KRIPTOVALUTE

Dević, Božena

SVEUČILIŠTE U SPLITU

EKONOMSKI FAKULTET

ZAVRŠNI RAD

KRIPTOVALUTE

Mentor:

prof.dr.sc Marko Hell

Studentica:

Božena Dević, 5171040

Split, kolovoz, 2018.

SADRŽAJ:

1. UVOD

1.1. **Predmet rada**

Predmet rada je objasniti što su kriptovalute i koje su najpopularnije vrste. U radu je objašnjena povezanost kriptovaluta s ekonomijom i tehnologijom. Kriptovalute se sve više koriste ali i dalje nemaju značajan utjecaj na ekonomiju, dok se blockchain tehnologija na kojoj se temelje rad kripotvaluta u zadnje vrijeme sve više primjenjuje u druge svrhe.

1.2. Definicija problema

S razvojem računalnih tehnologija i Interneta pojavila su se i novi oblici vrijednosti koji ne spadaju u tradicionalna oblike vrijednosti s kojima se gotovo svakodnevno susrećemo. Riječ je o kripotvalutama odnosno digitalnom novcu koji će biti proučena u radu. S vremenom se kriptovalute sve više upotrebljava, a samim time raste njihov značaj i utjecaj na ekonomiju. Nijedna financijska ili vladina institucija nije u mogućnosti mijenjati postavke blockchain sustava niti utjecati na plaćanje. Usvajanje i korištenje Bitcoina i drugih kriptovaluta raste iz godine u godinu, mnogi potrošači kao i firme žele iskoristiti njihove prednosti u povećanju svoje prodaje i plaćanju radnika.

1.3. Ciljevi rada

Kriptovalute su nova forma novca koja nije vezana za centralne banke već internetsku zajednicu, a tehnike bazirane na blockchainu utjecat će na sve dijelove društva. Glavni cilj rada je objasniti pojam i povijest kriptovaluta, te njihovu povezanost s ekonomijom i tehnologijom.

Sporedni ciljevi su:

- Prikaz najpopularnijih vrsta i njihov razvoj
- Utvrditi prednosti i nedostatke ulaganja u kriptovalute
- Provjera utjecaja na politiku banaka
- Opisati način oporezivanja kriptovaluta
- Prikaz tehnologije na kojoj se temelji rad kriptovaluta.

1.4. Metode rada

Metode rada primjenjene u radu su:[1]

- ***Metoda analize*** je postupak znanstvenog istraživanja raščlanjivanjem složenih pojmova,sudova i zaključaka na njihove jednostavnije sastavne dijelove i elemente. Analiza je proces redukcije nejednakoga na sve veću jednakost.

- ***Metoda sinteze*** je postupak znanstvenog istraživanja i objašnjavanja stvarnosti putem sinteze jednostavnih sudova u složenije. Sinteza je način sistematiziranja znanja po zakonitostima formalne logike, kao proces izgradnje teorijskog znanja u pravcu od posebnog ka općem, odnosno od vrste prema rodu.

- ***Povijesna metoda*** uzima u obzir kronologiju, razvoj i uzročno-posljedičnu vezu o predmetu istraživanja.

- ***Metoda deskripcije*** je postupak jednostavnog opisivanja ili očitavanja činjenica, procesa i predmeta u prirodi i društvu te njihovih empirijskih potvrđivanja odnosa i veza, ali bez znanstvenog tumačenja i objašnjavanja. Ova se metoda primjenjuje u početnoj fazi znanstvenog istraživanja, a ima veću vrijednost ako je jednostavno opisivanje povezano s objašnjenjima o uočenim važnijim obilježjima opisivanih činjenica, predmeta i procesa, njihovih zakonitosti i uzročnih veza i odnosa.

- ***Metoda kompilacije*** je postupak preuzimanja tuđih rezultata znanstvenoistraživačkog rada, odnosno tuđih opažanja, stavova, zaključaka i spoznaja. Metoda kompilacije može se upotrijebiti u kombinaciji s drugim metodama u znanstvenoistraživačkom radu, tako da djelo nosi u što većoj mjeri osobni pečat autora kompilatora, koji će, uz osobni pristup pisanju znanstvenog ili stručnog djela korektno i na uobičajen način citirati sve ono što je od drugih preuzeo.

[1] http://www.unizd.hr/portals/4/nastavni_mat/1_godina/metodologija/METODE_ZNANSTVENIH_ISTRAZIVANJA.pdf

1.5. Struktura rada

Rad se sastoji od pet cjelina. U prvom dijelu obuhvaćen je predmet rada, definicija problema, ciljevi i metode rada.

U drugom dijelu objašnjen je pojam i značaj kriptovaluta, njihove prednosti i nedostatci, te su analizirane i opisane najpopularnije vrste kriptovaluta.

U trećem dijelu analizira se povezanost kriptovaluta i ekonomije kroz oporezivanje, utjecaj na politike banaka te trgovanje kriptovalutama.

Četvrti dio prikazuje tehnologiju kriptovaluta. Objašnjena je blokchain tehnologija na kojoj se zasniva rad kriptovaluta, transakcije, proces rudarenja te novčanici (walleti) za kriptovalute.

Posljednji, peti dio je zaključak rada.

2. KRIPTOVALUTE

2.1. Povijest i pojam kriptovaluta

Kriptovalute su jedinstveni digitalni novčići koje je nemoguće kopirati ni svojevoljno proizvesti. Funkcioniraju kao elektronski zapisi o određenim vrijednostima pohranjenim u elektronskim novčanicama na internetskim stranicama koje pružaju takvu vrstu usluge. Proizvode ih brojni ljudi u cijelom svijetu koristeći softver koji rješava matematičke probleme. Vrijednost kriptovaluta utvrđuje se iz sekunde u sekundu iz ponude i potražnje i nije vezana ni za kakvu fizičku stvar. Kriptovalute su potpuno nov koncept koji mijenja ne samo način na koji plaćamo, već i način na koji doživljavamo novac. Kao i kod svake velike inovacije, potrebno je najprije promijeniti svijest korisnika.

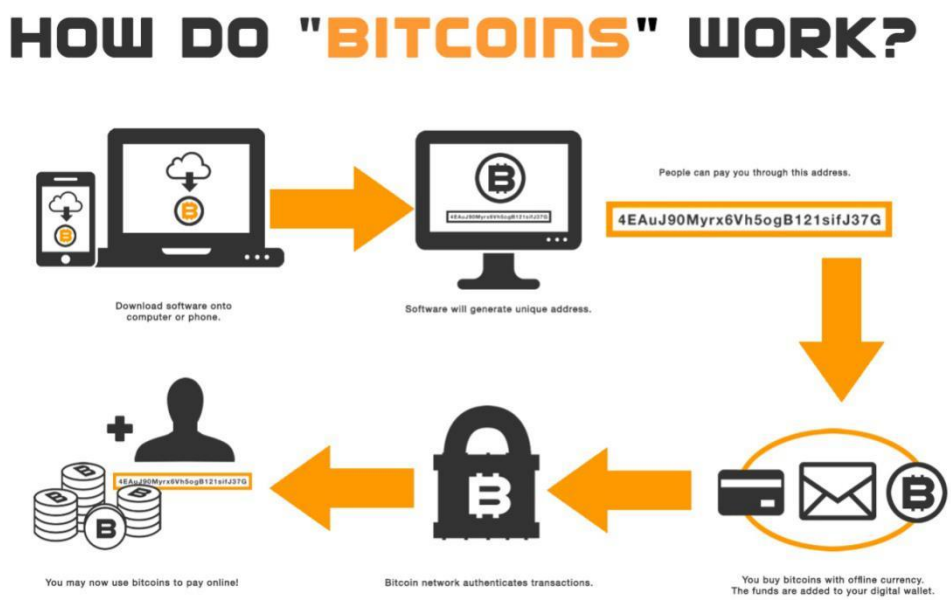
Njihov status kao novca nije čvrsto utvrđen, a status legalnosti još nije definiran i varira od države do države. U zemljama poput Bolivije, Maroca, Bangladeša, Ekvadora korištenje kriptovaluta je zabranjeno i kažnjivo, dok je u većini drugih zemalja legalno.

Ne postoji nikakva nadređena središnja institucija, vlada, agencija, banka ili korporacija koja izdaje ili vodi račune o tim valutama. To je sustav elektroničkoga plaćanja koji se zasniva na kriptografiji (šifriranju) – odatle *"*kripto*valuta*". Kriptografija se tisućljećima primjenjuje za osiguravanje tajnosti diplomatske i vojne komunikacije. Šifrira se kako bi komunikacija između dviju osoba ostala privatna i nekompromitirana, iako u komunikacijskom kanalu postoje treće osobe koje tu komunikaciju mogu pratiti. Budući da proces šifriranja i dešifriranja nije jednostavan, ni kriptovalute nisu jednostavne.[2]

Kod uvođenja prvih bakomata postojao je problem dvostuke potrošnje, gdje je bilo moguće dva puta podići sav iznos novca s računa na različitim bankomatima u kratkom vremenu jer informacije nisu bile usklađene. Decentralizacija novčanog sustava zahtjevala je rješavanje problema dvostuke potrošnje i krivotvorenja novca.

Prva i najpoznatija kriptovaluta je Bitcoin (BTC) stvorena 2009. godine od strane anonimnog programera, ili skupine programera, pod lažnim imenom Satoshi Nakamoto. Objavili su znanstveni rad pod nazivom Bitcoin: A Peer-to-peer Electronic Cash System u kojem su predstavili tehničke detalje platnog sustava koji bi omogućio pojedincima slanje i primanje uplata bez uključivanja bilo kojih posredničkih financijskih institucija.

[2] https://www.kriptovaluta.hr/bitcoin/princip-rada-kriptovaluta/



Slika1: Kako Bitcoin funkcionira

Izvor: https://www.alienvault.com/blogs/security-essentials/explain-bitcoin-to-me

Kriptovalute sklanjaju posrednike, pa se svaka transakcija obavlja veoma brzo i direktno između dva subjekta bez obzira na kojem su dijelu svijeta. Transakcije su sigurnije od standardnih bankarskih i mogu se obaviti bez obzira gde se korisnik nalazi. Decentralizirana priroda open-source protokola osigurava da kontrola mreže ostaje u rukama korisnika. Transakcije su ovisne o sudionicima u mreži, a korisnik je odgovoran za sigurnost vlastitih financija i podataka, bez potrebe da ovisi o trećoj strani poput bankarske institucije.

