KRIPTOVALUTE – DANAS I SUTRA

Baketarić, Ana

Undergraduate thesis / Završni rad

2018

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Split, Faculty of economics Split / Sveučilište u Splitu, Ekonomski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:124:711228

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-28**

Repository / Repozitorij:

REFST - Repository of Economics faculty in Split

zir.nsk.hr

UNIVERSITY OF SPLIT

dabar

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U SPLITU

EKONOMSKI FAKULTET

ZAVRŠNI RAD

KRIPTOVALUTE – DANAS I SUTRA

Mentor: **Student:**

prof. dr. sc. Nikša Nikolić **Ana Baketarić**

Split, kolovoz, 2018.

SADRŽAJ:

1. UVOD 1

1.1. Definicija problema 1

1.2. Ciljevi rada 1

1.3. Metode rada 1

1.4. Struktura rada 2

2. KRATKA POVIJEST RAZVOJA KRIPTOVALUTA 2

2.1. Povijest novca 2

3. NAJZNAČAJNIJE KRIPTOVALUTE DANAS 6

3.1. Značajne kriptovalute 6

3.2. Ostale kriptovalute 10

4. BITCOIN – ULOGA I ZNAČAJ 14

4.1. Transakcije 22

4.2. Kupnja i prodaja bitcoina na bankomatu 23

5. MOGUĆI UČINCI DALJNJEG RAZVOJA KRIPTOVALUTE 27

5.1. Ekonomski aspekt kriptovaluta 27

5.2. Pravni aspekt 28

5.3. Razlozi korištenja virtualnih valuta 29

5.4. Vrijednost virtualnih valuta 30

5.5. Rizici virtualnih valuta 31

5.6. Povezanost virtualnih valuta i kriminalnih radnji 32

5.7. Utjecaj virtualnih valuta na politiku centralnih banaka 32

5.8. Utjecaj kriptovaluta na monetatnu politiku centralnih banaka 33

6. ZAKLJUČAK 34

LITERATURA 35

SAŽETAK 37

SUMMARY 38

1. UVOD

1.1. Definicija problema

Pojava kriptovaluta i njihova sve veća popularnost potaknula je brojna pitanja o tome kako će se ove valute u budućnosti odraziti na razvoj novčanih sustava i njihove klasične institucije.

1.2. Ciljevi rada

Ciljevi rada su: pojasniti nastanak kriptovaluta te njihove najznačajnije vrste koje danas postoje - predvidjeti moguće učinke njihovog daljnjeg razvoja u budućnosti na novčane sustave i njihove klasične institucije.

1.3. Metode rada

Povijesna metoda - korištena za saznaje o tome kako su nastale te kako su se razvijele do danas kriptovalute.

Deskriptivna metoda - korištena za definiranje problema i njegovih ciljeva.

Analiza - metoda korištena za raščlanjivanje složenih misli na sve jednostavnije.

Sinteza - metoda korištena za spajanje misli.

Indukcija - metoda korištena kako bi se došlo do zaključka, polazeći od pojedinačnih premisa.

Dedukcija - logička metoda korištena kako bi od općih zaključaka došli do jednog posrednog.

Statistička metoda - korištena za prikupljanje, analiziranje i uređivanje brojčanih podataka.

1.4. Struktura rada

Rad je podijeljen u četiri poglavlja koja se odnose na: kratku povijest kriptovaluta te najznačajnije kriptovalute danas - to su dijelovi gdje je objašnjeno kako i kada su nastale kriptovalute, razlog njihovog nastanka, koliko ih danas ima te koje su najznačajnije i najpopularnije i zbog čega je to tako.

Treći dio rada odnosi se na najpopularnijeg predstavnika kriptovaluta danas, a to je bitcoin, njegovu ulogu i značaj.

Četvrti dio rada donosi moguće učinke daljnjeg razvoja kriptovalute, njihov utjecaj na novčane sustave i klasične institucije.

2. KRATKA POVIJEST RAZVOJA KRIPTOVALUTA

2.1. Povijest novca

Kako bi došli do razvoja kriptovaluta, potrebno je prije svega prevrtjeti povijest novca.

Najprije imamo razmjenu dobara. Dobro za dobro ili roba za robu. Bio je to barter ili trampa. Ljudi kako bi preživjeli, još ne poznajući novac kakav danas imamo razmjenjivali su dobra. Recimo jedna koza za par vreća krumpira. I ta razmjena je funkcionirala dok su obje strane imale korist od dobra koje su dobile razmjenom.

No, budući da je došlo do toga da jedna strana u razmjeni nije imala što ponuditi za uzvrat, a jako je željela neko dobro bilo je potrebno razmjenu podići na jedan viši nivo. Bilo je to doba naturalnog ili robnog novca. Znači da su se samo određene vrste robe upotrebljavale kao novac, a broj tih roba kroz povijest bio je izuzetno velik, neke od njih su: sol, perje, staklo, itd.

Kako se razvijala robna proizvodnja, razvijao se i robni novac, tako je došlo i do karakteristika koje novac treba imati, a to su: prenosivost, trajnost, djeljivost, standardiziranost i prepoznatljivost. Tako je novac sve više vodio ka plemenitim kovinama, zlatu i srebru. Novac nije imao oblik, bio je to komad metala kojeg je pri svakoj transakciji trebalo vagati kako bi mu se utvrdila vrijednost.

Tada nastupa moneta kao prvi kovani novac od strane države određenog oblika, težine i prepoznatljivosti, a iskovana od plemenitih metala. U početku je njena vrijednost bila jednaka njenoj nominalnoj vrijednosti, ali zbog krivotvorenja i habanja monete realna vrijednost je sve više zaostajala za nominalnom i tada nastaje simbolički novac.

Banknota – novac izrađen od papira, a zamjenjiv za zlato u banci koja ga je emitirala. Način na koji je funkcionirala banknota bio je sljedeći. Banke su bile mjesta koja čuvaju zlato u svojim sefovima za svoje klijente, također izdaju potvrde da određena osoba ima određenu količinu zlata u toj banci. I onda je ta osoba s tom potvrdom mogla već kupovati određeno dobro ili dobra na osnovu količine zlata koju je imala. Za određeno dobro davala se potvrda koju bi osoba koja ju je dobila mogla odnijeti u banku i uzeti za nju zlato ili je jednostavno s njom mogla nastaviti dalje kupovati - plaćati dok zadnja osoba koja ju je dobila ne bi otišla u banku po zlato.

Poslije nastupa doba zlatnog standarda. Valuta države svoju protuvrijednost ima u rijetkim metalima zlatu, srebru, bronci. Država je preuzela zlato od svojih rezidenata i za to im izdala papirnate zadužnice. Bio je to papirnati novac.

Papirnati novac - vezan za zalihe zlata neke države, sve u svrhu držanja inflacije pod kontrolom. Zalihe zlata imale su polagan rast, čak su i usporavale, zbog čega nije moglo doći do inflacije. Nije bilo moguće trošiti više nego se imalo. U vrijeme Velike Depresije, prekinut je odnos dolar - zlato, tiska se sve više papirnatog novca - papirnatih zadužnica, kako bi se potaknula ekonomija. Tako je proizišao i problem inflacije. U optjecaju je bilo previše papirnatog novca koji nije bio garantiran nikakvom konkretnom vrijednošću. Nije bilo moguće ni mijenjati dolar za zlato jer su štampani bez pokrića, tako su se počele prazniti državne rezerve zlata.

Sa sve razvijenijom informatikom danas, koju omogućuje sve veći razvoj interneta i različitih tehničkih programa sa njihovim elementima poput programiranja, kriptiranja i dr. jednostavno je potrebno pritisnuti samo jedan gumb za štampanje novca.

Došlo je i do razvoja elektroničkog novca, recimo putem plaćanja karticama, PayPal, itd. Kartice, grubo rečeno – komad plastike sa ugrađenim čipom pomoću kojeg se prenose podatci. (Nikolić, Pečarić, 2007.)

No, evolucija novca ne staje na elektroničkom novcu, nego nastaju još i virtualne valute, a zatim i kriptovalute koje su tema ovog rada, a sve kao odgovor na centralizirane valute, tj. valute koje su pod kontrolom države i koje danas koristimo.

Za kriptovalute možemo reći da su to digitalni novčići koje ne možemo proizvesti na svoju ruku niti kopirat, a imaju isti cilj kao i novac koji svakodnevno koristimo. Dupliciranje i falsificiranje kriptovaluta je jako teško, gotovo nemoguće, ogrničenog su broja, šalju se s jedne elektroničke adrese na drugu, a za razliku od kartica kojima plaćamo gdje se novac šalje s jednog na drugi bankovni račun i gdje jedna institucija kontrolira novac, stanje računa, transakciju, kod kriptovaluta cijela zajednica, blockhain može vidjeti transakciju i stanje računa.

