BITCOIN – PREDNOSTI I RIZICI

BITCOIN - BENEFITS AND RISKS

Petar Čekerevac [1], Zoran Čekerevac [2]

Rezime

Bitcoin, digitalni novac, novac novijeg datuma, lansiran 2009-e godine, došao je u žižu interesovanja posle bankrota MT.GOX i (samo)ubistva American Bitcoin exchange CEO u Singapuru februara 2014. U ovom radu biće prikazani tehnologija Bitcoina, prednosti ovog sistema i neki rizici kojima su izloženi korisnici.

Današnja plaćanja koja u sebe uključuju i finansijske institucije povezana su sa brojnim ograničenjima i uključuju relativno velike troškove. Bitcoin podrazumeva P2P interakciju, a elektronski novčić se definiše kao lanac digitalnih potpisa. Svaki vlasnik prenosi novčić sledećem vlasniku potpisivanjem heša prethodne transakcije i javnog ključa sledećeg 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 plaćanje i izbegava generisanje nepostojećeg novca. Provera može da potraje i nekoliko minuta.Pri ovim transakcijama se ne prenose lične informacije između učesnika u transakciji. Za razliku od potpuno anonimnih transakcija, pri plaćanju Bitcoinima ostaje zapis o transakciji 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.

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 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. 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 i pokušati da koriste servise treće-strane i da napadaju privatne Bitcoin novčanike (Bitcoin wallet). Iako je Bitcoin

[1] Kutpoint, Beograd

[2] Fakultet za poslovno industrijski menadžment, Univerzitet Union, Beograd

izrazito decentralizovan, ipak postoji mesto koje može dati podatke o učesnicima u plaćanju, a to je mesto gde se Bitcoini pretvaraju u fiat valutu, tj. dekretni novac.

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 bitkoine). Takođe, nema prepreka da čak i vlade država same koriste ovu tehnologiju. Ipak, u svemu ovom treba proveriti sigurnosne aspekte Bitcoina i pojačati zaštitu sistema.

Ključne reči: digitalni novac, transakcija, finansijske institucije, pojačati zaštitu sistema

Summary

Bitcoin, new digital money, launched in 2009-year, came into focus of interest after bankruptcy of MT.GOX and the American Bitcoin exchange CEO suicide(?) in Singapore in February 2014.In this paper we will present Bitcoin technology, the advantages of this system and some of the risks to whom users are exposed.

Today's payments which include the financial institution are associated with numerous limitations, and also include relatively high costs. Bitcoin means P2P interact, and the electronic coin is defined as a chain of digital signatures. Each owner transfers the coin to the next owner signing a hash of the previous transaction and the public key of the next owner, and adding it all to the end of the coin.The recipient can verify the signatures to verify the chain of ownership. Payment verification is accomplished by notifying the entire network about the transaction. This prevents double-spending and avoids the generation of non-existent money. Checking may take a few minutes. In these transactions personal information between parties in the transaction are not transfered. Unlike completely anonymous transaction, the Bitcoin transaction remains 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 the aliases.

Bitcoin offers to users lower transaction costs, increased privacy and for more time protection of the purchasing power from inflation. However, Bitcoin still have no enough participants and financial base to ensure stability, and price of Bitcoin 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.

Bitcoin due to the relative anonymity of its users, allows individuals to generate, transmit, to wash and / or stol funds. With its application it brings to investigators similar challenges as other virtual money, for example WebMoney, but also and additional difficulties connected with its decentralized nature. According to FBI, it is estimated, with medium certainty, in the near future criminals will treat Bitcoin as another payment option, but wouldn't leave the existing traditional methods of payment. This conclusion is based on the large fluctuations of Bitcoin ratio in the year 2011. With less certainty FBI believes that the Bitcoin will be used for money washing. This assumption is difficult to prove because there are not enough reports about Bitcoin.Because of the Bitcoin system decentralization, attacks will likely be a little successful, but criminals will focus their attacks to use of the third-party services attacking the private Bitcoin wallets. Although Bitcoin is highly decentralized, there is a place that can provide information about participants in the payment, and that is where the Bitcoin converts to fiat money.

Although the number of users of 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). Also, there is no obstacle that even the governments themselves use this technology. However, safety aspects of Bitcoin must be checked in order to enhance protection.

Keywords: digital money transactions, financial institutions, strengthen the protection system