Bitcoin je globalno prihvaćen za internetska plaćanja – iako nije izdan od središnji banke, niti se veže uz račune kod poslovnih banaka. Koristi decentraliziranu kontolu preko Bitcoin blockchain tehnologije kako bi jednistvenu bazu podataka svih postojećih transakcija prevela u decentraliziranu glavnu knjigu. Nijedna financijska ili vladina institucija nije u mogućnosti mijenjati postavke blockchain sustava niti utjecati na plaćanje. Da bi se priznala bilo kakva promjena na mreži za promjenu je potrebo 50% korisnika plus jedan kako bi se onemogućio svaki oblik falsificiranja ili prevare.

2.2. Prednosti i nedostatci kriptovaluta

2.2.1. Prednosti kriptovaluta

Niz je elemenata koji pozitivno utječu na ulaganje u kriptovalute: [3]

- Hakiranje Blockchain-a težak je posao, jer zahtijeva istovremeno hakiranje nekoliko tisuća računala, što je gotovo nemoguće,
- Ima ozbiljan potencijal da zamijeni trenutni novčani sustav u svijetu, jer broj korisnika kriptovaluta raste,
- Niko ne može promijeniti količinu novčića koji se koriste,
- Zbog ograničene količine novčića, otporan je na inflaciju, a kreiranje novca zahtjeva ulaganje u hardver i električnu energiju,
- Nema potrebe da trošimo novac za održavanje računa,
- Transakcije se verificiraju i trajno registriraju u javni registar (glavnu knjigu) koji je praktično neizmjenjiv,
- slanje novca nalikuje slanju e-maila, a cjelokupna tržišna kapitalizacija sustava stane na jedan USB stick,
- Svako može vidjeti sve transakcije koje su ikada napravljene,
- Nije kontroliran ni od koga, već ima svoju vlastitu mrežu po kojoj radi, odnosno koristi princip decentralizacije (takozvani "peer to peer").

[3] https://sh.wikipedia.org/wiki/Kriptovaluta

2.2.2. Nedostatci kriptovaluta

Kriptovalute pored prednosti imaju svoje nedostatke, prepreke i izazove. Iako se nazivaju valutama i žele preuzeti funkiju novca, trenutno ne ispunjavaju ni jednu funkciju novca. Budući da je novac općeprihvaćeno sredstvo razmjene i mjerilo vrijednosti jasno je da kriptovalute to nisu i ne preporuča se kao sredstvo razmjene kroz dulje vrijeme. Nedostatci kriptovaluta su: [4]

- Transakcije kriptovaluta su nepovratan proces nakon nekoliko potvrda transakcije. Jedna od stvari koje kriptovalute nemaju u odnosu na standardne kreditne kartice je zaštita korisnika od prijevare,
- Mnoge banke ne pružaju usluge kriptovalutama i njihovim korisnicima, također odbijajući suradnju sa digitalno-valutnim kompanijama,
- Kriptovalute trebaju zadovljiti mnoge uvjete da bi se mogle koristiti na globalnom nivou. Npr. broj trgovaca Bitcoin-om je mali, ali konstantno rastući,
- Sa tehnološkim napredovanjem, javljaju se potrebe za sve jačim računalima sa specijaliziranim hardverom i softverom za njihovo korištenje,
- Tradicionalni financijski proizvodi imaju jak i razvijen sustav za zaštitu potrošača, za razliku od kriptovaluta,
- Mogu biti zauvijek izgubljene/uništene zbog nekog štetnog softvera ili gubitka podataka na internetu,
- Zasnovane su na kompliciranim matematičkim algoritmima dekodiranja, tako da mnoge države imaju dosta oprezan pristup njima, bojeći se njihovih efekata na financijsku sigurnost,
- Zabrane u određenim državama su dostigle nivo ogromnih novčanih kazni.

[4] Ibid

2.3. Vrste kriptovaluta

Trenutačno je na tržištu prisutno više od 550 kriptovaluta, među kojima po vrijednosti i značaju dominira Bitcoin.

Tablica 1: 10 kriptovaluta s najvećom tržišnom vrijednosti na dan 19.06.2018.

Redni broj	Naziv kriptovalute	Oznaka	Vrijednost u američkim dolarima	Promjene vrijednosti (%)
1.	Bitcoin	BTC	6747,18	0,11
2.	Ethereum	ETH	533,18	2,8
3.	Ripple	XRP	0,5377	0,07
4.	Bitcoin Cash	BCH	898,4	0,86
5.	EOS	EOS	10,6	-1,17
6.	Litecoin	LTC	98,66	-0,07
7.	Stellar	XLM	0,2368	-0,27
8.	Cardano	ADA	0,1658	-0,1
9.	IOTA	MIOTA	1,18	-1,05
10.	TRON	TRX	0,0481	7,03

Izvor: izrada autora prema podacima s https://coinmarketcap.com/

1. Bitcoin

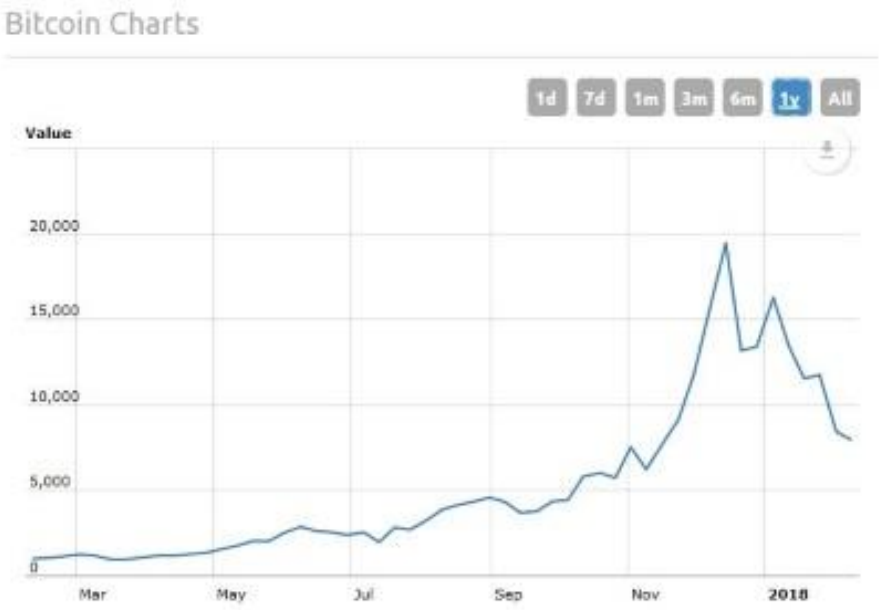
Bitcoin je prva, najpoznatiija i najrasprostranjenija kriptovaluta koju je predstavila osoba pod imenom Satoshi Nakamoto u znanstvenom radu pod nazivom Bitcoin: A Peer-to-peer Electronic Cash System u kojem su predstavili tehničke detalje platnog sustava koji omogućava slanje i primanje uplata bez uključivanja bilo kojih posredničkih financijskih institucija. Transakcije u mreži Bitcoin bilježe se u javnoj knjizi koristeći vlastitu valutu, koja se također zove bitcoin. Dva su načina stjecanja Bitcoina, prvi je kupnja novcem ili zamjena za druge proizvode i usluge, drugi na način je „rudarenje“ kada se pojedinci ili tvrtke uključuju u održavanje Bitcoin mreže u zamjenu za bitcoine. Korisnici na svojim računalima, mobilnim uređajima i na web aplikacijama mogu slati i primati bitcoine elektroničkim putem pomoću računalnih programa tzv. novčanika. Kod trgovanja bitcoinom nedostaje zaštita potrošača, naknadu za transakcije plaća kupac a ne trgovac kao kod kreditnih kartica, a bitcoin transakcije su nepovratne i nije ih moguće poništiti.

Najčešće upotrebe Bitcoina su:[5]

- **Kupnja** - mnogi prihvaćaju Bitcoin kao način plaćanja. Danas se može platiti školarinu bitcoin-om, kupiti umjetnička djela, ručati u nekim restoranima, proputovati svijet, kupiti kuću i automobil, a može se čak i putovati u svemir.
- **Slanje novca** - kada je slanje novca u pitanju, Bitcoin ima mnogo prednosti u odnosu na slanje tradicionalnog novca. Otvaranje korisničkog računa za korištenje Bitcoin-a je jednostavnije, jer se ne moraju donositi dokumenti, za razliku od pošte, banke, PayPal-a. Također, slanje Bitcoin-a je brže, jer ne postoje posrednici, što ujedino čini ovaj proces znatno jeftinijim. Ali jedini problem koji i dalje ostaje je konverzija Bitcoina u tradicionalni novac.
- **Investicija** - iako je Bitcoin kriptovaluta, u njega se može ulagati isto kao i u bilo koju tradicionalnu valutu (Euro, Dolar,…). Ono što razlikuje Bitcoin je volatilnost cijene koja se menja brzo a time čini ulaganje mnogo rizičnijim, međutim, mnogi koji su uložili u Bitcoin ranijih godina ostvarili su ogromne profite, tako da je njegova privlačnost enormno porasla.
- **Špekulacija** – tržište i cijena Bitcoina nisu centralizirani, a oscilacije u ponudi i potražni su česte i brze. Promjene cijene nekada mogu biti i preko 20% na dnevnoj razini. Sve ovo uvelike privlači špekulante da trguju Bitcoinom – kupi jeftino-prodaj skupo. Tržišna kapitalizacija Bitcoina od preko 60 milijardi dolara privlači brokere da ulaze u ovu igru i koriste najmoderinije alate iz svog poslovanja kako bi maksimizirali profit uz pomoć Bitcoina.

Usvajanje i korištenje Bitcoina raste iz godine u godinu, mnogi potrošači kao i firme žele iskoristiti njegove prednosti u povećanju svoje prodaje i plaćanju radnika. Vrijednost Bitcoina određuje se na temelju ponude i potražnje na tržištu te zbog toga dolazi do visoke stope volativnosti, odnosno vellikih oscilacija cijene na dnevnoj razini (i do +/-20%).

[5] https://kriptonovac.rs/?p=662



Slika 2: Kretanje vrijednosti Bitcoina 2017. godina

Izvor: https://www.zagorje-international.hr/index.php/2018/02/13/rast-i-pad-bitcoina-svi-ocekuju-ili-se-nadaju-jos-jednom-uzletu-crypto-marketa/

Na slici 2 vidljiv je značajan rast vrijednosti Bitcoina kroz 2017.godinu. Iz mjeseca u mjesec vrijednost je rasla, do 9/2017 vrijednost je bila ispod 5.000 USD, nakon toga kreće nagli porast i pred kraj godine dostiže vrijedost približno 20.000 USD. Ako usporedimo vrijednost na početku i na kraju godine vidljivo je da je porasla gotovo 13 puta.