Radi što relevantnijeg uvida i objašnjenja kriptovaluta, virtualnih valuta iznijet će se i definicija Europske centralne banke koja kaže da su virtualne valute : "vrsta nereguliranog, digitalnog novca, kojeg izdaju i kojeg najčešće kontroliraju njezini osnivači, koriste se i prihvaćeni su između članova određene virtualne zajednice". (ECB, 2012)

ECB (2012) također ističe podijelu na tri vrste virtualnih valuta, a to su:

- Zatvorene virtualne valute – nemaju utjecaj na realnu ekonomiju, stvorene samo za virtualni svijet, npr. videoigre.
- Virtualne valute s jednostrukim protokom – virtualna dobra možemo kupiti realnim novcem, ali virtualni novac ne možemo koristiti u realnom svijetu, npr. Nintendo bodovi.
- Virtualne valute s dvostrukim protokom – virtualne valute možemo mijenjati za realni novac i realni novac za virtualne valute. Obostrane transakcije. Imaju utjecaj na realnu ekonomiju, npr. bitcoin.

Zatim može se prenijeti i definicija virtualnih valuta od strane European Banking Authorityja – EBA, koja kaže da su virtualne valute: "digitalni prikaz vrijednosti koja nije izdana od centralne banke ili javne ovlasti niti je vezana za neki fiat novac, ali se koristi od fizičkih i pravnih osoba kao sredstvo razmjene i može biti transferirano, pohranjeno ili razmijenjeno elektronički." (EBA, 2014)

The Financial Crimes Enforcement Network (FinCEN) definira virtualne valute kao: „sredstvo razmjene koje radi kao valuta u određenim uvjetima ali nema svojstva pravog novca. " (FinCEN, 2013)

Da bi se što lakše razumjeli načini na koje su stvorene kriptovalute i način na koji funkcionira bitcoin koji će detaljno biti objašnjen u radu, potrebno je prije svega uočiti razliku između elektroničkog novca i virtualnih valuta.

Tablica 1 Razlika između fiat novca, elektronskog novca i kriptovaluta

Karakteristike	**Fiat novac**	**Elektronski novac**	**Kriptovaluta**
Format novca	Nedigitalan	Digitalan	Digitalan
Jedinica vrijednosti	USD, EUR	USD, EUR	Bitcoin, Ripple
Pravni status	Reguliran	Reguliran	Nereguliran
Anonimnost	Uglavnom da	Ne	Uglavnom da
Temeljena na dugu	Da	Ne	Ne
Kontrolabilnost	Središnja banka	Izdavatelj	Nema
Pohranjivanje i transferabilnost	Umjereno, složeno, skupo	Jednostavno, jeftino, brzo	Jednostavno, jeftino, brzo
Ponuda	Neograničena	Neograničena	Ograničena
Vrsta rizika	Pravni, kreditni, likvidni, operativni	Uglavnom operativni	Uglavnom operativni

Izvor: Izrada autora prema Europska Centralna Banka (2012), str. 16.

Za neke autore kriptovalute nisu isto što i virtualne valute dok su za druge one uži pojam virtualnih valuta. Uglavnom, razlika se pridaje kriptiranju – šifriranju, radu na anonimnosti, no više o tome u daljnjem tekstu. U ovom radu važnost se pridaje kriptovalutama, pa će one i biti detaljnije objašnjene jer su većinom sve definicije kriptovaluta tehničkog tipa.

3. NAJZNAČAJNIJE KRIPTOVALUTE DANAS

Prije no što navedemo kriptovalute potrebno je reći u koju skupinu virtualnih valuta one spadaju, to su virtualne valute s dvostrukim protokom – kriptovalute, prema svojim karakteristikama najsličnije novcu koji danas koristimo.

3.1. Značajne kriptovalute

Najznačajnije kriptovalute današnjice su: Bitcoin, Etherum, Bitcoin Chash, Ripple i Litecoin. Prije svega na Bitcoin ćemo se tu samo kratko osvrnuti jer će biti detaljno objašnjen u sljedećem dijelu rada.

BITCOIN

digitalno zlato, prva i najveća kriptovaluta današnjice. Ograničen je na 21 milijun i nikad ga neće biti više. Osnovan 2009. godine.

ETHEREUM

Decentralizrana softverska platforma pokrenuta 2015. godine. Služi za izgradnju i vođenje "pametnih ugovora"[1] , te "distribuiranih aplikacija (DApps)“[2] bez ikakvih zastoja , prijevare ili kontrole od trećih strana. Zasnovan na sličnom blockcain principu kao i bitcoin, za razliku

[1] Pametni ugovori su koncept koji se spominje u istom kontekstu kao blockchain sa izrazitom tehničkom složenošću.
[2] Distribuirane, otporne, transparentne i poticajne aplikacije.

od bitcoina ima brže transakcije, a pojedini dijelovi njegove mreže mogu biti iznajmljeni putem "smart contracta" za korištenje u druge svrhe. Rudarenje je isplativije, a ponuda neograničena.

Na dan 19. kolovoza 2018. druga rangirana kriptovaluta prema tržišnoj kapitalizaciji od 30.560.023.741 $.



Slika 1 Tržišna kapitalizacija kriptovalute Ethereum

Izvor: https://coinmarketcap.com/

Slika prikazuje tržišnu kapitalizaciju Ethereum – a izraženu u američkim dolarima i jedinicama bitcoina, vodeće kriptovalute.

BITCOIN CASH

Praktički klon bitcoina izveden "forkanjem"[3] bitcoina - odlikuje se povećanom količinom bloka i samim time bržim procesiranjem transakcija. Prihvaćen je kao dobra alternativa bitcoina. Tržišna kapitalizacija na dan 19. kolovoza 2018. godine bila je 9.806.308.829 $ i bila je 4. rangirana kriptovaluta prema tržišnoj kapitalizaciji.



Slika 2 Tržišna kapitalizacija kriptovalute Bitcoin Cash

Izvor: https://coinmarketcap.com/

RIPPLE

Jedina centralizirana kriptovaluta među najpoznatijima, pokrenuta 2012. godine. Izdana od strane istoimene tvrtke, a sve količine su unaprijed izrudarene i puštaju se po potrebi u opticaj.

[3] Kreiranje kopije procesa u tehničkom smislu.

Prednost Ripple - a je protokol za brza digitalna plaćanja za koji su zainteresirane i velike svjetske banke. Globalna mreža za dogovore u stvarnom vremenu, te za trenutačne, sigurne i jeftine međunarodne transakcije. Ripple ima tržišnu kapitalizaciju u iznosu od 1.26 milijardi dolara.

LITECOIN

" prva pratilja " bitcoina, pokrenut 2011. godine. Nastao od strane MIT - evca i bišeg Googleovog inženjera Charlia Lee - a . Zasnovan na principu bitcoina, ali ponešto drugačijim algoritmima moguće je rudariti i manje moćnim računalima.

Transakcije su brže nego kod bitcoina. Kao dokaz koristi se "skryt" - može se dekodrati pomoću procesora običnog računala. Tržišna kapitalizacija Litecoina na dan 19. kolovoza 2018. godine iznosi 3.346.007.145 $.



Slika 3 Tržišna kapitalizacija kriptovalute Litecoin

Izvor: https://coinmarketcap.com/

3.2. Ostale kriptovalute

Postoji još stotine alternativnih kriptovaluta. Neke od njih dolaze u prvi plan zbog špekulacija, a neke zbog hakiranja.

Šest valuta kojima se predviđa sjajan razvoj su: Litecoin, Etherum, Zcash (ZEC), Dash, Ripple, Monero (XMR).

ZCASH – „sigurnija verzija bitcoina". Decentralizirana kriptovaluta koja se temelji na otvorenom izvoru, a pokrenuta je 2016. godine. Nudi privatnost i selektivnu transparentnost transakcija. Sve su transakcije snimljene i objavljene na blockchainu, a identitet pošiljatelja, primatelja i količine ostaju privatni. Mogućnost zaklonjenih transakcija - kriptiranje sadržaja naprednim kriptografskim tehnikama. Tržišna kapitalizacija Zcash – a, 19. kolovoza 2018. iznosila je 663.047.408 $, bila je 20. rangirana kriptovaluta prema tržišnoj kapitalizaciji.



