BITCOIN – PREDNOSTI I RIZICI

BITCOIN - BENEFITS AND RISKS

Petar Čekerevac

Hilltop Strategic Services, Beograd, Srbija

Zoran Čekerevac

Fakultet za poslovno industrijski menadžment, "Union" Univerzitet, Beograd, Srbija

© MESTE NGO

JEL category: **E4, E41, E5, E51**

Apstrakt

Bitcoin, digitalni novac, danas dolazi u žižu interesovanja. On podrazumeva P2P interakciju, gde svaki vlasnik prenosi elektronski novčić sledećem vlasniku potpisivanjem i dodavanjem na kraj novčića heša prethodne transakcije i javnog ključa sledećeg vlasnika. Verifikacija plaćanja se ostvaruje obaveštavanjem cele Bitcoin mreže o izvršenoj transakciji. Na taj način se sprečava dvostruko plaćanje i izbegava generisanje nepostojećeg novca. Pri ovim transakcijama se ne prenose lične informacije između učesnika u transakciji. Za razliku od potpuno anonimnih transakcija, pri plaćanju Bitcoinima ostaje trag zabeležen i dostupan javnosti. Međutim, učesnici u transakciji ne moraju da posluju pod svojim imenima, već mogu da se prijavljuju preko pseudonima. Bitcoin nudi korisnicima niže troškove transakcije, povećanu privatnost i na duže vreme zaštitu kupovne moći od inflacije. Međutim, Bitcoin još uvek nema dovoljno učesnika i finansijsku bazu da bi obezbedio stabilnost pa cena Bitcoina značajno osciluje. Još uvek među korisnicima postoji neizvesnost o bezbednosti na krađu i prevare. I među nadležnim državnim organima postoje brojne dileme i analize postojećih i budućih rizika vezanih za primenu Bitcoina. Iako broj korisnika Bitcoin sistema raste, on je još uvek mali u poređenju sa kreditnim karticama i upotrebom USD, EUR i drugog novca. Ipak, Bitcoin sistem predstavlja izuzetno konceptualno i tehničko dostignuće. Njega mogu da koriste i postojeće finansijske institucije (koje mogu i same da emituju svoje bitcoine). Takođe, nema prepreka da čak i vlade država same koriste ovu tehnologiju. U ovom radu su prikazani tehnologija Bitcoina, prednosti i neki rizici kojima su izloženi korisnici ovog sistema.

Ključne reči: Bitcoin, heš, eNovčanik, finansijske transakcije, novac, fiat novac, zlato, srebro, dolar

Abstract

Bitcoin, new digital money, recently got into focus. It uses P2P interaction where each owner transfers the electronic coin to the next owner signing and adding to the end of the coin a hash of the previous transaction and the public key of the next owner. Payment verification is accomplished by notifying the entire network about the transaction. This prevents double-spending and avoids the generation of non-existent money. Personal information between parties in the transaction are not transferred. Unlike completely anonymous transaction, the Bitcoin transactions remain recorded and

Adresa autora zaduženog za korespondenciju::

Petar Čekerevac

petar@cekerevac.eu

exist money. Personal information between parties in the transaction are not transferred. Unlike completely anonymous transaction, the Bitcoin transactions remain recorded and

available to the public. However, participants in the transaction do not have to operate under their own names, and can log in through their aliases. Bitcoin offers lower transaction costs, increased privacy and for more time protection of the purchasing power from inflation, but still have no enough participants and financial base to ensure stability. So its price significantly oscillates. Still, among the users, there is uncertainty about the safety on the theft and fraud. Also, among the relevant state authorities, there are numerous dilemmas and analyses of present and future risks related to the implementation of Bitcoin. Although the number of users of the Bitcoin system grows, it is still small compared with the number of credit cards users, or use of the USD, EUR and other money. However, the Bitcoin system is high conceptual and technical achievement. It can be used by existing financial institutions (which also may emit their own bitcoins). There is no obstacle that even the governments themselves use this technology. In this paper, here will be presented Bitcoin technology, the advantages of this system and some of the risks to whom users are exposed.

Keywords: Bitcoin, hash, eWallet, transactions, money, fiat money, gold, silver, dollar

1 UVOD

U ljudskoj istoriji postojala su različita sredstva plaćanja. Američki dolar je bio najkorišćenije sredstvo plaćanja skoro pedeset godina posle Drugog svetskog rata, ali je zahvaljujući mnogim potezima Centralne banke SAD (Federal Reserve) ugled dolara znatno opao i mnogi su počeli da traže alternativu. (FEE, 2013) Ako se pogleda dublje u istoriju može se videti da su ljudi koristili različita sredstva plaćanja: srebro, zlato, pšenicu, školjke, duvan, so, papir... Mnoga

sredstva plaćanja su nestala iz upotrebe, a samo ih je nekoliko ostalo: zlato, srebro i papirni novac. Da bi neko sredstvo bilo pogodno za plaćanje potrebno je da poseduje neke bitne karakteristike, npr: da ostaje vredno u dugom vremenskom periodu, da ga ima u ograničenim količinama, da se može lako deliti na delove, da bude prenosivo... Ako se te karakteristike porede za dolar, zlato (srebro) i bitcoin mogu se dobiti rezultati prikazani u tabeli 1.

