash* koji je rezultovao Zkeš kriptovalutom u 2016. Zkeš transakcije su objavljene javno na blokčeinu, ali korisnici imaju mogućnost da koriste opciju privatnosti i sakriju pošiljaoca, primaoca i količinu tokena u transakciji. Ovo je jedna od ključnih razlika u odnosu na Monero gde su sve transakcije isključivo privatne.

4.5. Deš

Deš (DASH) je takođe *open-source peer-to-peer* kriptovaluta koja cilja na to da bude što više *user-friendly*. Pored svih karakteristika koje Bitkoin poseduje, Deš nudi instant transakcije (*InstantSend*) i privatne transakcije (*PrivateSend*). Mogućnost upravljanja i budžetski sistem čine Deš decentralizovanom autonomnom organizacijom (DAO). U januaru 2014-te je originalno objavljen kao XCoin (XCO), da bi već u februaru ime bilo promenjeno u Darkcoin. Sadašnje ime dobio je u martu 2015-te

4.6. Ripl

Ripl (XRP) se zasniva na protokolu koji reguliše transakcije koje se koriste za razmenu između banaka i firmi sa zvaničnim XRP tokenom. Mreža je potpuno decentralizovana i može da funkcioniše bez Ripple-a kao organizacije - ne može se ugasiti. U svojoj suštini Ripl je zasnovan na javno podeljenoj bazi podataka, koja koristi konsenzus za odobravanje plaćanja i razmene.

4.7. Itirijum

Itirijum (ETH) je platforma koja omogućava izradu decentralizovanih aplikacija na blokčein tehnologiji i koristi Itirijumov blokčein kao bazu podataka da skladišti informacije. Cela Itirijum mreža je skupina velikog broja čvorišta (kompjutera) konektovanih između sebe i može se zamisliti kao jedinstveni entitet koji se naziva Itirijum virtualna mašina (EMV). Sve transakcije su automatski ažurirane i upisane u distibuiranu bazu podataka.

Najveća vrednost koju Itirijum pruža, što je više čini platformom za aplikacije nego valutom, jeste što su nalozi kontrolisani od strane samog koda (tj. Pametnih ugovora), a ne od strane korisnika. Pametni ugovor je niz instrukcija, napisanih u programskom jeziku *Solidity*. Jednostavnost logike jeste ono što ih

čini privlačnim i gotovo univerzalno primenljivim. Svaka transakcija koja je izvršena preko Pametnih ugovora (*Smart contract*) je snimljena i upisana na mrežu.

Itirijum ima svoju valutu zvanu Iter (ETH), rudari validiraju svaku transakciju i za to dobijaju određeni deo itera ili "*Wei*" kao najmanju jedinicu ove kriptovalute. Raznolikost mogućih aplikacija koje mogu da se izgrade učinila je Itirijum jako popularnim.

4.8. ICO

ICO (*Initial Coin Offering*) je nov način podizanja kapitala za finansiranje projekta, gde startapovi ili onlajn projekti dobijaju investicije tako što kreiraju i prodaju njihove kripto valute, bez da prodaju akcije svoje kompanije ili da prilaze velikim kapitalnim fondovima. Kada startap želi da podigne sredstva kroz ICO pristupa nizu koraka da bi što bolje približili svoju ideju investitorima. Obično se kreće sa izradom ***Whitepaper***-a u kome specificiraju sledeće informacije

- Čime se projekat bavi i šta je potrebno da se uspešno izvede.
- Koliko novca je potrebno i kog tipa.
- Koliko novca osnivači planiraju da zadrže za sebe
- Koliko kampanja traje

Prva kampanja ovog tipa pokrenuta je od strane Masterkoina (*Mastercoin*) u julu 2013.

Ovaj relativno nov način finansiranja za razvoj novih aplikacija je pokrenuo dosta kontroverze oko nivoa rizika koji ovakvim načinom investiranja nastaje. Strah najviše proizilazi iz toga što ovaj ekosistem funkcioniše u potpunosti izvan trenutnog finansijskog sistema, regulatornih standarda i praksi. Pri tome dosta projekata ide ka tome da prevare investitore tako što će posle podizanja sredstava projekat završiti na smetlištu. Privlačna stvar oko ICO-ova jeste to da investitori mogu da ulože koliko god žele, što je jako slično "*crowdfunding*" kampanjama na "*Kickstarter*"-u.

