

Violeta Todorović
Ekonomski fakultet
Univerziteta u Kragujevcu
v.todorovic@kg.ac.rs

Nenad Tomić
Ekonomski fakultet
Univerziteta u Kragujevcu
ntomic@kg.ac.rs

Prevod
obezbedio
autor

NEODRŽIVOST KONCEPTA KRIPTOVALUTA BAZIRANIH NA PROOF-OF-WORK ALGORITMU

Rezime

Uspeh različitih sistema kriptovaluta uslovio je veliko interesovanje za njihovo funkcionisanje. Kretanje njihovih vrednosti je veoma nepredvidivo, pa su se periodi rasta često naglo prekidali stagnacijom ili izraženim padom. I pored toga, poslednjih godina se veliki broj investitora uključio u procese rudarenja i trgovine kriptovalutama. Kada se govori o negativnim efektima koje kriptovalute stvaraju, u fokusu su različiti oblici sajber kriminala. Broj hakerskih napada upotrebom softvera za ucenjivanje - tzv. ransomvera se povećava. Po pravilu, u ovakvim slučajevima se koriste kriptovalute kao sredstvo plaćanja otkupa. Međutim, energetska efikasnost određenih klasa kriptovaluta je nešto ređa tema. Rudarenje po Proof-of-work algoritmu (PoW) je energetski intenzivan i izuzetno skup proces, koji nakon ekonomske analize ne deluje isplativo kako se u prvi mah činilo. Trgovanje kriptovalutama može da donese velike prinose investitorima, ali i velike gubitke, jer u suštini predstavlja igru sa nultom sumom. Nagli rast broja rudara doneo je poremećaj na tržištu računarskih komponenata, izazvavši rast cena i čak potpuni nestanak određenih modela grafičkih kartica. Sve navedeno ukazuje da je njihovo funkcionisanje donelo brojne negativne manifestacije i poremećaje. Predmet rada je ekonomski aspekt kriptovaluta zasnovanih na PoW algoritmu. Cilj rada je ukazivanje na neodrživost njihovog aktuelnog koncepta, usled visokih troškova koji se stvaraju direktno učesnicima u procesu rudarenja i indirektno na tržištu računarskih komponenata.

Ključne reči: kriptovalute, PoW algoritam, Bitcoin, rudarenje, tržišni poremećaji, potrošnja energije, neodrživost modela

JEL: E42, L17, O33, P18

UNSUSTAINABILITY OF CRYPTOCURRENCY CONCEPT BASED ON THE PROOF-OF-WORK ALGORITHM

Violeta Todorović

Faculty of Economy
University of Kragujevac
v.todorovic@kg.ac.rs

Nenad Tomić

Faculty of Economy
University of Kragujevac
ntomic@kg.ac.rsTranslation
provided by
the author

Summary

The success of various cryptocurrencies' systems has triggered a great interest in their functioning. The fluctuation of their values is very unpredictable, so the periods of growth are often abruptly interrupted by stagnation or a pronounced decline. Nevertheless, a large number of investors have been involved in the processes of mining and trading cryptocurrencies in recent years. When it comes to the negative aspects of cryptocurrencies, the focus is primarily on various forms of cybercrime. The number of hacker attacks using the blackmail software - ransomware, is on the increase. In such cases, cryptocurrencies are often used as a means of paying ransom. However, the energy efficiency of certain types of cryptocurrencies is a less common topic. The Proof-of-Work (PoW) algorithm used for mining in some systems is an energetically intensive and really expensive process, which after economic analysis no longer seems as profitable as it first appeared to be. Cryptocurrency trading could bring a great income to the investors, but also great losses, because it essentially represents a zero-sum game. The sudden increase in the number of miners led to the disturbance on the computer components market, causing the price increase and even the complete disappearance of certain graphics card models. Everything previously mentioned indicates that cryptocurrencies have brought many negative aspects and disturbances. The subject of this paper is the economic aspect of cryptocurrencies based on the PoW algorithm. The aim of the paper is to indicate the economic unsustainability of their current concept, due to the high costs borne directly by participants in the mining process and indirectly by participants in the computer components market.

Keywords: cryptocurrencies, Bitcoin, PoW algorithm, mining, market disturbances, electricity consumption, model unsustainability

JEL: E42, L17, O33, P18

Uvod

Nakon pojave Bitcoina krajem 2008. godine, koncept kriptovaluta postao je predmet interesovanja šire društvene zajednice. Dok su akademske rasprave bile usmerene na mogući uticaj kriptovaluta na monetarne sisteme, entuzijasti su se uključili u rudarenje i trgovinu Bitcoina. U narednih nekoliko godina nastale su brojne alternativne kriptovalute, čije su funkcionalne karakteristike menjane u maloj i najčešće neznatnoj meri. Sve kriptovalute poseduju nekoliko zajedničkih karakteristika, koje ih odvajaju od ranijih sistema elektronskog novca. Pre svega, reč je o decentralizovanim sistemima, kojima ne upravlja jedinstven entitet, već mreža povezanih korisnika. Njihovim radom rukovodi unapred zadati i poznati algoritam, bez mogućnosti donošenja diskrecionih odluka. Konačno, svi sistemi su zasnovani na kriptografiji, konkretno haš funkciji, kao metodi očuvanja sigurnosti i sprečavanja falsifikovanja. Zapis izvedenih transakcija daje jedinstvenu glavnu knjigu konkretne kriptovalute. Za sastavljanje glavne knjige se koristi blockchain tehnologija, koja omogućava formiranje lanca informacija, takvog da sve nove informacije moraju biti saglasne sa prethodno unetim. Na taj način se onemogućava brisanje ili modifikovanje prethodno izvedenih transakcija (Iansiti & Lakhani, 2017). Kriptovalute se razlikuju po tome da li je glavna knjiga transakcija potpuno dostupna (kao u slučaju sistem Bitcoin, Ethereum, Ripple i većine drugih), ili pruža ograničeni set podataka (kao što je slučaj sa sistemima Monero i ZCash). Usled privatnosti glavne knjige, transakcije ovim kriptovalutama je mnogo teže pratiti, pa se sve češće baš one koriste u kriminalnim aktivnostima (Greenberg, 2017). Još je značajnija razlika u pogledu algoritma koji se koristi u blockchain tehnologiji, o čemu će više reči biti kasnije.

Pojedine kriptovalute su dostizale neočekivano visoke vrednosti, čiji vrhunac predstavlja kurs Bitcoina prema američkom dolaru krajem 2017. godine. Stoga se u javnosti često govori o mogućnosti zarade kroz procese rudarenja ili trgovanja kriptovalutama. Retko se dovodi u pitanje rashodna strana, tj. ne posvećuje se dovoljno pažnje troškovima koje

sistemi kriptovaluta produkuju. Najstariji sistemi elektronskog novca su prestajali sa radom upravo usled nemogućnosti kontrole visokih fiksnih troškova upravljanja. Smatralo se da su Bitcoin i druge kriptovalute otporne na troškovni pritisak usled decentralizovanosti. Početna premisa, da sistemi kriptovaluta ne stvaraju troškove jer je održavanje i upravljanje decentralizovano, predstavlja veliku grešku. Troškovi svakako postoje, ali su i oni decentralizovani. Kreatori algoritma mogu troškove potpuno preneti na rudare, a sebi u startu dodeliti određenu količinu novčića, ili učestvovati u procesu rudarenja i deliti troškove i koristi sa ostalima.

Nepravilna alokacija troškova sistema nije jedini nedostatak kriptovaluta. Tokom protekle decenije uočene su brojne negativne manifestacije i poremećaji koje njihovo funkcionisanje donosi. Ekonomski aspekti kriptovaluta zasnovanih na PoW algoritmu predstavljaju predmet rada. Cilj rada je ukazivanje na neodrživost njihovog aktuelnog koncepta, usled visokih troškova koji se stvaraju direktno učesnicima u procesu rudarenja i indirektno na tržištu računarskih komponenata. Cilj rada nije kritika tehnološke osnove kriptovaluta, jer i sami autori smatraju da je blockchain jedna od tehnologija koja će imati veliki uticaj na platni promet. U prvom delu rada će biti ukazano na energetske aspekt funkcionisanja sistema kriptovaluta, uz fokusiranje na finansijske i ekološke posledice. U drugom delu rada će biti ukazano na tržišne poremećaje i zloupotrebe koje je funkcionisanje kriptovaluta izazvalo.