Tabela 1 Poređenje karakteristika dolara, zlata (srebra) i bitcoina

Karakteristika
Zadržava vrednost	✗	✓	✓
Ima ga u ograničenim količinama	✗	✓	✓
Lako je deljiv	✓	✓	✓
Lako je prenosiv	✓	✓	✓✓

Autori po ugledu na (FEE, 2013)

Današnja plaćanja koja u sebe uključuju i finansijske institucije povezana su sa brojnim ograničenjima i uključuju relativno velike troškove čiji se iznosi mere procentima. Tako, npr. kada novac promeni nekoliko ruku znatna suma ostane u bankama. Zbog toga, a i niza drugih razloga, kreiran je i 2009-e godine lansiran bitcoin¹, digitalni novac. Za kreiranje bitcoina zaslužan je

autor koji se koristio pseudonimom Satoshi Nakamoto, koji je i objavio principe svoje kreacije u članku *Bitcoin: A Peer-to-Peer Electronic Cash System* (Nakamoto, 2008). Bitcoin² podrazumeva P2P interakciju, a elektronski novčić se definiše kao lanac digitalnih potpisa. Svaki vlasnik prenosi novčić sledećem vlasniku potpisivanjem heša³ prethodne transakcije i javnog ključa sledećeg

¹ bitcoin – napisan malim početnim slovom b podrazumeva bitcoin kao novčanu jedinicu (Anon, Some Bitcoin words you might hear, 2009-2014)

² Bitcoin – napisan velikim početnim slovom B podrazumeva Bitcoin kao concept (Anon, Some Bitcoin words you might hear, 2009-2014)

³ Hešing (hashing) predstavlja proizvodnju heš vrednosti za pristup podacima ili za obezbeđenje sigurnosti. Heš vrednost (ili jednostavno heš) predstavlja broj generisan iz niza karaktera nekog teksta. Heš je značajno kraći od samog teksta, a generiše se formulom koja je takva da je ekstremno

vlasnika, i dodavanjem svega toga na kraj novčića. Primalac može da proveri potpise da bi proverio lanac vlasništva. Verifikacija plaćanja se ostvaruje obaveštavanjem cele mreže o izvršenoj transakciji. Na taj način se sprečava dvostruko

plaćanje⁴ i izbegava generisanje nepostojećeg novca. Provera može da potraje i nekoliko minuta. Prosečno trajanje provere transakcije prikazano je na slici 1.

Slika 1 Prosečno trajanje provere transakcije od plaćanja do dobijanja potvrde o transakciji izraženo u minutama (Blockchain.info, 2014)

Pri ovim transakcijama se ne prenose lične informacije između učesnika u transakciji. Za razliku od potpuno anonimnih transakcija, pri plaćanju Bitcoinima zapis o transakciji ostaje zabeležen i dostupan javnosti. Učesnici u transakciji ne moraju da posluju pod svojim imenima, već mogu da se prijavljuju preko pseudonima.

Značajno pitanje je: Kako nastaju bitcoini? Da bi nešto imalo vrednost potrebno je da njegovo kreiranje bude skupo, skuplje od tržišne vrednosti toga što je kreirano. Npr. zlata ima u zemlji i svima je dostupno, ali njegovo dobijanje iz zemlje je skupo i neisplativo ogromnoj većini. Tako ogromna većina korisnika zlata nema mogućnost ni interes da rudari zlato, a svaki novi kilogram proizvedenog zlata donosi proizvođaču značajnu vrednost. Po sličnom principu se kreiraju bitcoini. Treba izvršiti mnoštvo računskih operacija po

komplikovanom algoritmu da bi se izrudario jedan bitcoin. Vrlo je verovatno da će se pojedinačni rudar bitcoina silno namučiti pre nego što izrudari neki bitcoin. Zato je preporuka da se više rudara udruži i da zajedničkim snagama i sa više računara pokušaju da izrudare bitcoine.

Problem koji rudari rešavaju se ugrubo svodi na sledeće: Neka je x niz blokova (tzv. *block chain*⁵), neka je y predloženi dodatni blok i neka je n dodatni broj. Cilj je da se pronađe n tako da rezultujuća heš funkcija $f(x,y,n)$ ima vrednost manju od postavljene vrednosti α . (Velde, 2013)

Heš funkcija mapira tekst ili brojeve proizvoljne dužine u broj fiksne dužine. Npr. uzimanje prvog slova reči ili sabiranje svih cifara jednog broja dok se kao rezultat ne dobije broj koji se može iskazati jednom cifrom mapira bilo koju reč ili broj hešom dužine jedan. Heš funkcija kod Bitcoina je deterministička, ali toliko kompleksna da rezultat

mala verovatnoća da će neki drugi tekst dati istu heš vrednost. (Anon, hashing, 2014) (Devoto, 2014)

⁴ Dvostruko plaćanje podrazumeva da maliciozni korisnik pokušava da istim bitcoinima plaća dva različita računa i da na taj način generiše nepostojeće bitcoine.

