Univerza v Ljubljani

Pravna Fakulteta

EKONOMSKA ANALIZA DECENTRALIZIRANIH KRIPTOGRAFSKIH VALUT

(seminarska naloga)

Avtor: Kristian Ilijevski

Ljubljana 2015

Kazalo

Uvod

Finančna kriza, katero smo doživeli leta 2009 in zategovanje pasov držav po svetu v nedogled, do nestabilnosti posameznih držav zaradi prezadolženosti. Skupna točka vseh globalnih trgov so centralizirane institucije, ki upravljajo monetarno politiko. Kot kontrast tem instutucijam bom predstavil sistem, ki je trenutno še v svoji infantilni fazi, ki pa je dolgoročno veliko bolj predvidljiv in omogoča akterjem na trgu, da prosto izberejo mehanizem plačevanja na katerega se lahko zanesejo in z svojo izbiro dejansko oblikujejo prihodnji razvoj, kar bi osredno pripeljalo do bolj učinkovite alokacije sredstev.

V tej seminarski nalogi se bom posvetil ekonomski analizi relativno mlade tehnologije, ki pa se je od njenega nastanka že bistveno spremenila. Glede na to, da konkretne zakonodaje glede o teh tehnologijah še ni se bom usmeril v bolj abstraktno presojo.

Prvi protokol pod imenom Bitcoin je začel z delovanjem januarja leta 2009 (bolj natančno 3.1.2009 ob 18:15:05)[1] na njegovi zasnovi oziroma osrednji ideji se je do zdaj razvilo že več tisoč alternativ, trenutno ima pa neko relevantno tržno vrednost 671 različnih valut. Iz teh razlogov sem se odločil za naslov, ki zajema vse te valute in ne zgolj Bitcoin. V prvem delu bom poskusil bralcu čim bolj približati tehnično delovanje teh valut saj menim, da je razumevanje osnove delovanja bistveno za razumevanje celotne seminarske naloge. Treba pa je poudariti, da se je beseda valuta ustalila v internetni skupnosti, ki obdaja vsako od njih, vendar pa je to zelo ozko pojmovanje protokolov, katere opisuje. Dejansko gre za sui generis obliko finančne dobrine, lahko se obnaša kot valuta ali kot neke vrste vrednostni papir. Valuta je zgolj ena od aplikacij, ki jih obravnavani protokoli omogočajo. V svojem jedru gre za mehanizem, ki odstrani potrebo po zaupanju tretji osebi pri prenašanju lastništva nad določenim premoženjem.

[1] https://blockchain.info/block-index/14849

Glede na to, da gre za mlado tehnologijo, ki živi na internetu in katera je distribuirana pod odprto kodno licenco ter si je posledično ne lasti nihče[2] sledi, da literature na tem področju praktično ni, zato bodo viri te seminarske naloge predvsem elektronski in se lahko zelo hitro spreminjajo oziroma zastarajo z nadaljnim razvojem tehnologije. Prav tako naj omenim, da bom tematika predvsem v luči emisije denarja in opravljanju transakcij in manj o dodatnih storitvah, ki gradijo na vrh tega.

[2] http://opensource.org/licenses/MIT

1. Delovanje decentraliziranih kriptografskih valut

Delovanje decentraliziranih kriptografskih valut bom orisal na primeru protokola Bitcoin saj je o njem (kot prvem primeru) na voljo največ virov in do zdaj največ izkušenj uporabe v svetu. Ostali protokoli sledijo Bitcoin-u, nekateri imajo zgolj drugo ime in uporabljajo praktično enako programsko kodo ali pa imajo spremenjenih le nekaj karakteristik in je delovanje v osnovi še vedno zelo podobno.

Bitcoin protokol sestavlja več različnih tehnologij, katere vsaka zase ne predstavljajo nič novega in obstajajo že vrsto let, tehnologije brez katerih si svet kot ga poznamo danes težko predstavljamo. Na primer, prijava v spletno banko s pomočjo certifikata v zaledju uporablja enake mehanizme privatnih-javnih ključev kot Bitcoin protokol za podpisovanje transakcij. Ena bistvenih inovacij je tako imenovana veriga blokov (ang. blockchain), katera predstavlja zapisnik vseh transakcij v omrežju od začetka delovanja, primerjamo jo lahko z tako imenovano glavno knjigo katera je značilna za banke. Zapisnik se počasi povečuje z vsakim novim dodanim blokom, vsak blok vsebuje transakcije, ki so se zgodile v določenem časovnem intervalu. Kopijo tega zapisnika hranijo vsi uporabniki v omrežju, ki na svojem računalniku poganjajo polno različico Bitcoin programske opreme.[3]

V primerjavi z načinom delovanja obstoječega finančnega sistema je Bitcoin decentraliziran, to pomeni, da ni centralne avtoritete niti v pravnem niti v dejanskem smislu, ki bi imela kakršnokoli možnost vplivati na delovanje protokola. S tem tudi ni nikogar, ki bi odločal kdo sme in kdo ne sme uporabljati omrežja, dostop je odprt za vse. Uporabnik, ki se želi priključiti v omrežje potrebuje le povezavo na internet in računalnik, ki je sposoben poganjati programsko opremo Bitcoin.