Energetsko opterećenje izazvano rudarenjem kriptovaluta

Proces stvaranja novih jedinica kriptovaluta se naziva rudarenje i kontroliše ga unapred zadati algoritam (Dinić, 2014, str. 114-116). Kao što je već naglašeno, postoje različiti tipovi algoritama koji upravljaju procesom stvaranja blockchainea. Najpoznatiji je Proof-of-Work algoritam (PoW), u kome se učesnici procesa rudarenja međusobno takmiče u rešavanju obrnute hash funkcije. Rezultat procesa treba da bude ugradnja novog bloka informacija u glavnu knjigu. Onaj računar koji prvi stigne do rešenja dobija kao nagradu novostvorene

Introduction

After the emergence of Bitcoin at the end of 2008, the concept of cryptocurrencies became a matter of interest for the wider community. While academic discussions were directed towards the possible influence of cryptocurrencies on monetary systems, the enthusiasts involved themselves in the mining and trading of Bitcoins. In the next few years, various alternative cryptocurrencies emerged, with slightly and sometimes insignificantly changed functional characteristics. All cryptocurrencies have several characteristics in common and those characteristics differentiate them from early electronic money systems. Primarily, they are decentralized systems, not managed by a unique entity but by the network of connected users. Their work is supervised by a pre-assigned, known algorithm without the possibility for making discretionary decisions. Finally, all systems are based on cryptography, i.e. the hash function, as a method for preserving security and preventing forgery. A record of all transactions gives a singular ledger of a specific cryptocurrency. Blockchain technology is used in order to make it, since it allows for the formation of a chain of information, such that all new blocks of information must be consistent with the ones previously entered. This prevents the deletion or modification of previously performed transactions (Iansiti & Lakhani, 2017). Cryptocurrencies vary according to whether the ledger is completely available (as is the case with Bitcoin, Ether, Ripple, and most others), or provides a limited set of data (as is the case with Monero and ZCash). Due to the privacy of the ledger, the transactions with these cryptocurrencies are more difficult to trace, which is why they are more often used in criminal activities (Greenberg, 2017). An even more significant difference is in terms of the algorithm used in blockchain technology, which will be discussed further on.

Certain cryptocurrencies reached unexpectedly high values, the peak being the rate of Bitcoin against the US Dollar at the end of 2017. Hence, the public usually raises the question of the possibility of making profit through the processes of cryptocurrency mining or trading. The expenditure side is rarely taken

into consideration, that is to say the expenditures generated by cryptocurrency systems do not get enough attention. The earliest electronic money systems stopped working precisely because of the incapability to control high fixed managing costs. Bitcoin and other cryptocurrencies were thought to be resistant to the cost pressure due to decentralization. The initial premise, that cryptocurrency systems do not generate costs because their maintenance and managing are decentralized, is a big mistake. Costs definitely exist, but they are also decentralized. Algorithm creators can completely transfer the costs to the miners, and award themselves with a certain amount of coins at the very beginning, or participate in the mining process and share the costs and benefits with others.

The improper system cost allocation is not the only disadvantage of cryptocurrencies. During the last decade, numerous negative aspects and disturbances created by its functioning have been noticed. Economic aspects of cryptocurrency systems based on the PoW algorithm are the subject of this paper. The aim of the paper is to indicate the economic unsustainability of their current concept, due to the high costs borne directly by the participants in the mining process and indirectly by participants in the computer components market. The aim of the paper is not the critique of the technological basis for cryptocurrencies, because the authors themselves believe that blockchain will significantly influence the payment industry. The first part of the paper will deal with the energy aspect of the functioning of cryptocurrency systems, with the focus on financial and environmental consequences. Market discrepancies and the misuse stemming from the use of cryptocurrencies will be discussed in the second part.

Energy Costs of Cryptocurrency Mining

The process of new cryptocurrency unit creation is called mining and is controlled by a previously established algorithm (Dinić, 2014, p. 114-116). As it was already mentioned, there are different types of algorithms that govern the process of blockchain creation. The most famous is the Proof-of-Work algorithm (PoW), in which

novčiće (Nakamoto, 2008, str. 3). PoW se koristi kod poznatih kriptovaluta kao što su Bitcoin, Litecoin i drugi. Najpoznatiji alternativni algoritam je Proof-of-Stake (PoS), kod koga se validator (računar u PoS terminologiji) koji će ugraditi novi blok informacija unapred određuju i to na osnovu broja novčića koje poseduju (Sajana i saradnici, 2018, str. 2966). Kada validator ugradi novi blok informacija, dobija nagradu u vidu provizije od izvedenih transakcija, ali se pomera na začelje liste, odnosno mora da čeka ostale čvorove da stignu na red. Pošto se u slučaju PoW algoritma računari takmiče, potrošnja električne energije raste sa povećanjem broja učesnika. U slučaju PoS algoritma nema potrebe za takmičenjem, jer je validator unapred određen, pa je i potrošnja energije dosta niža. PoS se koristi kod kriptovaluta kao što su Peercoin, NXT i drugi.

U sekundarnom prometu se pojavljuju samo jedinice koje su već „izrudarene“ i čiji su vlasnici uključeni u održavanje sistema. Nakon velikog pada vrednosti u drugoj polovini 2011. godine (Lee, 2013), Bitcoin se nalazio u gotovo konstantnom rastu sve do kraja 2013. godine. Nakon stagnacije i pada vrednosti tokom 2014. i 2015. godine, vrednosti Bitcoina i većina drugih kriptovaluta značajno su porasle u 2017. godini. (Chaparro, 2017). Iako je zabeležio ogroman prinos od preko 1000% tokom 2017. godine, Bitcoin ne spada ni u prvih deset kriptovaluta po rastu vrednosti. Kumulativni rast celokupnog tržišta motivisao je veliki broj pojedinaca da se uključe u proces rudarenja, sa ciljem ostvarivanja zarade u sekundarnom prometu. U Tabeli 1 se može videti kako je 2017. godina bila uspešna za sve investitore u kriptovalute.

Tabela 1: Kriptovalute prema rastu vrednosti u periodu 1. januar - 31. decembar 2017. godine

Naziv kriptovalute	Godišnji rast vrednosti u procentima
Ripple	36,018%
NEM	29,842%
Ardor	16,809%
Stellar	14,441%
Dash	9,265%
Ethereum	9,162%
Golem	8,434%
Binance Coin	8,061%
Litecoin	5,046%
Omise GO	3,315%
Bitcoin	1,318%

Izvor: <https://cointelegraph.com/news/the-cream-of-the-crypto-crop-10-best-performing-assets-in-2017>

Standardni kućni računari nisu veliki potrošači električne energije. Računari koji se koriste u rudarenju predstavljaju modifikacije kućnih računara. Kako su za matematičke operacije PoW algoritma grafičke kartice gotovo uvek uspešnije od procesora, računari koji se koriste u ove svrhe ih često sadrže po nekoliko, što im značajno uvećava potrošnju električne energije. Vlasnici praktično nikada ne isključuju računare, jer žele da stalno budu uključeni u rudarenje. Koncentracija grafičkih kartica proizvodi veliku količinu toplote, pa su potrebni dodatni sistemi za hlađenje. Pojedinci koji se bave rudarenjem retko to čine sa jednim uređajem, već kombinuju više računara da bi povećali mogućnost dobijanja nagrade. Kada se svi računari nalaze u istoj prostoriji, dolazi do velikog zagrevanja, za šta je rešenje jedino autonomni rashladni sistem. Posledica svega navedenog je ogromna potrošnja električne energije.

