7.29 Using Bitcoin to provide privacy for online payments

Alsafa Hassan Suliman Ahmed[1], Amna Abdulrahman Abdallah Elhassan[1]

Isra Abdelsalam Mohammed Tahir[1], alsafa.hassan@gmail.com

Keywords: Third party; Digital Currencies; Block Chain; Miners; Bitcoin address

Online payment is a process of exchanging money over the internet to purchase or sell goods and services; this process includes a payer, a payee, and a central authority (third party). The third party is located in the middle, in order to verify the payment process and check the account. Due to the role of the third party, some people who use online payment are concerned about them, because their information can be abused or made vulnerable. In other words, they are concerned about their privacy. On the other hand, the on-line payment has good features to be used such as scalability and availability. With the improvement of the technologies, new techniques of the online payment have appeared; one of these techniques is a digital currency. It provides the possibility of a direct money exchange between the payer and the payee. One of the most famous and dominant digital currencies is a Bitcoin, Bitcoin is a digital currency "crypto-currency" that is based on peer to peer network in which all the nodes of the network share files and resources to provide more scalable, reliable (without a single point of failure), and faster communication . Bitcoin technology has two main concepts; universal place to keep all the transaction that occurs in the system that is shared in the entire Bitcoin network (public ledger – block chain), and connected peers called miners who verify and add the new block into the block chain. Bitcoin hides user identity by using Public key cryptography technique to create a pseudonym address to participate in each transaction, which leads to increase user's privacy. The aim of this project is to investigate online payment and its privacy, then implement the bitcoin system to prove that it provides enough privacy for the online payments. Therefore, the researchers have deeply studied the material necessary to understand online payment, bitcoin system and its component and Test bed technique was chosen and used as a project methodology. A bitcoin application has been implemented and the basic functionalities have been addressed; from those functions the researchers have conducted the test which have shown that the raw bitcoin

transaction is not understandable and the identity of the user is hidden.so bitcoin have showed that it is suitable to address and handle privacy issue.