PROJECT TOPIC

Analysis of Bitcoin

Abstract:

Bitcoin is a relatively new form of currency that is just beginning to hit the mainstream, but many people still don't understand why they should make the effort to use it. This project serves to explain a purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution, in other words, a decentralized currency. It provides virtually instantaneous transaction time, and is accessible through the dozens of bitcoin wallets. It can be used anywhere in the world, to send value almost instantly, nearly for free and cannot be counterfeited or duplicated. Bitcoin Core is the name of open source software which enables the use of this currency.

Bitcoin is a complex scheme, and its implementation involves a combination of cryptography, distributed algorithms, and incentive driven behavior. Bitcoin relies on two cryptographic schemes: digital signatures and cryptographic hash functions. Bitcoins reside in what is known in the bitcoin system as bitcoin addresses. The ownership of a particular amount of bitcoins reduces to the capability of sending payments from the bitcoin addresses. The capability of sending payments from Bitcoin addresses is controlled via digital signatures that involve pairs of a public key and a private key. Each bitcoin address is indexed by an unique public ID. The private key, which is the counterpart of public key, gives control over the bitcoins held in this address.

Moreover, recent developments suggest that Bitcoin operations may involve risks whose nature and proportion are little, if at all, understood. In light of these considerations, the purpose of this paper is to provide the necessary technical background to understand basic Bitcoin operations and a set of empirical regularities related to Bitcoin usage. We present the micro-structure of the Bitcoin transaction process and highlight the use of cryptography for the purposes of transaction security and distributed maintenance of a ledger. From this project we hope to research about more secure models and provide more security to the electronic money exchange system.

References : Satoshi Nakamoto.2008. Bitcoin: A Peer-to-Peer Electronic Cash System

Anton Badev and Matthew Chen.2014. Bitcoin: Technical Background and Data Analysis

Group Members:

Nishant Bhatia **2014UCP1006**

Raj Mehta **2014ucp1005**