Troškovi električne energije su očigledni primeri cene funkcionisanja kriptovaluta zasnovanih na PoW. Egzaktan proračun ukupne potrošnje električne energije zahtevao bi precizne podatke o broju rudara, stepenu njihovog angažovanja i geografskoj distribuciji, što je nemoguće obezbediti. Ipak, na osnovu određenih znanja moguće je napraviti proračun, koji se može koristiti kao orijentir prilikom davanja ocene o ekonomskoj isplativosti kriptovaluta. Proračun je najlakše pratiti na

the participants in the mining process compete with each other in solving a reversed hash function. The result of the process should be the installation of a new block of information in the ledger. The computer who reaches the solution first, gets the newly created coins as a reward (Nakamoto, 2008, page 3). The PoW is used with some well-known cryptocurrencies such as Bitcoin, Litecoin etc. The best-known alternative is the Proof-of-Stake (PoS) algorithm, in which the validators (computers in PoS terminology) that will install a new block of information are predetermined based on the number of coins they possess (Sajana et al., 2018, p. 2966). When a validator embeds a new block of information, it receives a reward in the form of a fee from executed transactions, and moves to the end of the list, i.e. it now has to wait for the other nodes. As the PoW algorithm is competitive, the power consumption rises with the increase in the number of miners. In the case of the PoS algorithm there is no need for competition, because the validator is predetermined, so the energy consumption is much lower. The PoS is used with cryptocurrencies such as Peercoin, NXT, etc.

On the secondary market one can buy only the units which have already been mined and whose owners are included in the system maintenance. After a great decrease in value in the second half of 2011 (Lee, 2013), Bitcoin was experiencing constant growth until the end of 2013. After the stagnation and decline during 2014 and 2015, the values of Bitcoin and most other cryptocurrencies increased significantly in 2017 (Chaparro, 2017). Although it recorded a great increase in value by 1000% during 2017, Bitcoin is not even in the first ten cryptocurrencies according to value growth. The cumulative growth of the whole market motivated a big number of individuals to engage in the mining process, with the aim of earning profit on the secondary market. Table 1 shows how successful 2017 was for all cryptocurrency investors.

Table 1: Cryptocurrencies listed according to value growth in the period from 01.01.2017 to 31.12.2017

Criptocurrency	Annual Value Growth in Percentage
Ripple	36.018%
NEM	29.842%
Ardor	16.809%
Stellar	14.441%
Dash	9.265%
Ethereum	9.162%
Golem	8.434%
Binance Coin	8.061%
Litecoin	5.046%
Omise GO	3.315%
Bitcoin	1.318%

Source: <https://cointelegraph.com/news/the-cream-of-the-crypto-crop-10-best-performing-assets-in-2017>

Standard personal computers are not major electricity consumers. Computers used in the mining process are modified personal computers. As the graphics cards are almost always more successful in solving mathematical operations of the PoW algorithm than the computer processors, computers used for these purposes often contain several of these, which significantly increase their electricity consumption. The owners almost never turn off their computers because they want to be always included in the mining process. The concentration of graphic cards produces a great amount of heat, which is why additional cooling systems are needed. The individuals involved in mining rarely do that with just one device, instead usually combining several computers in order to enhance the possibility for winning the prize. When all computers are located in the same room, there is a massive accumulation of heat, the only solution being an autonomous cooling system. The consequence of the abovementioned is huge electricity consumption.

The electricity costs are an obvious example of the price paid for the functioning of all cryptocurrencies based on PoW. The exact calculation of the total electricity consumption would require precise data about the number of miners, their degree of engagement and geographical distribution, which is impossible to provide. However, it is possible to make a calculation based on certain previous

primeru Bitcoina, ali važi na praktično isti način i za ostale kriptovalute.

Ne postoji centralni registar svih mašina uključenih u proces rudarenja, ali se može izračunati broj haš operacija koje se izvrše u jedinici vremena. Haš operacije predstavljaju osnovu procesa rudarenja. De Vries (2018) navodi da je 16. marta 2018. godine u celokupnom sistemu Bitcoina prosečno vršeno 26 triliona (10^{18}) haš operacija u sekundi. Da bi se utvrdila potrošnja električne energije, potrebno je znati strukturu računarskih mašina koje učestvuju u procesu rudarenja. Od tipa mašina zavisi broj haš operacija u sekundi i potrošnja energije po jednoj operaciji. U poslednjih nekoliko meseci najveći deo rudarskih uređaja čine specijalizovane mašine. Isti autor navodi da je specijalizovana mašina za rudarenje „Antminer S9“ energetski najefikasnija. Kada bi se celokupna mreža sastojala samo od ovih uređaja, snaga mreže bi iznosila oko 2,55 GW. Na taj način se može utvrditi da je donja granica godišnje potrošnje električne energije u trenutku pisanja rada bila preko 20 TW/h. Samson (2018) dodaje da je procenjena potrošnja električne energije kriptovalute Ether takođe u stalnom rastu i da je tokom 2018. godine prerasla dvocifren broj TW/h godišnje. Prema modelu koji je predstavio de Vries, sajt Digiconomist prati dinamiku promene očekivane godišnje potrošnje električne energije.

Isti sajt je izradio proračun ukupnih godišnjih prihoda od rudarenja (proizvod broja emitovanih novčića i njihove cene u sekundarnom prometu) i ukupnih troškova rudarenja (proizvod očekivane godišnje potrošnje električne energije i njene tržišne cene). Zaključak do kojeg je tim sajta došao je da godišnji troškovi električne energije čine 74,2% ukupnih godišnjih prihoda od rudarenja. Najpre treba imati u vidu da je postupak kojim su utvrđeni ukupni godišnji prihodi i troškovi diskutabilan. Tržišna cena električne energije varira u zavisnosti od države i ukupne potrošnje domaćinstva/preduzeća. U ukupne troškove električne energije nisu uračunati troškovi autonomnih rashladnih sistema. Takođe, treba uzeti u obzir da je mnogo teže izraziti oportunitetni trošak uloženog vremena i amortizacije angažovanih uređaja, koji svakako postoje i nisu zanemarivi. Prihodi variraju u zavisnosti od promene tržišne cene

Bitcoina u sekundarnom prometu. Stoga, pomenuti rezultat ne treba shvatiti kao egzaktni odnos, već kao nagoveštaj ukupnog konteksta u kom kriptovalute funkcionišu. Trenutno visoka otkupna cena na sekundarnom tržištu omogućava procenjenim ukupnim prihodima da se održavaju iznad troškova. Krajem 2016. godine cena je bila čak osam puta niža nego u trenutku pisanja rada, što govori o mogućnostima nagle promene posmatranog odnosa.

Komparacija troškova i prihoda sistema kriptovaluta predstavlja poređenje dve procenjene vrednosti. Za potpuno razumevanje energetskog opterećenja kriptovaluta veći značaj ima poređenje procenjenih troškova sa pouzdano utvrđenim vrednostima. Tako se potrošnja mreže Bitcoina može porediti sa potrošnjom električne energije nacionalnih ekonomija. Kada bi rudari Bitcoina predstavljali nacionalnu ekonomiju, njihova godišnja potrošnja električne energije bi bila veća nego u 159 drugih država, uključujući sve republike bivše Jugoslavije ili sve baltičke sovjetske republike (Williams-Grut, 2017). Holthaus (2017) je analizirao povećanje broja rudara u periodu rasta vrednosti Bitcoina 2017. godine. Zaključio je da će, ako se trend rasta nastavi, već 2020. godine rudari trošiti više električne energije nego ostatak sveta. Pretpostavka je hipotetička i teško ostvariva u praksi, ali odlično ilustruje neodrživu prirodu tržišta kriptovaluta.