Za razumevanje kako omrežju uspe doseči decentralizacijo in kljub temu uspešno opravljanje transakcij v katere ljudje zaupajo, je treba razumeti kako v obtok prihajajo nove enote valute. Skozi postopek kateremo pravimo rudarjenje (anologija z rudarjenjem zlata) se v povprečju na 10 minut v

[3] Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System

omrežju pojavijo dodatne enote valute kot nagrada rudarjem. V prvih štirih letih je to bilo 50 bitcoin-ov, v času pisanja te seminarske naloge je 25 bitcoin-ov, kmalu pa bo padlo na 12,5 bitcoin-ov. Vrednost se prepolovi na 4 leta in tako se bo nadaljevalo dokler ne bo v obtoku vseh 21 milijonov bitcoin-ov, to količino bo omrežje doseglo okrog leta 2150.

Funkcija rudarjenja je trojna, prvič v obtok prihajajo nove enote bitcoin-ov, drugič skozi nagrajevanje rudarjev se doseže motivacija, da to počne čim več ljudi in s tem omrežju prispeva veliko procesorske moči in s tem varuje omrežje pred morebitnimi poskusi napadov in tretjič gradi se zapisnik transakcij, t.i. veriga blokov.

Rudarjenje je v osnovi reševanje matematične uganke, uganka temelji na SHA256 zgoščevalni funkciji. Za to uganko je značilno to, da jo je možno rešiti le z poskušanjem saj omenjena funkcija za določeno vhodno vrednost izda povsem naključno vrednost. Da je rudarjenje donosno torej potrebujemo strojno opremo, ki je zmožna na časovno enoto narediti čim več poskusov in pri tem porabi čim manj električne energije. Ker se omrežju priključuje vedno več rudarjev, računalniška tehnologija pa hitro napreduje se Bitcoin protokol prilagaja in sicer težavnost uganke se povečuje. Cilj omrežja je, da se blok reši na povprečno 10 minut, če se to začne dogajati hitreje ali počasneje se težavnost omrežja prekalibrira, da doseže cilj 10 minut.

Pomembna lastnost te uganke je v tem, da jo je težko rešiti, ko pa je enkrat rešena je zelo enostavno preveriti, če je rešitev pravilna. Dobra analogija je igra sudoku, rešiti jo je težko, ko je pa enkrat rešena lahko hitro preverimo, da ni prišlo do goljufije. Torej ko eden od rudarjev reši blok in ga priključi verigi blokov vsi ostali preverijo njegovo rešitev in takoj v naslednjem trenutku začnejo reševati naslednji blok in tako se tekmovanje nadaljuje. V rešeni blok pa rudar hkrati vključi vse transakcije, ki so se zgodile v omrežju od rešitve prejšnjega bloka.[4]

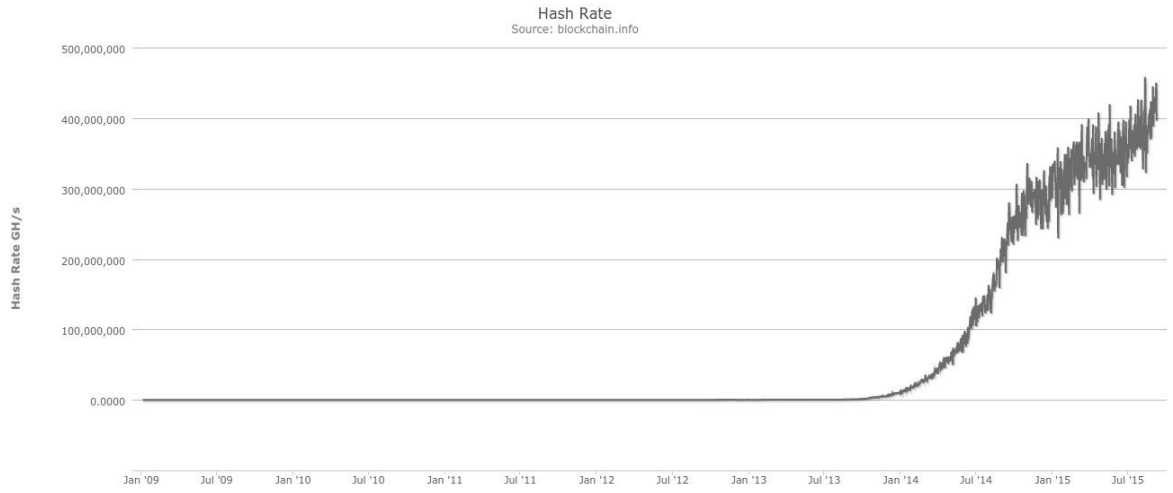
[4] Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System

Na ta način na približno 10 minut v omrežju dosežemo konsenz o trenutnem stanju bitcoin-ov v omrežju, brez nadzora centralne avtoritete. Ker je Bitcoin omrežje kolektivno najmočnejši super računalnik na svetu (vendar zgolj pri preračunavanju SHA256 zgoščevalne funkcije), za več sto krat prekaša seštevek petstotih najmočnejših super računalnikov na svetu, ga je praktično nemogoče napasti.

