Chapter 21
Bitcoin:
Digital Decentralized Cryptocurrency

Feroz Ahmad Ahmad
Galgotias University, India

Prashant Kumar
GCET Noida, India

Gulshan Shrivastava
National Institute of Technology Patna, India

Med Salim Bouhlel
Sfax University, Tunisia

ABSTRACT

In this chapter, a digital decentralized cryptocurrency system where transactions are secured by cryptography and are independent of any centralized third party is discussed. The different characteristics of bitcoins and how transactions occur between two bitcoin users along with some facts and examples are also discussed. The rapid internet development facilitates cyber-attacks to all type of online transactions and also to bitcoin network transactions. Some security issues are also discussed in the chapter along with the cyber-crimes and their punishments.

INTRODUCTION

Online transaction processing using electronic means has revolutionized human society altogether. It has brought the era which leads towards the cashless e-commerce using electronic gadgets. To transfer money into an account one need not wait for hours in bank queues. For buying a laptop or for reserving an air ticket, one needs not to carry a large amount of cash to the shopkeeper. Now there is no need to maintain a lengthy register by a shopkeeper or by a bank employee to keep a record of monthly transactions. Now booking a hotel room or reserving a plane or buying a laptop is just a click away. This is all because of the computing and communication technologies. Though easy and powerful, there are some

DOI: 10.4018/978-1-5225-4100-4.ch021

limitations with these electronic financial transactions and one of these limitations is that these transactions involve some third party as intermediaries for processing electronic payments. In case required financial institutes are not able to reverse the transactions and are unable to handle the intermediate disputes. Involvement of third part becomes costlier as per transaction cost.

To overcome the limitations associated with the conventional approach of electronic financial transactions, Nakamoto (2008) and Moore (2013) proposed a different electronic payment system. An electronic decentralized payment system called Bitcoin cryptocurrency system. This system is based on cryptographic proof and security which provides the customers with this virtual currency to sell or buy services or goods. This currency is called as bitcoin.

Bitcoin was introduced as a peer-to-peer-based digital currency in Nakamoto (2008). The conventional cashless transaction systems which were used before bitcoins are third party dependent which requires that trusted third party for clearing the transaction between the two parties. In bitcoins, unlike other transaction systems, the whole bitcoin network performs the role of the trusted third party to carry out transactions between two accounts. The transactions under process are verified for legitimacy by the nodes in the network. These nodes create a ledger like data recording file that keeps track of the account balances and verifies transactions by using the records in that ledger as per the current state and updates the same accordingly. Unlike other digital transactions systems, bitcoins are the irreversible type of transaction networks. Once the transaction is committed there are no means to reverse the transaction except the receiver returns the amount to the sender through another transaction. As a consequence, bitcoin has no charge-backs and hence has a drawback that the bitcoins lost or being fraudulently stolen are non-refundable.

Bitcoin, a form of electronic digital cryptocurrency is created and controlled by the network itself. These are created by the miners using high computational computers to solve mathematical problems related to bitcoins. Bitcoin is not printed like currencies of the nations and is independent of the boundaries of countries hence accepted and used internationally.

How Are Bitcoins Different From Other Currencies?

Bitcoin can be used for buying thing online like normal currencies which are traded digitally. In that sense, bitcoins are like conventional currencies like dollars, euros, rupees or yen.

However, the characteristic which makes Bitcoin more powerful than the traditional digital currencies is that it is decentralized. In case of currency transactions between two parties, a centralized third party like the bank is responsible for the transaction. But there is no requirement of any third party to control the transactions in bitcoin network. This makes it easy and cheaper to perform a transaction because a large bank is not needed to control the money. A third party like banks charges for the transactions every time, which is not the case in bitcoin network.

Who Created It?

Satoshi Nakamoto named unknown person designed Bitcoin and also created its original implementation. It was an electronic system based on mathematical proof. The basic idea was to produce a digital currency network independent of any third party intervention that is decentralized, should perform instantly electronically transferable, and with very little transaction charges.