Da bi se stekao uvid u energetsku efikasnost Bitcoina kao sistema plaćanja, potrošnja električne energije mreže se može porediti sa potrošnjom drugih sistema plaćanja. Sajt Digiconomist pružio je proračun potrošnje električne energije za VISA transakcije. Kao izvor podataka su korišćeni zvanični izveštaji kompanije VISA. Za obradu 100.000 VISA transakcija prateća infrastruktura potroši 169 kW/h električne energije. Deljenjem procenjene potrošnje električne energije i broja Bitcoin transakcija (što je egzaktni broj koji se lako može utvrditi), tim sajta je zaključio da je za obradu samo jedne transakcije procenjena potrošnja 837 kW/h električne energije. Na osnovu iznetog se može zaključiti da je VISA kao reprezentativni primer starijih elektronskih sistema plaćanja gotovo 500.000 puta energetski efikasnija. Još jedanput, ove cifre treba uzeti kao orijentir, a ne kao egzaktni pokazatelj,

knowledge, which could be used as a guide when evaluating the economic viability of cryptocurrencies. The calculation could be easily followed on the example of Bitcoin, but it could also be applied to other cryptocurrencies.

There is no central register of all computers included in the mining process, but the number of operations carried out in a unit of time could be calculated. Hash functions represent the basis of the mining process. De Vries (2018) states that on 16 March 2018, 26 quintillion (10^{18}) hash functions were performed per second in the entire Bitcoin system. In order to determine the electricity consumption, it is necessary to know the structure of the computer network. The number of hash functions per second as well as electricity consumption per operation depends on the device type. In the last few months, most of the mining equipment has been made up of specialized machines. The same author states that the specialized device, "Antminer S9", is the most energy efficient. If the entire network consisted of only these devices, the network power would amount to 2.55 GW. In this way, it could be concluded that the lowest limit of electricity consumption at the moment of writing this paper was beyond 20 TW/h. Samson (2018) adds that the calculated electricity consumption of the Ether cryptocurrency is also in constant growth and that during 2018 it grew past a two-digit number of TW/h per year. According to the model represented by de Vries, the Digiconomist website follows the change dynamics of the expected annual electricity consumption.

The same website calculated the total annual mining income (the result of the number of emitted coins multiplied by their prices on the secondary market) and the total expenses of mining (the result of the expected annual electricity consumption multiplied by its market price). The conclusion of the website team is that annual electricity consumption makes up for 74.2% of the total annual income. Primarily, it should be noted that the procedure for determining the total annual income and expenses is debatable. The market price of electricity varies depending on the country and the total consumption of a household/company. The total amount of electricity expenses does not include the expenses for

autonomous cooling systems. Also, it should be taken into consideration that it is more difficult to express the opportunity cost of time spent and the depreciation of engaged devices, which definitely exists and is not negligible. The income varies according to the fluctuation of Bitcoin prices on the secondary market. Hence, the previously mentioned result could not be taken as an exact ratio, but as an indication of the overall context in which cryptocurrencies function. At the moment, high prices on the secondary market enable the estimated total income to be above the expenses. At the end of 2016, the price was as far as eight times lower than at the time of writing this paper, which confirms the possibility of sudden changes in the observed ratio.

The comparison of the cryptocurrencies system's expenses and revenues is the comparison of two estimated values. The comparison of estimated expenses with reliably determined values has greater importance for the complete understanding of the cryptocurrency energy burden. Thus, the expenses of the Bitcoin network could be compared to the electricity consumption of national economies. If Bitcoin miners represented the national economy, their annual electricity consumption would be higher than the annual consumption in 159 countries, including all countries of ex-Yugoslavia or all Baltic Soviet states (Williams-Grut, 2017). Holthaus (2017) has analyzed the increase in the number of miners during the Bitcoin's growth period in 2017. He concluded that, if the trend of growth continues, miners will spend more electricity in 2020 than the rest of the world. The assumption is hypothetical and hardly achievable in practice, but it excellently illustrates the unsustainable nature of the cryptocurrency market.

In order to get insight into energy efficiency of Bitcoin as a payment system, the electricity consumption of the network could be compared to the consumption of other payment systems. The website Digicomist provided the calculation of the electricity consumption for VISA transactions. As a source, they used official reports of the VISA Company. For the processing of 100 000 VISA transactions, the supporting infrastructure spends 169 KW/h of electricity. By dividing the estimated

ali one svakako govore u prilog energetskeg opterećenja kriptovaluta. Svjesni ovog problema, u Bitcoin zajednici rade na razvoju i implementaciji Lightning Network protokola, koji će omogućiti simultano izvođenje većeg broja transakcija. Krajnji cilj ovog protokola je istovremeno omogućavanje uštede u potrošnji električne energije, koja će se odraziti na niže provizije za izvedene transakcije.

Ekološke posledice predstavljaju poslednji aspekt energetskeg opterećenja. Rogers (2017) je izneo pretpostavku da se prilikom proizvodnje električne energije za Bitcoin mrežu godišnje emituje 17,7 miliona tona ugljen-dioksida. Za utvrđivanje preciznog iznosa emisije štetnih gasova pored nepoznate ukupne potrošnje potrebno je utvrditi proporciju električne energije koja se proizvede upotrebom fosilnih goriva. Hileman & Rauchs (2017, str. 93) navode da se 58% svih rudarskih računara nalazi u Kini, a oko 16% u SAD-u. Poznato je da Kina najveći deo električne energije proizvodi u termoelektranama, koje emituju ugljen-dioksid. Ovo ipak nije dovoljno da se približno utvrdi uticaj rudarenja kriptovaluta na zagađenje i globalno zagrevanje.

Tržišni poremećaji izazvani kriptovalutama

Same kriptovalute predstavljaju jedan veliki poremećaj na međunarodnom finansijskom tržištu. Iako su nominalno elektronski novac, predviđen za izvođenje transakcija u internet okruženju, kriptovalute nemaju veliku primenu u plaćanjima. Njihova vrednost je oduvek izrazito nestabilna, pa su korisnici koji ih poseduju izloženi mogućnosti gubitka u slučaju upotrebe u plaćanjima. Zabeleženi su ekstremni primeri transakcija iz 2010. godine, kada je Bitcoin imao jako nisku vrednost, ali je mogao biti korišćen za plaćanje određenih proizvoda i usluga. Iznosi kojima su tada plaćani uobičajeni proizvodi danas vrede više desetina miliona američkih dolara (Price, 2017). Ako se kriptovalute posmatraju kao novac, na njihovom primeru važi modifikovan Grešamov zakon. Izvorni Grešamov zakon kaže da kada u platnom prometu paralelno egzistiraju dve vrste novca, stanovništvo teži da troši „loš novac“, odnosno novac čija je vrednost sklona

opadanju (jer je precenjen državnom odlukom), a čuva „dobar novac“, čija je vrednost stabilna (Sparavigna, 2014, str. 81). Kriptovalute vlasnici ne čuvaju zato što im je vrednost stabilna, već naprotiv, zato što nije. Vlasnici se nadaju da će doći do apresijacije kriptovalute koju poseduju, pa će njenom prodajom ostvariti zaradu. U prilog ovoj tvrdnji, Wang (2014) je još ranije ukazao da će do rasta vrednosti Bitcoina doći samo ako bude ostao sredstvo čuvanja vrednosti, dok će mu masovna upotreba u plaćanjima umanjiti vrednost.

Problem nastaje kada svi vlasnici kriptovaluta imaju isključivo špekulativne namere. Rudari ulažu u računarsku opremu kako bi došli do novčića koje će kasnije skupo prodati. Trgovci kupuju od rudara novčiće nadajući se da će ih prodati skuplje nego što su kupili. Međutim, kriptovalute predstavljaju sintetički robni novac (Coase, 1972, str. 143-144), što znači da nemaju nemonetarnu primenu iz koje bi crpele vrednost (Selgin, 2014, str. 93-94). Za razliku od valuta baziranih na PoS algoritmu, valute bazirane na PoW algoritmu ne donose prinos posedovanjem, pa nema razlike da li ih vlasnik odmah prodaje ili drži dugo. Jedini način da vlasnici ostvare zaradu od kriptovaluta je da ih prodaju uz kapitalni dobitak, odnosno po ceni višoj od kupovne.