Za boljšo predstavo, trenutna moč bitcoin omrežja je 5.255.425 petaFLOP na sekundo[5], trenutno najmočnejši super računalnik na svetu je kitajski Tianhe-2, ki premore 33,86 petaFLOP na sekundo[6]. Bitcoin omrežje je po teh številkah približno 160.000 krat močnejše od najmočnejšega super računalnika.

Hkrati pa je pred napadom omrežje zavarovano z osnovno logiko teorije iger. Akterju, ki bi zbral večino procesorske moči se ne izplača napasti omrežja saj bi z uničenjem omrežja oziroma porušenjem zaupanja vanj, s tem samo izgubi svojo investicijo v strojno opremo, ki je zmožna zadostnega preračunavanja. Tak akter bo rajši rudaril nove bitcoine in s tem zaslužil.

Trend naraščanja procesorske moči omrežja Bitcoin:[7]



Eksponentni porast rudarske moči se je zgodil z izdelavo posebnih naprav, katere poznamo pod akronimom ASIC (angl. Aplication Specific Integrated Circuit - slov. Integrirana vezja za specifično

[5] http://bitcoinwatch.com/
[6] https://en.wikipedia.org/wiki/Tianhe-2
[7] https://blockchain.info/

aplikacijo). V svojih začetkih, kjer je krivulja na grafu še blizu ničle, je rudarjenje bilo izvajano na običajnih domačih računalnikih, uporabljal se je zgolj procesor. Kasneje se je rudarjenje preselilo na grafične procesorje, saj so le ti nekajkrat bolj učinkovito preračunavali SHA256, še vedno pa je to bila strojna oprema katero vsebuje vsak domači računalnik. ASIC naprave pa so procesorje in grafične kartice pustile v prahu, na watt porabljene moči dosegajo neprimerno boljše rezultate. Od takrat je poskok rudarske moči in s tem težavnost omrežja dosegla eksponentno rast, ki se še danes nadaljuje.

S tem se pojavijo dvomi v decentraliziranost omrežja o katerih bom več povedal kasneje. Bitcoin je dosegel točko, kjer je ekonomija obsega prevladala in za običajnega uporabnika rudarjenje ni več donosno. Kljub temu zaupanje v omrežje ostaja kar je razvidno predvsem iz povečevanja števila uporabnikov in zadostnem povpraševanju, ki kljub močni emisiji valute še vedno ohranja ceno.

2. Pravo in decentralizirane kriptografske valute

Pravo je tradicionalno vedno nekaj korakov za razvojem tehnologije in se pojavi z zamikom, ko pa govorimo o internetnih tehnologijah, ki se razvijajo najhitreje, je teh korakov še nekaj več. Bistveno vprašanje, ki se odpira pri teh disruptivnih tehnologijah je, ali je pravo sploh še relevantno oziroma ali je sploh lahko relevantno. Govorim o pravu, kot ga najširše razumemo danes v moderni družbi, to je pravo katerega ustvari centralna suverena državna oblast v obliki ustave, zakonov in drugih predpisov.

Kot v zloglasnem primeru priljubljene spletne strani za izmenjavo datotek “The Pirate Bay”, kjer je pravosodje že večkrat izvedlo izklop in zaplembo strežnikov, se ta spletna stran vedno znova pojavi, seveda v drugi državi kjer je druga jurisdikcija in postopek se znova prične.

Tehnologije, katere opisujem v tej seminarski nalogi imajo to specifiko, da nimajo točke izvora, nimajo centralne avtoritete, ni enega strežnika na določenem teritoriju ali določene osebe. Torej oblast ne more priti niti do te točke, kot je v primeru “The Pirate Bay” saj ni nikogar, katerega bi privedli pred sodišče.

Internet se že sam po sebi izmika oblasti zaradi svojega mednarodnega elementa že pri običajnem centraliziranem strežniškem modelu, ko pa internetu dodamo dimenzijo decentraliziranih tehnologij, poznano tudi pod angleškim izrazom "peer to peer" (od uporabnika do uporabnika) pa je nadzor praktično nemogoč.[8]

Pri decentraliziranih kriptografskih valutah gre še za dodatno lastnost, gre za obliko denarja, pri kateri ni potrebno podati davčne številke ali številke osebnega dokumenta, da bi ga lahko uporabljali in s tem je uporabnik neznan, čeprav lahko vsak v javnem zapisniku vidi, da se izvajajo določene transakcije ni nikjer podano kdo je ta oseba.

