Chapter 28
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

ABSTRACT

Bitcoin is considered to be the world's first peer-to-peer and unregulated crypto-currency which has received widespread popularity in the last few years. It is issued and controlled by the members of the Bitcoin system. The success of Bitcoin has spurred the launch of many other crypto-currencies. Despite being widely adopted by various large-scale businesses, Bitcoin transactions are still exposed to many known as well as zero-day attacks due to various vulnerabilities being exploited by the malicious entities. In order to achieve reliable and secure transactions, extensive research needs to be carried out to critically examine Bitcoin architecture and its level of security. In this regard, this chapter presents a holistic analysis of Bitcoin architecture and a survey of the attacks prevalent to its transactions. As an evaluation of the Bitcoin system, a comparison of different crypto-currencies has been presented, based on their features, possible attacks, disadvantages, and the advantages which they possess over Bitcoin.

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 worldwide 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.

DOI: 10.4018/978-1-5225-7766-9.ch028

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, 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