⁵ Block chain – javni zapis Bitcoin transakcije po hronološkom redosledu. On se razmenjuje među Bitcoin korisnicima, a koristi se verifikaciju Bitcoin transakcija i sprečava dvostruko plaćanje. (Anon, Some Bitcoin words you might hear, 2009-2014)

liči na slučajne brojeve. Zato je rudarima veoma teško da dođu do odgovarajućeg rešenja problema. Potrebno je da isprobaju mnogo različitih kombinacija za različite vrednosti n , što zahteva velike računarske kapacitete i veliku potrošnju vremena i energije dok se ne ispuni traženi uslov. Što je niža vrednost α to je uslov teže ispuniti. Za razliku od toga, predloženo rešenje (x, v, n) se može lako proveriti. Deo broja n uključuje verifikaciju da bitcoin unet u blok y nije već potrošen u bloku x .

Kod omogućava svakom rudaru da u blok y uključi određenu vrstu transakcije koja kreira N novih bitcoina i pripisuje ih samom rudaru. Prvi rudar koji dođe do rešenja šalje informaciju svim ostalim rudarima koji tu informaciju verifikuju. Posle verifikacije (kada verifikaciju izvrši većina rudara) novi blok se dodaje lancu i srećni rudar postaje vlasnik N novih bitcoina.

Deo Bitcoin protokola reguliše vrednosti N i α u vremenu. Težina α se podešava svake dve nedelje kako bi se obezbedila dinamika kreiranja bitcoina od šest puta na sat. Što više rudara radi na kreiranju novih bitcoina uslovi su strožiji. Početna vrednost broja N od 50 prepolovljava se svakih 210.000 blokova. Time je definisano da se broj raspoloživih bitcoina asimptotski približava broju 21.000.000. (Velde, 2013) Tako, kao što u rudnicima posle duže eksploatacije nalazište postaje sve siromašnije i dobijanje zlata sve manje isplativo, i rudarenje bitcoina postaje neprofitabilno. Da rudarenje ne bi zamrlo i ovde je predviđeno da se rad rudara može nagraditi iz drugih fondova. Pri Bitcoin transakcijama, učesniku u transakciji je omogućeno da „plati“ tu transakciju kako bi se obavila po bržoj proceduri. Tarifa za transakciju se definiše po posebnom algoritmu u kome se uzimaju u obzir veličina transakcije, starost zapisa i/ili dužina zapisa u kB. Ukoliko je bilo koja „novčanica“⁶ iz novčanika⁷ u transakciji manja od 0,01 XBT⁸, ili ako je kusur od pri transakciji manji od 0,01 XBT onda je obavezno plaćanje naknade za transakciju u iznosu 0,0001

XBT po takvoj novčanici. Na taj način se želi da se obeshrabri slanje isuviše malih vrednosti. Zadatak novčanika je izabere najpovoljniju kombinaciju novčanica pri plaćanju.

Primer načina plaćanja bitcoinima prikazan je na slici 2. Plaćanje po kB podrazumeva da se naknada za transakciju određuje na osnovu dužine zapisa u bajtima. Veličina zapisa zavisi brojeva ulaza i izlaza pri toj transakciji. Dužina zapisa L se ugrubo određuje prema formuli:

$$L = 148 \cdot \text{ulazni_broj_novčanica} + \\ + 34 \cdot \text{izlazni_broj_novčanica} + 10$$

Ulazni broj novčanica podrazumeva broj novčanica, zapisa, koji se izuzima iz novčanika, a izlazni broj novčanica obuhvata iznos koji se šalje, ali i povraćaj razlike uplaćene i potrebne sume, kusur. Ukoliko je $L < 10000$ bajtova i vrednost transakcije dovoljno visoka, a zapisi dovoljno stari, transakcija je besplatna. U protivnom se naplaćuje. U slučaju plaćanja naknade po KB ne naplaćuju se druge naknade.

Pri transakcijama prioritet imaju stariji bitcoin zapisi i zapisi sa većom vrednošću. U svakoj transakciji je naznačen prioritet određen starošću, veličinom i brojem inputa. Za svaki input novčanik računa proizvod vrednosti inputa sa starošću inputa u bloku, a zatim se sumiraju ti proizvodi i dobijena suma deli veličinom transakcije izraženom u bajtovima. Ako je dobijeni količnik manji od 0,576 takva transakcija zahteva plaćanje naknade. (Bitcoin Transaction Fees Explained, 2014) To znači da se u transakciju može uključiti i mnogo sitnih i/ili novih novčanica i da se ne plati naknada za transakciju ukoliko se uz njih priključi i neka valika stara novčanica, jer se pri proračunu naknade kao merodavna uzima srednja vrednost. Može se desiti da je u jednom trenutku potrebno platiti naknadu, a da ukoliko se transakcija izvrši kasnije naknada više nije potrebna, jer su novčanice dovoljno odležale. Detaljnije o primeni Bitcoin tehnologije i radu novčanika (Bitcoin klijenata) objašnjeno je u tezi Rostislava Skudnova Bitcoin Clients (2012)

⁶ Na računu korisnika (novčanik, Bitcoin novčanik, eWallet) se bitcoini ne sabiraju prosto dajući neki broj, već se zadržavaju u obliku u kom su pristigli u novčanik, pa se može reći da su ekvivalentni novčanicama iz uobičajenog načina plaćanja.

⁷ Novčanik – Bitcoin novčanik u Bitcoin mreži je ekvivalent fizičkom novčaniku iz uobičajenog načina plaćanja. Novčanik sadrži korisnikov privatni ključ koji

mu omogućava da troši svoje bitcoine iz lanca blokova (block chain).