Slika 4 Tržišna kapitalizacija kriptovalute Zcash

Izvor: https://coinmarketcap.com/

DASH - znan kao "darkcoin" - tajnija verzija bitcoina. Nudi višu anonimnost, transakcije je gotovo nemoguće pratiti. Kriptovaluta razvijena od strane Evana Duffielda, a pokrenuta u siječnju 2014. godine. Tržišna kapitalizacija, 19. kolovoza 2018. bila je 1.316.689.583 $, 14. rangirana kriptovaluta.



Slika 5 Tržišna kapitalizacija kriptovalute Dash

Izvor: https://coinmarketcap.com/

MONERO - privatna valuta kojoj se ne može ući u trag. Kriptovaluta otvorenog izvora pokrenuta u travnju 2014. godine. Njen razvoj temelji se isključivo na donacijama, a njime upravlja cijela zajednica. Jak fokus na decentralizaciju i nadogradnju, te omogućuje potpunu privatnost posebnom tehnikom "potpisi prsteno"- prikazivanje cijele grupe kriptografskih potpisa, s tim da je barem jedan potpis pravi, no kako svi djeluju valjano, pravog se ne može izolirati. Tržišna kapitalizacija na dan 19. kolovoza 2018. bila je 1.579.559.146 $, bila je 10. rangirana kriptovaluta prema tržišnoj kapitalizaciji.



Slika 6 Tržišna kapitalizacija kriptovalute Monero

Izvor: https://coinmarketcap.com/

Tablica 2 Tržišna kapitalizacija dvadeset najpopularnijih kriptovaluta

	Naziv kriptovalute	Tržišna kapitalizacija	Cijena	Ponuda
1	Bitcoin	$110.265.175.073	$6.405,73	17.213.512 BTC
2	Ethereum	$29.632.842.183	$292,33	101.366.860 ETH
3	XRP	$11.663.335.639	$0,296231	39.372.399.467 XRP *
4	Bitcoin Cash	$9.167.719.806	$530,04	17.296.413 BCH
5	EOS	$4.275.997.958	$4,72	906.245.118 EOS *
6	Stellar	$4.078.423.382	$0,217264	18.771.752.700 XLM *
7	Litecoin	$3.278.895.237	$56,66	57.873.909 LTC
8	Cardano	$2.508.193.627	$0,096740	25.927.070.538 ADA *
9	Tether	$2.410.272.673	$1,00	2.407.140.346 USDT *
10	Ethereum Classic	$1.537.323.279	$14,81	103.833.949 ETC
11	Monero	$1.501.687.257	$92,00	16.323.079 XMR
12	TRON	$1.310.754.930	$0,019936	65.748.111.645 TRX *
13	IOTA	$1.298.049.146	$0,467003	2.779.530.283 MIOTA
14	Dash	$1.270.705.323	$153,82	8.261.153 DASH
15	NEO	$1.095.476.213	$16,85	65.000.000 NEO *
16	Binance Coin	$949.997.796	$9,95	95.512.523 BNB *
17	NEM	$933.977.761	$0,103775	8.999.999.999 XEM *
18	Tezos	$788.046.745	$1,30	607.489.041 XTZ *
19	Zcash	$657.473.907	$143,25	4.589.806 ZEC
20	VeChain	$616.977.110	$0,011126	55.454.734.800 VET *

Izvor: Izrada autora prema podatcima: https://coinmarketcap.com na dan 16. kolovoza 2018.

4. BITCOIN – ULOGA I ZNAČAJ

Bitcoin vrsta digitalnog novca koji se stvara i čuva elektronički, ne printa se i ne kontrolira od strane bilo koga. Proizvodi se pomoću računalnog softwarea koji riješava matematičke probleme. Za bitcoin možemo reći da je kriptovaluta (cryptocurrency). Te da predstavlja početak revolucije digitalnog novca.

Bitcoin se koristi za za kupovinu u elektroničkom obliku i u tom smislu ne možemo ga razlikovati ni od jedne druge valute kojom se također trguje digitalno npr. kuna, dolar, euro, itd. Ali bitcoinova najznačajnija karakteristika je upravo i najveća razlika između njega i ostalih valuta, a to je decentraliziranost bitcoina kao valute. Bitcoin mrežu ne kontrolira niti jedna institucija što trenutni pobornici bitcoina smatraju ogromnim plusom jer do oscilacija u vrijednosti dolazi zbog ljudi.

Bitcoin - ideja pretvorena u djelo software developera Satoshi Nakamoto-a - elektroničko plaćanje na temelju matematičkih dokaza. Developer je imao ideju da stvori valutu bez centralne vlasti s elektroničkim prijenosom i s vrlo malim ili nikakvim transakcijskim troškovima. Zbog toga bitcoin ne izdaje nitko, te nije u sjeni centralnih banaka gdje ga ljudi ne mogu prebrojati i gdje banke postavljaju svoja pravila. Jer banke kada upadnu u dug, izdaju više novca što rezultira inflacijom. A bitcoin je stvoren digitalno i platformi se može pridružiti bilo tko.

Bitcoin se rudari (Mined) pomoću računala, koristi se procesorsko vrijeme i distribuira bitcoin u platnu mrežu, a mreža procesira transakcije napravljene pomoću bitcoina što rezultira stvaranjem vlastite platne mreže. Bitcoin protokol - algoritam pomoću kojeg funkcionira cijeli sustav ograničen je na izdavanje 21 milijuna bitcoinova. Svaki bitcoin ima puno veću vrijednost nego što ju ima tradicionalna valuta, te je zbog toga podijeljen na manje dijelove od kojih je najmanji milijuniti dio "Satoshi" nazvan po izumitelju bitcoina.

Tradicionalne valute nekoć su se temeljile na zlatu i srebru, imaju svoju pozadinu u zlatu. Prije nego su zemlje uvele svoje valute poput dolara, eura, bogatstvo se mjerilo sjajnim i rijetkim stvarima. Vrijendost zlata bila je velika zbog samog rada potrebnog da se do njega dođe i zbog težine pronalaska novog izvora. Kada su uvedene valute svaka valuta dobila je svoju središnju banku i ovisno o količini zlata koju je posjedovala dobila je i svoju vrijednost.

Problem je u tome što svaku valutu kontrolira centralna banka, tj. bar neka vrsta vlasti. Kada ta vlast dođe u opasnost ona ima mogućnost izdavanja više novčanica te valute. Prema ovome možemo zaključiti da zlato više nema direktnu vezu sa samom vrijednošću valute, te da ta vlast pazi na samu sebe, jer kad se izdaju novčanice bez pokrića, vrijednost novčanica pada jer ih sad ima više u opticaju. U ovakvom slučaju nastaje inflacija, npr. ako je prije jedna Coca Cola koštala 1 novčanicu, budući da ih sad imamo više jer ih je vlast izdala više, onda je Coca Cola za nas postala "jeftinija" i njen prodavač će morati podići njenu cijenu. Bitcoin kao valuta nastoji izbjeći ove probleme. I zato se bitcoin ne temelji na zlatu već ovisi o matematici.

Za izradu bitcoina koristi se matematička formula koja je javno dostupa svima jer je napisana OpenSource kodom, tako da se svatko može uvjeriti da radi ono za što je i stvoren. Bitcoin ima svoje rudare koji troše procesorsko vrijeme "kopajući" po algoritmu i iz njega izvlače bitcoinove - rudarenje.

```
//concat it all
$header_hex = $version . $prevBlockHash . $rootHash . $time

//convert from hex to binary
$header_bin  = hex2bin($header_hex);
 //hash it then convert from hex to binary
$pass1 = hex2bin(  hash('sha256', $header_bin )  );
//Hash it for the seconded time
$pass2 = hash('sha256', $pass1);
//fix the order
$FinalHash = SwapOrder($pass2);

echo   $FinalHash;
```