Iako zvanično ljudi kupuju tokene da bi mogli da koriste usluge aplikacija, u stvarnosti najveći razlog za ovo jeste očekivanje da će cena tokena porasti. Ova očekivanja u suštini nisu neosnovana. Na primer kada je Stratis token izbačen u prodaju u julu 2016, vredeo je manje od centa, dok već u oktobru 2017 vredi 3.41 dolar, što je 487 puta više. Vrednost podignutih sredstava kroz ICO u 2017-oj je preko 2 milijarde dolara, što je preko 10 puta veća nego u 2016-oj, što jasno pokazuje kakav trend ova pojava ima.

5. Novčanici

5.1. Uvod u novčanike

Svi smo navikli da svoj novac čuvamo u novčanicima ili na računima. Prilično slično je i sa kriptovalutama. Kriptovalute se nalaze na adresama. Svaka kriptovaluta ima svoj sistem adresa i one se razlikuju u broju karaktera, početnim karakterima i slično. Prilikom slanja sredstava, onaj ko šalje sredstva mora da dokaže da je on i vlasnik adrese s koje pokušava da pošalje kriptovalutu. Ovo se radi tako što on svojim privatnim ključem potpisuje transakciju i na taj način dokazuje svima da je vlasnik te adrese i onoga što se na njoj nalazi. Proces digitalnog potpisivanja transakcije je niz kriptografskih i matematičkih funkcija kojim se dokazuje vlasništvo nad nekim sredstvima.

Primeri adresa:

- Bitkoin adresa - 132gPNDnWV7FmUYH19BvRMjmP4cxPMr2fD
- Lajtkoin adresa - LTtEnW3eDjx9QirrLkgesEUT3PM1D3pWiG
- Itirujum adresa - 0x0536806df512d6cdde913cf95c9886f65b1d3462
- Deš adresa – XqHt831rFj5tr4PVjqEcJmh6VKvHP62QiM

Za najveći broj korisnika kriptovaluta podatak da se njihove kriptovalute nalaze na nekoj adresi i da je potreban privatni ključ kako bi potrošili svoja sredstva ne znači previše. Da bi se korišćenje kriptovaluta olakšalo i približilo svima potrebno je imati jednostavniji način za skladištenje i slanje kriptovaluta. Ovde se pojavljuju digitalni novčanici za čuvanje i slanje kriptovaluta. Digitalni novčanik (Wallet) predstavlja softversko rešenje za skladištenje kripto adresa i privatnih ključeva za otključavanje tih adresa. Jedan novčanik može sadržati praktično neograničeno mnogo adresa.

5.2. Desktop novčanici

Kao što se može zaključiti iz imena, namenjeni su korišćenju na računarima. Prilikom korišćenja ovih novčanika, u zavisnosti od tipa desktop novčanika, korisnik na svom računaru može instalirati i "*full*" klijenta, koji dolazi sa celokupnim blokčejnom. U zavisnosti od toga koja je kriptovaluta u pitanju, ovo može zahtevati dosta memorijskog prostora na hard disku. Privatni ključevi su zajedno sa pripadajućim adresama sačuvani na hard disku računa na kome su instalirani. S aspekta sigurnosti ovo je dosta dobar način čuvanja sredstava. Kriptovaluta je na našem računaru i ukoliko uspemo da bezbednost računara održimo na dovoljno visokom nivou, onda su i naša sredstva sigurna.

Nedostaci ovog načina čuvanja kriptovaluta se ogledaju u nedovoljnoj mobilnosti sredstava, naročito ako je u pitanju desktop računar, a ne laptop. Često nove valute nemaju dovoljno kvalitetne i dovoljno dobro testirane desktop novčanike pa se onda primenjuju neke druge opcije. Desktop novčanici su uglavnom jednostavni za korišćenje. Nakon instalacije, ako je u pitanju i *full* klijent, potrebno je da prođe određeno vreme kako bi se desktop novčanik sinhronizovao sa ostatkom mreže. U slučaju bitkoina

i itirijuma, čiji su blokčejnovi i najveći, sinhronizacija može trajati i nekoliko dana, zavisno od kvaliteta brzine internet konekcije.