⁸ XBT – nova skraćenica za Bitcoin koju dolazi od ISO koja održava listu valuta. Ukoliko valuta nije povezana sa nekom državom njena skraćenica počinje sa „X“. SAD dolar ima skraćenicu USD, a zlato ima oznaku XAU. Prethodno je za bitcoin korišćena oznaka BTC (Matonis, 2013)

Slika 2 Tehnologija plaćanja bitcoinima

Izvor: Autori po uzoru na (Anon, Bitcoin Transaction Fees Explained, 2014)

Neki primeri plaćanja i određivanja naknade prikazani su u Bitcoin Transaction Fees Explained (2014)

2 PREDNOSTI KORIŠĆENJA BITCOINA

Bitcoin nudi korisnicima niže troškove transakcije, povećanu privatnost i na duže vreme zaštitu kupovne moći od inflacije. Međutim, Bitcoin još uvek nema dovoljno učesnika i finansijsku bazu da bi obezbedio stabilnost pa cena Bitcoina značajno osciluje. Još uvek među korisnicima postoji neizvesnost o bezbednosti na krađu i prevare. I među nadležnim državnim organima postoje brojne dileme i analize postojećih i budućih rizika vezanih za primenu Bitcoina. I pored svih dilema mnogi, uključujući i Ron Pola⁹, vide u bitcoinu vide odlično sredstvo plaćanja koje omogućava (Lukić, 2013):

- Kupovinu bilo čega u tajnosti,
- Nepostojanje banaka u lancu plaćanja,
- Plaćanje bez provizije,
- Nema brige da će inflacija obezvređiti novac u budućnosti.

Kao primer može da posluži analiza promene vrednosti USD u vremenu. Ukoliko je neko npr.

1952. godine u novčaniku imao 100 USD, zbog inflacije bi, koristeći Consumer Price Index, danas mogao da računa sa 11,56USD. Situacija je i gora ako se računa prema drugim kriterijumima. U tabeli 2 date su vrednosti današnjeg broja USD koje predstavljaju ekvivalent vrednosti 100USD iz 1912. i 1962. godine.

Kako je došlo do tolikog pada vrednosti USD? Jednostavno. Štampanjem novca bez pokrića. Do sedamdesetih godina prošlog veka štampanje dolara je bilo uz brojna ograničenja, a onda je poslednjih decenija Centralna banka SAD šampala milijarde dolara devalvirajući vrednost USD. Kod Bitcoina je tačno poznato koliko će kada biti bitcoina na tržištu. Zahvaljujući primenjenom algoritmu zna se da će se broj bitcoina asimptotski približavati cifri od 21 miliona. Od prvog bitcoina lansirano 2009. godine, njihov broj je porastao na oko 12 miliona decembra 2013 (blockchain.info, Total Bitcoins In Circulation, 2014) i da će ih 2024. biti oko 18 miliona, a 2140. oko 21 milion. Posle toga broj emitovanih bitcoina se praktično neće ni menjati. Na taj način je obezbeđen drugi bitan kriterijum vrednosti iz tabele 1.

⁹ Ronald Ernest "Ron" Paul, američki lekar i republikanski političar, često nazivan I "Doktor Ne" zbog konzistentnog i upornog protivljenja i

glasanja protiv svakog predloga zakona za koji veruje da krši Ustav SAD.

Tabela 2 Vrednost u 2012. godini ekvivalentna vrednosti 100 USD iz 1914. i 1964. godine

	\$100 iz godine	1912.	1964.
Ekvivalent u 2012.	koristeći Consumer Price Index (Index potrošačkih cena)	\$2400	\$751
	koristeći GDP deflator (BDP deflator)	\$1730	\$579
	koristeći unskilled wage (plata nekvalifikovanog radnika)	\$9900	\$794
	koristeći Production Worker Compensation (plata proizvodnog radnika)	\$14000	\$966
	koristeći nominal GDP per capita (nominalni BDP po glavi stanovnika)	\$14300	\$1490
	koristeći relative share of GDP (relativni udeo u BDP)	\$45600	\$2450

Autori prema podacima iz Williamson (2014)

I USD i srebro i zlato je teško falsifikovati. S obzirom da je bitcoin baziran na softveru otvorenog koda može se učiniti da ga je lakše falsifikovati. Međutim, Bitcoin je baziran na kriptografiji i praktično je nemoguće (ili bolje rečeno, neisplativo) falsifikovati bitcoin. Pored toga, svaka transakcija zahteva potvrdu ostalih učesnika u sistemu, što sprečava eventualne malverzacije dvostrukog plaćanja.

Uz prethodno navedene pogodnosti, prednosti Bitcoina su i:

- Bitcoin se može izuzetno lako prenositi iz bilo koje tačke u bilo koju tačku na planeti Zemlji nezavisno od količine i geografskog položaja ukoliko postoji Internet konekcija;

- Prihvatanje bitcoina je besplatno;
- Nema povraćaja novca (chargeback);
- Bitcoin se može zameniti za bilo koju valutu.

Kao rezultat sagledavanja ovih prednosti beleži se i povoljan gradijent porasta ukupnog broja transakcija prikazan na slici 3.

Teško je neki od načina plaćanja proglasiti najboljim, pogotovu što se uslovi stalno menjaju, ali je verovatno da će Bitcoin zahvaljujući nizu navedenih prednosti uspeti da zauzme vrlo visoku poziciju. Takođe, najverovatnije je i da će današnji dolarski način plaćanja doći u situaciju da bude potisnut na (znatno) niže pozicije. (FEE, 2013).