Nadzor še dodatno oteži dejstvo, da sploh ne potrebujemo fizičnega nosilca, v primeru bitcoin-a si lahko niz besed iz katerih zgeneriramo privatni ključ preprosto zapomnimo in s tem vsakomur preprečimo dostop. Kot primer lahko navedemo prehod državne meje, za katero veljajo omejitve glede prenosa gotovine, zgoraj opisana lastnost omogoča, da kdorkoli preko meje prenese ogromne zneske denarja brez, da bi kdo sploh karkoli opazil.[9]

Zaradi teh lastnosti se odpira vprašanje, kako se bodo države skozi zakonodajo odzvale na te tehnologije, tako v primerih iz kazenskega prava kot pri običajnih davčnih postopkih. Te tehnologije rušijo ene glavnih mehanizmov s katerimi države ohranjajo svojo oblast, to je z možnostjo zaplembe premoženja, zamrznitve transakcijskih računov in podobno. In nenazadnje tudi monopol nad izdajanjem denarja.

Kot je bilo rečeno že v uvodu, smo v zgodnjih fazah teh tehnologij in primerov resnejše regulacije zaenkrat še ni.

Pojavlja se pa posebna oblika prava, to je pravo, ki je integrirano v same protokole kot sklop pravil v skladu s katerimi omrežje in njegovi uporabniki funkcionirajo. Koncept zaupanja v oblikah kot ga poznamo v večini transakcij postaja nerelevanten.

[8] https://en.wikipedia.org/wiki/Peer-to-peer
[9] https://en.bitcoin.it/wiki/Brainwallet

3. Primerjava storškov decentraliziranih kriptografskih valut z obstoječim svetovnim finančnim sistemom

Kot vsak sistem katerega pozna človek tudi finančni sistem za svoje vzdrževanje zahteva določene stroške. Glede na to, da skozi denar vrednotimo vse ostale stroške v družbi, bi bilo idealno, če bi bili stroški povezani z transakcijami čim bližje ničli, tako bi imeli najbolj realno sliko in toliko več bi šlo za dejansko blago ali storitev katero plačujemo, družba bi operirala na višji ravni učinkovitosti. V primerjavi se bom dotaknil pomembnejših vidikov, predvsem tistih, ki jih je na tej točki razvoja sploh mogoče opredeliti. Primerjava je omejena zgolj na jedro delovanja obeh sistemov in ne na dodatne plasti storitev, ki se razvijajo na njuni podlagi. Kot jedro je mišljeno pošiljanje določene količine vrednosti iz točke A v točko B.

Čeprav navidez, pri izročitvi bankovca osebi x v zameno za neko blago ne občutimo nikakršnih stroškov se v ozadju dogaja veliko več. Če primeroma naštejem nekaj vidikov, kot so nabava papirja in črnila, tiskanje bankovcev, eliminiranje obrabljenih bankovcev in zamenjava z novimi, njihov transport do banke, prevoz z blindiranim vozilom z oboroženimi varnostniki do vsakega bančnega avtomata, plače zaposlenih v bankah, klimatiziranje in ogrevanje delovnih prostorov, stroški elektrike bančne infrastrukture, stroški vzdrževanja in posodabljanja bančnih strežnikov, storški državne kontrole in regulacije in še bi lahko naštevali. Pri plačilih z plačilnimi karticami lahko dodamo še stroške kraje in zlorab podatkov s posledico neavtoriziranih plačil in podobno. Vsemu temu pa lahko še dodamo vplive na okolje v obliki onesnaženja in izpuščanja ogljikovega dioksida v ozračje.

Torej, če celostno pogledamo na situacijo bi z eliminiranjem določenih zgoraj omenjenih elementov na koncu v zameno za tisti bankovec dobili nekaj več blaga saj bi manj zapravili za samo

transakcijo. Dodamo pa lahko še dejstvo, da je trenutno le del sveta opremljen z finančno infrastrukturo, da bi omogočili dostop do sodobnega finančnega sistema celotnemu svetu bi bilo potrebno všteti še stroške izgradnje infrastrukture.

Pri decentraliziranih kriptografskih valutah bi lahko našteli predvsem stroške elektrike katero rudarji porabijo za preračunavanje, stroške internetnega priključka, stroške izgubljenih, pozabljenih ali ukradenih privatnih ključev in s tem izgubo enot valute.

Da lahko opravimo del primerjave z decentraliziranimi kriptografskimi valutami moram izpostaviti ključno razliko v načinu doseganja varnosti v obeh sistemih. Prvi, torej obstoječi finančni sistem črpa varnost v izključitvi nepooblaščenih oseb iz sistema. Na primer banka skrbno hrani zapise stanj svojih klientov, nepooblaščena oseba, ki bi pridobila dostop bi lahko denar prenakazala kamorkoli drugam. Hkrati to vodi do tega, da je komunikacija med dvema bankama šifrirana, komunikacija med osebo, ki uporablja spletno bančništvo in banko, ki storitev ponuja je prav tako šifrirana in tako naprej. Če napadalcu uspe ujeti ta pogovor in ga dešifrirati je varnost izgubljena, pride lahko do kraje.

