PAYMENT FOR CLOUD SERVICES USING BITCOINS

Ranadheer K
ranadheer.kakkireni@iiitb.org

Kurada Sravya
sravya.kurada@iiitb.org

Raghav Bali
raghav.bali@iiitb.org

Ruchi Juneja
ruchi.juneja@iiitb.org

Vijay Huddar
vijay.huddar@iiitb.org

Technical Report IIITB-OS-2012-5D April 2013

Abstract

Blah blah blah Blah blah blah Blah blah blah Blah blah blah Blah blah blah
Blah blah blah Blah blah blah Blah blah blah Blah blah blah Blah blah blah
Blah blah blah Blah blah blah Blah blah blah Blah blah blah Blah blah blah
Blah blah blah Blah blah blah Blah blah blah Blah blah blah Blah blah blah

Acknowledgement

Blah blah blah Blah blah blah Blah blah blah Blah blah blah Blah blah blah
Blah blah blah Blah blah blah Blah blah blah Blah blah blah Blah blah blah
Blah blah blah Blah blah blah Blah blah blah Blah blah blah Blah blah blah
Blah blah blah Blah blah blah Blah blah blah Blah blah blah Blah blah blah

Contents

1 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

2 Project Description

2.1 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.

2.2 Description

2.2.1 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

2.2.2 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

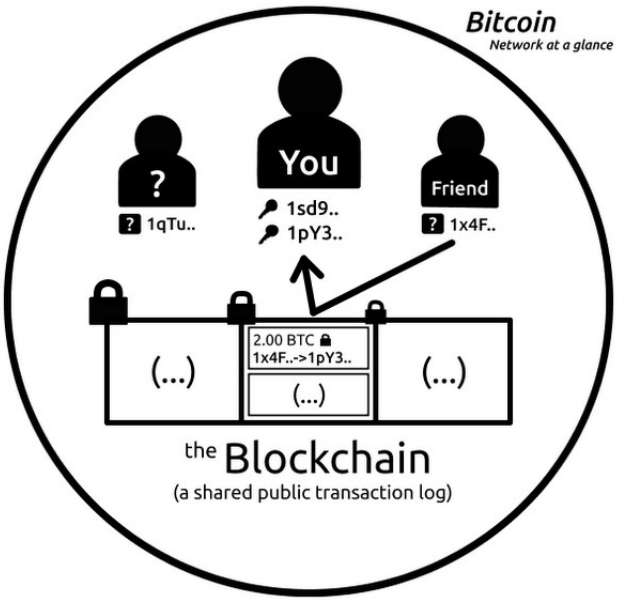

Figure 1: Blockchain

2.2.3 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.

3 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.

- Dewlance Windows VPS and Hosting. BitCoins for Cloud
- Yoku Cloud Hosting and Cloud Servers

- Optical Cube Web Hosting, VPS and IT consulting
- 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.

4 Architecture

Infrastructure as a Service (IaaS) provides the consumer with some fundamental computing resources where the consumer can run arbitrary software .InstaRS is an IaaS application which provides access to a VM instance which runs on Node Controller of Eucalyptus Cloud set up . Eucalyptus is a Linux-based software platform for creating cloud computing systems based on computer clusters. Eucalyptus works with a number of virtualization systems like VMWare, Xen and Kernel Based Virtual Machine (KVM).

System Architecture : The system architecture is shown in figure X. The client requests the service through InstaRS Application.BitCoin API is integrated in the application which communicates with the BitCoin peer-peer network to verify the payment made by the client.Once the transaction is

successful,the AWS API is used to spawn the instances on the Node Controller .The client can then perform a ssh login into the instance. Metering for the service is done based on time.The application is designed in such a way that,the instance gets terminated as per the chosen plan and the user will no longerhave access to the instance.

Cloud Architecture : 2-tier cloud architecture has been adopted in-

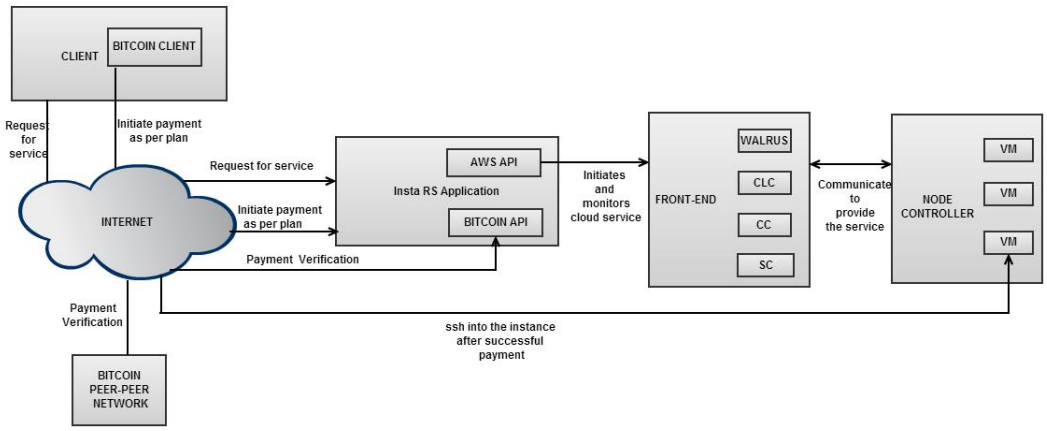

Figure 2: Architecture

order to ensure scalability and to accomodate large number of customers. This is because the number of backend servers(node controllers) can be increased easily without affecting the overall architecture.