Prilikom kupovine akcija investitori koriste znanje i pretpostavke o kompaniji u koju ulažu. Tom prilikom se rukovode finansijskim izveštajima i najavama poslovnih poduhvata. Kod kriptovaluta ne postoji nijedan parametar, niti izveštaj, koji bi mogao da signalizira investitorima racionalnu odluku. Zbog toga se investitori prilikom kupovine mogu samo nadati da će u budućnosti biti dovoljno novih investitora, spremnih da kupe iste kriptovalute po višoj ceni. U ekonomskoj praksi se ovaj poslovni pristup naziva „teorija veće budale“. Iako se može naći više članaka koji objašnjavaju da neće doći do pucanja cenovnog balona, prestižni časopis *The Economist* upozorava da je ulaganje u Bitcoin sve opasnije kako su cene postale veće. Investitori se izlažu realnoj opasnosti da plate visoke cene, koje kasnijom prodajom neće biti u mogućnosti da nadoknade.

Svi trgovci ulaze na tržište kriptovaluta sa ciljem da ostvare zaradu. Pitanje je koji procenat je svestan da trgovina kriptovalutama predstavlja

electricity consumption with the number of Bitcoin transactions (which is an exact number that could be easily determined), the website team concluded that the estimated electricity consumption for processing one transaction is 837 kW/h. Based on the previously stated, it could be concluded that VISA, as a representative example of older payment systems, is almost 500 000 times more energy efficient. Once again, these numbers should be taken as guidelines, not as exact indicators, but they absolutely highlight the energy burden of cryptocurrencies. Being aware of this issue, Bitcoin activists are working on the development and implementation of the Lightning Network protocol, which will enable a simultaneous execution of multiple transactions. The ultimate goal of this protocol is to provide lower energy consumption, which will result in lower fees for executed transactions.

Environmental changes are the last aspect of energy burdening. Rogers (2017) gave a presumption that in the course of producing electricity for Bitcoin, 17.7 million tonnes of carbon dioxide is emitted annually. In order to determine the exact amount of toxic gas emission, it is necessary to determine the share of electricity produced by the use of fossil fuels. Hileman & Rauchs (2017, p.93) cite that 58% of all mining computers are located in China, and about 16% in USA. It is well known that in China the biggest share of electricity is produced in thermal power plants that emit carbon dioxide. However, this is not enough for determining the mining impact on pollution and global warming.

Market Disturbances Provoked by Cryptocurrencies

Cryptocurrencies themselves represent one great disturbance on the international financial market. Although they are nominally electronic money, made for performing transactions in the internet environment, cryptocurrencies are not largely applicable in payments. Their value is extremely unstable, so users who own them are exposed to the possibility of loss if using them in payments. Extreme examples of transactions were recorded in 2010, when Bitcoin had a very low value, but could be used as payment for

certain products and services. The amounts paid back then for ordinary products, are nowadays worth several dozen millions of US dollars (Price, 2017). If cryptocurrencies are considered to be money, modified Gresham's Law could be applied on their example. Original Gresham's Law says that when two kinds of money exist in the payment system, people seek to spend the "bad money", or money whose value is prone to decline (because it was overestimated by a state decision), and to hold on to "good money" whose value is stable (Sparavigna, 2014, p.81). People do not keep cryptocurrencies because their value is stable, but on the contrary, because it is not. They hope for the appreciation of the cryptocurrency they own, so they could make profit. To support this assertion, Wang (2014) had previously pointed out that Bitcoin value would rise only if it remained a means of value preservation, while a massive use in payments would decrease its value.

The problem arises when all cryptocurrency owners have exclusively speculative intentions. Miners invest in the computer equipment in order to mine the coins which they will later sell at a high price. Traders buy coins from miners hoping that they will sell them at an even higher price. However, cryptocurrencies represent synthetic commodity money (Coase, 1972, p. 143-144) which means that they do not have non-monetary application from which they could draw their value (Selgin, 2014, p. 93-94). Unlike the cryptocurrencies based on the PoS algorithm, cryptocurrencies based on the PoW algorithm do not yield anything through their possession alone, so there is no difference whether the holder immediately sells them or holds on to them for a long time. The only way for owners to gain profit from these cryptocurrencies is to sell them with capital gain, i.e. at the selling price higher than the buying price.

When buying stocks, investors use knowledge and presumptions about the company in which they invest. On that occasion they use financial reports and the announcements of business ventures. When it comes to cryptocurrencies, there is not a single parameter, nor report, which could lead the investors to make a rational decision. Because of this, investors can only hope that in the future there would be enough new

igru sa nultom sumom na sistemskom nivou. Prilikom prodaje, zarada jednog trgovca je jednaka izdatku drugog (provizije se u ovom trenutku mogu zanemariti). Krug se zatvara svaki put kada se cena kriptovalute nađe na nekom ranijem istorijskom nivou. U tom krugu su jedni trgovci zaradili, a drugi izgubili isti iznos. Sistem nije stvorio novu vrednost, niti će na ovom nivou organizacije kriptovaluta moći da je stvori. Društvo nije postalo bogatije, samo je došlo do redistribucije bogatstva. Ako vrednost kriptovalute padne na nulu, sve trgovine će na kraju dati nultu sumu.

Nagli porast broja rudara izazvao je poremećaj na tržištu računara i računarskih komponenata. Tržište personalnih računara je nakon konstantnog rasta u prvoj deceniji XXI veka počelo da se hladi. Prvi kvartal 2012. godine bio je poslednji u kojem je tržište beležilo rast, da bi nakon toga usledio višegodišnji trend opadanja prodaje (Rossof, 2016). Jedan od uzroka ovakvih kretanja je usporavanje privrednog rasta u zemljama u razvoju i smanjenje narudžbina korporativnog sektora. Drugi uzrok je jačanje mobilnih operativnih sistema, koji su omogućili mobilnim telefonima i tablet uređajima da preuzmu brojne funkcije računara. Nakon što se prodaja personalnih računara našla na decenijskom minimumu, Gartner je izneo podatke da je u prvoj polovini 2018. godine tržište računara zabeležilo rast, prvi put nakon 6 godina. Jedini događaj koji je stimulusao naglu promenu trenda je eksponencijalni rast vrednosti kriptovaluta u drugoj polovini 2017. godine, koji se sa kašnjenjem od nekoliko meseci prelio na tržište računara, rezultirajući naglim rastom prodaje. Ovaj podatak je potpuno konzistentan sa zaključcima koje su izneli Holthaus (2017) i sajt Digiconomist o stalnom rastu broja rudarskih mašina od kraja 2017. godine.

Još veći poremećaj je nastao na tržištu pojedinačnih komponenata. Kako su grafičke kartice najvažnija komponenta rudarskih računara, ovo tržište je potpuno destabilizovano već više od godinu dana. Samo u 2017. godini, rudari su kupili 3 miliona grafičkih kartica (Osbourne, 2018). Velika potražnja u Evropi i Severnoj Americi rezultirala je rastom cena od čak 80% za najpotentnije modele kartica (na primer, cena NVidia Ge Force GTX 1070 je porasla sa 380 na 700 američkih dolara -

Warren, 2018). Nakon rasta cene usledila je i nestašica grafičkih kartica, koja je pogodila sva regionalna tržišta. Ponuda grafičkih kartica je relativno neelastična, jer zahteva visoka ulaganja u otpočinjanje/proširenje procesa proizvodnje. Stoga su proizvođači grafičkih kartica nevoljni da povećavaju ponudu, budući da su svesni nestabilne prirode povećanja tražnje za njihovim proizvodima. Jedini potez proizvođača je preporuka distributerima da kartice prodaju igračima (najveća tradicionalna primena grafičkih kartica je u grafičkoj obradi i video igrama), a ne rudarima.