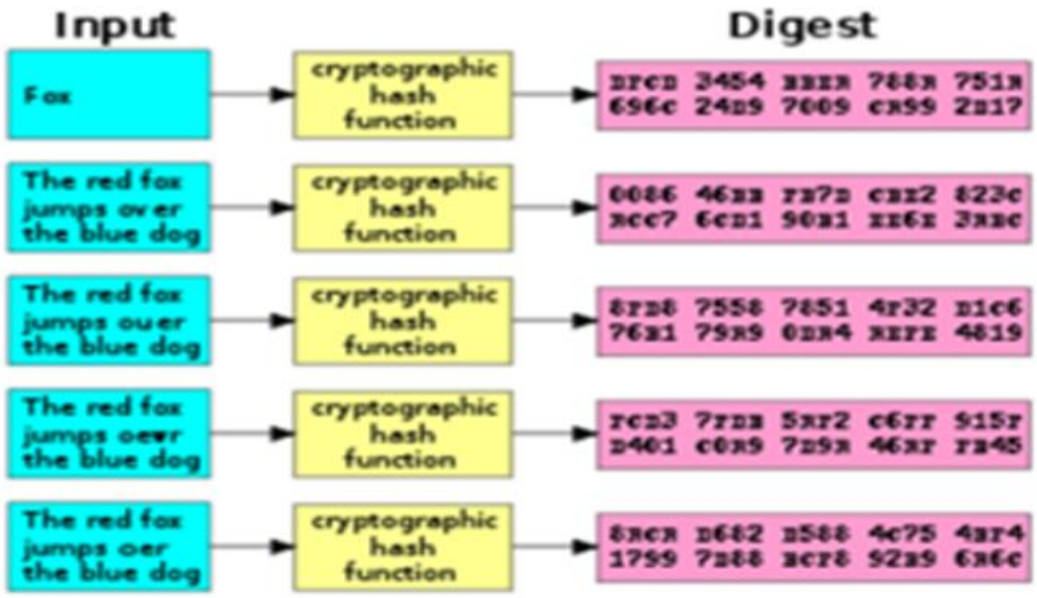
Slika 7 Stvaranje konačnog Hash – a

Izvor:
https://www.google.ba/search?biw=1367&bih=639&tbm=isch&sa=1&ei=Y7h6W9DHJuqY6ATk3LegDg&q=hash+bitcoin&oq=hash+bitcoin&gs_l=img.3..0i19k1l2j0i8i30i19k1l8.3227.6128.0.6727.8.8.0.0.0.0.320.1244.0j7j0j1.8.0....0...1c.1.64.img..0.8.1238...0j0i30k1j0i30i19k1.0.fp7T6px54qw

Algoritam služi i za praćenje svake obavljene transakcije i njeno spremanje u blok. Jedan blok sadrži 25 bitcoina za čije je spremanje potrebno nekih 10 minuta. Bitcoin mreža sve transakcije obavljene u određenom periodu skuplja i stavlja u lanac blokova (block chain), a kao nagradu rudar dobije svotu bitcoina.

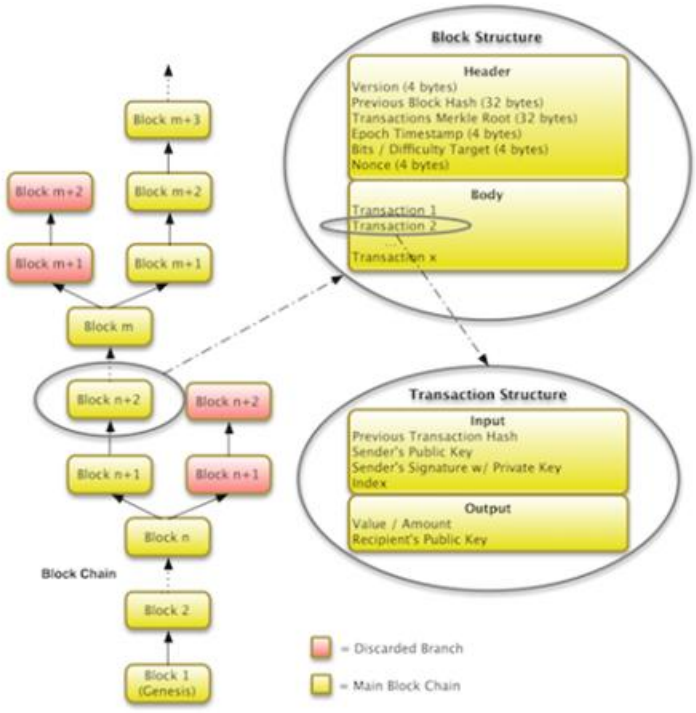
Glavna knjiga je dugi lanac blokova. Knjiga služi za provjeru bilo koje transakcije napravljene između bilo kojih bitcoin adresa u bilo kojem vremenu. Svaki novi transakcijski blok dodaje se u lanac blokova te se tako stvara doista duga lista svih transakcija ikad napravljenih na bitcoin mreži. Nova kopija glavne knjige konstantno se daje svima koji sudjeluju kako bi mogli znati što se događa. Sve se pohranjuje digitalno i glavna knjiga mora biti sigurna.

Glavnu ulogu u tome da lanac blokova ostane nedotaknut i da ga nitko neće moći izmjeniti imaju rudari. Jer kad je transakcijski blok jednom stvoren rudari ga stavljaju u proces obrade, tako što uzimaju informacije pohranjene u bloku i primjenjuju matematičku formulu - pretvarajući informacije u nešto puno kraće, a naizgled nasumični niz brojeva i slova. To je hash. Hash se pohranjuje zajedno s blokom na kraju lanca blokova. Hashevi imaju i zanimljive karakteristike. Hash je lako proizvesti iz podataka kao što je bitcoin blok ali je isto tako gotovo nemoguće otkriti koji su to podatci gledajući samo hash. Isto tako hash je lako proizvesti iz velike količine podataka ali ipak svaki hash je unikatan. Ako promijenimo samo jedno slovo ili brojku mijenjemo odmah u cijelosti hash. Rudari ne koriste samo transakcijski blok kako bi generirali hash već koriste i druge podatke, a jedan od tih podataka je hash zadnjeg bloka pohranjnog u lancu blokova.



Slika 8 Primjer kriptiranja

Izvor:
https://www.google.ba/search?tbm=isch&q=slike+kriptiranja&chips=q:slike+kriptiranja,online_chips:kriptografija&sa=X&ved=0ahUKEwi8upK50_vcAhXMCJoKHdbjDw8Q4lYIJygD&biw=1367&bih=639&dpr=1#imgrc=_Qo0n-bf1jT4fM:



Slika 9 Primjer Blockchain - stvaranje blokova

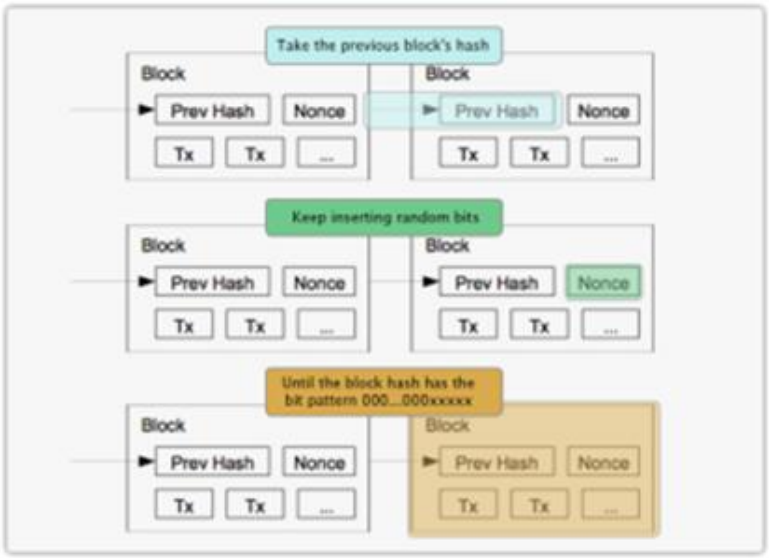
Izvor: https://www.google.ba/search?tbm=isch&q=slike+kriptiranja&chips=q:slike+kriptiranja,online_chips:kriptografija&sa=X&ved=0ahUKEwi8upK50_vcAhXMCJoKHdbjDw8Q4lYIJygD&biw=1367&bih=639&dpr=1#imgrc=_Qo0n-bf1jT4fM:

Svaki blok napravljen pomoću hasha bloka prije njega postaje digitali oblik pečata, te potvrđuje da je taj blok i svaki poslije njega legitiman jer ukoliko bismo ga dirali svi bi to znali. Ako se transkcija pokušava krivotvoriti mijenjajući blok koji je već pohranjen u lancu blokova to će promijeniti hash tog bloka. Jer ako netko provjerava autentičnost bloka tako što pokreće hash funkciju na njemu, otkrit će da je hash drugačiji od onoga bloka koji je već pohranjen pokraj njega u lancu blokova, blok bi bio krivotvoren.

To je razlog što je hash svakog bloka korišten za stvaranje sljedećeg bloka u lancu, te bi onda mijenjanje jednog izazvalo promjenu sljedećeg bloka. Tj., mijenjanjem jednog bloka izaziva se lančana reakcija koja se proteže do kraja lanca.