Decentralizirane kriptografske valute svojo varnost črpajo v odprtosti. Sistem je odprt za kogarkoli, podatki o stanjih so javni, vsak uporabik, ki poganja ustrezno programsko opremo in s tem služi kot člen v decentraliziranem omrežju hkrati hrani celotno kopijo glavne knjige stanj vseh uporabnikov. Rudarji z svojim tekmovanjem konstantno preverjajo, da glavne knjige nihče ni samovoljno spreminjal, če to odkrijejo tako kopijo glavne knjige preprosto ignorirajo. Omrežje vsaka trenutek preplavljajo transakcije katere za sabo nimajo kritja, torej konstantno prihaja do napadov, če omrežje po preverbi kopije glavne knjige o kateri se strinja večina omrežja v tistem trenutku ugotovi, da transakcija ni legitimna jo zavrže.

Iz te primerjave zaprtega centraliziranega sistema in odprtega decentraliziranega lahko izpeljemo, da je z slednjim povezanih bistveno manj stroškov saj varnosti omrežja ni potrebno namenjati posebne

pozornosti ali vzpostavljati dodatnih mehanizmov ali preganjati ljudi, ki sistem napadajo saj ima sistem sam v svojem jedru delovanja to lastnost, da tega ne potrebuje.

Naslednji vidik je v ljudeh, ki jih potrebuje vsak od sistemov za svoje vzdrževanje, kar predstavlja svoj sklop stroškov. Ta primerjava bo precej kratka, saj v svetu decentraliziranih kriptografskih valut ni zaposlenih ljudi v pravem pomenu besede. Gre za mednarodni pojav razvijanja odprtokodne programske opreme, kjer veliko ljudi prispeva k razvoju, največkrat prostovoljno v svojem prostem času. V večini primerov imajo ti ljudje v lasti določeno količino valute v katero prispevajo svoje veščine in čas in želijo, da bi v prihodnosti pridobila na vrednosti.

Na tej točki naj menim, da Bitcoin omrežje s trenutno procesorsko močjo zadostuje za zavarovanje omrežja tudi v primeru, če bi ga uporabljal vsak prebivalec na tem planetu. Prilagoditve bi morale biti narejene v protokolu za doseganje večjega števila transakcij na sekundo vendar vsak dodatni uporabnik ne pomeni dodatnih stroškov. Nadalje primerjava Bitcoin omrežja z obstoječim finančnim sistemom v konkretnih številkah iz vidika porabe energije, podatki iz leta 2013[10].

	Letni stroški
Izdelava fizičnega denarja	28 milijard $
Poraba elektrike bančnega sistema	63,8 milijard $
Bitcoin rudarjenje	0,66 milijard $

	Porabljena energija (GJ)	Emisije CO2 (t)	Emisijski trend
Izdelava fizičnega denarja	39,6 milijonov	6,7 milijonov	narašča
Poraba elektrike	2340 milijonov	390 milijonov	narašča

[10] Hass McCook: An Order-of-Magnitude Estimate of the Relative Sustainability of the Bitcoin Network

bančnega sistema			
Bitcoin rudarjenje	3,3 milijone	0,55 milijonov	upada

Iz vidika vplivov na okolje emisijski trend Bitcoin rudarjenja upada saj so integrirana vezja, ki se uporabljajo za rudarjenje bitcoin-ov podvržena Moorovem zakonu[11]. Interirana vezja so z razvojem tehnologije vedno bolj energjsko učinkovita in tako puščajo na okolju vedno manjši odtis.

Podatkov ni dovolj, da bi prišli do definitivnih zaključkov. Trenutni finančni sistem sestavlja več komponent. Nekatere od njih se zrcalijo tudi v svetu decentraliziranih kriptografskih valut in s tem za seboj potegnejo več sredstev kot zgolj rudarjenje, ki je v osnovi temeljni nivo na katerem se gradijo druge finančne storitve. Vendar pa po grobi oceni teh podatkov lahko ugotovimo, da Bitcoin omrežje doseže enak oziroma boljši učinek z bistveno manj sredstvi.

4. Prosti trg denarja

Prvič v zgodovini človeštva je mogoče opazovati popolnoma prosti trg denarja, vrednost posamezne kriptografske valute določa zgolj ponudba in povpraševanje igralcev na trgu, brez poseganja, brez določanja obrestnih mer in količine denarja v obtoku. To regulacijo nadomeščajo protokoli z svojimi integriranimi fiksnimi navodili, katera pa so lahko podvržena spremembam ob pogoju, da obstaja konsenz med večino uporabnikov.