Niskoj zastupljenosti kriptovaluta u plaćanjima treba dodati činjenicu da određen procenat transakcija čini finansiranje ilegalnih aktivnosti (Tomić i saradnici, 2017). U kombinaciji sa „mračnim delom interneta“, kojim se pristupa preko TOR (*the onion routing*) pretraživača, kriptovalute su obezbeđivale infrastrukturu za kompletan ciklus ilegalnog elektronskog poslovanja. Dok su korisnici konvencionalnog interneta lako prepoznatljivi na osnovu IP adrese, korisnici mračnog veba kriju svoju pravu lokaciju kroz preusmeravanje sadržaja preko čitavog niza drugih korisnika (Liška i saradnici, 2010, str. 542-544). Zbog toga nije poznato ko je korisnik koji je zatražio pristup određenom sadržaju, niti na kom je serveru taj sadržaj lociran. Kriptovalute sa javnom glavnom knjigom pružaju „anonimnost od 99%“, tj. moguće je pratiti transakcije svakog računa, ali je za pouzdano utvrđivanje identiteta vlasnika računa potrebno sučeliti ove podatke sa nekima u kojima se otkriva identitet vlasnika - na primer kupovinom određenih proizvoda ili transakcijom na berzi kriptovaluta.

Najpoznatiji primer svakako je Silk Road, sajt koji je praktično predstavljao kopiju najpoznatijeg aukcionog sajta eBay. Na njemu su se mogli kupiti oružje, narkotici, pornografski sadržaji, krađene kreditne kartice, lažni lični dokumenti i druga ilegalna roba (Van Hout & Bingham 2013). Kao jedino sredstvo plaćanja, korišćen je Bitcoin. U oktobru 2013. godine FBI je uhapsio Vilijama Ulbrihta pod optužbom da je organizovao i vodio sajt Silk Road pod imenom „Dread Pirate Roberts“, dok je sam sajt ugašen. Procena ukupnog prometa sajta se kreće oko 9,5 miliona Bitcoina, što je po tadašnjem kursu iznosilo oko milijardu

investors, ready to buy cryptocurrencies at a higher price. In economic practice, this business approach is called “the greater fool theory”. Although there are many articles which explain that there is not going to be a price bubble burst, the prestigious magazine *The Economist* warns that investing in Bitcoin is more and more dangerous as prices have become higher. Investors are exposed to the real dangers of paying high prices for which subsequent selling will not be able to compensate.

All traders enter the cryptocurrency market in order to make profit. The question is which percentage of them is aware that cryptocurrency trading is a zero-sum game on the systemic level. When selling, the income of one trader is equal to the expenses of another (commissions could be ignored at this point). The circle closes every time the price of a cryptocurrency reaches a previous historic level. In that circle some traders made profit and others lost the same amount. The system has not created a new value nor is it going to create it on this level of organization. Society has not become richer, there has only been a redistribution of wealth. If a cryptocurrency's value dropped to zero, all trades would ultimately give a zero sum.

The sudden increase in the number of miners caused a disruption on computer and computer components markets. The PC market, after a constant increase in the 2000s, started to cool down. The first quarter of 2012 was the last one in which the market recorded an increase, and it was followed by a years-long downward trend in sales (Rossof, 2016). One of the causes of these movements was the slowdown of economic growth in the developing countries and a reduction in the corporate sector demand. Another cause was the strengthening of mobile operating systems, which allowed mobile phones and tablet devices to take over numerous functions from computers. After the sale of personal computers dropped to a decade minimum, Gartner said that in the first half of 2018, the computer market recorded an increase, for the first time in six years. The only event which stimulated a sudden change in trend was the exponential growth of cryptocurrency value in the second half of 2017, which spilled over to the computer market after several months of delay, and which resulted in

a sudden increase in sales. This information is completely consistent with the conclusions reached by Holthaus (2017) and the Digicomist website about the constant increase in mining devices since the end of 2017.

An even bigger disturbance occurred on the components market. Bearing in mind that graphics cards are the most important components of mining computers, this market has been completely destabilized for more than a year. Just in 2017, miners bought 3 million graphics cards (Osbourne, 2018). The great demand in Europe and North America resulted in the price growth of 80% for the most powerful card models (for instance, the price of NVidia GeForce GTX 1070 grew from 380 to 700 USA dollars - Warren, 2018). The price growth was followed by a shortage of graphics cards, which affected all regional markets. The supply of graphics cards is relatively inelastic, because it requires high investments when starting/expanding the production process. Hence, the manufacturers are reluctant to increase their offer, since they are aware of the unstable nature of the increased demand. The manufacturers' only move was to recommend to the distributors to sell cards to gamers (the largest traditional application of graphics cards is in graphic processing and video games), instead of to miners.

The low usage of cryptocurrencies in payments goes along with the fact that a certain percentage of transactions are used to finance illegal activities (Tomić et al, 2017). Together with the “Dark Web”, which can be accessed via TOR (the onion routing) browsers, cryptocurrencies provided infrastructure for the complete cycle of illegal electronic business. While the users of conventional Internet are easily recognized by their IP addresses, the users of the Dark Web hide their real location by redirecting content across a number of other users (Liška et al., 2010, p. 542-544). Because of this, the identity of the user who requested access to certain content is not known, and the server where the content is located remains unknown as well. Cryptocurrencies with a public ledger provide “99% anonymity”, which means that it is possible to follow the transactions of every account, but it is necessary to compare this information with some that reveal the identity of the owner - such as a

američkih dolara, dok je trenutno vrednost tog iznosa daleko viša (Konrad, 2013).

Gašenje jednog sajta nije dovelo do zamiranja kriminalnih aktivnosti finansiranih kriptovalutama. Novi ilegalni projekti, poput sajtova Silk Road 2.0, AlphaBay i Hansa, pokušali su da zauzmu upražnjeno mesto. Čak je i dominantno sredstvo plaćanja promenjeno, pa se umesto Bitcoina koristi kriptovaluta Monero. Međutim, svi pomenuti sajtovi su imali isti infrastrukturni problem - centralizovane servere. Nakon akcija jedinica za sajber kriminal u više država, sajtovi su jedan za drugim ugašeni (Liao, 2017). Pravi izazov za vlasti će biti decentralizovana crna tržišta, poput mreže Eden (Devoe, 2018). Primenom blockchain tehnologije u svrhe izgradnje sajta izbegava se centralizovano gašenje, jer ne postoji jedan server preko koga se ostvaruje kontrola. Postojanje ovakvih sajtova ne znači da će porasti nivo nasilja i ilegalnih aktivnosti, već samo da će učesnici lakše i brže komunicirati, ali nemogućnost vlasti da im se suprotstave može imati nesagledive posledice. Na dugi rok će biti ohrabren svaki oblik ilegalnog elektronskog poslovanja, a moguću primenu u terorističkim aktivnostima ne treba posebno naglašavati.

U cilju sprečavanja upotrebe kriptovaluta za pranje novca i finansiranje terorizma, Evropska komisija je donela Petu direktivu za sprečavanje pranja novca (Directive 2018/843). U njoj je jasno naglašena opasnost od upotrebe kriptovaluta (koje autori direktive nazivaju „virtuelnim valutama“) i kartica sa unapred uplaćenom monetarnom vrednošću u svrhe finansiranja terorizma. Ranije je dokazana upotreba ovih sredstava plaćanja u svrhe finansiranja kriminalnih aktivnosti na tlu Evropske unije (Marria, 2018). Ključni zahtevi koje nova direktiva postavlja pred berze kriptovaluta, kompanije koje izrađuju digitalne novčanike i korisnike odnose se na ukidanje anonimnosti. S jedne strane, sve kompanije će imati obavezu da se registruju kod regulatornih vlasti i predaju podatke o korisnicima na zahtev. S druge strane, pojedinci će morati da dokažu poreklo sredstava prilikom konverzije kriptovaluta u konvertibilni novac. Zahtevane izmene čine radikalnu promenu, kojom će raspolaganje elektronskim novcem biti približeno upravljanju tekućim računom.