Slika 3 Ukupan broj transakcija 2009 – 2014 (blockchain.info, Total number of transactions, 2014)

3 RIZICI PRI KORIŠĆENJU BITCOINA

Bitcoin omogućava korisniku da kreira neograničen broj novčanika. Zato se ne može sa sigurnošću reći koliko je rudara na mreži i koliki je stvarni broj korisnika Bitcoina, ali je primetno da je

broj novčanika u periodu januar 2013 – januar 2014 porastao velikom brzinom. Od nastanka (januar 2009) do januara 2013 bilo je kreirano oko 50 hiljada novčanika, a za sledećih godinu dana još preko 1,2 milion novčanika. Prikaz ukupnog broja Bitcoin novčanika dat je na slici 4.

Slika 4 Ukupan broj korisnika Bitcoin novčanika (blockchain.info, My Wallet Number Of Users, 2014)

Bitcoin zbog relativne anonimnosti svojih korisnika, omogućava pojedincima da generišu, prenesu, operu i/ili ukradu novčana sredstva. On svojom primenom donosi pred istražitelje slične izazove kao i drugi virtualni novac, npr. WebMoney, ali i dopunske teškoće zbog svoje decentralizovane prirode. Prema procenama FBI, sa priličnom pouzdanošću, u bliskoj budućnosti će kriminalci tretirati Bitcoin kao drugu opciju plaćanja, mada neće napuštati postojeće tradicionalne načine plaćanja. Ovaj zaključak je baziran na velikim fluktuacijama kursa bitcoin-a u 2011-oj godini. Sa manjom pouzdanošću FBI smatra da će se Bitcoin koristiti za pranje novca. (FBI, 2012) Ovu pretpostavku je teško dokazati jer ne postoji dovoljno izveštaja o Bitcoinu. Zbog

svoje decentralizacije napadi na sistem će se verovatno pokazati kao malo uspešni, ali će se kriminalci fokusirati na napade na privatne Bitcoin novčanike i pokušati da pri tom koriste servise treće-strane.

Bitcoin transakcije su javno publikovane, ali jedina informacija koja identifikuje Bitcoin korisnika je pseudo slučajno generisana Bitcoin adresa koja čini transakciju prilično anonimnom. Transakcija ipak nije potpuno anonimna, jer, iako je Bitcoin izrazito decentralizovan, ipak postoji mesto koje može dati podatke o učesnicima u plaćanju. To je mesto gde se Bitcoin pretvaraju u *fiat valutu*, tj. dekretni novac¹⁰. Da povećaju anonimnost transakcije korisnici mogu da (Wiki, 2013) (Coderrr, 2011) (Lee, 2011) (Lowenthal, 2011):

¹⁰ fiat novac, ili fiducijarni novac; savremene vrste novca nemaju unutrašnju vrednost, već samo deklarativno predstavljaju novac pa se zato

nazivaju fiat novcem ili fiducijarnim novcem (lat. fiducija = poverenje) (Čičin-Šain, 2007)

- Kreiraju i koriste novu Bitcoin adresu za svako dolazno plaćanje;
- Rutiraju celokupan Bitcoin saobraćaj preko anonimajzera;
- Kombinuju stare Bitcoin adrese u novu adresu da bi izvršili nova plaćanja;
- Koriste specijalizovane servise za pranje novca;
- Koriste eWallet (eNovčanik) usluge treće strane da konsoliduju adrese. Danas postoje usluge treće strane koje nude opciju kreiranja eNovčanika koji omogućava korisnicima da konsoliduju mnoge Bitcoin adrese i omoguće jednostavan pristup svojim bitcoinima sa bilo kog uređaja;
- Pojedinci mogu da kreiraju Bitcoin klijente da lako povećaju anonimnost (kao i da imaju mogućnost izbora Bitcoin adrese sa koje će da izvrše plaćanje), pri čemu korisnici ne moraju da budu posebno tehnički obrazovani da bi transakcije učinili anonimnim.

Specifičnosti Bitcoina danas predstavljaju poseban izazov otkrivanju i zaustavljanju ilegalnih aktivnosti. Kao decentralizovani sistem, Bitcoin nema neku centralnu instituciju i nije u mogućnosti da kontroliše i da izveštava o sumnjivim aktivnostima u skladu sa programom sprečavanja pranja novca ili da prihvata i izvršava zakonske zahteve, npr. sudske pozive. Prema FBI (2012) glavne ranjivosti decentralizovanih sistema plaćanja su:

- Nepostojanje softvera ili sposobnosti praćenja i identifikovanja sumnjivih monetarnih šablona koji se javljaju pri pranju novca;
- Nepostojanje identifikacije o stvarnim vlasnicima računa kao i o njihovoj stvarnoj lokaciji;
- Nepostojanje zapisa o istoriji transakcija povezanog sa stvarnim učesnicima u transakciji;
- Znatno teža identifikacija izvora sredstava plaćanja u poređenju sa drugim vrstama onlajn novca;

- Organi za sprovođenje zakona ne mogu da ciljaju jednu centralnu lokaciju ili kompaniju pri istražnim radnjama ili da isključe sistem.