5.3. Mobilni novčanici

Mobilni novčanici predstavljaju aplikacije koje se nalaze na našem mobilnom telefonu. Oni predstavljaju. Instalacija ovih novčanika traje jako kratko i oni ne zahtevaju puno memorije. U ovom slučaju, privatni ključevi su sačuvani na našem mobilnom telefonu. Ovo uvodi sa sobom i potencijalne rizike. Šta se dešava u slučaju gubitka ili krađe mobilnog telefona? Postoji nekoliko mehanizama zaštite. Prvi je postavljanje pin koda koji sprečava onoga ko dođe u posed našeg telefona da neovlašćeno potroši naša sredstva. Ipak, ostaje problem izgubljenih sredstava.

Bez obzira na to što neko ko neovlašćeno pristupi našem telefonu neće moći da potroši naša sredstva, bitno je imati i način pomoću kojeg je moguće povratiti izgubljena sredstva. Ovo je takođe moguće uraditi. Deterministički novčanici nam omogućuju da pomoću "*seed words*"-a jednostavno "bekapujemo" svoj novčanik. Sve što je potrebno uraditi jeste da se ovih, najčešće 12 reči, zapišemo i bezbedno sačuvamo. Ovo nam je dovoljno da u svakom trenutku jednostavno svoja izgubljena sredstva povratimo natrag.

Mobilni novčanici su pogodni za mala i česta plaćanja. Ovom prilikom nije potrebno kopitati Ili ručno unositi adresu primaoca već je dovoljno skenirati QR kod koji tu adresu predstavlja. Ovo olakšava primenu kriptovaluta u svakodnevnom životu. Pomoću telefona moguće je platiti neku uslugu, robu ili podići gotovinu na nekom od specijalizovanih automata.

5.4. Onlajn novčanici

Onlajn novčanici predstavljaju najmanje bezbednu kategoriju digitalnih novčanika, jer se privatni ključevi ne nalaze kod vas. Nema potrebe za preuzimanjem ili instaliranjem bilo kakvog softvera. Novčanik dobijamo tako što napravimo korisnički nalog na nekom od onlajn servisa koji pružaju ovu uslugu. Sve se svodi na to da napravite korisnički nalog na nekom od sajtova koji pružaju mogućnost čuvanja kriptovaluta. Svojim sredstvima kasnije možete pristupiti pomoću bilo kojeg uređaja koji ima mogućnost pristupa internetu. Ovo vam daje dodatnu slobodu i mobilnost jer ne morate brinuti o gubitku mobilnog telefona ili nositi računar sa sobom.

Nedostatak ovih novčanika ogleda se u tome što se u ovom slučaju, kao što smo pomenuli, privatni ključevi ne nalaze u vašem posedu već se praktično nalaze u posedu provajdera onlajn novčanika, na serveru drugog lica. Nikako nije preporučljivo čuvati veće iznose na onlajn novčanicima.

5.5. Papirni novčanici

Papirni novčanici se najčešće koriste u situacijama u kojima neko želi da svoje bitkoine dugoročno čuva ili da ih nekome pokloni. Pomoću specijalizovanih sajtova prave se papirni novčanici koji na sebi imaju kripto adresu kao i privatni ključ za pristup sredstvima sa te adrese. Potom se ovakvi novčanici štampaju i odlažu na neko bezbedno mesto. Kada odlučimo da povučemo sredstva sa adrese, jednostavnim skeniranjem ili unosom privatnog ključa sredstva prebacujemo u neki od novčanika. Za dodatnu sigurnost se praktikuje da računar i štampač budu isključeni sa mreže kako neko zlonameran ne bi ipak došao do osetljivih podataka.

Na ovaj način smo sigurni da tajni podaci ipak nisu negde sačuvani i da im neko neće naknadno pristupiti. Onaj ko se odluči na ovaj vid čuvanja svojih bitkoina mora imati na umu da svako ko dođe u posed papirnog novčanika može lako da dođe u posed i samih sredstava koja se tu nalaze, osim ako se tokom kreiranja novčanika nije ubacila i dodatna šifra. Pored toga, ukoliko se papirni novčanik izgubi, pocepa ili na neki drugi način ošteti, sredstva su trajno izgubljena. Stoga je jako bitno na pravi način zaštiti papirni novčanik. Najčešće je to čuvanje u sefu ili sličnom mestu zaštićenom od oštećenja i neovlašćenog pristupa.