Trenutni broj korisnika Bitcoina nemoguće je točno utvrditi iz razloga što jedan korisnik moze imati više adresa. Japan je vjerojatno vodeća zemlja kada je u pitanju usvajanje Bitcoin-a. Vodeće avio-kompanije, trgovci elektronskih uređaja i neki od najpoznatijih i najuticajnijih kompanija u zemlji prihvaćaju Bitcoin kao digitalnu valutu.

Slika 3: Stupanj legalnosti Bitcoina u svijetu

Izvor: https://bitfalls.com/hr/2018/01/17/the-legality-of-bitcoin-across-the-world/

U zemljama označenim zelenom bojom bitcoin je legalan i nitko mu javno ne pokušava stati na kraj iako nije jasno porezno i zakonski reguliran. Kod zemalja narančaste boje država se nije izjasnila ″za″ ni protiv Bitcoina. Svijetlo rozom bojom označene države ograničile su legalnost uvodeći mjere za otežavanje poslovanja s Bitcoinom. U zemljama jako roze boje zabranjeno je trgovanje i posjedovanje Bitcoina, čak se gleda kao kriminalno djelo.

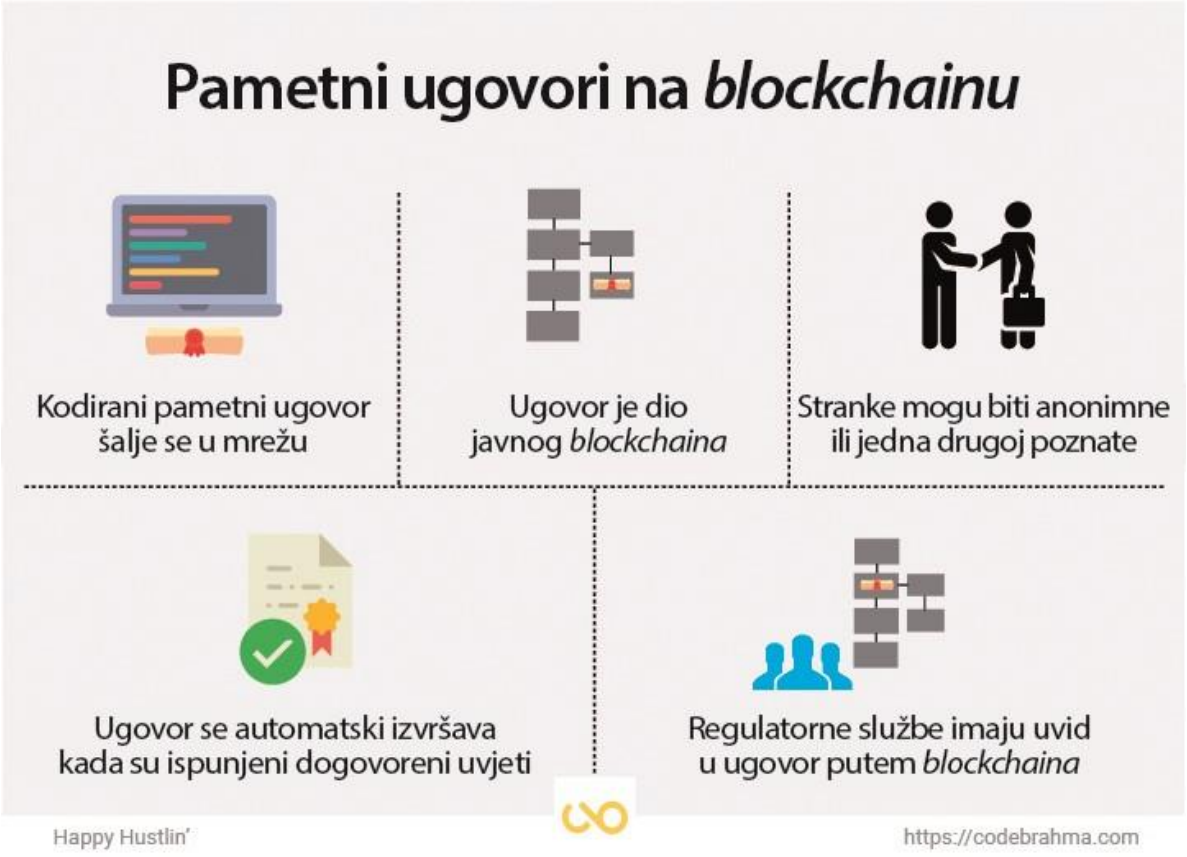
2. Ethereum

Ethereum je kreirao ruski programer Vitalik Buterin krajem 2013-te, a u siječnju 2014. najavio je Ethereum na The North American Bitcoin konferenciji u Miamiju, US. Ethereum je otvorena blockchain platforma koja bilo kome omogućava izgradnju i korištenje decentralizirane aplikacije (pametnih ugovora) koje izršava blockchain tehnologija. Aplikacije rade onako kako su programirane, bez mogućnosti bilo kakvog kašnjenja, cenzure, prevare ili uplitanja treće strane.

Na Ethereum blockchain ugrađen je poseban token Ether kojeg kao nagradu za potvrđivanje interakcija s blockchainom dobivaju tzv. rudari, a kojima korisnici Ethereum blockchaina plaćaju korištenje te tehnologije. Pametni ugovor je pojam koji se koristi za računalni program koji služi za olakšavanje razmjene kao što su novac, sadržaj, nekretnina, udjeli ili nešto drugo što predstavlja nekakvu razmjenu vrijednosti. Kada se pametni ugovor izvršava na blockchain mreži on postaje računalni program koji se samostalno izvršava kada su određeni preduvjeti zadovoljeni.[6]

Ethereum se često naziva svjetskim računalom, jer se operacije izvršavaju na velikom broju čvorova koji su decentralizirani što znači da su aplikacije ugrađene u blockchain nazaustavljive. Decentralizirane aplikacije su napravljene od izvornog koda koji se pokreće i izvršava na blockchain mreži, a njegovo ponašanje nije moguće kontrolirati preko nekog centraliziranog entiteta. Svaka centralizirana aplikacija ili usluga poput on-line glasanja, podizanja kredita od strane banke može biti decentralizirana pomoću Ethereuma. Najveća prednost Ethereuma je najsnažnija razvojna zajednica te širok raspon primjena zbog čega i je najveći izvor novih projekata, tehnologija i rješenja. Vjeruje se da Ethereum čeka svijetla budućnost, da će na njemu biti mnogo vrijednih i korisnih informacija koje ćemo svi jednog dana moći koristiti. Omogućavat će kompliciranije i veće aplikacije, veći broj transakcija, postojat će brži, sigurniji i snažniji. Zbog naglog rasta vrijednosi Ethereum ima dosta kritičara i skeptika, a sve više privlači dosta mrzitelja jer napreduje više od drugih kriptovaluta. Tržišna kapitalizacija Bitcoin-a je 40 milijardi eura što je skoro duplo više od Ethereum-a međutim, mnogi investitori vide ogroman potencijal i moć u Ethereumu i mogućnostima koje pružaju pametni ugovori.

[6] https://crobitcoin.com/altcoin/ethereum/



Slika 4: Pametni ugovori na blockchainu

Izvor: https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011

Bitcoin je zamišljen kao digitalna valuta i, da bi kao takav bio realiziran, izumljena je blockchain tehnologija. U bitcoinu se ta tehnologija koristi samo za bilježenje transakcija među korisnicima bitcoina. To znači da se na tom bitcoin lancu zapisa upisuju samo transakcije. S druge strane, Ethereum je dizajniran da bude prilagodljiv i fleksibilan, da se na njegovom lancu mogu upisati ne samo bilješke o transakcijama nego bilo kakav računalni kod koji se može izvršavati. Ethereum je programabilan blockchain, umjesto da korisnicima pruža unaprijed određeni i ograničeni set mogućih operacija (npr. bitcoin transakcije), Ethereum omogućava korisnicima da kreiraju vlastite operacije bilo koje razine kompleksnosti. Tako Ethereum služi kao platforma za mnogo različitih tipova decentraliziranih blockchain aplikacija, što uključuje, ali nije ograničeno samo na kriptovalute.[7]

[7] http://www.netokracija.com/ethereum-valuta-tomislav-mamic-139768

Slika 5: Kretanje vrijednosti Ethereuma

Izvor: https://www.coindesk.com/ethereum-prices-hit-record-high/

Ethereum je danas jako bitan i na njemu i njegovom blockchainu temelji se mnogo aplikacija. Kriptovalute i blockchain tehnologija su tek u fazi razvoja i sasvim očekivano bi bilo da ukoliko krenu u masovnu upotrebu i donesu novu tehnologiju ljudima njihova cijena raste. Cijena Ethereuma strahovito je porasla pogotovo zato jer je poput "Bitcoina", pa su investitori željeli što priije uložiti i kupiti veću količinu dok su cijene još umjereno niske. Trenutna vrijednost Ethereuma je 469,58 USD.

3. IOTA

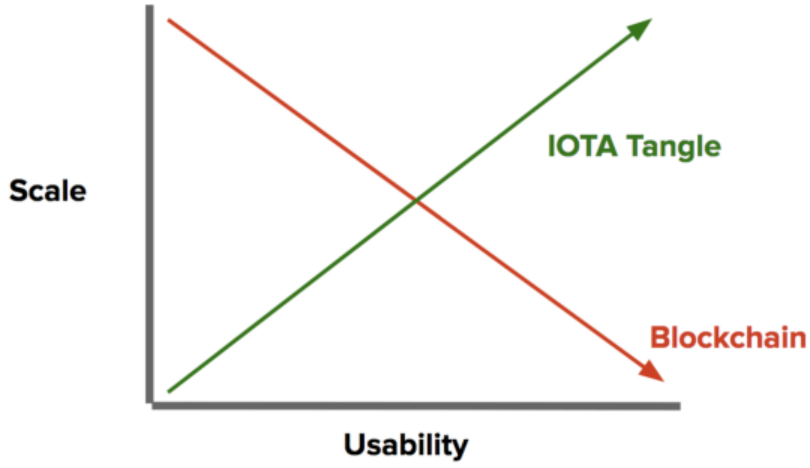
IOTA je prva kriptovaluta koja ne koristi blockchain tehnologiju. Lansirana je na tržište 1. lipnja 2017. g., a razlikuje se od većine drugih kriptovaluta po svom jedinstvenom ustroju jer koristi ″Tangle″ koji se zasniva na DAG tehnologiji koja omogućava razne funkcije među kojima su ključne transakcije bez troškova, neograničena skalabilnost ili offline transkacije. Kod "Tangle" tehnologije, svaka pojedinačna transakcija stvara novi blok koji sam sebe potvrđuje.