Kao što je ranije izloženo, Bitcoin, kao i većina virtualnog novca, zahteva od korisnika da koriste usluge treće strane pri pretvaranju bitcoina u fiat novac. Kupovina, prodaja, trgovina bitcoinima ili njihova konverzija u drugu vrstu novca obavlja se van P2P sistema. Zbog broja i različitosti trećih strana realna je mogućnost prebacivanja i eventualnog pranja novca. (Selling bitcoins, 2014) (Buying bitcoins, 2014) (Secure trading, 2012) Korisnici koji ne žele da koriste usluge treće strane imaju na raspolaganju i mogućnost da postavljaju svoj „kupujem“ („buy“) ili „prodajem“ („sell“) zahtev na *freenode IRC (Internet relay chat)*¹¹.

Jula 2011 FinCEN¹² je revidirao definiciju "usluge prenosa novca" pa sada znači "prihvatanje novca, sredstava ili druge vrednosti koja se zamenjuje za novac od jedne osobe i prenos novca, sredstava ili druge vrednosti na drugo mesto ili osobu na bilo koji način." Vrlo je verovatno da poslovni model mnogih trećih strana Bitcoin usluga kvalifikuje te treće strane kao prenosnika novca, a samim tim i poslove usluge prenosa novca podvodi pod 31 CR Part 1010.100 (ff) (FDIC, 2013). Treće strane, pružaoci Bitcoin usluga koji se kvalifikuju kao prenosnici novca i koji žele da rade legitimno moraju da se registruju kod FinCEN, i da sprovedu programe za borbu protiv pranja novca, da drže određene evidencije, i da podnese izveštaje o sumnjivim aktivnostima i izveštaje o valutnim transakcijama kao što se od njih zahteva. U nekim državama se zahteva i da treće strane, pružaoci Bitcoin usluga, obezbede državnu licencu. (Federal Register, 2011) Zato, pod pritiskom zakonskih normi, neki od pružalaca Bitcoin usluga postavljaju kao uslov da se „članovi slažu da pruže tačne, ažurne i kompletne podatke o sebi kao što je to zahtevano u procesu registracije i da ih održavaju ažurnim“. (MT.GOX, 2012)

Rizik korišćenja Bitcoina postoji i sa aspekta korisnika sistema. Kriminalci ne mogu da napadaju neku centralu, ali mogu da napadaju pojedinačne novčanike i treće strane – pružaocima Bitcoin usluga. Prvi malver program dizajniran da

¹¹ <http://webchat.freenode.net/>

¹² Financial Crimes Enforcement Network – US Department of the Treasury

krađe bitcoine iz kompromitovanih Bitcoin novčanika, „Infostealer.Coinbit” je otkriven sredinom juna 2011. godine. Program je mogao da inficira korisnikov računar i da digitalni Bitcoin novčanik prenese na server u Poljskoj. (Poulsen, 2011) Posebno su izloženi riziku korisnici koji ne koriste enkripciju kod svojih Bitcoin novčanika. O slučajevima krađe 25000 bitcoina, pokušaju lažne prodaje bitcoina u vrednosti 7 miliona USD i krađi bitcoina sa onlajn igračkih sajtova u 2011. godini, kao i o krađi kompjuterskih resursa za potrebe rudarenja bitcoina detaljnije se govori u izveštaju FBI (2012).

Činjenica je da i banke neće blagonaklono gledati razvoj konkurencije i ne bi bilo čudno da pokušaju da ometaju poslovanje bitcoinima. Nezavisno od toga, krajem februara 2014. godine pojavili su se glasovi da Bitcoin kod nije sasvim pouzdan i da su moguće i greške u kodu, ali je najveći dosadašnji udar na Bitcoin došao od jednog od najvećih pružalaca usluga razmene Bitcoina za druge valute. Mt.Gox-a. Na njihovom sajtu se 07.02.2014 pojavila poruka sa slike 5: „U svetlu nedavnih novinskih izveštaja i potencijalnih posledica na poslovanje MtGox-a i tržišta, doneta je odluka da se za sada zatvore sve transakcije, kako bi se zaštitili sajt i naši korisnici. Mi ćemo se pažljivo pratiti situaciju i shodno tome reagovati.“ (Mt.Gox Team, 2014)

Slika 5 Obaveštenje korisnicima sajta (Mt.Gox Team, 2014)

Kao razlog za prekid rada naveli su tehničke razloge, a zatim pad cena na berzi bitcoina za

20% - skoro 180USD zbog prevelikog porasta povlačenja bitcoina. Prema nezvaničnim informacijama u ovom procesu oduzeto je oko 750.000 bitcoina, što znači da je, u slučaju da je reč o hakovanju ili nasilnoj blokadi aktivnosti na web sajtu, gubitak Mt.Goxa oko 350 miliona dolara. (A.N.R., 2014) Ovo nije prvi put da klijenti Mt.Gox-a imaju problem sa pristupom svojim računima. Ostalih šest velikih pružalaca usluge razmene Bitcoina za fiat novac su se ogradili od postupka Mt.Gox-a i objavili da nastavljaju normalno da rade. U vezi sa ovim događajem interesantna je izjava nemačkog studenta fizike Max Hampela koji na svom blogu objavio da bi Bitcoin zajednica trebalo da bude spremna da se jednom za svagda odrekne razmene bitcoina za novac preko Mt.Gox-a. Detaljnije o ovom stavu može se naći u članku Roba Wile-a objavljenom u Business Insider-u (Wile, 2014)

