Use of Bitcoin for Internet Trade

Sadia Khalil
NUST School of Electrical Engineering and Computer Science, Pakistan

Rahat Masood
NUST School of Electrical Engineering and Computer Science, Pakistan

Muhammad Awais Shibli
VisionIT, USA

INTRODUCTION

The advent of the digital currency systems has revolutionized the concept of money transfer by allowing the internet based creation, storage and transference of money. In the past few years, the digital currency systems have emerged as an efficient means of money transfer. They have received world-wide adoption by providing a medium of exchange based on mathematical operations and by taking the currencies out of the control and manipulation of the governments. In addition to being used in the e-commerce and commercial sectors, the digital currencies have also attracted a large population of the earth which cannot get access to the formal banking systems. The crypto-currencies, being one of their types, involve different cryptographic functions for their creation and transference, in a trusted and secure environment. The use of crypto-currencies has progressed from a virtual concept to reality by the evolution of Bitcoin. The success of this concept has led to the creation of many other crypto-currencies which include Litecoin, PeerCoin, Namecoin, Quarkcoin, Primecoin and Zetacoin (Stevenson, 2013). Bitcoin, along with the other crypto-currency systems, is very popular in the business world and the global economy, due to its decentralized peer-to-peer architecture. In comparison with the other payment platforms, which maintain a private communication network for sending and receiving money, Bitcoin uses the internet as its medium of transference.

By Looking critically into the Bitcoin protocol, we can find some weaknesses that can be violated by the attackers for malicious purposes. In the past few years, a lot of vulnerabilities have been exploited causing the users to lose their bitcoins (L., n.d.), (Blasco, 2013), (arXiv, 2014). Matthew Wilson et al. (Yelowitz, 2014) analyze the characteristics of the Bitcoin users based on the Google search data and found that illegal activities and programming enthusiast are related to Bitcoin search but no correlation was found with political and investment motives. As of March 2014, bitcoins of worth 502,081,166.11$ have been stolen (L., n.d.). Based on the empirical analysis of Bitcoin exchange risks, it is found that the failure rate of bitcoin exchanges is 40% (Christin, 2013). Mt. Gox that was considered to be the largest Bitcoin exchange, got bankrupt in February 2014, allegedly due to theft, resulting in the loss of 850,000 bitcoins, out of which 20,000 were later recovered (https://en.bitcoin.it/wiki/Mt._Gox, n.d.).

BACKGROUND

The Bitcoin[1] protocol was first introduced in 2009 by a pseudonymous developer Satoshi Nakamoto (Nakamoto, 2008). Since then, it has been widely adopted as a payment procedure for many e-commerce businesses as well as regular stores. This crypto-currency along with the others,

DOI: 10.4018/978-1-5225-2255-3.ch251

is considered to be a convenient way of achieving the open source peer-to-peer money. It operates in the cyberspace and requires Bitcoin wallets for storage purposes as well as for the generation of Bitcoin addresses. At the time of this writing, the Bitcoin market capitalization is $5.8 billion (Crypto-Currency Market Capitalizations, n.d.). Keeping in view its frequent usage, Bitcoin ATMs have been deployed in various parts of the world to facilitate its users (Bitcoin ATM News, n.d.). In comparison with the Visa transactions, where the transaction speed is 2000 tps (transactions per second) and PayPal which has 115tps transaction speed, the Bitcoin network is restricted to 7 tps (Scalability, n.d.). In spite of these statistics, the advantages of Bitcoin transaction over other transaction mechanisms like PayPal, Western Union and M-Paisa etc. cannot be neglected. It gives the users the advantage of carrying out instant, anonymous and irrevocable transactions with very low transaction fees. The original Bitcoin paper (Nakamoto, 2008) presents a brief overview of the architecture and the protocol but a lot of details are missing in it. With the passage of time, a number of suitable changes and ideas have been suggested through the Bitcoin Improvement Proposals (BIPs) which are incorporated after being approved by the Bitcoin community.

In the last few years, researchers all over the world are working on Bitcoin security and there is still a need for a comprehensive assessment of attacks that are targeting the Bitcoin transactions. In this chapter, we investigate the Bitcoin protocol in detail. We have analyzed the Bitcoin architecture and its major components. We then review the Bitcoin protocol considering a use case scenario to demonstrate how a Bitcoin transaction takes place. The vulnerabilities and attacks section heuristically show how attacks like double spending, selfish mining, compromising anonymity and malware attacks can be carried out in the currently deployed versions of Bitcoin protocol. A comparison between different crypto-currencies with respect to their features and possible attacks is also presented.

BITCOIN ARCHITECTURE

In comparison with the traditional currencies that depend on a trust based model for their creation, circulation and transference, Bitcoin relies on a Proof-of-work (discussed in detail later in this chapter) based peer-to-peer model.

Being a crypto-currency, the Bitcoin protocol makes use of the hash functions and public key cryptography for the generation and transmission of bitcoins. A single bitcoin can be regarded as a series of digital signatures. For sending bitcoins to another entity, the sender digitally signs a hash of the involved previous transactions out of which the bitcoins are sent to the receiver as proof of possession of those bitcoins. The receiver can easily verify the series of digital signatures. Figure 1 shows the major components that constitute the Bitcoin Architecture.

The Bitcoin exchanges are not an inherent part of the Bitcoin protocol, however, they are one of the means for obtaining the bitcoins. The Bitcoin users can trade the bitcoins in exchange of the traditional or digital currency. Another way is to get bitcoins personally by asking the possessor of the bitcoins to transfer them to the buyer’s Bitcoin wallet.

The Bitcoin users require Bitcoin wallets to carry out the transactions. Just like real life wallets, which are used to keep cash, Bitcoin wallets are also responsible of keeping record of the bitcoins sent and received by the owner. Bitcoin wallets generate a public/private key pair for carrying out a transaction.

The Bitcoin miners are the entities in the Bitcoin network that possess computational resources to compete in the mining process. Mining is the mechanism through which the transactions are recorded in the block chain. Mining involves a complex cryptographic mechanism known as Proof-of-Work (PoW). The motivation for the miners to perform mining is the Bitcoin reward that is granted to each miner. This reward is the source of creation of new bitcoins in the system. Initially, its value was 50 BTCs and is set in a way