Hkrati lahko torej opazujemo razvoj določene vrste demokracije, kjer vsak uporabnik na nek način glasuje z izbiro programske različice katero bo sam poganjal. Znotraj spletne skupnosti kriptografskih valut pa se vedno bolj pojavlja politika v posebnem pomenu beseda. Gre za dolge razprave na spletnih forumih o tem v katero smer naj se določena kriptografska valuta razvija in kako odpraviti

[11] https://en.wikipedia.org/wiki/Moore%27s_law

določene probleme, na koncu pa vedno prevlada dejanski konsenz na podlagi števila aktivnih klientov določene različice programske opreme, ki vsebuje ali ne vsebuje prerekanih sprememb.[12]

Vse to pa se dogaja na globalni ravni, brez ozira na lokalne jurisdikcije. Programski jezik in matematični zakoni kriptografije, v zaledju teh valut je skupen celotni internetni skupnosti. Ustvarja se neka nova plast organizacije in sprejemanja odločitev, ki gre popolnoma mimo obstoječih mehanizmov sprejemanja odločitev kot jih poznamo danes, na primer preko izvoljenih predstavniških teles, ki podpisujejo in ratificirajo take in drugačne mednarodne pogodbe.

Kot je bilo omenjeno v uvodu, je trenutno aktivnih 671 različnih kriptografskih valut, vsaka ima določeno posebno lastnost. Potrebno je omeniti, da ves čas nastajajo nove, nekatere od obstoječih pa izumrejo zaradi pomankanja uporabnikov. Ker se na tem trgu obračajo precejšnje količine denarja se pojavljajo valute ustvarjene zgolj z namenom hitrega zaslužka, cena hitro poskoči, v nekem trenutku pa trg preplavi prodaja in valuta izgubi svojo vrednost. Kot na vsakem drugem področju, tudi tukaj velja caveat emptor. Nekatere so deflacionorne kot je primer bitcoina, druge so inflacionorne. Med seboj ves čas tekmujejo z različnimi dodanimi funkcijami. Bitcoin še vedno močno prevladuje, zaenkrat ohranja prvo mesto in kakor kaže bo tam še nekaj časa ostal. Kaj bo pa prinesla prihodnost na tem hitro razvijajočem področju pa ni znano. V nadeljevanju navajam nekaj primerov.

4.1. Litecoin

Po nastanku takoj sledi Bitcoin protokolu. Zgornja meja količine je 84 milijovnov litecoin-ov v primerjavi z 21 milijoni bitcoin-ov. Čas potrditev oziroma povprečni čas v katerem rudarji rešijo bloke transakcij je 2,5 minuti v primerjavi z 10 minutami z Bitcoin protokolom. Algoritem reševanja blokov je namesto SHA256 tako imenovani scrypt algoritem, ki zahteva druge vrste strojno opremo za rudarjenje.

[12] Travis Parton: The Bitcoin Revolution: An Internet of Money 99.

4.2. Dash[13]

V začetku se je imenoval Darkcoin, pred kratkim je bil preimenovan v Dash (Digital Cash). Glavna funkcija tega kovanca je njegova popolna anonimnost v omrežju. Tudi tukaj imamo javno glavno knjigo transakcij vendar pa se pri pošiljanju od osebe A do osebe B ta transakcija pomeša z ostalimi v omrežju in posledično je nemogoče oziroma zelo težko ugotoviti komu je A pošiljal. Za rudarjenje uporablja x11 algoritem, ki ima določene lastnosti, ki preprečujejo morebitno dolgoročno centralizacijo rudarjenja.

4.3. Peercoin[14]

Podobno kot Bitcoin temelji na SHA256 rudarjenju, vendar le v začetni fazi z namenom zagotovitve enakomerne distribucije po svetu. V določeni fazi rudarjenje ne bo več mogoče in bodo novi kovanci prihajali v obtok uporabnikom, ki imajo pozitivno stanje v svoji digitalni denarnici v obliki obresti. Ta valuta zgornje meje količine nima, predvidena je konstantna 1% stopnja inflacije.

4.4. Safecoin[15]

Valuta katere sploh ni mogoče rudariti. V obtok je prišla kot IPO za financiranje projekta decentraliziranega interneta. Valuto je bilo mogoče kupiti v zameno za bitcoine in v tem trenutku nima druge posebne uporabne vrednosti kot zgolj naložba v projekt Maidsafe. Gre za programsko opremo, ki bo nezaseden prostor na računalniku uporabnika delila z internetom, ta prostor bodo drugi uporabniki lahko uporabljali. Valuta za najem tega prostora pa naj bi bila Safecoin. Bistvo projekta je, da skozi

[13] Evan Duffield, Daniel Diaz: Dash: A PrivacyCentric CryptoCurrency
[14] Sunny King, Scott Nadal: PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake
[15] https://github.com/maidsafe/Whitepapers/blob/master/Project-Safe.md

decentralizacijo shranjevanja podatkov z visoko stopnjo varnosti in anonimizacije omeji oziroma onemogoči možnost vpogleda v podatke centralni avtoriteti.