5.6. Hardverski novčanici

Najsigurniji način za čuvanje kriptovaluta predstavljaju hardverski novčanici, ali su to jedini novčanici koji nisu besplatni. Ovi novčanici su zapravo hardverski uređaji poput usb-flash uređaja. Oni imaju složen sistem za skladištenje i čuvanje parova privatnih ključeva i odgovarajućih adresa. Prilikom prve upotrebe ovakvih novčanika korisnik sa uređaja prepisuje 12 ili 24 reči koje kasnije mogu poslužiti da se povrate sredstva u slučaju gubitka uređaja. Hadverski novčanici dolaze sa sistemom za unos šifre. U slučaju da šifra bude pogrešna određeni broj puta, novčanik se zaključa i nakon toga je potrebno uneti gorepomenutih 12 (24) reči kako bi se novčanik otključao.

Prilikom slanja bitkoina, uglavnom se koriste onlajn aplikacije ili desktop novčanici podržani od strane proizvođača hardverskog novčanika. Hardverski novčanik se najpre poveže usb kablom sa računarom, nakon toga se hardverskom novčaniku šalje nepotpisana transakcija, zatim korisnik na ekranu svog uređaju vidi iznos koji šalje i adresu primaoca i nakon provere podataka i unosa šifre na hardverskom novčaniku, on nazad vraća potpisanu transakciju čime je svima dokazao da je on vlasnik tih sredstava i da zaista želi da izvrši tu transakciju. Ovaj vid čuvanja kriptovaluta, iako skuplji od svih drugih, predstavlja najsigurniji način za čuvanje kriptovaluta i pruža odličan nivo sigurnosti svima onima koji planiraju dugoročnije čuvanje kriptovaluta. Papirni i hardverski novčanici su bezbedniji od ostalih jer se kod njih vaši privatni ključevi nalaze oflajn.

6. Berze

6.1. Uvod u berze

Berze predstavljaju specijalizovane platforme na kojima se trguje kriptovalutama. Na ovakvim servisima moguće je menjati različite kriptovalute jedne za druge, a često i za dolare i druge nacionalne valute. Prvenstveno, cilj berzi je da omoguće korisnicima jednostavnu i laku razmenu kriptovaluta za novac ili razmenu jedne kriptovalute za drugu. Prva berza koja je omogućila trgovanje kriptovalutama bila je japanska berza MtGox. MtGox je nastao još 2006. godine, prvobitno je to bila onlajn platforma namenjena igračima društvenih igara. Ova platforma im je omogućavala da trguju i razmenjuju kartice za igranje društvenih igara.

U julu 2010. godine, samo dva meseca nakon što je bitkoin prvi put upotrebljen za plaćanje ("*Bitcoin Pizza Day*") MtGox je lansirao platformu za trgovinu bitkoinima. U momentu u kom se pojavila, ova berza je ljudima ponudila nešto potpuno novo, mogućnost da iz svog doma, uz nekoliko klikova na svom računaru kupe ili prodaju bitkoine bilo kome.

U godinama koje su usledile ispostavilo se da je ova berza ostaviti ogroman uticaj kako na cenu bitkoina tako i na trgovinu kriptovalutama. Procenjuje se da se tokom 2013-te i početkom 2014-te godine čak 70% celokupne svetske trgovine bitkoinima odvijalo na ovoj berzi. 2014-te godine se dešava veliki hakerski napad, nakon čega mnogi korisnici MtGox-a ostaju bez velikog dela svojih bitkoina. Ovo je značajno uticalo na cenu bitkoina, koja je jako brzo pala sa preko 1200 dolara na nešto vise od 200 dolara.

6.2. Bezbednosni problemi

U međuvremenu su se razvijale i druge berze poput Bitstamp.net, Poloniex.com, itd. Na primeru MtGox-a se najbolje uočava koliko je bitno da svoja sredstva čuvamo tako da budu sigurna i bezbedna. Kada Bitkoine ili neku drugu kriptovalutu čuvamo na berzi, privatni ključevi naših adresa, koji su i sve što je potrebno za slanje sredstava, se nalaze u posedu nekog drugog. To znači da ukoliko neko uspe da ugrozi sigurnost berze i prodre u njihov sistem za skladištenje privatnih ključeva vrlo verovatno će trajno otuđiti i veliki deo sredstava, što direktno znači da će i nas ugroziti. Berze najčešće ne preuzimaju odgovornost na sebe u ovakvim situacijama pa su korisnici ti koji snose gubitak.