Karakteristike IOTE su:[8]

- **Nema provizije po transakciji** - IOTA je prvenstveno namjenjena za buduće, nadolazeće IoT (eng. *Internet of Things – "Internet stvari"*) tržište. IoT tržite je ono koje se temelji na transakcijama između 2 uređaja koja se mogu povezati na internet (mobiteli, TV, nadzorne kamere). Provizije su velik problem u kripto svijetu, pogotovo kod najpoznatijih valuta poput Bitcoina, gdje provizije po transakciji iznose više od 4$. IOTA je jedina valuta bez provizija po transakciji.

- **Neograničena skalabilnost** - U Bitcoin mreži, koja je zasnovana na blockchain tehnologiji, zbog dizajna mreže transkacije su spore. Transakcije u kriptovalutama se mjere u TPS (eng. *Transactions Per Second – "transakcije po sekundi"*). Ta brojka u načelu pada sa sve većim brojem korisnika u mreži. Skalabilnost je pojam koji definira nesmetano funkcioniranje sustava bez obzira na količinu korisnika ili broj transakcija. Viša skalabilnost = što je više korisnika u mreži, to je TPS veći, tj. transakcije se brže obavljaju. Tangle se ponaša suprotno od blockchain tehnologije, gdje što više korisnika je u mreži, to je ona sporija, tj. skalabilnost je niža**.**

[8] https://www.kriptovaluta.hr/altcoin/iota-kriptovaluta-3-generacije/



Slika 6: Prikaz neograničene skalabilnosti

Izvor: https://www.kriptovaluta.hr/altcoin/iota-kriptovaluta-3-generacije/

- **Trenutačne transakcije –** zahvaljujući principu rada te neograničenoj skalabilnosti, vrijeme potrebno za provedbu transakcije u IOTA mreži gotovo je trenutačno, u teoriji. Trenutno vrijeme potrebno za provedbu tranakcije je oko 15 minuta, a to je iz razloga što je IOTA još uvijek u razvoju te još nema dovoljno korisnika. Ukoliko se postigne dovoljan broj korisnika transakcije će biti trenutačne.

Stručnjaci predviđaju Ioti veliki uspjeh i ona je danas jedna od 10 najvećih kriptovaluta. Osobno mi je zanimljiva IOTA i u razgovoru s osobama koje su dobro upoznate sa svijetom kriptovaluta dobila sam preporuku za ulaganje. Govori se kako bi vrijednost IOTE do 2020. mogla porasti do 100 USD, a njena trenutna vrijednost je 1,02 USD. Na sljedećoj stranici je potvrda moga ulaganja u IOTU.

Najmanja količina IOTE koja se može kupiti je 200 komada. Cijena prilikom moje kupnje bila je 1,36 USD. Ukoliko je iznos ulaganja manji od 15.000kn nisu potrebni osobni dokumenti.

Slika 7: Primjer potvrde o ulaganju u IOTU

Izvor: vlastiti primjer

3. KRIPTOVALUTE I EKONOMIJA

Ono što su u prošlom stoljeću bile dionice, danas je to kriptovaluta. Za razliku od dionica koje rastu i padaju u ovisnosti o poslovanju firme, kriptovalute mnogo češće osciliraju i ovise isključivo o potražnji na tržištu. Danas to može biti mala potražnja, sutra velika. Teško je predvidjeti kretanje kriptovaluti, ali iz dostupnih primjera je vidljivo da mnoge od tih valuta rastu kroz vrijeme.

3.1. Trgovanje kriptovalutama

Trgovanje kriptovalutama postaje sve popularnije, ali svako ulaganje novaca je rizično. Kriptovalute se na burzi jednostavno kupuju prebacivanjem novca na jednu od burzi na kojoj se licitira za cijenu kriptovalute koju želimo, kada cijena dođe na tu razinu obavlja se transakcija i novac se mijenja za traženi iznos kriptovalute. Trgovanje kriptovalutama ovisi o više faktora od kojih je prvi veličina kriptovalute u koju se planira uložiti. Veliki broj investitora radije ulaže u već poznate kriptovalute iako to ne mora značiti sigurnost. Pojedine kriptovalute u početku imaju niski profit a samim time i niske cijene, ali to ne znači da će u budućnosti ostati tako. Drugi kriterij je razvoj kriptovaluta što znači da će kriptovaluta postati primamljiva za ulaganje ako se procijeni da bi u bliskoj budućnosti cijena mogla rasti.

Koji su rizici povezani s kriptovalutama? [9]

- Uglavnom neregulirano područje, uslijed čega je češća mogućnost prijevara i drugih nepravilnosti
- Manjak pouzdanih i relevantnih informacija
- Visok rizik od gubitka dijela ili svih uloženih sredstava
- Izrazita volatilnost vrijednosti ulaganja i nemogućnost svakodobnog „izlaska“ iz ulaganja
- Rizici vezani uz informatičku tehnologiju koja se koristi za izradu i distribuciju tokena (primjerice, hakerski napadi, nemogućnost pristupa tokenima, gubitak ključa za pristup tzv. digitalnom novčaniku).

[9] https://www.ictbusiness.info/poslovanje/hanfa-veliki-rizici-ulaganja-u-kriptovalute-i-ico

Stručnjaci upozoravaju potencijalne ulagatelje u kriptovalute na odgovorno i oprezno ponašanje, da se prije donošenja odluke o ulaganje detaljno informiraju o karakteristikama kriptovaluta i rizicima koje to ulaganje nosi. Posebna pažnja usmjerena je na rizik gubitka novca s obzirom da ne postoje posebni regulatorni mehanizmi zaštite.

Mišljenje HNB-a je da većina članica Europske unije smata da kriptovalute ne udovoljavaju pravnim kriterijima da bi bile kvalificirane kao zakonsko sredstvo plaćanja, elektronički novac ili instrument plaćanja, ali da njihovo korištenje nije ilegalno iako javna vlast nije regulirala niti nadzire takve oblike plaćanja.[10]

Kriptovalutama se može trgovati na specijaliziranim burzama, a princip trgovanja najbliže se može usporediti s trgovanjem dionicama. Mjenjačnice kriptovaluta i kripto burze su posebne web stranice na kojima je moguće kupovati i prodavati kriptovalute za eure, dolare ili druge valute ili ih međusobno mijenjati. Prednost burze kriptovalute je to što nisu potrebni posrednici (brokeri) već korisnik sam upravlja svojim sredstvima.

Vrste mjenjačnica:[11]

1) **Brokerske mjenjačnice** - ove mjenjačnice su najjednostavnije i najpraktičnije za sve nove korisnike u kripto svijetu gdje se direktno kupuju i prodaju preko brokera. Jedna od takvih mjenjačnica je upravo i bitcoin-mjenjačnica sa sjedištem u Zagrebu.

2) **Platforme za "direktnu" trgovinu** - ove platforme su namijenjene da spoje direktno kupca i prodavača neke kriptovalute no cijenu određuju sami po dogovoru i preuzimanju. Najpoznatiji primjer ove platforme je online platforma LocalBitcoins gdje preprodavači nude bitcoine za određenu cijenu te se potom nalaze fizički kako bi obavili preprodaju.

3) **Burze odnosno platforme za trgovanje** - burze su platforme gdje se korisnici mogu registrirati i direktno trgovati s drugim korisnicima na toj platformi te stvarati tržište ponude i potražnje. Velika količina trgovaca se susreće na ovim platformama i daju svoju cijenu po kojoj su spremni kupiti ili prodati kriptovalutu. Jedna takva koja se nalazi u hrvatskoj je Bitkonan burza kriptovalutama koja se trenutno nalazi u Splitu.

[10] https://zimo.dnevnik.hr/clanak/hnb-tvrdi-kriptovalute-nisu-elektronicki-novac-ulaganje-je-vas-rizik---490348.html
[11] https://crobitcoin.com/burze-i-mjenjacnice/

3.2. Utjecaj kriptovaluta na politike banaka

Ukoliko kriptovalute zavladaju svijetom vlada svake države i centralna banka izgubit će svoju ulogu posrednika u svjetskoj ekonomiji. Vlada neće moći upravljati inflacijom u država, a centralne banke neće moći utjecati na ponudu i potražnju novca. Države bi trebale pronaći nove načine upravljanja budžetom, a moglo bi doći do problema gdje neće postojati državne valute pa je upitno kako će se države zaduživati. Prihvaćanjem kriptovaluta mijenja se ekonomija svake zemlje, a one trenutno nisu u vlasništvu nijedne banke što ne znači da neće biti u budućnosti. Kriptovalute imaju potencijal postati valute budućnosti iz razloga što nisu podređene nijednoj zemlji, nisu pod utjecajem vlade i politike te oslobađaju tržište dominacije od strane centralnih banaka. Do sada se nijedna središnja banka nije konkretnije pozabavila pitanjem kriptovaluta i njihovim utjecajem na stabilnost financijskog sustava, ne samo pojedine zemlje već i šireg prostora.

U manje od jednog desetljeća, bitcoin je izrastao iz nepoznanice u najpoznatiju kriptovalutu. Njegova je vrijednost porasla od nekoliko centi po bitcoinu na više od 6.000 dolara. U posljednje vrijeme kriptovalute privlače veliku pozornost središnjih banaka. Banke nisu u mogućnosti uzimati provizije jer nema posrednika, a ne mogu ni čuvati nečiji novac jer svaki korisnik svoj novac čuva sam. To znači i da ne mogu koristiti nečiji novac za vlastiti profit. Problem za bankarski sustav leži u činjenici da su kriptovalute zapravo složene matematičke formule, a ne nešto što ovisi o tržišnoj vrijednosti zlata ili drugih sirovina na burzama.

BIS ili središnja banka svih središnjih banaka smatra da su kriptovalute prenestabilne, u njihovo nastajanje troši se prevelika količina električne energije te je subjekt previše manipulacija i prijevara da bi mogla biti sredstvo razmjene u globalnoj ekonomiji. Štoviše, decentralizirana struktura kriptovaluta, za njihove zagovornike jedna od glavnih prednosti, za BIS je jedan od ključnih nedostataka. Analitičari te institucije smatraju da bi masovno korištenje kriptovaluta u platnim transakcijama dovelo do zagušenja internetskih veza. Zbog krhkosti decentraliziranih mreža o kojima kriptovalute ovise, povjerenje u njih može nestati praktički "preko noći", smatraju u BIS-u. Naime, bilo koji oblik novca zahtijeva povjerenje u

stabilnost svoje vrijednosti, a to kriptovalute nemaju. Kod kriptovaluta dobar dio njihovih vlasnika drži ih iz čisto špekulativnih razloga, a ne zato jer njime žele plaćati robu i usluge.[12]

3.3. Oporezivanje kriptovaluta

Porezno-pravna regulacija prilično se razlikuje unutar i izvan Europske unije. Izvan EU većina država ima neku vrstu općeg poreza na promet koji se ne odnosi na plaćanja dobra valutom koja je zakonsko sredstvo plaćanja u toj zemlji. U većini zemalja izvan Europske unije postoji tendencija oslobođenja oporezivanja kriptovaluta neposrednim porezima jer države nisu spremne prihvatiti pravnu kvalifikaciju virtualnih valuta kao pravog novca, nego ih one gledaju kao dobro ili imovinu. Ukoliko je kriptovaluta kupljena „pravom " valutom na to se ne mora plaćati porez. Unutar Europske unije zakoni su ipak malo drugačiji, jer na virtualne valute gleda kao na novac koji ne podliježe PDV-u.