Kada rudari zapečate blok svi se međusobo natječu pomoću softwarea koji je specifičo napisan samoza to. Za svaki spješno kreiran hash rudari dobiju 25 bitcoina, lanac blokova se ažurira isvi na mreži znaju za to.

To je poticaj da se nastavi s rudarenjem i da transakcije budu funkcionalne. Problem je bio što je vrlo lako kreirati hash od tih podataka . Računala su iznimno dobra u tome. Zbog toga je Bitcoin mreža učinila stvari težima da se ne bi stvarale tisuće hasheva svake sekunde, a svi bitcoini bi bili "iskopani" u par minuta. "Dokaz rada" - ono pomoću čega bitcoin protokol namjerno otežava situaciju.



Slika 10 Primjer Hash – a

Izvor:
https://www.google.ba/search?biw=1367&bih=639&tbm=isch&sa=1&ei=Y7h6W9DHJuqY6ATk3LegDg&q=hash+bitcoin&oq=hash+bitcoin&gs_l=img.3..0i19k1l2j0i8i30i19k1l8.3227.6128.0.6727.8.8.0.0.0.0.320.1244.0j7j0j1.8.0....0...1c.1.64.img..0.8.1238...0j0i30k1j0i30i19k1.0.fp7T6px54qw

Bitcoin protokol ne prihvaća bilo kakav hash, već zahtjeva da hash određenog bloka izgleda na određen način tj., mora imati određen broj nula (0) na početku. Ne postoji niti jedan način pomoću kojeg bismo mogli znati kako će izgledati hash prije nego ga stvorimo, jer svaki put kada i samo djelomično izmijenimo samo jedan podatak hash izgleda u potpunosti drugačije. Rudari ne smiju mijenjati podatke unutar transakcijskog bloka, a kako bi kreirali drugačiji hash moraju mijenjati podatke. To rade na način da koriste drugi, nasumični dio podataka nazvan "nonce". Koristeći "nonce" zajedno s transakcijskim podatcima stvara se hash. Ukoliko hash ne odgovara određenom formatu nonce se mijenja i postupak se ponavlja.

Potreban je iznimo velik broj pokušaja da se pronađe nonce koji odgovara, a svi rudari rade isti postupak u isto vrijeme i tako zarađuju bitcoine.

Tri su glavne kategorije bitcoin hardwarea za rudarenje, svaki skuplji i jači od prethodnog. Prilikom odabira hardwarea važno je promatrati brzinu hasha i potrošnju energije. Stopa hasha jednaka je broju operacija koje hardware može odraditi svake sekunde kada pokušava razbiti matematički problem. Stopa se mjeri u megahashu, gigahashu i terahashu po sekundi (MH/s, GH/s, TH/s). Što je stopa hasha veća, veće su i šanse za rješavanje transakcijskog bloka, naravno u usporedbi sa prosječnom stopom. Jako je važno odabrati hardware koji neće potrošiti više energije nego što ćemo zaraditi rudarenjem.

Bitcoin hardwarei za rudarenje:

- GPU
- FPGA
- ASIC

CPU/GPU Bitcoin rudarenje

Najslabija kategorija od tri nabrojane je samo računalo. Teoretski se CPU računala može koristiti za rudarenje bitcoina ali u praksi ono je jako sporo i nema smisla na današnjem tržištu. Stopa hasha može se povećati dodavanjem grafičkog hardwarea računalu. Grafičke kartice sadrže GPU-e, dizajnirane za teške matematičke probleme kako bi mogle računati kompleksne poligone u najnovijim računalnim igrama. Zato su dobre za rješavanje bitcoin algoritma, tj. u rješavanju trasakcijskog bloka. Jedna od velikih prednosti GPU – a je što se može koristit za rudarenje i drugih kriptovaluta osim bitcoina, npr. Litecoin koji koristi drugačiji algoritam.

FPGA Bitcoin rudarenje

FPGA (Filed Programmable Gate Array) – integrirani strujni krug koji se konfigurira nakon što je izgrađen. Zbog toga proizvođači hardwarea sami kupuju čipove i slažu opremu. Zbog toga što je konfiguriran za rudarenje FPGA često daje bolje rezultate od CPU I GPU – a.

ASIC Bitcoin rudarenje

ASIC (Application Specific Integrated Circuits) – specifično dizajniran samo da rudari bitcoine zapanjujućom brzinom te s relativno niskom potrošnjom energije.Čipovi dizjnirani za ovaj zadatak su izuzetno skupi i vremenski zahtjevni za proizvesti, a prednost im je brzina kojom osvajaju.

Cloud rudarenje – cloudhashing

Za rudarit bitcoin ili bilo koju drugu kriptovalutu potrebno je investirati u hardware opremu, posvećenu i optimizranu samo za rudarenje. Zbog toga je jedan od trendova koji se javlja u Bitcoin industriji „rudarenje u oblaku“. Rudarenje se odvija u oblaku što znači da pružatelje ovakve usluge brine za sve procese potrebne za rudarenje. A razlog zbog kojeg tvrtke prodaju svoju rudarsku snagu- svoje rudarske opreme je diversifikacija rizika.

4.1. Transakcije

Bitcoin transakcije – trasfer vrijednosti između dva digitalna novčanika, koja se tada registrira u Blokchain, tj. sustav ulančanih blokova. Privatni ključ ili sjeme je tajni dio podataka Bitcoin novčanika, a služi za potpisivanje transakcija pružajući matematički dokaz da je taj ključ došao od vlasnika novčanika. Potpis osigurava da se transakcija ne može promijeniti jednom kada je izdana. Sve transakcije su javne na blockchain mreži, te se sve procesirane transakcije mogu pratiti sve do prve transakcije.

Kako bi se izvršila transakcija određenog iznosa bitcoina sa jednog digitalnog novčanika na drugi, potrebne su :

- Adresa ili javni ključ (Public Key)
- Privatni ključ (Private Key)
- Kriptografski potpis

ADRESA ILI JAVNI KLJUČ

Adresa – kao „bankovni rračun“, pomoću odgovarujućih pružatelja postavi se u nekoliko sekundi. Adresa je generirana određenim postupkom te izgleda kao nasumična kombinacija slova i brojeva, jedinstvenih i povezanih na taj račun, jedan korisnik može imati više adresa.

PRIVATNI KLJUČ

Tajni dio podataka koji dokazuje vaše pravo za prenošenje bitcoinova s odrđenog novčanika uz pomoć kriptografskog potpisa. Privatni ključ sprema se na računalu ako se koristi softwerski novčanik ili na serveru ako se koristi web novčanik.

KRIPTOGRAFSKI POTPIS

Matematički mehanizam pomoću kojeg se dokazuje vlasništvo nad određenom adresom, odnosno digitalnim novčanikom. Nakon što Bitcoin software potpiše transakciju odgovarajućim privatnim ključem, tada cijela Bitcoin mreža može vidjeti da taj potpis odgovara transakciji koja se izvršava, ali nije moguće vidjeti privatni ključ koji štiti račun.

4.2. Kupnja i prodaja bitcoina na bankomatu

Kako kupiti bitcoin na bankomatu ? – upute prenesene prema Demonstration of The Netherland's first 2-way Bitcoin ATM.