Mnogi ljudi praktikuju da svoje kriptovalute čuvaju na berzama. Razlozi za to su različiti. Neki žele da im kriptovalute budu lako dostupne za slučaj da odluče da ih prodaju. Neki su jednostavni lenji da otvore novčanik i sami čuvaju svoja sredstva, a ima i onih koji nisu svesni rizika koji postoje kod čuvanja kriptovaluta na berzama. Koji god bili razlozi, ovakva praksa je veoma opasna. Ne postoji manje bezbedno mesto za čuvanje kriptovaluta od berzi. Zbog velike količine novca koji se na njima nalazi, berze su pod konstantnim napadima hakera. Nemojte ni pomišljati na korišćenje berzi bez 2-faktor autentikacije, mada time samo sprečavate da vaš nalog bude hakovan, ako hakuju samu berzu, tu pomoći nema.

Istina je da su od kraha MtGox-a, berze značajnije shvatile koje su potencijalne pretnje pa su sa tim u vezi i počele značajno više da ulažu u sigurnost i pravljenje mehanizama za sigurnije skladištenje

osetljivih podataka. Najpoznatije berze, na kojima se odvija i najviše trgovine su prisutne na tržištu skoro od samog začetka trgovine kriptovalutama tako da one trenutno pružaju koliko-toliko efikasnu i sigurnu uslugu. Ipak se, i pored svih mera zaštite, uspešni napadi na velike berze su nastavili da se dešavaju i posle MtGox incidenta. 2015-te je hakovan Bitstamp, a 2016-te Bitfinex.

6.3. Trgovanje na berzama

Najčešći razlog za korišćenje berzi jeste trgovina kritpovalutama. Princip trgovanja je isti kao i na svakoj drugoj berzi. Osoba koja želi da trguje kriptovalutama mora prvo da obezbedi određena sredstva na berzi. Najčešće se deponuju bitkoini na berzu, na nekim berzama je moguće deponovati i nacionalne valute poput evra ili dolara. Nakon toga se odabere određena kriptovaluta koja se kupuje i koja se kasnije prodaje po povoljnijoj ceni.

Ono što berze kriptovaluta razlikuje od klasičnih berzi je pre svega labaviji regulatorni okvir (tamo gde uopšte postoji), što prouzrokuje i veći rizik, ali i značajno veće oscilacije cena i mogućnosti za ostvarivanje enormnog profita. Postoje i razne napredne opcije za ozbiljnije trejdere, ali to je van okvira ovog kursa. Prilikom trgovanja na berzi jako je bitno voditi računa i o uslovima korišćenja kao i o pravnoj regulativi, kako u zemlji onoga ko ulaže novac na berzu, tako i u zemlji u kojoj je sedište određene berze. Ovim se sprečavaju pravni problemi koji mogu nastati prilikom podizanja novca sa berze. Situaciju ovde malo komplikuje to što je trgovina kriptovaluta u mnogim zemljama potpuno neregulisana, ali se to polako menja.

Trgovanje kriptovalutama je oblast koja se sve više razvija. U poslednje vreme dnevni obim trgovanja često prelazi 10 milijardi dolara, a broj novih korisnika koji se dnevno registruje na berzama se meri desetinama, pa i stotinama hiljada. Značajan broj trgovaca sa nekih drugih platformi ili iz drugih sistema poput trgovanja plemenitim metalima, indeksima i obveznicama se vremenom prebacio na trgovanje kriptovalutama jer su potencijalni profiti veći. Razvijeni su i specijalizovani alati koji korisnicima olakšavaju praćenje različitih berzi, stanja i trendova kretanja cena na njima. Predviđa se da će uz napredak regulative oko cele oblasti porasti i broj krupnih investitora koji će ući na tržište kriptovaluta, a koji ga sad izbegavaju baš zbog pravne nesigurnosti.

6.4. Tipovi korisnika berzi

Različiti ljudi koriste berze za različite stvari i četiri su glavna tipa aktivnosti na berzi:

- Investicija
- jednokratna kupoprodaja
- špekulacija
- arbitraža

Investicija i jednokratna kupoprodaja su potpuno različite stvari, ali se u oba slučaja berza koristi vrlo ograničeno. Investitori kupe željenu kriptovalutu na koju gledaju kao na dugoročnu investiciju. Nakon

kupovine, ako su pametni, kriptovalutu povuku sa berze i nemaju više potrebu za korišćenjem berze osim kada odluče da prodaju ili eventualno dokupe još.