U SAD-u je kriptovaluta kapitalno dobro. Na kapitalno dobro se plaća porez na dohodak na neto vrijednost kapitalnog dobitka. Kako bi se odredila neto vrijednost potrebno je znati točnu tržišnu vrijednost, primjerice bitcoina, izraženu u nacionalnoj valuti na dan kada je virtualna valuta kupljena. Ako se ta virtualna valuta drži više od godinu dana ona će se smatrati dugotrajnom investicijom koja se oporezuje nižim poreznim stopama. Kapitalni gubitak odbija se od kapitalnog dobitka, a ukoliko ga premaši može se odbiti od "običnog dohotka" do visine 3000 dolara godišnje. Osoba koja za prodanu robu ili uslugu primi virtualnu valutu mora znati tržišnu vrijednost te valute izraženu u dolarima na dan kad je valuta primljena. Osoba koja svoju kriptovalutu zaradi rudarenjem kao samozaposlena osoba onda će se u skladu s tim i oporezivati. Ako zaposlenik primi kriptovalutu kao nagradu za odrađeni posao to će predstavljati plaću u dolarskoj protuvrijednosti. U ostalim zemljama poput Australije, Singapura, Ujedinjenog Kraljevstva, Slovenije, Austrije i sličnih, način oporezivanja kriptovaluta ovisi o tome u kakvim transakcijama se kriptovaluta koristi, jesu li one privatne ili poslovne, koja je vrijednost valute u pitanju, na koji se način stekla valuta, je li to bilo kupnjom, rudarenjem ili primanjem plaće.[13]

[12] http://www.poslovni.hr/trzista/bis-bitcoin-nikada-nece-biti-novac-342094
[13] https://bitfalls.com/hr/2018/02/09/croatias-announcement-taxing-cryptocurrency/

Osobe koje trguju kriptovalutama dužne su Republici Hrvatskoj platiti porez jer se radi o ostvarivanju dobiti od kupoprodaje instrumenata na tržištu novca. Iznos poreza koji se plaća je razlika između nabavne i prodajne cijene umanjena za troškove trgovanja (provizija brokera). Stopa poreza na trgovanje kriptovalutama u Hrvatskoj iznosi 12%, a potrebno je zaračunati i lokalni prirez čija stopa ovisi o općini i gradu. Prema članku 70. Zakona o porezu na dohodak svaka osoba koja ostvari prihod od trgovanja kriptovalutama dužna je sama do kraja veljače naredne godine obračunati i platiti porez na svoju zaradu. Ukoliko je porezni obveznik ostvario gubitak od prodaje bitcoina, on ga može odbiti od drugih kapitalnih dobitaka u toj godini, pa makar to bila dobit od prodaje dionica.

3.3.1. Proces prijave poreza

Prema članku 78. i 79. Pravilnika o porezu na dohodak porezni obveznici dužni su dostaviti izvješće JOPPD Poreznoj upravi prema svom prebivalištu ili boravištu do kraja veljače tekuće godine za prethodnu godinu. Dan i oznaka izvješća je 31. prosinca prethodne godine. Sav profit koji se ostvari na temelju kriptovaluta mora se prijaviti. Pod profitom se smatra novac koji je primiljen na račun na temelju isplate sa neke burze ili mjenjačnice.

Što je potrebno za prijavu poreza: [14]

1. Obrazac JOPPD – izvješće o primicima, porezu na dohodak i prirezu te doprinosima za obvezna osiguranja, ispunjeno na propisani način.
2. Izračun poreza – izračun iznosa za plaćanje poreza prema first-in, first-out načelu. To znači da se bilježi svaka pretvorba kune - kriptovalute sa datumom i tečajem po kojem je kupljena. Potrebno je čuvati mailove koji budu primljeni kao potvrda od burzi i mjenjačnica te bilježiti pretvorbe kriptovalute - kune. Na temelju tih informacija se izračunava profit.
3. Bankovna uplatnica – uplatnica s iznosom, brojem računa i propisanim pozivom na broj, kako bi se plaćanje ispravno povezalo s obrascem JOPPD.
4. Obrazac RPO – obrazac za prijavu u Registar poreznih obveznika za osobe koje su ostvarile dohodak iz inozemstva. Ovaj obrazac podnosi se ako je primljen novac od inozemne mjenjačnice/burze.

[14] https://www.kriptovaluta.hr/vijesti/porez-na-kriptovalute-hrvatska/

3.4. Kriptovalute novi financijski instrumenti

Nekoliko vlada pokušalo je steći kontrolu nad kriptovalutama, dok će neke vjerojatno izdati i vlastite valute. Zanimljivo je da su brojne vlade ignorirale nastanak kriptovaluta, sve do trenutka dok pojedinci nisu postali multi-milijunaši u kratkom periodu rasta njihove vrijednosti. Veliki broj ljudi tvrdi da su kriptovalute idealan način trgovanja kojim bi se mogao srušiti klasični monetarni sustav. Bitcon je kao predstavnik svih kriptovaluta na putu razvoja preživio negativne stavove i napade koji su na kraju zapravo pomogli njegovom prihvaćanju i afirmaciji. Bitcoin je privukao mnogobrojne investitore i prihvaćen kao financijski instrument.

Na vrijednost Bitcoina utječu ponuda i potražnja kao i nivo znanja o tehnologiji na kojoj se temelje kriptovalute. Prednost kriptovaluta u odnosu na klasične valute je u ograničenoj ponudi zbog čega su zaštićenije od inflacije.

Bitcoin i druge kriptovalute prema mišljenju Europske Centralne Banke (ECB) ne ispunjavaju uvjete da bi se mogle smatrati valutom. Prema ECB kriptovalute su vrsta nereguliranog digitalnog novca, koje emitiraju, kontroliraju i koriste članovi posebnih virtualnih grupa.[15]

Kriptovalute su se pojavile kao prijetnja klasičnim valutama te su izazvale strah određenih institucija od gubitka kontrole i moći nad novcem. Bankarski sektor osjetio se ugroženim jer je stvorena mogućnost brzog i jednostavnog prijenosa novca bez provizija posrednika. Financijske institucije ostvaruju velike prihode na temelju provizija, a kriptovalute im to ugrožavaju pa je očekivano da će pokušati sve kako bi spriječile njihov opstanak. Razvojem tehnologije i prihvaćanjem blockchain sustava dolazi i do prihvaćanja kriptovaluta, a vremenom se blockchain tehnologija počela primjenjivati za potrebe državnih organa i velikih državnih organizacija.

[15] ECB. (European Central Bank). 2012. Virtual currency schemes.
https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

4. TEHNOLOGIJA KRIPTOVALUTA

Rad kriptovaluta zasnovan je na blockchain tehnologiji koja obećava riješiti neke od najvećih problema u financijskoj tehnologiji. Vodeće svjetske financijske institucije rade na vlastitim implementacijama blockchaina jer će zasigurno ova tehnologija promijeniti financijsku industriju. Osim u financijskoj industriji ova tehnologija može se primjeniti u osiguranju, zdravstvu, tržištu nekretnina i mnogim granama ekonomije.

4.1. Transakcije

Transakcija je transfer vrijednosti između dva digitalna novčanika koja se tada registrira u Blockchain odnosno sustav ulančanih blokova. Transakcija javlja mreži da je vlasnik kriptovalute dao ovlasti za prijenos istih drugom vlasniku, a novi vlasnik na isti način može drugom transakcijom omogućiti prijenos trećem vlasniku. Izlazi iz jedne transakcija može se koristiti kao ulaz u novu transakciju, stvarajući tako lanac vlasništva jer se vrijednost premješta s adrese na adresu. Transakcija sadrži dokaz o vlasništvu za svaku količinu kriptovaluta čija se vrijednost prenosi u obliku digitalnog potpisa vlasnika. Transakcija prenesena preko mreže nije potvrđena sve dok ne postane dio globalne knjige blockchaina. Kako bi se potvrdila vjerodostojnost transakcije potrebno je da prođe proces verifikacije kojeg obavljaju rudari, a za rudarenje svakog bloka i verifikaciju transakcije potrebno je otprilike 10 minuta.

Da bi se izvršila transakcija određenog iznosa kriptovaluta sa jednog digitalnog novčanika na drugi, potrebne su tri stvari:

- Adresa ili javni ključ (Public Key) – izmišljen je sedamdesetih godina i matematička je osnova za račununalnu i informacijsku sigurnost. Javni ključ koristi se za stvaranje ključnog para koji kontrolira pristup kriptovalutama te za primanje kriptovaluta. Generiran je određenim postupcima i izgleda kao nasumična kombinacija slova i brojeva koja je jedinstvena i povezana na taj račun s tim da korisnik može imati više adresa (javnih ključeva).

- Privatni ključ (Private Key) – je broj odabran slučajnim odabirom. Vlasništvo i kontrola nad privatnim ključem korijen je kontrole korisnika nad svojim kriptovalutama. Upotrebljava se za stvaranje potpisa koji je potreban za dokazivanje

vlasništva nad sredstvima koja se koriste u transakciji. Tajni je dio podataka koji dokazuje pravo prenošenja kriptovaluta iz određenog novčanika pomoću kriptografskog potpisa. Bitno je da ostane tajna u svakom trenutku jer je otkrivanje drugim osobama jednako kao da smo im dali kontrolu nad kriptovalutama koje su osigurane tim ključem. Potrebno je zaštititi privatni ključ od slučajnog gubitka jer su u tom slučaju sredstva njime osigurana zauvijek izgubljena.

