Communications Dept, COIS Gurgaon
Indian Oil Corporation Ltd

Introduction to Bitcoin

Irfan Naseef
naseefi@indianoil.in

May 20, 2017

Content

- Introduction
  - What is Bitcoin ?
  - Cryptocurrency
- Legality status
  - Legality in India
  - Worldwide status
- Ledger and Transactions
- Security
  - Security

Introduction

- **Bitcoin** is a peer to peer payment system introduced as open-source software in 2009.
- The transactions in the system are recorded in a public ledger called **Blockchain**
- Bitcoin system has no central repository and no single administrator. It is a Decentralized virtual currency.
- Bitcoin is a Cryptocurrency, ie It is cryptography based digital currency

Cryptocurrency

Cryptocurrency is a bearer instrument

- Holder has ownership
- No Other records kept to identify the owner
- Easy to keep anonymous
- Hard or impossible to replace if lost or stolen
- is based on Cryptography.

Introduction
How to Obtain Bitcoin

- Bitcoins can be obtained by mining.
- Bitcoins can be exchanged for other currenciesm products and services.

Mining

- Bitcoins are created as a reward for payment processing work in which users offer their computing power to verify and record payments into a the public ledger. This process is called **Mining**.
- Individuals or companies can engage in this activity in exchange for transaction fees and newly created bitcoins.
- Besides mining, bitcoins can be obtained in exchange for flat money, products and services.
- Users can send and receive bitcoins electronically for an optional transaction fee using wallet software on a personal computer, mobile device or a web application.

Legality in India

- Bitcoin is **LEGAL** in India.
- Response from RBI - *"As of now we are watching and learning about the developments in Bitcoins but are not regulating it"*
- Caution notice by RBI - *"Any user, holder, investor or trader dealing with virtual currencies is doing it at their own risk"*
- Despite the Reserve Bank's call for caution to people against the use of virtual currencies, domestic Bitcoin exchanges reports that they are adding over 2,500 users a day and has reached total five lakh downloads.

History

World wide status

- Bitcoin was first mentioned in a 2008 research paper published under the name *Satoshi Nakamoto*.
- Some mainstream websites began accepting bitcoins 2013. *WordPress* started in November 2012 followed by OKCupid in April 2013, Atomic Mall in November 2013, TigerDirect in January 2014, and Overstock.com that same month.
- In October 2013, Chinese internet giant *Baidu* had allowed clients of website security services to pay with bitcoins. During November 2013, the China-based bitcoin exchange BTC China overtook the Japan-based Mt. Gox and the Europe-based Bitstamp to become the largest bitcoin trading exchange by trade volume.
- The first bitcoin ATM was installed in October 2013 in Vancouver, British Columbia, Canada.

World wide status

- As of February 2015, over 100,000 merchants and vendors accept bitcoin as payment.
- According to a research produced by Cambridge University in 2017, there are 2.9 to 5.8 million unique users actively using a cryptocurrency wallet, most of them using bitcoin.
- Over 80% of bitcoins are traded on a Tokyo-based digital currency exchange called Mt. Gox

Ledger and Transactions
Block Chain

- The most important part of the bitcoin system is a public ledger that records financial transactions in bitcoins - The Blockchain.
- Recording transactions is accomplished without the intermediation of any single, central authority.
- Instead, multiple intermediaries exist in the form of computer servers running bitcoin software. By connecting over the Internet, these servers form a network that anyone can join. Transactions of the form "***payer X wants to send Y bitcoins to payee Z***", are broadcast to this network using readily available software applications. Bitcoin servers can validate these transactions, add them to their copy of the ledger, and then broadcast these ledger additions to other servers.

Ledger and Transactions

Block Chain

The blockchain is a **distributed database** – to achieve independent verification of the chain of ownership of any and every bitcoin (amount), each network node stores its own copy of the blockchain. Approximately six times per hour, a new group of accepted transactions, a block, is created, added to the blockchain, and quickly published to all nodes. This allows bitcoin software to determine when a particular bitcoin amount has been spent, which is necessary in order to prevent double-spending in an environment without central oversight. Whereas conventional ledger records the transfers of actual bills or promissory notes that exist apart from it, the blockchain is the only place that bitcoins can be said to exist in the form of unspent outputs of transactions.

Security

There are two main ways the block chain ledger can be corrupted to steal bitcoins: by fraudulently adding to or modifying it. The bitcoin system protects the blockchain against both using a combination of digital signatures and cryptographic hashes.

Security

The Addition Attack and Digital Signatures:

Payers and payees are identified in the blockchain by their public cryptographic keys: most bitcoin transfers are from one public key to a different public key.

The Modification Attack And Mining:

The other principal way to steal bitcoins would be to modify blockchain ledger entries. Eve could buy something from Alice, like a sofa, by adding a signed entry to the blockchain ledger equivalent to *Eve pays Alice 100 bitcoins*. Later, after receiving the sofa, Eve could modify that blockchain ledger entry to read instead: *Eve pays Alice 1 bitcoin*, or even delete the entry. Digital signatures cannot prevent this attack. Eve can simply sign her entry again after modifying it. Bitcoin uses various timestamping schemes to avoid the need for a trusted third party to timestamp transactions added to the blockchain ledger.

Thank you!