O nesigurnosti ulaganja u bitcoine govorio je i Mark Karpeles, bivši direktor servisa Mt.Gox. On je u svom izlaganju objašnjavao da je investiranje u bitcoine rizično i da se visoka vrednost bitcoina zasniva na velikoj potražnji, ali da nema garancije da će se već sutra vrednost svesti na 0. U toj izjavi je naveo da se to ne očekuje, ali da je moguće. (Karpeles, 2014)

4 ZAKLJUČAK

Iako broj korisnika Bitcoin sistema raste, on je još uvek mali u poređenju sa brojem korisnika kreditnih kartica i upotrebom USD, EUR i drugog novca. Ipak, Bitcoin sistem predstavlja izuzetno konceptualno i tehničko dostignuće. Njega mogu da koriste i postojeće finansijske institucije (koje mogu i same da emituju svoje bitkoine). Takođe, nema prepreka da čak i vlade država same koriste ovu tehnologiju.

Primena Bitcoin sistema donosi niz prednosti korisnicima omogućavajući im da izvrše transakcije besplatno ili sa minimalnom naknadom i to u razumno kratkom vremenu, omogućavajući im slobodu i nezavisnost od finansijskih institucija. Sa porastom broja učesnika u Bitcoin sistemu sistem će postajati sve stabilniji, a vrednost bitcoina će sve manje oscilovati omogućavajući vlasnicima bitcoina sigurnost u pogledu vrednosti njihovog novca, njihovih bitcoina.

S druge strane, kada se Bitcoin stabilizuje i kada mu poraste broj korisnika, prema mišljenju FBI i

mnogih drugih, Bitcoin će postati vrlo korisno sredstvo za razne malverzacije i kriminalne aktivnosti. Međutim, isto je i sa svakim drugim novcem bilo da je elektronski ili fiat novac. Šta više, ni na zlatu, ni na papirnim novčanicama ne postoji bilo kakav zapis o prethodnim vlasnicima novca. Doduše, postoje brojevi novčanica koji se evidentiraju pri primopredaji u bankama, ali to se uglavnom odnosi samo na USD novčanice većih apoen.

Na usporavanje rasta broja korisnika Bitcoin sistema mogu da utiču neprijatni događaji kao što

je to bilo u slučaju prestanka poslovanja jednog od najvećih pružalaca usluge zamene bitcoina za druge valute Mt.Gox-a, kao i neki prijavljeni slučajevi krađe bitcoina, zakonskih zabrana trgovine bitcoinima u slučajevima Kine i Indije, ali će se vremenom, kad se situacija stabilise i uspostavi pravna regulativa klima promeniti u pozitivnom smeru za Bitcoin.

Na osnovu izloženog može se verovati da Bitcoin neće biti samo prolazna pojava i da će se odomaćiti na Internetu kao regularno sredstvo plaćanja.

WORKS CITED

- A.N.R. (2014, 02 25). *Platforma za trgovinu bitcoin valutom Mt.Gox prestala sa radom*. From Pobjeda: http://www.pobjeda.me/2014/02/25/platforma-za-trgovinu-bitcoin-valutom-mt-gox-prestala-sa-radom/#.Uw0nS_IdWYw
- Anon. (2009-2014). *Some Bitcoin words you might hear*. From bitcoin: <https://bitcoin.org/en/vocabulary#bitcoin>
- Anon. (2009-2014). *Some Bitcoin words you might hear*. From bitcoin: <https://bitcoin.org/en/vocabulary#block-chain>
- Anon. (2014, 02 05). *Bitcoin Transaction Fees Explained*. From Bitcoin Fees: <http://bitcoinfees.com/>
- Anon. (2014). *hashing*. From webopedia: <http://www.webopedia.com/TERM/H/hashing.html>
- bitcoin.it. (2012, 10 24). *Secure trading*. From Bitcoin wiki: https://en.bitcoin.it/wiki/Secure_Trading
- bitcoin.it. (2014, 02 19). *Buying bitcoins*. From Bitcoin wiki: https://en.bitcoin.it/wiki/Buying_bitcoins
- bitcoin.it. (2014, 01 20). *Selling bitcoins*. From Bitcoin wiki: https://en.bitcoin.it/wiki/Selling_bitcoins
- Blockchain.info. (2014, 02 19). *Average Transaction Confirmation Time*. From BlockChain: https://blockchain.info/charts/avg-confirmation-time?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=
- blockchain.info. (2014, 02 19). *My Wallet Number Of Users*. From BlockChain: https://blockchain.info/charts/my-wallet-n-users?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=
- blockchain.info. (2014, 02 19). *Total Bitcoins In Circulation*. From BlockChain: <https://blockchain.info/charts/total-bitcoins>
- blockchain.info. (2014, 02 19). *Total number of transactions*. From BlockChain: https://blockchain.info/charts/n-transactions-total?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=
- Coderrr. (2011, 06 30). *Patching the Bitcoin Client to Make it More Anonymous*. From Bitcointalk Forum: <https://bitcointalk.org/index.php?topic=24784.msg307661#msg307661>
- Čičin-Šain, D. (2007, 11 05). *Novac i poslovno bankarstvo*. From Sveučilište u Zadru: http://www.unizd.hr/portals/4/nastavni_mat/1_godina/ekonomija/ekonomija_28.pdf
- Devoto, E. (2014). *Information Security Glossary H*. From seattle.gov: http://www.seattle.gov/informationsecurity/glossary_H.htm#Hash
- FBI. (2012). *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity*. Directorate of Intelligence. Washington: Federal Bureau of Investigation. From http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf
- FDIC. (2013, 09 16). *FDIC Law, Regulations, Related Acts*. From FDIC Federal Deposit Insurance Corporation: <http://www.fdic.gov/regulations/laws/rules/8000-1400.html#dic8000fra1010.100>