- Kriptografski potpis - je matematički mehanizam koji omogućuje osobi da dokaže da je jedinstveni vlasnik te adrese, odnosno novčanika. Kada Bitcoin softver potpiše transakciju odgovarajućim privatnim ključem, cijela Bitcoin mreža može vidjeti da taj potpis odgovara transakciji koja se izvršava, ali je zato nemoguće vidjeti privatni ključ koji zaštićuje račun.[16]

4.2. Blockchain tehnologija

Blockchain (glavna knjiga) ili lanac blokova je podatkovni blok koji je povezan u jednosmjerni lanac u kojem svaki blok ovisi o vrijednosti starijeg bloka. Povezivanje blokova temelji se na kriptografiji jer je bitna sigurnost i privatnost. Blockchain možemo gledati i kao decentraliziranu knjigu događaja koju nije moguće uređivati nakon što su podaci jednom upisani. Blockchain pruža alternativu klasičnom sustavu eliminiranjem treće centralizirane strane. Identitet osobe u transakcijama je šifriran, netko može koristiti samo jednu šifru ili adresu ali na taj način se može razotkriti njegov identitet. Iza računala koja se nalaze u mreži može stajati bilo tko tko želi zaraditi potvrđivanjem transakcija, odnosno ″izrudariti″ kriptovalute. Blockchain sadrži povjerljive zapise svake pojedine transakcije koja je ikada napravljena, a svaka transakcija u javnoj knjizi potvrđena je konsenzusomm većine sudionika u sustavu.

Svaki novi događaj u mreži sudionici evidentiraju u svojoj kopiji knjige te mogu provjeravati stanje lanca nakon dodavanja novog bloka. Na taj način sustav više ne ovisi o centralnom čvoru već su sudionici sustava istovremeno i čuvari integriteta podataka u knjizi. Svaki blok u lancu ima svoju adresu koja se temelji na sadržaju toga bloka. Kriptografski algoritmi sažimanja omogućavaju izračun i provjeru valjanosti adrese temeljem sadržaja, a čak i najmanja promjena u sadržaju (npr. samo jedan bit podataka u velikom bloku) rezultira

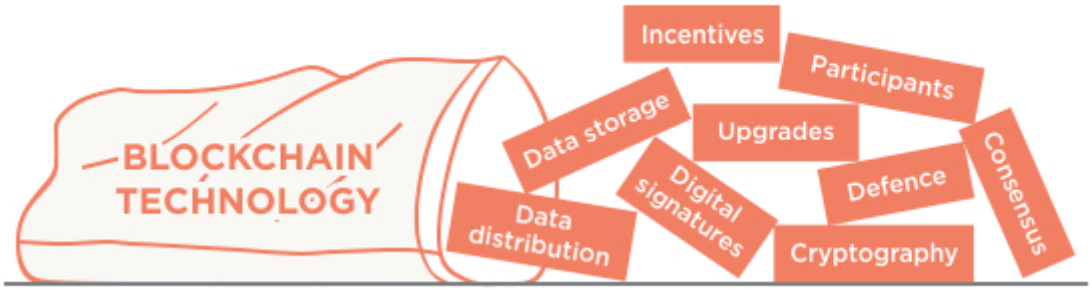
[16] https://crobitcoin.com/bitcoin/transakcije/

potpuno drugačijom adresom. Blockchain na taj način osigurava da se podaci u nizu ne mogu nikada promijeniti, a računalni sustavi utvrđuju vjerodostojnost podataka. Blockchain tehnologiija prvi je put omogućila transparentne transakcije koje ne zahtijevaju povjerenje među sudionicima. Na primjer ukoliko jedan sudionik želi poslati novac drugome mora to javiti svim ostalim sudionicima u mreži koji moraju taj događaj (transakciju) provjeriti te podvrditi, odnosno upisati u svoje knjige. Na taj način omogućena je razmjena ne samo financijskih već svih oblika podataka.[17]

Bitcoin je najpopularniji primjer koji koristi blockchain tehnologiju. Jedan je od najkontroverznijih primjera jer omogućuje anonimne transakcije velikih vrijednosti bez vladine i bankarske kontrole. Financijske institucije i banke vide blockchain tehnologiju kao prijetnju tradicionalnom poslovnom modelu. Tehnologija Blockchain je pokazala znatnu prilagodljivost posljednjih godina, budući da su različiti tržišni sektori tražili načine uključivanja u svoje poslovanje. Dok je do sada većina pozornosti bila na industriji financijskih usluga, nekoliko projekata u drugim područjima povezanim s uslugama pokazuju da se ovo počinje mijenjati. Financijska industrija razmatra uvođenje blockchaina u svoje poslovanje, dok nefinancijska industrija priprema uvođenje blockchain tehnologije u izradu dokumenata, zemljišnim knjigama, distribuciji glazbe.

Glavna knjiga stalno raste kako rudari svakih 10 minuta dodaju nove blokove, a dodaju ih kronološki. Svaki čvor odnosno računalo povezano s mrežom ima kopiju blockchaina koji se automatski preuzima kada se rudar pridružuje mreži. Blockchain je javna knjiga što znači da svaki sudionik u bilo kojem trenutku može pogledati svoje transakcije, primjerice transakciju u kojoj je primio svoju prvu kriptovalutu. Blockchain omogućava decentralizaciju svih transakcija bilo koje vrste na globalnoj osnovi. Korisnici mogu vjerovati sustavu javne knjige koja se pohranjuje diljem svijeta na mnogo različitih čvorova održavanih od strane "rudarskih računovođa", za razliku od uspostavljanja i zadržavanja povjerenja kod transakcijskog partnera ili posrednika (npr. banke). Blockchain je poput divovske proračunske tablice za registraciju sve imovine i računovodstveni sustav za njihovo poslovanje na globalnoj razini koja uključuju sve oblike imovine. Može poslužiti kao arhiva javnih zapisa za cijelu državu, uključujući registar dokumenata, događaja, identiteta i imovine.[18]

[17] https://www.vecernji.hr/techsci/kako-funkcioniraju-kriptovalute-i-blockchain-1196944
[18] Swan M. (2015): Blockchain: Blueprint for a New Economy, str. 27-34



Slika 8: Blockchain tehnologija

Izvor: https://pcchip.hr/ostalo/tech/uvod-u-blockchain-tehnologiju/

4.2.1. Sigurnost blockchaina

Sigurnost blockchaina garantiraju 3 faktora:[19]

- **Kriptografija** – Blokchain se sastoji od niza podatkovnih paketa (blokova) od kojih svaki sadržava skup transakcija ostvarenih u određenom periodu. Svaki podatkovni paket u lancu, logički je povezan s prethodnim paketom jednom vrstom kriptografskog potpisa koji još zovemo i – hash. Hash je broj ispisan u posebnom formatu i izgleda kao niz nasumično odabranih znakova:

  7c96cf30947914ab1d9844d93707baf2435f9d9b290c8258622ab635054c8041

  Hash je rezultat hash funkcije koja s jedne strane prima bilo koji digitalni sadržaj kao što je tekst, fotografija, video, pdf ili bilo koji drugi tip datoteke te nad njima izvršava niz matematičkih operacija, a kao rezultat vraća unikatan potpis u obliku niza znakova točno određene duljine. Različitim hashevima ne možemo ukazati gdje je u knjizi nastala promjena, ali ono što možemo dokazati bez sumnje je da sadržaj knjige nije identičan zbog toga što se hashevi razlikuju.

[19] http://www.netokracija.com/sto-je-blockchain-132284

- **Proof of work (dokaz rada)** - Onaj tko želi izmijeniti podatak u blockchainu bi mogao preračunati sve hasheve kompletnog lanca u vrlo kratko vrijeme, da nema jednog sitnog pravila u Bitcoin protokolu koji definira uvjet ispravnog hasha, a on kaže da hash mora započeti s određenim brojem nula**.**

  0000000000000000d9844d93707baf2435f9d9b290c8258622ab635054c8041

  Isti skup transakcija svaki put vratiti isti hash, a ako taj hash ne počinje za određenim brojem nula, hash se smatra neispravnim. Kako bi dobili drugačiji hash, moramo nešto izmijeniti u sadržaju koji ulazi u hash funkciju. Hash je potpuno nepredvidiv pa zato računalu ne preostaje ništa drugo nego metodom pokušaja i pogodaka izračunavati hasheve sve dok ne pronađe pravi, odnosno onaj koji počinje sa zadanim brojem nula. Ovaj proces pogađanja nazivamo proof of work jer svaki ispravan hash je ujedno i dokaz da se računalo 'naradilo' dok ga nije pronašlo**.**

- **Distribuirani sustav** - U Bitcoin mreži, onoga tko pronađe ispravan hash, protokol nagrađuje novim bitcoinima. Ljude koji traže hasheve nazivamo mineri (rudari) jer u opticaj unose nove bitcoine, jednako kao što rudari iskapaju novo zlato. Za pogađanje hasha potrebna je procesorska snaga računala i vrijeme. Jednom pronađeni hash znači da je blok podataka uspješno zatvoren i rudar objavljuje svoj pronalazak ostatku Bitcoin mreže. Ostali sudionici u mreži će također provjeriti i dodati novonastali blok na svoju kopiju blockchaina pa se tako ujedno ostvaruje i sinkronizacija blockchaina između računala**.**

4.3. Rudarenje (mining)

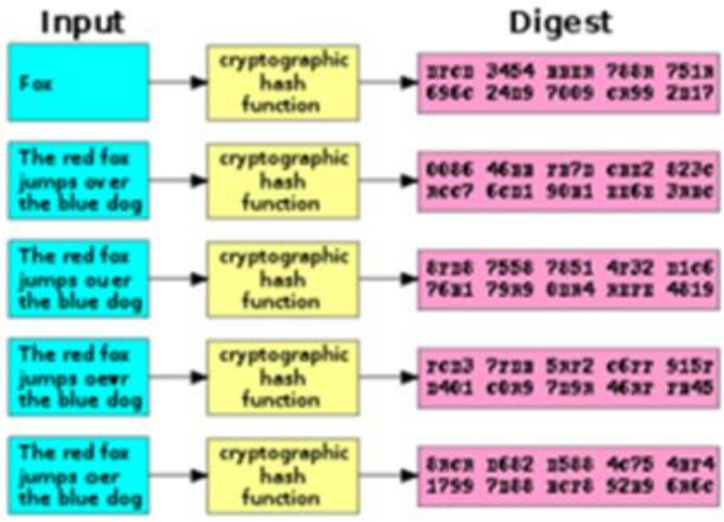
Rudarenje je proces kojim se novom bitcoinu dodaju novčana sredstva. Rudarenje služi za osiguranje sustava bitcoina od prijevarnih transakcija ili dvostruke potrošnje. Rudari pružaju procesorsku moć bitcoin mreži u zamjenu za priliku da budu nagrađeni bitcoinom.
Blockchain rješava problem dvostruke potrošnje kombinirajući tehnologiju peer to peer s kriptografijom javnih ključeva kako bi se stvorio novi oblik digitalnog novca. Peer-to-peer mreža je koncept povezivanja računala bez središnje točke (centralnoga servera) te koncept dijeljenja datoteka među računalima. Ondje svako računalo pronalazi i izravno komunicira s drugim računalima. Najpoznatiji primjer takve mreže su torrenti, te programi poput Bittorrent-a. Sustav je usmjeren da kriptovaluta s vremennom dobiva na vrijednosti i da nikada ne bude inflacije iz razloga što nema središnje institucije koja bi ubacila valutu u sustav i zato jer je softver tako programiran.
Proces rudarenja služi za dvije svrhe u bitcoinu:

1. Rudarstvo stvara nove bitcoine u svom bloku, a količina bitcoina stvorena po bloku je fiksna i smanjuje se vremenom
2. Rudarstvo stvara povjerenje osiguravajući da transakcije budu potvrđene samo ako računalo ima dovoljnu snagu. Više blokova znači više računanja što znači i više povjerenja.