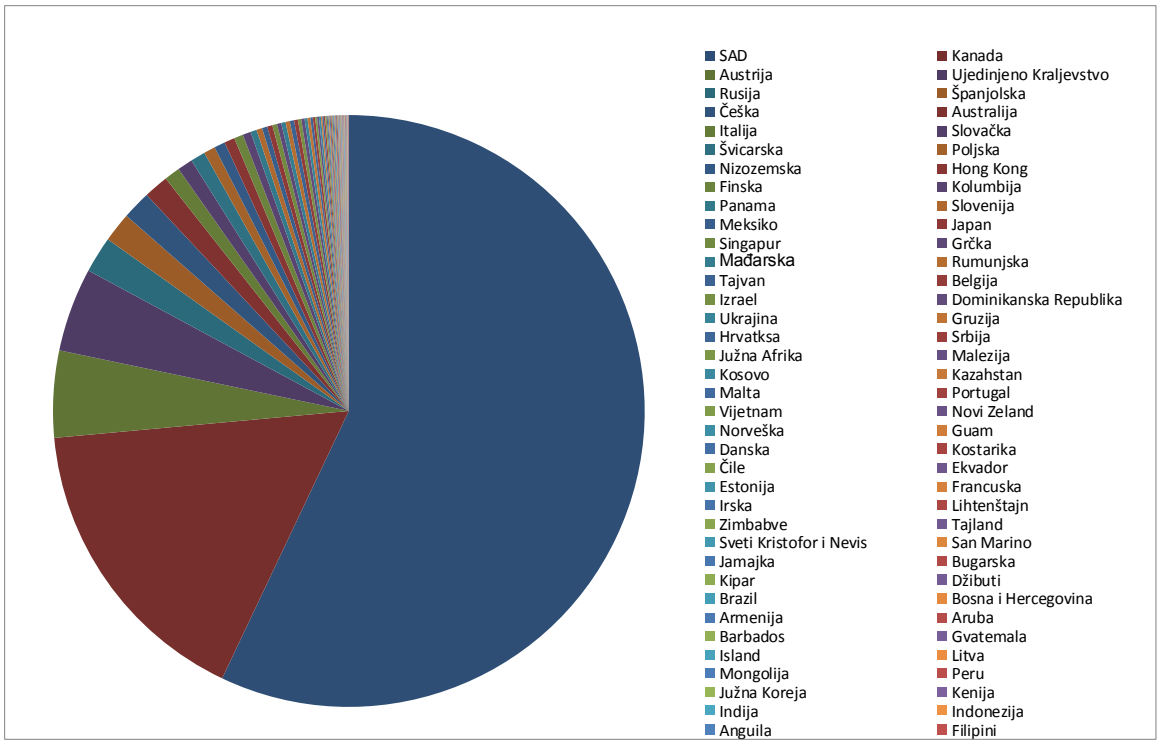
- Odabrati jezik
- Opcija „započni“
- Unijeti broj mobitela
- Unijeti verifikacijski kod sa SMS – a
- Opcija – kupi bitcoin
- Ako imate Bitcoin novčanik – opcija „da“, ako nemate – opcija „ispiši na papiru“

- Skenirati QR kod
- Ubaciti gotovinu
- Opcija “Završi”
- Bitcoini se šalju na vašu Bitcoin adresu i Vi će te primiti potvrdni SMS
- Možete ispisati potvrdu

Kako prodati Bitcoin na bankomatu ? - upute

- Unijeti broj Vašeg mobitela
- Unijeti primljeni (SMS) verifikacijski kod
- Odabrati “Prodaj bitcoine”
- Unijeti iznos
- Poslati bitcoine na predstavljeni QR kod
- Uzeti gotovinu
- Ispisati potvrdu o obavljenoj transakciji

BitAccess uređaji imaju prikazanu kupnju i prodaju Bitcoina u slikama, a instalirani su u Zagrebu i Rijeci. U Hrvatskoj se Bitcoin – bankomati nalaze na tri lokacije, a to su: Zagreb, Split i Rijeka – svugdje po jedan, dok recimo BiH ima samo jedan takav bankomat, Srbija dva, a Slovenija osam.



Graf 1 Gustoća Bitcoin bankomata u svijetu

Izvor: Izrada autora prema: https://www.bitcoin.com/

Moguća je i osobna prodaja, no nije dostupna svima i sa sobom nosi probleme povjerenja između prodavatelja i kupca, a većinom je dostupna samo u velikim gradovima. Pri ovakvim osobnim prodajama moguće je postići i najnižu moguću cijenu transakcije i do određene mjere ostati anoniman. Također tu su i internetske stranice preko kojih se može pronaći partner za trgovinu, poput „Find your people“ i „Meetup“.

I na kraju potrebno je navesti da je Bitcoin vodeća kriptovaluta te da se prema njoj obračunava vrijednost svih ostalih kriptovaluta. Prema tome tržišna kapitalizacija Bitcoina na dan 19. kolovoza 2018. godine bila je 111.102.743.320 $.



Slika 11 Tržišna kapitalizacija kriptovalute Bitcoin

Izvor: https://coinmarketcap.com/

5. MOGUĆI UČINCI DALJNJEG RAZVOJA KRIPTOVALUTE

Prije bilo kakvih predviđanja daljnjih učinaka i razvoja kriptovaluta potrebno je zastati i vidjeti gdje se sad nalaze kriptovalute, te kakav je njihov ekonomski i pravni aspekt, razloge njihova korištenja, prednosti i vrijednosti.

5.1. Ekonomski aspekt kriptovaluta

Jedna od glavnih karakteristika kriptovaluta je ta da nastoje biti decentralizirane, odnosno ne biti pod kontrolom države. No, ipak svaku kriptovalutu treba netko izdati (osmisliti). No, kad je riječ o kriptovalutama njihova centraliziranost se odnosi na smisao postojanja autoriteta od strane izdavatelja, a ne na centraliziranost u smislu izvedbe tehničkog rješenja.

Ključna prednost kriptovaluta koja se najviše ističe je njena neovisnost od klasičnih institucija – centralnih banaka i kontrola novca – pitanje inflacije u smislu nekontroliranog „tiskanja“ novca. Većina kriptovaluta ima unaprijed određenu – transparentnu ponudu novca, a ona je određena tehničkim putem poput rudarenja što smo vidjeli kod bitcoina ili auto – regulacijom pri stvaranju novih blokova u Blockchain sustavu.

Pri procjeni pojedine valute opet treba odgovoriti na pitanje inflacije. Ako uzmemo kriptovalute, gledajući ih pojedinačno većina njih pošto ima unaprijed programirane – određene količine jedinica i ako dođe na primjer do gubitka jedinica iz sustava zbog recimo tehničkog kvara, onda kriptovalute i dalje pokazuju stabilne trendove.

Ako i dođe do inflacije u pojedinom slučaju ona je u potpunosti predvidljiva.

Treba postaviti i pitanje inflacije na cijelo tržište digitalnih valuta. Digitalne valute na tržištu djeluju u sinergiji. Treba napomenuti da se stalno pojavljuju i nove valute i imaju sve značajniju tržišnu kapitalizaciju i sve veća vrijednost se pohranjuje u zajedničko tržište. Kakvi su onda ukupni zajednički efekti nastali pod utjecajem svih aktivnih valuta?!

Dolazimo do toga da nema svojevrsnog faktora sigurnosti i diferencijacije pojedinih država i njihovih ekonomija kao kod klasičnih valuta i onda se s pravom možemo zapitati utječe li svaka pojava nove digitalne valute na cijenu svih ostalih.

Razlike među kriptovalutama su najčešće posljedica nekih tehničkih specifičnosti i zbog toga među kriptovalutama postoji značajan faktor supstitucije.

Sigurnosni propusti u pojedinim tehničkim sustavima mogu uzrokovati značajne gubitke vrijednosti, ali i nestajanje tih valuta. Prema dosadašnjim trendovima većina kriptovaluta kada skupi određenu kapitalizaciju nastavlja rasti i pratiti zajednički trend. Bitcoin je vodeća kriptovaluta koju prati izniman rast alternativnih digitalnih valuta.

5.2. Pravni aspekt

U Republici Hrvatskoj virtualne valute nisu zakonsko sredstvo plaćanja, a ne spadaju niti u devize. Prema Zakonu o platnom prometu ne možemo izvršiti platne transakcije, a platnom uslugom ne možemo smatrati trgovanje i plaćanje virtualnim valutama. " Organizacije ili pojedince koji izdaju virtualne valute ili njima trguju nije licencirala Hrvatska narodna banka, niti ona nadzire njihovo poslovanje, kao ni bilo koja druga institucija u RH. " - HNB (https://www.hnb.hr/-/sto-su-virtualne-valute-) Virtualne valute su legalne ali u većini zemalja prevladava mišljenje da one ne udovoljavaju svim aspektima novca da bi se mogle koristiti u jednakoj mjeri kao i novac.

HNB - također navodi kako su " virtualne valute - bez rizika na monetarnu politiku HNB - a u smislu održavanja stabilnosti cijena i financijske stabilnosti bankovnog sustava u Republici Hrvatskoj. "

U SAD - u kriptovalute su deklarirane kao kapitalno dobro i kao kovertibilna valuta. Dok su u Australiji kriptovalute sredstvo razmjene, u Singapuru - materijalni oblici pohrane vrijednosti - zamjenjivi za dobra i usluge, u Norveškoj, Estoniji i Finskoj kriptovalute se deklariraju kao imovina.

Dok, pak za Nizozemsku, Veliku Britaniju novac je samo zakonsko i centralizirano sredstvo plaćanja, Njemačka kriptovalute ne smatra ni stranim valutama ni elektroničkim novcem, a u Austriji one nisu financijski instrument.