Jednokratna kupoprodaja zapravo predstavlja situacije kada ili nekome treba kriptovaluta za nešto, pa koristi berzu kako bi je nabavio ili ima neku količinu kriptovalute koju želi da unovči (često rudari spadaju u ovu grupu). I ovde se berza samo iskoristi za određenu svrhu i nakon što je ta svrha ispunjena, najčešće se korišćenje berze vrlo brzo završava.

Oni koji se bave špekulacijom i arbitražom, za razliku od prethodne dve grupe, provode puno vremena na berzi i, ako su vešti, lepo i zarađuju. Špekulanti su oni koji pokušaju da profitiraju na osnovu svoje veštine da dobro procene kretanje cene. Naravno da postoje manje i više uspešni špekulanti. Jasno je da ne postoji špekulant koji uvek može biti u pravu, ali to nije ni neophodno, dovoljno je biti u pravu u više od 50% slučajeva.

Arbitraža je aktivnost koja je u principu mnogo manje rizična od špekulisanja. Ovde trejder ne pokušava da predvidi kretanje cene, već profitira na razlikama u ceni između berzi. Ako je, na primer, na jednoj berzi cena bitkoina 7500 , a na drugoj 7600 , on može na prvoj kupiti bitkoine po 7500 , a na drugoj istu količinu prodati za 7600 i tako zaraditi 100$ po bitkoinu. Trejder je ovde potpuno imun na trend kretanja cene kriptovalute. Ipak, i on ima neke izazove sa kojima se suočava. Dobre prilike za arbitražu se ne ukazuju toliko često, pogotovo kad je tržište stabilno. Trejder mora na nekoliko berzi imati "zarobljenu" značajnu količinu sredstava kako bi mogao efikasno da radi arbitražu, a uvek je rizično držati puno novca na berzama. Arbitraža je upravo i razlog što su na većim berzama cene uglavnom prilično ujednačene, jer kad god se pojavi malo veća razlika, trejderi je iskoriste za arbitražu kojom zapravo smanjuju te razlike.

Trgovanje ne berzama deluje vrlo primamljivo i zaista može biti veoma profitabilno. Ipak, treba biti vrlo oprezan. Pored toga što su berze same po sebi rizične, problem je što su one takozvani “zero-sum game”. To znači da je zbir dobitaka na berzi onih koji dobijaju, jednak zbiru gubitaka onih koji gube. Ako ste neiskusan trejder, nije teško pogoditi u kojoj ćete grupi verovatnije završiti. Potrebno je dosta znanja, discipline, vremena, pa i malo sreće, da biste na berzama dugoročno lepo prihodovali i mogli da od berze živite.

6.5. Alternative berzama

Iako su berze glavni način da se dođe do kriptovaluta ili da se one prodaju, postoje i drugi načini. Ti drugi načini su često značajno skuplji (prosečna provizija na berzama je negde oko 0.2%), ali uglavnom brži i neretko sigurniji.

Servisi za kupovinu i prodaju kriptovaluta funkcionišu slično kao menjačnice. Kada pričamo o tradicionalnim valutama, na berze morate deponovati novac i onda tamo trgujete sa drugim učesnicima. Sa druge strane, u menjačnicu odnesete novac i odmah ga sa samom menjačnicom zamenite za drugu valutu. Isto funkcioniše i sistem kod kriptovaluta - na berze deponujete novac i trgujete sa drugima, a kod servisa (menjačnica) prodajete firmi koja drži taj servis i od nje kupujete. Ovakvi servisi se često nazivaju menjačnicama, ali ovo nije potpuno precizno, jer se u većini država kriptovalute ne smatraju novcem.

Kriptovalute se mogu kupovati i prodavati i na specijalizovanim automatima. Tu se kriptovalute mogu zameniti za gotovinu i obrnuto. Ovo je često najskuplji način za kupovinu ili prodaju kriptovauta (provizije za prodaju su u proseku blizu 7%, a za kupovinu blizu 10%), ali je nekima i najpraktičniji, jer nije neophodno da se ima bankovni račun, neki su dostupni 24/7, a i mogu ga koristiti i stranci kojima lokalni servisi obično nisu dostupni.