Transakcija postaje potvrđena kada postane dio globalne distribuirane knjige blockchain gdje rudari svakih 10 minuta rade novi blok koji sadrži sve transakcije od posljednjeg bloka. Nove transakcije stalno dolaze u mrežu korisničkih novčanika i drugih aplikacija te idu u privremeni bazen nepotvrđenih transakcija. Rudari rade novi blok i dodaju nepotvrđene transakcije iz tog bazena u novi blok prema kriteriju najviše transakcije. Kada je transakcijski blok stvoren, rudari ga stavljaju u proces obrade. Oni uzimaju informacije pohranjene u bloku i primjenjuju na to matematičku formulu, pretvarajući informacije u naizgled nasumični niz brojeva i slova - hash. Svaki rudar pokreće proces miniranja, odmah stvara novi blok, ispunjava ga transakcijama i počinje izračunavati dokaz rada za novi blok. Ako pronađe rješenje koje taj blok čini valjanim on osvaja nagradu jer je njegov uspješni blok dodan globalnom blokchainu. Rudari dobivaju dvije vrste nagrade za rudarstvo: nove novčiće stvorene novim blokom i transakcijske naknade od svih transakcija uključenih u blok. Da bi zaradili ove nagrade rudari se natječu rješavajući teške matematičke probleme zasnovane na

kriptografiji hash algoritma. Opskrba bitcoin novcem ide kroz rudarstvo slično kao što središnja banka tiskanjem izdaje novi novac. Rudari ostvaruju zaradu kroz naknade od transakcija koje predstavljaju 0,5% ili manje prihoda rudara.[20]

Rudarenje je izum koji bitcoin i ostale kriptovalute čini posebnim, decentraliziranim i sigurnim mehanizmom. Nagrada kroz kriptovalute i naknade na transakcije poticajni su program koji usklađuju rad rudara sa sigurnošću mreže. U vrlo konkurentnom okruženju rudari koji rade sami nemaju šanse za uspjeh, a vjerojatnost da će pronaći blok koji će nadoknaditi troškove električne energije i hardvera jednaka je igri na sreću. Rudari surađuju kako bi formirali rudarske bazene i dijele nagradu. Surađujući rudari dobivaju manji dio ukupne nagrade, ali obično svakodnevno budu nagrađeni. Kada netko u bazenu uspješno minira jedan blok dobivena nagrada bude podijeljena svim rudarima koji su tome pridonijeli. Većinom rudarskih bazena upravlja tvrtka ili pojedinačni voditelj. Rudari ulažu novac u opremu i ostvaruju povrat kroz 6 do 10 mjeseci, ovisno o trenutnim tržišnim cijenama kriptovaluta. Trenutno najpopularnija kriptovaluta za rudarenje je Ethereum. Ono što ga čini tako popularnim kod rudara je činjenica da ga skoro svatko tko ima bolju grafičku karticu u svom kućnom računalu može rudariti i tako zarađivati.



Slika 9: Stvaranje hash-eva

Izvor: https://crobitcoin.com/bitcoin/rudarenje-mining/

[20] Antonopoulos A. (2014): Bitcoin: Unlocking digital Cryptocurrencies, str. 25,137,173

4.4. Novčanik (wallet) za kriptovalute

Novčanik ili wallet je posebna adresa sa koje je moguće slati i primati kriptovalute. Novčanici spremaju privatne ključeve koji su potrebni za pristup bitcoin adresi i novčanim sredstvima. Oni dolaze u različitim oblicima namijenjenima za različite tipove uređaja. Svatko može imati koliko god adresa poželi i ne postoji način da se adresa poveže s pravim identitetom korisnika, osim ako korisnik sam ne učini neke propuste ili to javno objavi.

Način na koji se sredstva na nekoj adresi koriste je da se pomoću privatnog ključa (kombinacije brojki i slova koju je matematički nemoguće pogoditi) potpiše izjava (tzv. transakcija) da se vrši prijenos sredstava s adrese A na adresu B, i to se onda šalje u blockchain na potvrdu od strane svih drugih korisnika. Sredstva se u kriptovalutama ne miču doslovno, nego se vlasnikom neke valute smatra ona adresa koja je bila zadnja objavljena u blockchainu kao vlasnik te količine te valute. Transakcije, tj. potvrde prijenosa vrijednosti, potpisuju se privatnim ključem kojeg ima samo vlasnik adrese.

Da bi se dobio vlastiti novčanik (dakle javna adresa + privatni ključ), postoji više načina:[21]

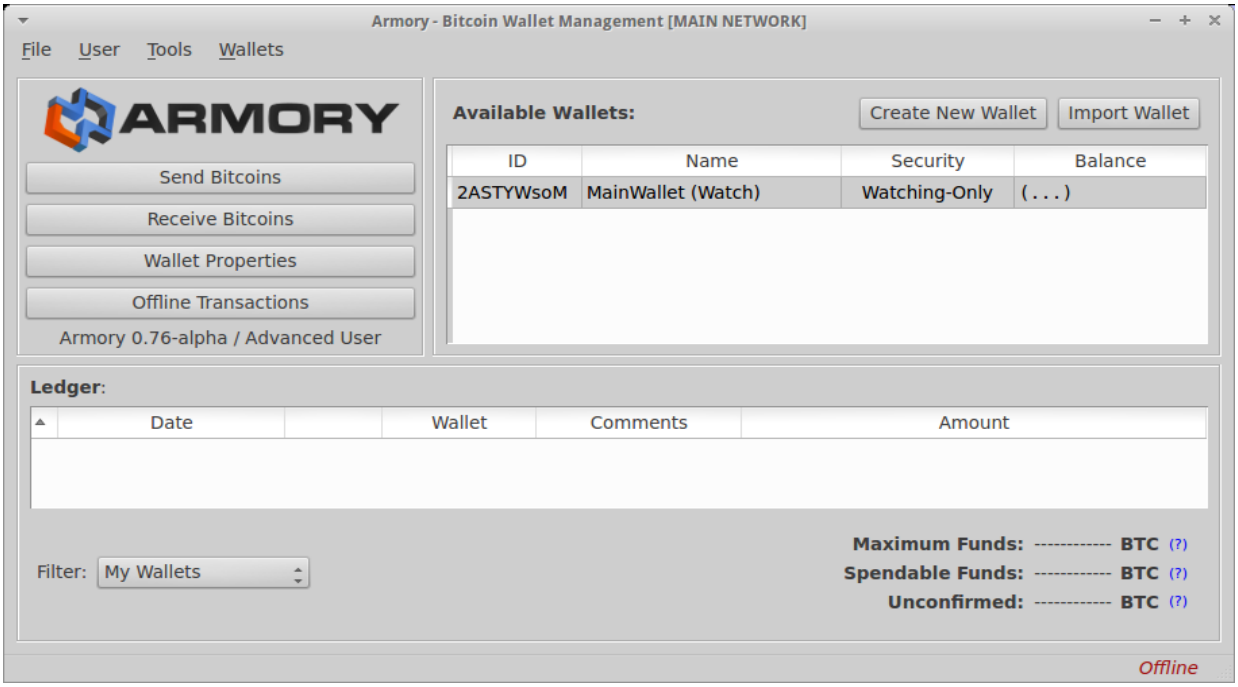
- generiranje svog ključa i adrese uz pomoć klijenta (program blockchaina valute koja nas zanima – kod Bitcoina to je npr. Electrum, kod Ethereuma to je npr. Mist, itd.)
- korištenje nekog hardverskog rješenje poput Ledger Nano S – uređaja nalik USB sticku koji sprema privatni ključ za korisnika i može sadržavati više adresa za više raznih valuta
- otvaranje račun na nekoj kripto-mjenjačnici - Otvaranje računa na mjenjačnici je daleko najjednostavnije, jer mjenjačnice čuvaju privatni ključ za korisnika, ali bilo kakvo dugotrajno držanje sredstava na takvim servisima je opasno.

[21] https://bitfalls.com/hr/2017/08/31/what-cryptocurrency-wallet/

Postoje tri vrste kripto novčanika – softverske, hardverske i papirne.

1. **Softverski novčanici** mogu biti desktop, mobilni ili online/web.

   a) Desktop novčanici se preuzimaju sa interneta i instaliraju na računalu. Kada su u pitanju ovi novčanici treba biti oprezan i ne instalirati ih na bilo kojem računalu jer ukoliko se ne napravi backup i nema privatni ključ, u slučaju kvara hard diska, sredstva mogu biti zauvijek izgubljena. Primjeri mobilnih novčanika: Bitcoin wallet, Mycelium, Blockchain.[22]



Slika 10: Desktop novčanik

Izvor: https://crobitcoin.com/kako-poceti-bitcoin/bitcoin-novcanici-wallets/#prettyPhoto

