OS Technical Report

# Introduction

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[1].

The payments done for usage of such services via credit/debit cards pass through a central agency (like a bank) which authorizes and in some cases even a transaction fee is charged. Such agencies, under various circumstances have the right to restrict access to their services. There might also be cases where some places may not have a presence for such service or may not have an option for payments in their local currency. Scenarios like these bring down the advantages that Cloud offers.

BitCoins, a digital currency can be used to overcome such impediments. It is a decentralized peer-peer currency. It is highly secure and carries minimum transactional cost. It even allows for direct client to business payment without the involvement of any third party in between.

The objective of this project is to develop a BitCoin API based payment module and integrate it with a cloud service to enable users to make payments directly in BitCoins.

For the project, we work with the following assumptions:

1. The client has Bitcoin wallet in his system
2. Client knows how to generate PGP public and private key pair.
3. PGP encryption is a safe mode of encryption and decryption

# Project Description

## Objective

The aim of the project is to develop a BitCoin API based payment module and integrate it with a cloud service to enable users to make payments directly in BitCoins. The project implements IaaS on cloud and provides the client with an instance on a remote system.

## Description

### Bitcoins

Bitcoin is a peer-to-peer network based digital currency. Peer-to-peer (P2P) means that there is no central authority to issue new money or keep track of transactions. Instead, these tasks are managed collectively by the nodes of the network. The necessity of a trusted third party in order to ensure reliable transactions is sidelined by the use of bitcoins.

### Why bitcoins ?

1. Reliable transactions
2. Strong control of ownership
3. No need of a trusted third party
4. Minimal transaction fees
5. Common currency in all countries throughout the globe

### How Bitcoins work

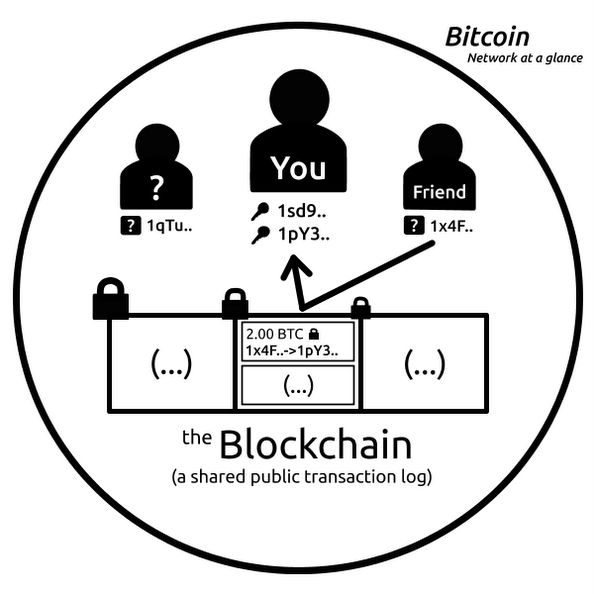
1. As a new user [A], you only need to choose a wallet that you will install on your computer or on your mobile phone. Once you have your wallet installed, it will generate your first Bitcoin address and you can create more whenever you need one. You can disclose one of your Bitcoin addresses to your friends so that they can pay you or vice versa, you can pay your friends if they give you their addresses.
2. Each owner transfers a coin by digitally signing a hash and public key of next owner
3. New transactions will be publicly announced
4. A payee can verify the signatures to verify the chain of ownership
5. The payee accepts the payment if majority of nodes agrees that it is the first received

## **Blockchain**

The blockchain is a **shared public transaction log** on which the entire Bitcoin network relies. All confirmed transactions are included in the blockchain with no exception. This way, new transactions can be verified to be spending bitcoins that are actually owned by the spender. The integrity and the chronological order of the blockchain are enforced with cryptography

## **Transaction**

A transaction is **a transfer of value between Bitcoin addresses** that gets included in the blockchain. Bitcoin wallets keep a secret piece of data called a *private key* for each Bitcoin address. Private keys are used to sign transactions, providing a mathematical proof that they come from the owner of the addresses. The *signature* also prevents the transaction from being altered by anybody once it has been issued.



BitCoins as an alternative currency can be employed for various online (in some cases offline) paid services and products. Our project aims at exploring the option of developing a payment solution wherein we explore cloud service payment using BitCoins. The project will consist of a payment module integrated with a IaaS cloud service.

The project provide the client with a web application named “InSTaRS (Instance Renting Service)” where the client can rent an instance for a particular amount of time based on the metering plans and make payment using BitCoins.

### Existing Products and Gap Analysis

The instance providing services works similar to the Amazon EC2 Reserved Instances that enable you to maintain the benefits of cloud services while lowering costs and reserving capacity. With Reserved Instances you pay a low, one-time fee and in turn receive a significant discount on the hourly charge for that instance. Reserved Instances can provide substantial savings over owning your own hardware or running only On-Demand instances as well as help assure that the capacity you need is available to you when required.

Also using Bitcoins for Cloud based services is not a new concept. The following are examples of virtual private server providers which accept payments via BitCoins.

1. Dewlance Windows VPS and Hosting. BitCoins for Cloud
2. Yoku Cloud Hosting and Cloud Servers
3. Optical Cube Web Hosting, VPS and IT consulting
4. Tailored VPS

Cloud Computing encapsulates a range of different technologies that have developed through the evolution of commercial computing [3]. Infrastructure as a service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.

Payments to these services involve real money and are usually made through payment gateways using credit/debit cards. Bitcoins, a peer-peer decentralized digital currency stands as an effective alternative to carry out payments to any services availed by the client .The use of powerful cryptography and the concept of "block-chains" in order to prevent double-spending makes bitcoins even more reliable. Ease of use, security, minimal transaction charges of bitcoins justifies the idea of using them in the existing "infrastructure as a service" cloud computing scenario.

This project aims to "build a cloud which accepts payment through bitcoins". In other words, a cloud which provides infrastructure services is built and clients who use those services are expected to pay in terms of bitcoins.