Zaključak

Rudarenje kriptovaluta je troškovno mnogo intenzivnije nego što se u prvi mah čini. Budući da se svi proračuni zasnivaju na posrednim indikatorima, može se konstatovati da su pre aproksimacije nego egzaktni rezultati. Zato njihov ključni doprinos nije utvrđivanje preciznog finansijskog rezultata, već stvaranje predstave o ekonomskim rezultatima rudarenja. Mogu se izdvojiti dva opšta zaključka.

Prvo, troškovi električne energije koje stvaraju računarske mašine, čak i bez uzimanja u obzir sistema za hlađenje, toliko su visoki, da ukupna isplativost celog procesa zavisi samo od visine vrednosti kriptovaluta na sekundarnom tržištu. Na primeru Bitcoina je pokazano da se tržište rudara sporo prilagođava kretanju vrednosti kriptovalute u sekundarnom prometu. To znači da će do porasta broja rudara (i samim tim rasta troškova celokupnog sistema) doći nakon velikog rasta sekundarne cene, kakav je bio u drugoj polovini 2017. godine. U slučaju naglog pada cene nakon nekoliko meseci, većina rudarske zajednice će se naći u zoni gubitka, jer produkuje više troškova nego što može da zaradi.

Drugo, čak i kada celokupna rudarska zajednica posluje pozitivno, odnosno može da prodajom novih novčića isplati sve troškove, vrlo malo je poznato o distribuciji prihoda. Distribucija troškova je poznata i zavisi od broja i vrste računara koje rudari koriste. Algoritam je dizajniran tako da nagrađuje rudare koji učestvuju u radu sistema prema ostvarenim rezultatima, ne po rotirajućem principu. To znači da nagrada, odnosno dobijanje novih novčića nije zagarantovana ni u kom vremenskom horizontu. Ako se rudari odluče da se ne udružuju u male zajednice, mogu doći u situaciju da bez obzira na vreme koje njihovi računari budu angažovani, ne zarade ništa. To znači da čak i kada ukupan sistem posluje pozitivno, rudari mogu zaraditi ništa, ili toliko malo da ne mogu da pokriju sopstvene troškove.

Što se tiče trgovanja kriptovalutama, jasno je da pojedinci mogu ostvariti visoke prinose u periodu rasta tržišta. Međutim, kretanje cena svih kriptovaluta previše je hirovito i nepodesno za predviđanje. U prilog ovoj tvrdnji

purchase of real-life products or a transaction at the cryptocurrency exchange.

The most infamous example is certainly the Silk Road, a website that is practically a copy of the famous eBay auction site. It provided an online marketplace for buying weapons, narcotics, pornographic content, stolen credit cards, false personal documents and other illegal goods (Van Hout & Bingham 2013). Bitcoin was used as the sole means of payment. In October 2013, the FBI arrested William Ulbricht on charges of organizing and running the Silk Road website under the name "Dread Pirate Roberts", while the website itself was shut down. The total website traffic was estimated to around 9.5 million Bitcoin, which at the current exchange rate was worth about one billion US dollars, while the current value of that amount is much higher (Konrad, 2013).

The shutdown of one website did not result in the abolishment of criminal activities financed with cryptocurrencies. New illegal projects, such as Silk Road 2.0, AlphaBay and Hansa, tried to take up the vacant space. Even the dominant means of payment changed, so instead of Bitcoin, the cryptocurrency Monero has been used. However, all mentioned websites had the same infrastructure problem - centralized servers. Following the actions of cyber-criminal units in several countries, websites were shut down one by one (Liao, 2017). The real challenge for the authorities would be decentralized black markets, such as the Eden network (Devoe, 2018). With the application of blockchain technology for the purposes of website construction, the centralized shutdown is avoided, because there is no single server through which control is exercised. The existence of these sites does not mean that violence and illegal activities' level will rise, but that the participants will communicate more easily and quickly. It also signals the inability of the authorities to confront them, which could create unimaginable consequences. In the long run, every type of illegal electronic business would be encouraged, and the possible application in terrorist activities need not be especially emphasized.

In order to prevent the use of cryptocurrencies for money laundering and terrorism financing, the European Commission has adopted the fifth

Anti-Money Laundering Directive (Directive 2018/843). This Directive clearly highlights the danger of using cryptocurrencies (which the Directive authors named "virtual currencies") and cards with prepaid monetary values for the purposes of terrorism financing. The usage of these payment means for financing criminal activities on the territory of the European Union has been previously proven (Marria, 2018). The key requests which the new Directive sets for cryptocurrency exchanges, the companies that issue digital wallets and the users, refer to abolishing anonymity. On the one hand, all companies would have an obligation to register with regulatory authorities and to submit data about users when required. On the other hand, individuals have to prove the origin of means during the conversion of cryptocurrencies to convertible money. The required amendments have introduced a radical change, which would make electronic money distribution similar to managing a current account.

Conclusion

Cryptocurrency mining is much costlier than it first appears to be. Having in mind that all calculations are based on indirect indicators, one can conclude that they are approximations rather than exact results. This is why their key contribution is not in determining the precise financial result, but in clarifying the mining economic results. Two general conclusions could be drawn.

Firstly, the electricity costs made by computer networks, even without taking into consideration cooling system, are so high that the overall profitability of the complete process depends only on secondary market prices. On the example of Bitcoin, it is shown that the miners' market is slowly adapting to the movement of cryptocurrencies on the secondary market. This means that the increase in the number of miners (therefore an increase in cost to the whole system) would occur after a great increase of the secondary price, which already happened in the second half of 2017. In the case of a sudden price downfall after a few months, most of the mining community would experience a loss because it spends more than it can earn.

govori činjenica da su sve kriptovalute koje su postigle najviši rast u 2017. godini, tokom prve polovine 2018. godine ostvarile negativni rast. Samim tim, trgovci koji su kupovali na početku godine gotovo sigurno su ostvarili gubitke. Kretanje cena svih kriptovaluta je praćeno čestim oscilacijama izraženih amplituda, što umanjuje mogućnost da trgovac, koji često trguje, zabeleži ukupan pozitivni rezultat. Visoke stope rasta dovele su do nerealnih vrednosti više desetina kriptovaluta. Ključno je pitanje da li pad vrednosti u 2018. godini predstavlja stabilizaciju ili pucanje cenovnog balona. Ukoliko balon još nije pukao, onda će se to dogoditi u budućnosti, pri čemu će trgovci koji poseduju velike količine kriptovaluta podneti najveći gubitak.

Težnje Evropske unije da institucionalizuje poslovanje sa kriptovalutama mogu imati pozitivne i negativne efekte. Suzbijanje prostora za upotrebu kriptovaluta u svrhe finansiranja terorizma i kriminalnih aktivnosti, kao i pranja novca, svakako se mogu posmatrati kao pozitivni pomaci. Obaveza da se dokaže poreklo sredstava prilikom razmene za konvertibilni novac predstavlja osnov za stvaranje konzistentne poreske politike, čime bi se sprečila mogućnost nekontrolisanog bogaćenja pojedinaca i grupa. Ipak, u nastojanjima da se

tržište kriptovaluta reguliše treba biti obazriv. Prevelik stepen kontrole može dovesti do odliva uložених sredstava u nove hibridne forme koje ne podležu regulaciji. Identičan proces je već viđen sa aktivnostima bankarstva u senci, u godinama koje su prethodile finansijskoj krizi iz 2007. godine. Zamena za kriptovalute može biti stvorena neočekivano, baš kao što se i Bitcoin pojavio. Lako se može dogoditi da taj novi supstitut bude komplikovaniji za praćenje i kontrolisanje. Zato bi regulatorne vlasti trebalo da imaju pristup minimalnog potrebnog nivoa kontrole, da bi očuvale kriptovalute, kao opasnost koja je u najvećoj meri poznata.

Može se zaključiti da su kriptovalute danas daleko od njihove prvobitne namene - sredstva plaćanja u elektronskoj trgovini. Trenutno predstavljaju neregulisane špekulativne predmete trgovine, bez jasne unutrašnje vrednosti. Nagli rast tokom 2017. godine je naišao na granicu, za čiji prelazak je potreban sveži kapital. Takav ekonomski model je neodrživ, ali celokupan koncept ne treba shvatiti potpuno negativno. Blockchain će kao tehnologije definitivno imati velike primene u budućnosti i to ne samo u platnom prometu. Treba očekivati razvoj državnih ili regulisanih privatnih kriptovaluta, čiji će sistemi biti troškovno efikasni.