Postoje i servisi koji, za određenu proviziju, pomažu kupcima i prodavcima da se povežu, vodeći pri tom računa o sigurnosti obe strane, najčešće korišćenjem “escrow” sistema. Ovde se bikoini prodavca zaključaju unutar servisa i ostaju zaključani dok prodavac ne potvrdi da je primio novac od kupca. Kad on to potvrdi, bitkoini se automatski šalju kupcu. Najpoznatiji ovakav servis je LocalBitcoins. Postoji i opcija kupovine i prodaje preko oglasa, kao što se i razne druge stvari mogu preko oglasa kupiti. Ova metoda je najrizičnija jer nikad ne znate sa kim možete imati posla, iako ponekad može biti najpovoljnija jer nema posrednika da se "ugradi".

7. Dodatni materijal

https://en.wikipedia.org/wiki/Money

http://www.investopedia.com/insights/what-is-money/

https://en.bitcoin.it/wiki/Main_Page

https://en.wikipedia.org/wiki/Bitcoin

https://www.microsoft.com/en-us/research/wp-content/uploads/2016/12/The-ByzantineGenerals-Problem.pdf

https://en.wikipedia.org/wiki/Blockchain

https://www.coindesk.com/information

http://blog.b92.net/text/25991/Bitkoin-virtuelni-novac-ili-tehnologija-buducnosti

https://www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business?language=sr

https://www.youtube.com/watch?v=UlKZ83REIkA

https://www.youtube.com/watch?v=i9nUMvpT2rM

https://sr.wikipedia.org/sr-el/He%C5%A1_funkcija

https://en.bitcoin.it/wiki/Proof_of_work

https://en.wikipedia.org/wiki/Proof-of-stake

https://en.wikipedia.org/wiki/Proof-of-space

https://en.bitcoin.it/wiki/Proof_of_burn

https://www.youtube.com/watch?v=QBFNaCNlBdk

https://anders.com/blockchain/

http://www.investopedia.com/terms/a/altcoin.asp

http://www.finder.com/cryptocurrency/altcoins

http://en.bitcoin.it/wiki/Altcoin

https://bitcoinmagazine.com/guides/what-altcoin/

http://www.cryptocoinsnews.com/altcoin/

http://www.coindesk.com/short-guide-bitcoin-forks-explained/

http://altcoins.com/

http://www.cryptomorrow.com/2017/08/28/alternatives-to-proof-of-work/

http://fortune.com/2017/08/11/bitcoin-cash-hard-fork-price-date-why/

https://blog.coinbase.com/a-beginners-guide-to-litecoin-d9b455d44cd3?gi=4936f0ed469e

http://www.cryptocompare.com/coins/guides/what-are-coloured-coins-and-meta-coins/

https://coincenter.org/entry/what-are-forks-alt-coins-meta-coins-and-sidechains

https://tonyy.in/blockchain-eli5/

https://blockgeeks.com/guides/ethereum-token/

http://strategiccoin.com/wp-content/uploads/sites/89/2017/09/Filecoin-ICO-Report.pdf

https://coinlist.co/filecoin

http://www.nytimes.com/2017/10/27/technology/what-is-an-initial-coin-offering.html

https://bitcoin.org/en/choose-your-wallet

http://searchsecurity.techtarget.com/definition/private-key

https://en.bitcoin.it/wiki/Private_key

https://bitcoinmagazine.com/articles/bitcoin-address-sign-1399914228

https://en.bitcoin.it/wiki/Transaction

https://bitcoin.org/en/secure-your-wallet

http://cryptocurrencyfacts.com/what-is-a-cryptocurrency-wallet

https://trezor.io

https://beebom.com/types-of-bitcoin-wallets

https://en.bitcoin.it/wiki/Paper_wallet

https://en.wikipedia.org/wiki/Mt._Gox

https://blogs.wsj.com/briefly/2014/02/25/5-things-about-mt-goxs-crisis

https://blockgeeks.com/guides/best-cryptocurrency-exchanges

https://en.wikipedia.org/wiki/Digital_currency_exchange

https://steemit.com/cryptocurrency/@kumablack/security-tips-when-using-cryptocurrencyexchanges

http://bitcoinsecurity101.com/getting-started