Prema publikacijama ECB -a - utjecaj virtualnih valuta na platni promet i tržište novca na globalnoj razini je mali, ali u stalnom porastu. Podatci za dan 14.12.2017. - bitcoin kao najpopularnija virtualna valuta - pomoću njega obavljeno je 490 000 transakcija - najveći dnevni broj transakcija u virtualnom svijetu do tada, a za usporedbu možemo uzeti 274 000 000 bezgotovinskog platnog prometa po danu u Europskoj Uniji.

5.3. Razlozi korištenja virtualnih valuta

Sa sustavom centralnih banaka i valutama kojima se svakodnevno koristimo, nameće se pitanje zašto koristiti puno nesigurnije virtualne valute. Dosta akademskih članaka navodi razloge njihova korištenja, najznačajniji su:

- Ideološki razlozi – postojanje sustava i valute, a da nisu pod kontrolom središnje banke
- Virtualna valuta dobiva funkciju pohrane vrijednosti
- Niski transakcijski troškovi bez posrednika

Naravno, tu je i špekulacija zbog čestih promjena cijena kriptovaluta. A i bitcoin se pojavio upravo nakon kriza, pa je i to razlog koji se povezuje s njegovom ekspanzijom, a znamo da u vrijeme krize ljudi gube povjerenje u banke.

Posjedovanje virtualnih valuta

ECB (2015) ističe pet načina za posjedovati virtualnu valutu:

- Kupnja virtualne valute - BitStamp i specijalizirani bitcoin bankomati
- Virtualna valuta kao nagrada za sudjelovanje u određenim aktivnostima
- Rudarenje
- Dobitak virtualne valute prilikom uplate
- Dobitak virtualnih valuta na dar

Prednosti korištenja virtualnih valuta

European Banking Authority (EBA) (2014) prednosti korištenja virtualnih valuta dijeli u dvije kategorije, a to su: individualne i ekonomske koristi, a u ovome radu one se najviše odnose na bitcoin.

Individualne koristi prema EBA – u :

- Sigurnost osobnih podataka – bankovni račun je povezan s osobnim podatcima klijenta – korisnika, dok za korištenje virtualnih valuta nisu potrebni osobni podatci
- Ograničeno uplitanje javnih vlasti – središnje tijelo poput centralne banke koje kontrolira sustav ne postoji. Tu su samo algoritam i kod koji kreiraju nove jedinice.
- Financijske inkluzije izvan EU – mogućnosti za pruzimanje ideja za poboljšanje financijskog sustava – svatko tko poznaje programske jezike može sudjelovati u njihovu poboljšanju – opensource – prema ECB –u (2015a)

Ekonomske koristi prema EBA – u:

- Transakcijski troškovi – koji prema njima ne bi trebali postojati jer nema posrednika i to je prebacivanje s računa na račun, ali ipak postoje manji transakcijskit troškovi nego kod drugih oblika plaćanja
- Vrijeme potrebno kako bi se transakcija realizirala – za bitcoin obično 10 – 60 minuta
- Sigurnost primljenih uplata – nepostojanje povratne opcije u transakciji , kada neki proizvod ili uslugu platimo ne možemo dobiti nazad jedinice virtualne valute
- Ekonomski rast – rudarenje – unaprijeđenje hardware – a – sigurnija pohrana kapaciteta.

5.4. Vrijednost virtualnih valuta

Nestabilnost virtualnih valuta je ono što se najviše povezuje s njima. Virtualne valute nisu vezane za neku stavarnu valutu, npr. kao što se stvarne valute vezuju, recimo tečaj kune vezan je za tečaj eura već je njihova vrijednost uzrokovana ponudom i potražnjom, prema objavama akademskih članaka, ali utjecaj na njih ima i špekulacija.

Prema istraživanju Ciaian (2014) potražna strana bitcoina će najviše kreirati njegovu cijenu u budućnosti jer ima utjecaj na broj obrtaja bitcoina dok je strana ponude prema njemu egzogena..

U faktore potražnje koji utječu na razinu cijena virtualnih valuta još utječu i očekivani povrat na držanje valute, rizik posjedovanja takve valute, prednosti u odnosu na posjedovanje klasičnih valuta, ideološke preferencije određene valute te troškovi pri razmjene između virtualnih i klasičnih valuta.

5.5. Rizici virtualnih valuta

Virtualne valute ne bilježe ni desetak godina postojanja pa su tako i većina njihovih problema ostali ne riješeni, a ti problemi su uglavno manifestirani kao rizici s kojima se susreću njihovi korisnici.

EBA (2014) navodi više razloga zbog kojih se stvaraju rizici korištenja virtualnih valuta. Neki od njih su:

- Anonimnost – kreiranje virtualne valute od bilo koga i korištenje od strane bilo koga
- Korištenje na globalnoj razini – ne poštivanje državnih zakona
- Odsutnost pravnih osoba
- Nedostatak definicija i standarda
- Neadekvatna sigurnost - nemogućnost prijave prijevare te nepostojanje stabilizirajućeg autoriteta.

ECB (2015) navodi četiri vrste rizika vezanih za virtualne valute, a to su: pravni rizik, kreditni rizik, rizik likvidnosti i operativni rizik, još kao mogući rizici navode se rizik od prijevare i nedostatka regulacije. Dok Finan et al. (2013) ističe kako u decentralizirani sustavima poput virtualnih valuta postoji samo operativni rizik, dok likvidni i kreditni rizik ne mogu postojati.

The Clearing House (TCH) (2014) ističe pet osnovnih vrsta rizika za korisnike virtualnih valuta:

- Krađa virtualne valute – npr. propust u sustavu
- Neautorizirano upravljanje virtualnim valutama od strane drugih
- Greška prilikom transakcije – npr. određen broj jedinica valute poslan na krivu adresu – nemogućnost povratka
- Greška u novčaniku – zaborav šifre – nemogućnost pristupa
- Nepostojanje obveze regulatora za objavom troškova transakcija virtualnih valuta

Jedan od osnovnih i najvećih rizika s kojim se mogu susresti korisnici virtualnih valuta jesu varijacije u njihovoj vrijednosti.

5.6.Povezanost virtualnih valuta i kriminalnih radnji

Mogućnost zlouporabe kripvaluta je velika. Počevši od plaćanje za izvršavanje raznih kriminalnih radnji. Financiranja terorizma, kupovine ilegalnih sredstava i dr. Kriptovalute su pogodne za ove radnje zbog njihove anonimnosti.

SilkRoad – web stranica povezana s plaćanjem djelatnosti kriminala. Slučaj kupnje droge s bitcoinima te drugih ilegalnih dobara. Za korištenje te stranice bio je potreban software pomoću kojega bi korisnici ostajali anoimni. Razdoblje postojanja web stranice 2011. – 2013. godine.

Global Drug Police Obcervatory (2013) navodi kako je stranica zatvorena u listopadu, 2013. Godine od FBI – a.

5.7.Utjecaj virtualnih valuta na politiku centralnih banaka

Postavlja se pitanje imaju li virtualne valute utjecaj na rad i politiku centralnih banaka. Prije svega da razjasnimo, imamo tri vrste virtualnih valuta, a to su: zatvorene virtualne valute,

virtualne valute s jednostrukim protokom i virtualne valute s dvostrukim protokom. Virtualne valute s dvostrukim protokom su kriptovalute poput bitcoina. Na rad centralnih banaka utječu ove valute s jednostrukim i dvostrukim protokom, ali više virtualne valute s dvostrukim protokom - kriptovalute. (ECB) (2012)

Kako bi se najjednostavnije objasnilo funkcioniranje centraliziranih i decentraliziranih virtualnih valuta možemo se reći da:

Iza centraliziranih virtualnih valuta stoji središnja institucija – centralana banka, iza te institucije stoji država i njeni zakoni,koji pak na neki način daju sigurnost, kontrolu i stabilnost toj valuti. Primjer takve valute je liden dolar.

Decentralizirane virtualne valute kreiraju se anonimo od strane bilo koga, najčešće su kreirane u određenom broju pomoću algoritama gdje se do novih jedinica dolazi tehnikama poput rudarenja. Primjer ovakve valute je bitcoin.

ECB (2015) navodi i da se kriptovalute međusobno razlikuju po:

- Transakcijama – sustavima potvrđivanja
- Matematičkim načinima obračuna podataka – algoritmima
- Fiksnoj i fleksibilnoj ponudi virtualnih valuta
- Funkcionalnoj perspektivi

5.8.Utjecaj kriptovaluta na monetatnu politiku centralnih banaka

Kada gledamo utjecaj na monetarnu politiku analiziramo utjecaj na: platni sustav, financijsku stabilnost te stabilnost cijena. Stabilnost cijena je ujedno jedan od osnovnih ciljeva ECB –a, a prema tome i HNB – a.