Secondly, even when the entire mining community operates positively, which means it can pay off all costs by selling the coins, very little is known about the income distribution. Cost distribution is known and it depends on the number and type of computers used by the miners. The PoW algorithm is designed to reward the miners who are involved in the system operations according to the accomplished results, not according to the rotating principle. That means that the award, or gaining new coins, is not guaranteed at any point. If the miners decide not to form small communities, it may happen that they do not earn anything, regardless of how their computers are engaged. This means that even when the complete system operates positively, miners could earn nothing or so little that they could not cover their own expenses.

When it comes to cryptocurrency trading, it is clear that individuals could make high profits in a period of market growth. However, the price movements of all cryptocurrencies are too whimsical and unsuitable for predictions. The fact that all cryptocurrencies which achieved the highest growth in 2017 recorded a negative growth during the first half of 2018 fully supports this assertion. Therefore, those traders which were buying it in the beginning of the year have definitely suffered losses. The movement of cryptocurrencies' prices is characterized by frequent oscillation with prominent amplitudes, which diminishes the possibility for a trader, who trades often, to record a total positive result. High rates of growth led to the unrealistic values of more cryptocurrencies. The key question is whether the value drop in 2018 represents stabilization or a burst of the price bubble. If the bubble has not burst yet, then this will happen in the future, whereby the traders who own great amount of cryptocurrencies will endure the greatest loss.

The aspirations of the European Union to institutionalize the cryptocurrency

business could have positive and negative effects. Decreasing the leeway for using cryptocurrencies for the purposes of financing terrorism and criminal activities, as well as money laundering, can absolutely be seen as a positive move. The responsibility to prove the origin of funds during exchange for convertible money represents the base for the creation of a consistent tax policy, which would prevent the possibility of individuals and groups uncontrollably amassing wealth. However, in order to regulate the cryptocurrency market, one should be careful. An excessive degree of control could lead to an outflow of funds invested in new hybrid forms which are not subject to the regulation. An identical process has already been seen with the activities of shadow banking, in the years which preceded the financial crisis in 2007. A replacement for cryptocurrencies could be created as unexpectedly, as Bitcoin appeared. It could easily happen that this new substitute is more complicated to monitor and control. Because of that, regulatory authorities should embrace an approach of minimal level of control necessary, in order to preserve cryptocurrencies, as a danger that is mostly known.

It can be concluded that cryptocurrencies today are far from their original purpose - a means of payment for electronic commerce. Currently, they represent unregulated speculative trade items, without clear internal value. An accelerated growth in 2017 reached the limit, and fresh capital is needed to overcome it. Such an economic model is unsustainable, but the whole concept should not be taken completely negatively. As far as technology goes, blockchain will definitely have great application in the future, and not just in the payment industry. The development of state or regulated private cryptocurrencies, whose functioning would be cost effective, should be expected in the future.

Literatura / References

1. Chapparo, F. (2017), Bitcoin Went Bonkers in 2017 - Here's What Happened as the Cryptocurrency Surged More Than 1000%, *Business Insider*, December 30th
2. Coase (1972), Durability and Monopoly, *Journal of Law and Economics*, 15(1), pp. 143-149
3. de Vries, A. (2018), Bitcoin's Growing Energy Problem, *Joule*, 2(5), pp. 801-805
4. Devoe, R. (2018), Decentralized Darknet Markets Could Lead to Unstoppable Silk Road Clones, *Blockonomi*, July 12th
5. Dinić, V. (2014), Bitkojn kao decentralizovana kriptovaluta, *Bankarstvo*, 17(2), str. 108-137
6. European Commission (2009), Directive 2018/843 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, *Official Journal of European Union*, L series
7. Greenberg, A. (2017), Monero, the Drug Dealer's Cryptocurrency of Choice, Is On Fire, *Wired*, January 25th
8. Hileman, G., Rauchs, M. (2017), *Global Cryptocurrency Benchmarking Study*, University of Cambridge - Judge Business School
9. Holthaus, E. (2017), Bitcoin Could Cost Us Our Clean-Energy Future, *Grist*, December 5th
10. Iansiti, M., Lakhani, K.R. (2017), The Truth About Blockchain, *Harvard Business Review*, 62(1)
11. Konrad, A. (2013), Feds Say They've Arrested 'Dread Pirate Roberts,' Shut Down His Black Market 'The Silk Road', *Forbes*, October 2nd
12. Lee, T.B. (2013), An Illustrated History of Bitcoin Crashes, *Forbes*, April 11th
13. Liao, S. (2017) After AlphaBay and Hansa, There Are Only More Dark Web Takedowns to Come, *The Verge*, June 22nd
14. Liška, T., Sochor, T., Sochorová, H. (2010), Comparison Between Normal and TOR-Anonymized Web Client Traffic, *Procedia - Social and Behavioural Studies*, 9, pp. 542-546
15. Marria, V. (2018), The EU's 5th Anti-Money Laundering Directive: What Does It Mean?, *Forbes*, September 13th
16. Nakamoto, S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*, bitcoin.org
17. Osbourne, C. (2018), Cryptocurrency Miners Bought 3 Million GPUs in 2017, *ZDNet*, March 1st
18. Price, R. (2017), Someone in 2010 Bought 2 Pizzas with 10,000 Bitcoins - Which Today Would Be Worth \$100 Million, *Business Insider*, November 28th
19. Rogers, A. (2017), The Hard Math Behind Bitcoin's Global Warming Problem, *Wired*, December 15th
20. Rosoff, M. (2016), PC Sales Hit an Eight-Year Low in 2015, *Business Insider*, January 13th
21. Sajana, P., Sindhu, M., Sethumadhavan, M. (2018), On Blockchain Application: Hyperledger Fabric and Ethereum, *International Journal of Pure and Applied Mathematics*, 118(18), 2965-2970
22. Samson, A. (2018), 'Environmental Disaster': BIS Warns on Cryptocurrencies, *Financial Times*, June 18th
23. Selgin, G. (2014), Synthetic Commodity Money, *Journal of Financial Stability*, 17(C), pp. 92-99
24. Sparavigna, A.C. (2014), Some Notes on Gresham's Law of Money Circulation, *International Journal of Sciences*, 3(2), pp. 80-91
25. Tomić, N., Todorović, V., Jakšić, M. (2017), Misuses of Electronic Payment Systems, *Contemporary Issues in Economics, Business and Management - EBM 2016*, Stojanović-Aleksić, V. (ed.), Faculty of Economics University of Kragujevac, pp. 245-253

26. Van Hout, M.C., Bingham, T. (2013), „Silk Road“, the Virtual Drug Marketplace: A Single Case Study of User Experience, *International Journal of Drug Policy*, 24, pp. 385-391
27. Wang, J.C. (2014), A Simple Macroeconomic Model of Bitcoin, Bitquant Research Laboratories Working Paper No. 1
28. Warren, T. (2018), Bitcoin Mania is Hurting PC Gamers by Pushing Up GPU Prices, *The Verge*, January 30th
29. Williams-Grut, O. (2017), The Electricity Used to Mine Bitcoin This Year is Bigger Than the Annual Usage of 159 Countries, *Business Insider*, November 26th

Ostali izvori / Other Sources

1. <https://digiconomist.net/bitcoin-energy-consumption> (datum pristupa 03.10.2018.)
2. <https://www.economist.com/buttonwoods-notebook/2017/11/01/the-bitcoin-bubble> (datum pristupa 04.10.2018.)
3. <https://www.gartner.com/newsroom/id/3881812> (datum pristupa 05.10.2018.)
4. <https://cointelegraph.com/news/the-cream-of-the-crypto-crop-10-best-performing-assets-in-2017> (datum pristupa 06.10.2018.)