[22] http://becrypt.me/novcanici-za-cuvanje-kriptovaluta/

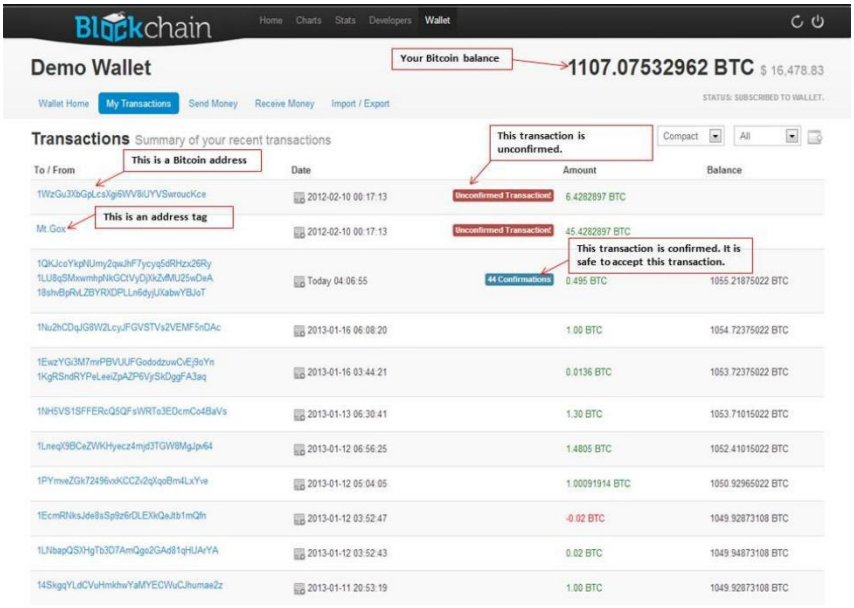
b) Mobilni novčanici kao aplikacija na smartphoneu spremaju privatne ključeve od bitcoin adresa i omogućuju plaćanje direktno putem uređaja. Zajednička karakteristika mobilnih novčanika je u tome što nisu potpuni bicoin klijenti. Potpuni bitcoin klijent mora skinuti cijeli bitcoin blockchain koji uvijek raste i veličine je nekoliko gigabajta. Umjesto toga mobilni novčanici su dizajnirani pomoću SPV-a (Simplified payment verification) i skidaju mali dio blockchaina.[23]

Slika 11: Mobilni novčanik

Izvor: https://crobitcoin.com/kako-poceti-bitcoin/bitcoin-novcanici-wallets/#prettyPhoto

[23] https://crobitcoin.com/kako-poceti-bitcoin/bitcoin-novcanici-wallets/#prettyPhoto

c) Web/online novčanici su specijalizirane internetske stranice na kojima se kreiraju nalozi sa kojih se šalju i primaju kriptovalute. Kontorlira ih netko „treći“ tako se smatraju najsigurnijima, a velika im je prednost što im se može pristupiti sa bilo kojeg mjesta. Ukoliko nisu dobro implementirani mogu omogućiti organizaciji koja je u vlasništvu novčanika da vidi i upravlja ključevima, što znači da mogu upravljati novcem korisnika bez njegovog znanja i dozvole.[24]



Slika 12: Web/online novčanici

Izvor: https://crobitcoin.com/kako-poceti-bitcoin/bitcoin-novcanici-wallets/#prettyPhoto

[24] http://becrypt.me/novcanici-za-cuvanje-kriptovaluta/

2. **Hardverski novčanici** su uređaji nalik usb-u na kojima se čuvaju privatni ključevi. Ukoliko korisnik želi obaviti transakciju spoji uređaj na računalo i unese zaštitni pin. Transakcija se potpisuje privatnim ključem koji se čuva samo na ovom uređaju. Ovi uređaju imaju zaštitnu šifru (najčešće 12 ili 24 riječi) koja služi u slučaju gubitka uređaja za povrat sredstava koja su bila na njemu.

Slika 13: Hardverski novčanik

Izvor: https://bitfalls.com/hr/2017/09/08/hardware-wallets-like-ledger-nano-s-work/

3. **Papirni novčanici** pružaju visoki nivo sigurnosti i njima se izbjegava digitalno čuvanje valuta. Ključ se može prepisati na papir i papir spremiti na sigurno mjesto daleko od web kamera i tehnologije jer samo jedan pogled na ključ dovoljan je da napadač preuzme adresu.

5. ZAKLJUČAK

Kriptovalute su digitalni novčići koje je nemoguće kopirati ni svojevoljno proizvesti. Funkcioniraju kao elektronski zapisi o određenim vrijednostima pohranjenim u elektronskim novčanicama na internetskim stranicama koje pružaju takvu vrstu usluge. Kriptovalute su s razvojem informatičkih tehnologija postale sve važniji faktor u ekonomiji te su sve većim razvojem počele zabrinjavati centralne banke koje su morale reagirat na njihov rast. Kriptovaluta je u potpunosti digitalna valuta čije se korištenje temelji na povjerenju zasnovanom na kriptografiji. Brzi razvoj informacijsko-komunikacijskih tehnologija doveo je do vrlo snažnih kućnih računala, koja omogućavaju korištenje moćnih standarda kriptografije koji su praktično neprobojni. Proizvode ih brojni ljudi u cijelom svijetu koristeći software koji rješava matematičke probleme.

Decentraliziranost i nereguliranost sustava smatra se najvećom prednosti kriptovaluta, ali se pokazalo i kao glavni uzrok velike volatilnosti jer cijena bitcoina i ostalih kriptovaluta ovisi isključivo o odnosu ponude i potražnje. Rad kriptovaluta zasnovan je na blockchain tehnologiji koja obećava riješiti neke od najvećih problema u financijskoj tehnologiji. Izum blockchaina i sustav konsenzusa znatno će smanjiti troškove organizacije i koordinacije na velikim sustavima. Blokchain je distribuirana baza podataka koju je, za praktične potrebe, nemoguće promjeniti. Primjena blockchain tehnologije te raalizacija direktnih umjesto centraliziranih transakcija može uvelike uvesti promijene u društveno-ekonomski svijet.

LITERATURA

Knjige:

1. Antonopoulos A. (2014): Bitcoin: Unlocking digital Cryptocurrencies, str. 25,137,173
2. Swan M. (2015): Blockchain: Blueprint for a New Economy, str. 27-34

Izvori s Interneta:

1. http://www.unizd.hr/portals/4/nastavni_mat/1_godina/metodologija/METODE_ZNANSTVENIH_ISTRAZIVANJA.pdf
2. https://www.kriptovaluta.hr/bitcoin/princip-rada-kriptovaluta/
3. https://sh.wikipedia.org/wiki/Kriptovaluta
4. https://kriptonovac.rs/?p=662
5. https://crobitcoin.com/altcoin/ethereum/
6. http://www.netokracija.com/ethereum-valuta-tomislav-mamic-139768
7. https://www.kriptovaluta.hr/altcoin/iota-kriptovaluta-3-generacije/
8. https://www.ictbusiness.info/poslovanje/hanfa-veliki-rizici-ulaganja-u-kriptovalute-i-ico
9. https://zimo.dnevnik.hr/clanak/hnb-tvrdi-kriptovalute-nisu-elektronicki-novac-ulaganje-je-vas-rizik---490348.html
10. https://crobitcoin.com/burze-i-mjenjacnice/
11. http://www.poslovni.hr/trzista/bis-bitcoin-nikada-nece-biti-novac-342094
12. https://bitfalls.com/hr/2018/02/09/croatias-announcement-taxing-cryptocurrency/
13. https://www.kriptovaluta.hr/vijesti/porez-na-kriptovalute-hrvatska/

14. ECB. (European Central Bank). 2012. Virtual currency schemes. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

15. https://crobitcoin.com/bitcoin/transakcije/

16. https://www.vecernji.hr/techsci/kako-funkcioniraju-kriptovalute-i-blockchain-1196944

17. http://www.netokracija.com/sto-je-blockchain-132284

18. https://bitfalls.com/hr/2017/08/31/what-cryptocurrency-wallet/

19. http://becrypt.me/novcanici-za-cuvanje-kriptovaluta/

20. https://crobitcoin.com/kako-poceti-bitcoin/bitcoin-novcanici-wallets/#prettyPhoto

21. https://www.alienvault.com/blogs/security-essentials/explain-bitcoin-to-me

22. https://coinmarketcap.com/

23. https://www.zagorje-international.hr/index.php/2018/02/13/rast-i-pad-bitcoina-svi-ocekuju-ili-se-nadaju-jos-jednom-uzletu-crypto-marketa/

24. https://bitfalls.com/hr/2018/01/17/the-legality-of-bitcoin-across-the-world/

25. https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011

26. https://www.coindesk.com/ethereum-prices-hit-record-high/

27. https://www.kriptovaluta.hr/altcoin/iota-kriptovaluta-3-generacije/

28. https://pcchip.hr/ostalo/tech/uvod-u-blockchain-tehnologiju/

29. https://crobitcoin.com/bitcoin/rudarenje-mining/

30. https://bitfalls.com/hr/2017/09/08/hardware-wallets-like-ledger-nano-s-work/

PRILOZI

Popis slika:

Popis tablica:

SAŽETAK

Nagli razvoj informatičke tehnologije i Interneta omogućio je početak elektroničkog trgovanja uslugama i robama. Trgovina na Internetu oslanjala se isključivo na financijske institucije koje su posrednici u trgovanju. 2009. godine stvoren je sustav koji čini osnovu sustava digitalnog novca pod nazivom Bitcoin. Bitcoin je prva digitalna valuta izgrađena na decentraliziran način, često se naziva i prvom kriptovalutom, iako su postojale neke kriptovalute prije njega. Kriptovaluta je digitalno sredstvo razmjene čija je glavna karakteristika nepostojanje središnje institucije koja ih izdaje ili upravlja njima. Čimbenici koji utječu na porast popularnosti kriptovaluta su velika praktičnost i brzina obavljanja elektroničkih transakcija. Za razliku od tradicionalnih valuta, kriptovalute su potpuno virtualne, nema fizičkih niti digitalnih kovanica. Korisnici kriptovaluta imaju ″ključeve″ koji im omogućavaju dokaz vlasništva, potrošnju ili prodaju kripovaluta. Bitcoin je nastao na blockchain tehnologiji koja spriječava mogućnost dvostruke potrošnje novca. U zadnje vrijeme uočeno je kako blockchain tehnologija može biti primjenjena i u druge svrhe, u bankama, državnoj upravi, zdravstvu, obrazovanju, za elektroničko glasanje.

Ključne riječi: kriptovalute, blockchain tehnologija, transakcija

SUMMARY

Sudden development of information technology and the Internet enabled the beginning of electronic trading of services and goods. Internet trading relied solely on financial institutions that acted as intermediaries. In 2009, a model was created which made the base of the digital monetary system called Bitcoin. Bitcoin was the first digital asset contructed in a decentralized manner, often called the first cryptocurrency, though there were some cryptocurrencies before it. Cryptocurrency is a digital medium of exchange whose main characteristic is the absence of a central institution that issues or manages them. Factors affecting the rise in popularity of cryptocurrencies are high practicality and high rate of electronic transactions. Unlike traditional currencies, cryptocurrencies are completely virtual, without physical or digital coins. Cryptocurrency users have ″keys″ which verify proof of ownership, enable consumption or sale cryptocurrencies. Bitcoin is based on blockchain technology that prevents the possibility of double spending. It has been noticed recently that blockchain technology can be applied in other areas, such as; banking, state administration, healthcare, education, electronic voting, etc.

Key words: cryptocurrencies, blochain technology, transaction