Mali je broj dostupnih i preciznih podataka koji se mogu analizirati za ovaj konkretni utjecaj.

Stabilnost cijena – utjecaj na očuvanje obračunske jedinice, rizik za efektivnost monetarne politike te njenu implementaciju i moguće utjecaje na informacije o monetarnim agregatima (ECB, 1998, 2012)

Ako postoji utjecaj između virtualnih valuta i realne ekonomije, prema ECB – u onda virtualne valute imaju utjecaj na brzinu kretanja novca u optjecaju, izračun monetarnih agregata.

ECB (2012) ističe da virtualne valute stvaraju novu vrijednost, recimo za bitcoin ona se rudari.

Ako smatramo da virtualne valute utječu na količinu novca, odnosno stvaraju promjenu u količini novca tada bi virtualne valute trebali smatrati novcem. Iako u prijašnjim definiranjima, napominje se da virtualne valute nemaju sve karakteristike novca.

6. ZAKLJUČAK

Rad iznosi objašnjenje kriptovaluta, tj. virtualnih valuta s dvostrukim ptotokom koje su do sada najsličnije novcu. Objašnjava se njihov nastanak i načini na koje se razvijaju te njihovi ciljevi.

Objašnjen je i utjecaj na centralne banke, njihov rad i monetarnu politiku.

Iz svega navedenoga možemo zaključiti da kriptovalute nemaju sve karakteristike koje ima klasični novac, ali ipak od tri vrste virtualih valuta one su najsličnije novcu. Zbog porasta upotrebe kriptovaluta klasične institucije su sve više zabrinute, tako da sve više istražuju načine upotrebe i nastanka virtualnih valuta. No, do sada nisu ponudile neko konkretno rješenje već su dale samo izvješća i istraživale Blockchain tehnologiju.

Može se zaključiti da su karakteristike kriptovaluta: anonimnost, decentraliziranost, izbjegavanje inflacije, tehnička pismenost.

LITERATURA

1. Ciaian, P., Rajcaniova, M., Kancs, d'A., (2015), The Digital Agenda of Virtual Currencies: Can Bitcoin become global currency. Luxembourg: European Commision, Publications Office of the European Union [Internet] Raspoloživo na: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC97043/the%20digital%20agenda %20of%20virtual%20currencies_final.pdf [15.8.2018.]
2. European Banking Authority (2014) EBA Opinion on ‘virtual currencies'. [Internet] Raspoloživo na: https://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies [15.06.2018.]
3. European Central Bank (2012) Virtual currency schemes. Frankfurt am Main: European Central Bank. [Internet] Rapoloživo na: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf [15.6.2018.]
4. European Central Bank (2015a) Virtual currency schemes - a further analysis. Frankfurt am Main: European Central Bank. [Internet] Raspoloživo na: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf [02.08.2018.]
5. European Central Bank (2015b) Monetary developments in the euro area: March 2015. Frankfurt am Main: European Central Bank. [Internet] Raspoloživo na: https://www.ecb.europa.eu/press/pdf/md/md1503.pdf [02.08.2018.]
6. European Central Bank (2015c) Monetary developments in the euro area: June 2015. Frankfurt am Main: European Central Bank. [Internet] Raspoloživo na: https://www.ecb.europa.eu/press/pdf/md/md1506.pdf [17.07.2018.]
7. European Central Bank (2015d) Monetary developments in the euro area: September 2015. Frankfurt am Main: European Central Bank. [Internet] Raspoloživo na: https://www.ecb.europa.eu/press/pdf/md/md1509.pdf [17.07.2018.]
8. European Central Bank (2015e) Monetary developments in the euro area: December 2015. Frankfurt am Main: European Central Bank. [Internet] Raspoloživo na: https://www.ecb.europa.eu/press/pdf/md/md1512.pdf [17.07.2018.]
9. European Central Bank (2016a) Monetary developments in the euro area: March 2016. Frankfurt am Main: European Central Bank. [Internet] Raspoloživo na:

https://www.ecb.europa.eu/press/pdf/md/md1603.pdf [10.07.2018.]

10. European Central Bank (2014) Monetary developments in the euro area: December 2014. Frankfurt am Main: European Central Bank [Internet] Raspoloživo na: https://www.ecb.europa.eu/press/pdf/md/md1412.pdf [02.08.2018.]
11. Garača Ž. (2007.): Informatičke tehnologije
12. Global Drug Police Observatory (2013) SilkRoad and Bitcoin.[Internet] Raspoloživo na: http://www.swansea.ac.uk/gdpo/ [18.8.2018.]
13. Nikolić N., Pečarić M. (2007): Osnove monetarne ekonomije
14. The Financial Action Task Force (2014) Virtual currencies: key definitions and potential AML/CFT risk. [Internet] Raspoloživo na: http://www.fatfgafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cftrisks.pdf [15.8.2018.]

Izvori s interneta:

1. https://coinmarketcap.com/exchanges/ripplefox/ [19.08.2018.]
2. https://data.bitcoinity.org/markets/volume/30d?c=e&t=b [20.05.2018.]
3. https://data.bitcoinity.org/markets/volume/30d?c=e&t=b [20.05.2018.]
4. https://en.wikipedia.org/wiki/Bitcoin [14.5.2018.]
5. https://rs.cointelegraph.com/news/ny-fed-economists-advanced-economies-may-not-need-crypto [01.08.2018.]
6. https://tradingeconomics.com/ [19.08.2018.]
7. https://www.bitcoin.com/ [20.05.2018.]
8. https://www.dzs.hr/ [19.08.2018.]
9. https://www.index.hr/vijesti/clanak/jedna-od-najvecih-svjetskih-banaka-priznala-da-su-kriptovalute-prijetnja-njenom-poslovanju/1029959.aspx [02.08.2018.]
10. https://www.index.hr/vijesti/clanak/spekulanti-s-wall-streeta-ocekuju-rast-cijene-zlata-i-pad-bitcoina/1028538.aspx [02.08.2018.]
11. https://www.thoughtco.com/macroeconomics-student-resource-center-1146337 [18. 07.2018.]
12. https://zimo.dnevnik.hr/clanak/sredisnje-banke-ne-mogu-i-ne-smiju-ignorirati-kriptovalute---489449.html [15.8. 2108.]
13. https://www.youtube.com/watch?v=yoaviCX4Urw [16.8.2018.]

SAŽETAK

Završni rad na temu Kriptovalute – danas i sutra donosi razvoj, upotrebu i utjecaj virtualnih valuta s dvostrukim protokom na realnu ekonomiju.

U prvom dijelu rada objašnjava se povijest novca te problemi s kojima se susreće pri upotrebi klasičnog novca. Kao odgovor na te probleme koji se uglavnom odnose na centralizirani sustav klasičnih institucija javljaju se kriptovalute.

Drugi dio rada donosi popis najznačajnijih kriptovaluta današnjice prema njihovoj tržišnoj kapitalizaciji. Vodeća kriptovaluta je bitcoin.

Bitcoin je decentralizirana kriptovaluta, ograničenog broja jedinica s ciljem izbjegavanja inflacije.

U zadnjem dijelu rada objašnjeni su apekti kriptovaluta: ekonomski i pravni te njihove prednosti i razlozi zbog kojih se mogu upotrijebiti u kriminalne svrhe. Na koncu rada donosi se utjecaj na klasične institucije poput centralnih banaka i na monetarnu politiku.

KLJUČNE RIJEČI: kriptovalute, decentralizazija, inflacija.

SUMMARY

Concluding to this work on the topic of Cryptocurrecies - today and tomorrow, the paper brings us development, use and impact of virtual currency with double flow to the real economy.

The first part of this work explains the history of money and the problems of using the classic money. As response to these problems which are mainly related to the centralized system of classical institutions comes cryptovalutes..

The second part of the work presents a list of the most significant cryptocurrencies of today based on their market capitalization. The leading cryptovcurrency is bitcoin.

Bitcoin is a decentralized cryptocurrency with a limited number of units which has the aim of avoiding the inflation.

In the last part of the work about the cryptocurrencies a prominent parts about the economic and legal aspects, their advantages and the reasons why they can be used for criminal purposes. At the end of the paper the most important is the influence of cryptocurrency on classical institutions such as central banks and their monetary policy.

KEY WORDS: cryptocurrencies, decentralization, inflation.