4.5. Ethereum[16]

Bolj kot valuta je neke vrste programska platforma za razvijanje dodatnih aplikacij. Izvorna ideja je, da se na decentraliziranem modelu verige blokov poleg funkcije valute uveljavijo tudi drugi načini prenašanja vrednosti. Razvijalci uporabljajo izraz "pametne pogodbe", kar zelo poenostavljeno pomeni, da je mogoče sprogramirati pogodbo, da sama prenese določeno vrednost od ene pogodbene stranke k drugi v trenutku, ko pogodbena stranka izpolni določeno obveznost.

Navedeni primeri so zgolj za ilustracijo raznolikosti med različnimi kriptografskimi valutami. Vsaka od alternativ ima določen ciljni krog uporabnikov in področji uporabe. Na primer pri plačevanju kosila v restavraciji bomo rajši plačali s hitrejšo valuto, ki ima krajši čas potrditve, saj je nepriročno čakati 10 minut na potrditev transakcije v primeru Bitcoin-a. Po drugi strani je bitcoin primernejši za prihranke, zaradi svoje deflacionarne narave je dober hranilec vrednosti. Za zakup prostora na spletu bi se uporabljalo zgoraj omenjeni Safecoin, in tako naprej. Teoretično bi ekonomsko dosegli najbolj optimalno točko, če bi za vsako dovolj specifično področje uporabili vrsto plačila, ki temu ustreza. Hkrati pa dosegli pretvorbo med temi plačili z čim manjšim trenjem.

Za vse kriptografske valute je značilno, da se z njimi trguje na različnih izmenjevalnicah. Prehod iz ene valute v drugo je izjemno enostaven in lahko traja le nekaj sekund. Torej ko uporabnik enkrat vstopi v prostor kriptografskih valut je popolnoma svoboden pri izbiri valute, ki jo potrebuje.

[16] https://github.com/ethereum/wiki/wiki/White-Paper

5. Primer wikileaks

Kot primer koristne uporabe decentralizirane kriptografske valute navajam primer wikileaks. Po razkritju razne tajne dokumentacije, ki razkriva sporno ravnanje države so finančne institucije pod pritiskom ameriške vlade blokirale prejemanje donacij preko običajnih plačilnih kanalov kot so kreditne kartice in paypal. Debata o tem ali je razkritje dokumentacije iz strani wikileaks primerno je preobširna za to seminarsko nalogo.[17] Moje mnenje je, da je primerno iz vidika vzpostavljanja ravnovesja med prebivalci in državno oblastjo, postavlja omejitev državi, da ne gre predaleč pri uporabi svoje moči.

Odziv države pa bi lahko opredelili kot sporen. Država je lahko zgolj s političnim pritiskom, brez posebnega postopka dosegla blokado donacij namenjenih wikileaks. Po eni strani to kaže na šibkost centraliziranih sistemov, katere je mogoče s pritiskom na določeno točko hitro onemogočiti, manipulirati, cenzurirati ali prirediti. Po drugi strani pa se odpira vprašanje, če je tako moč sploh pamento zaupati neki entiteti.

V času primera wikileaks je Bitcoin protokol že bil v delovanju in z njegovo pomočjo je organizacija lahko nemoteno prejemala donacije svojih podpornikov, do tega dne je bitcoin naslov wikileaks prejel količino transakcij, ki v skupni količini izraženi v vrednosti evra znaša preko 850.000 EUR[18].

Primer kaže na boj med (pre)močno državo in posamezniki, ki se ji zoperstavijo. Decentralizirane valute omogočajo posameznikom, da dobijo podporo iz globalne skupnosti neposredno. Dejansko odpira trg človekove svobode in neomejenega izražanja sebe. Kot je že internet zagotovil možnost, da ima vsak posameznik, če to želi, globalno občinstvo, dodajajo kripto valute še dodatni nivo, da posameznik prejme plačilo od globalne skupnosti, če ljudje ocenijo da je sporočilo, katerega človek podaja vredno plačila.

[17] http://www.forbes.com/sites/jonmatonis/2012/08/20/wikileaks-bypasses-financial-blockade-with-bitcoin/
[18] https://blockchain.info/address/1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v

6. Mikro transakcije

Pomembno področje, ki ga na novo razvijajo so mikro transakcije preko spleta. Zaradi odsotnosti mehanizma, ki bi dovolj učinkovito in s tem z nizkimi transakcijskimi stroški dosegel prenos vrednosti primeroma v višini nekaj euro centov se to področje do sedaj ni uspešno razvijalo. Transakcija z kreditno kartico mora biti vredna vsaj nekaj eurov, da se nam izplača. Iz tega razloga so spletne strani pričele svoje stroške pokrivati z nameščanjem sporočil oglaševalcev. Večje družbe pa kot dodatek oglaševanju služijo tudi z analizo in preprodajo brskalnih navad svojih strank interesentom na trgu. Za potrošnika je sistem neugoden, saj dejansko nima zadostne izbire. Na primer, težko je kupiti le en članek v spletnem časopisu, ponavadi je potrebno skleniti mesečno naročnino in dostop imamo do celotne vsebine, katera nas pa morda sploh ne zanima.[19]

Kripto valute nudijo platformo, ki omogoča tako majhne transakcije z nizkimi stroški in bi tako pripomogle k boljši alokaciji sredstev. Vzpostavil bi se nov trg in z njim meanizem odkrivanja cen vsebin na internetu za katere danes v večini zmotno domnevamo, da so brezplačne.