- Federal Register. (2011, 07 21). *Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services*. From Rules and regulations: <http://www.gpo.gov/fdsys/pkg/FR-2011-07-21/pdf/2011-18309.pdf>
- FEE. (2013, 12 11). *The truth about Bitcoin and alternative Currencies*. From YouTube: www.youtube.com/watch?v=AVdKgQ0jmH8
- Karpeles, M. (2014, 02 25). Ugasio se najveći servis za razmjenu bitcoina. (L. M. Aljazeera, Interviewer) From <http://balkans.aljazeera.net/video/ugasio-se-najveci-servis-za-razmjenu-bitcoina>
- Lee, T. B. (2011, 07 14). *How Private Are Bitcoin Transactions?* From Forbes: <http://www.forbes.com/sites/timothylee/2011/07/14/how-private-are-bitcoin-transactions/>
- Lowenthal, T. (2011, 07 14). *Bitcoin: More Covert than it Looks*. From Active Rhetoric: <http://activerhetoric.wordpress.com/2011/07/14/bitcoin-more-covert-than-it-looks/>
- Lukić, M. (2013, 12 07). *Elektronska valuta Bitkoin bi mogla uništiti dolar*. From Biznis & Finansije: <http://bif.rs/2013/12/elektronska-valuta-bitkoin-bi-mogla-unistiti-dolar/>
- Matonis, J. (2013, 09 17). *Bitcoin gaining market-based legitimacy as XBT*. From CoinDesk: <http://www.coindesk.com/bitcoin-gaining-market-based-legitimacy-xbt/>
- MT.GOX. (2012, 01 20). *Terms of use*. From MT.GOX: https://mtgox.com/terms_of_service
- Mt.Gox Team. (2014, 02 25). *Mt.Gox*. From Mt.Gox: <https://www.mtgox.com/>
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. From bitcoin: <https://bitcoin.org/bitcoin.pdf>
- Poulsen, K. (2011, 06 16). *New Malware Steals Your Bitcoin*. From Wired: <http://www.wired.com/threatlevel/2011/06/bitcoin-malware/>
- Skudnov, R. (2012). *Bitcoin clients*. Turku: Turku University of Applied Sciences.
- Velde, F. R. (2013, 12). *Bitcoin: A primer*. From Chicago Fed Letter: http://www.chicagofed.org/digital_assets/publications/chicago_fed_letter/2013/cfldecember2013_317.pdf
- Wiki. (2013, 05 30). *Anonymity*. From Bitcoin wiki: <https://en.bitcoin.it/wiki/Anonymity>
- Wile, R. (2014, 02 07). *The Fall Of Mt. Gox*. From Business Insider: <http://www.businessinsider.com/mt-gox-2014-2>
- Williamson, S. H. (2014). *Seven Ways to Compute the Relative Value of a U.S. Dollar Amount - 1774 to Present*. From MeasuringWorth.com: http://www.measuringworth.com/uscompare/result.php?year_source=1952&amount=100&year_result=2012

Datum prve prijave: 11.03.2014
Datum prijema korigovanog članka: 20.06.2014
Datum prihvatanja članka: 25.07.2014

Kako citirati ovaj rad? / How to cite this article?

Style – **APA Sixth Edition:**

Čekerevac, P., & Čekerevac, Z. (2015, 01 15). Bitcoin - Prednosti i rizici. (Z. Čekerevac, Ed.) *FBIM Transaction*, 3(1), 37-48. doi:10.12709/fbim.03.03.01.05

Style – **Chicago Sixteenth Edition:**

Čekerevac, Petar, and Zoran Čekerevac. 2015. "Bitcoin - Prednosti i rizici." Edited by Zoran Čekerevac. *FBIM Transaction* (MESTE) 3 (1): 37-48. doi:10.12709/fbim.03.03.01.05.

Style – **GOST Name Sort:**

Čekerevac Petar and Čekerevac Zoran Bitcoin - Prednosti i rizici [Journal] // FBIM Transaction / ed. Čekerevac Zoran. - Beograd : MESTE, 01 15, 2015. - 1 : Vol. 3. - pp. 37-48.

Style – **Harvard** Anglia:

Čekerevac, P. & Čekerevac, Z., 2015. Bitcoin - Prednosti i rizici. *FBIM Transaction*, 15 01, 3(1), pp. 37-48.

Style – **ISO 690** Numerical Reference:

Bitcoin - Prednosti i rizici. **Čekerevac, Petar and Čekerevac, Zoran. 2014.** [ed.] Zoran Čekerevac. 1, Beograd : MESTE, 01 15, 2015, FBIM Transaction, Vol. 3, pp. 37-48.