7. Kritike Bitcoin plačilnega sistema

Kot je bilo že omenjeno, so rudarjenje prevzele ASIC naprave. To so zelo sposobne naprave za preračunavanje SHA256, ne znajo pa popolnoma nič drugega. V primeru, da Bitcoin čez noč ugasne, so te naprave zgolj za na odpad. Problem, ki se odpira pri teh napravah je sledeč, na svetu obstaja le nekaj proizvajalcev, ki imajo tehnične zmožnosti in kapacitete za proizvodnjo teh naprav. S tem se odpirajo vrata centralizaciji omrežja. Omrežje v katerem je prej lahko sodeloval vsak z običajnim računalnikom je zdaj postala igra velikih igralcev. Ker se težavnost omrežja konstantno viša zaradi vedno večjega vlaganja v rudarjenje so mali rudarji počasi izrinjeni iz tekme. Oblikovanje monopola rudarjev bi najverjetneje

[19] Travis Parton: The Bitcoin Revolution: An Internet of Money 111.

porušil zaupanje v omrežje in prišlo bi do propada. Vendar pa to ne pomeni propada izuma kriptovalut, sredstva bi se porazdelila v druge alternativne kriptovalute še preden bi se monopol vzpostavil. Tako bi monopolist imel več koristi, če se monopolu odreče in s tem zagotovi zaupanje v omrežje iz katerega črpa svojo vrednost.[20]

Dodatna kritika omrežja je, da porabi ogromno električne energije za procesiranje uganke, ki sama po sebi nima nobene koristi. Deloma je to pravilno, vendar je težko oceniti, če se ta porabljena energija na koncu izravna z dodanimi vrednostmi, ki jih tehnologija prinaša. Na to vrsto ocene bo treba počakati na širšo uporabo kripto valut. Primerjava stroškov nekaj strani nazaj pa pokaže, da je prmerjalno poraba elektrike bitcoin omrežja zanemarljiva.

Zaključek

Pojav fiat denarja, denar katerega država razglasi kot plačilno sredstvo in se kot tako mora uporabljati ni prisoten od nekdaj. Pred njegovim nastankom tem je človeštvo uporabljalo predvsem dragocene kovine in tudi druga sredstva na določenih teritorijih. Denar je torej začel svojo pot na prostem trgu, nato ga je pod svoje okrilje prevzela država, kaj sledi v prihodnosti pa zaenkrat še ni znano.

Jasno pa je, da z nadzorom nad kreiranjem denarja in nadziranjem plačilnih kanalov preko katerih denar potuje prihaja ogromno moči. Kot že omenjeno, lahko pride do omejitev pravic posameznikov, ki se poskušajo upreti oblasti. Vprašanje je ali je smiselno to moč zaupati centraliziranemu organu, ki lahko to moč zlorabi.

Po drugi strani pa ne govorimo zgolj o zlorabah, omeniti je vredno tudi napake. Če centralna banka na podlagi podatkov katere prejme sprejme napačno odločitev pri reguliranju monetarnega sistema s tem lahko povzroči ogromno škode v gospodarstvu. Stanje je podobno kot pri spodletelih poskusih centralnega planiranja. Sistem, ki je tako kompleksen kot gospodarstvo neke države ali pa v globalnem

[20] Travis Parton: The Bitcoin Revolution: An Internet of Money 22.

merilu, po mojem ni mogoče centralno planirati in regulirati. Slej ko prej se bo vrnil v optimalno točko, izbira zakonodajalca pa je ali bo to beli, sivi ali črni trg.

Ključno pri nadaljnem razvoju teh tehnologij in načina regulacije iz strani držav bo temeljno razumevanje mehanizmov tako obstoječega finančnega sistema kot opisanih disruptivnih tehnologij. Napačen pristop zaradi podcenjevanja enega ali drugega bi privedel do nepotrebnih stroškov zaradi katerih bo družba kot celota bila na slabšem.

Seznam literature

Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System: https://bitcoin.org/bitcoin.pdf

Cooter, Robert, Ulen, Thomas (2005) Ekonomska analiza prava: prevod četrte izdaje 1.natis. Ljubljana: Častnik Finance.

Hass McCook: An Order-of-Magnitude Estimate of the Relative Sustainability of the Bitcoin Network: https://bitscan.com/articles/is-the-bitcoin-network-sustainable

Travis Parton: The Bitcoin Revolution: An Internet of Money. Diginomics (March 11, 2014)

Bajt, Aleksander, Štiblar, Franjo (2004) Ekonomija. Ekonomska analiza in politika. Ljubljana: GV založba.