Components of Server 1 and their Functionality[5]:

1. Cloud Controller (CLC): Monitor the availability of resources on various components of the cloud infrastructure and the cluster controllers that manage the hypervisor nodes. Deciding which clusters will be used for provisioning the instances and Monitoring the running instances. Cloud Controller is front end for the collection of computers/servers we have set up. It CLC provides an web services interface to the client on one side and interacts with the rest of the components of the Eucalyptus infrastructure on the other side.

2. Cluster Controller (CC):Node Controllers basically get themselves registered to CC. Cluster Controllers are one that manages the number of

Node Controllers and deploys or manages the instance on them. CC has two important functions: Receive requests from CLC to deploy instances and it must choose which NC should deploy this instance. To report the information gathered from the NC to CLC.

3. Walrus Storage Controller (WS3): It is a simple le storage system. WS3 stores the machine images. It also stores and serves files using S3 APIs

4. Storage Controller (SC): SC provides persistent block storage for use by the instances.

Components of Server 2 and their Functionality Node Controller (NC) Server 2 is capable of running KVM as the hypervisor. Hypervisor is one that provides a uniform environment for di_erent virtual machines to run.A virtual machine is nothing but implementation of machine in software mode. Virtual Machine has its own kernel, OS and applications.Virtual Machines running on Hypervisors are called instances. Node Controller interacts with 3 other components, namely the OS ,Hypervisor and cluster controller (installed on Server1). NC gathers the information from the OS to learn about the VM instance running on the current node, number of cores, the size of memory and disk space. It then transmits this information to Cluster Controller.

5 Implementation

Implementation of this project is to build the nexus between Bitcoin and cloud technologies. The cloud setup for the project was chosen as Infrastructure as a Service (IaaS) model. The web application acts as a means of user interface for payments in Bitcoins is "InStaRS" or Instance Renting Service. The following sections describe in detail the different software components, cloud setup and various APIs used in the process of implementation of this project.

5.1 Components

The software components for this project can be divided broadly as Cloud Software Components and Bitcoin-Web application Software Components.

5.1.1 Software Components

- Eucalyptus
  Eucalyptus is open source software for building AWS-compatible private and hybrid clouds. The installation package chosen was Eucalyptus FastStart 3.2.2 which comes preconfigured for CentOS and KVM. This package facilitates installation of Eucalyptus components on CentOS 6.0 , an Enterprise class Linux Distribution, along with AWS compatible addons.

- Euca2ools
  Euca2ools is a Eucalyptus management utility. It provides with command line based management of various Eucalyptus components like :

  - Instance Key Management.
  - Image Management.
  - Instance Management.
  - Network Management.

  Apart from being management utility for cloud setup management, Euca2ools also provides with the necessary interfacing with AWS which

is required by the web application to remotely control the cloud as per the client requests.

- KVM − Qemu
  Kernel Virtual Machine or KVM is a Linux module which allows user programs to utilize hardware virtualization features of the modern processors. Qemu−KVM fork is used for x86 machines. It allows us to create multiple virtual machines which run as normal Linux processes.

5.2 Bitcoins−Web Application Software Components

- Bitcoin−Qt
  Bitcoin-Qt is a desktop Bitcoin client application. This comes bundled with bitcoind service. Bitcoin−Qt along with bitcoind allows users to maintain a wallet on local system and make transactions. It works by downloading the complete blockchain on the local system, current blockchain size stands at 6400MBs. Bitcoin−Qt also allows uses to generate Bitcoin addresses required for any type of Bitcoin transactions.

- Bitcoin JSON−RPC APIs
  Bitcoin supports various APIs to enable merchants or businesses join and make use of the Bitcoin payment network for their daily business transactions. These APIs are available in a variety of programming languages like Python, Ruby, Java etc. These APIs are also available as lightweight and heavy, where heavy APIs make use of local resources for all Bitcoin related activities. For the implementation of payment module of InStaRS, we have made use of JSON APIs provided by blockchain.info network. This set of APIs is lightweight as it utilizes the blockchain.info′s infrastructure for Bitcoin transactions. Since local resources are not burdened, the transaction verification process is sped up remarkably as compared to heavy APIs like BitcoinJ.

- Bouncy−Castle Open−PGP encryption
  Bouncy Castle is a collection of lightweight Java APIs used for cryptography. As part of InStaRS′s Bitcoin payment module, an extra layer of security based upon Open−PGP encryption is implemented using Bouncy Castle API for Open−PGP.

5.3 System Design

This project uses 4 machine configuration to create a private cloud using Eucalyptus integrated with a web server to host the InStaRS web application for payments and cloud control as shown in the below figure :

- A web server running the InStaRS web application on Apache Tomcat Server 7.0 using struts2 framework for client interfacing and cloud management.
- A front end server, running Eucalyptus Front End components : cloud controller, cluster controller Walrus storage service and storage controller.
- A Back end server also known as Node Controller to run the virtual machines. A client system to bundle, test and register the images for the cloud service.

To showcase the scalability of cloud setup, the split architecture is used. The complete project setup has also been readied and tested with the Back−end and Front−end systems clubbed onto a single machine. InStaRS is designed in such a manner that with minimum configuration changes, the web application can be made to work in tandem with the monolithic cloud architecture as well.

5.4 Cloud Setup

The cloud setup is done using three machines - Server1, Server2 and the Client.
The Front-End comprises the Cloud Controller, Cluster Controller, Walrus

Hardware	Front−End Server	Node Controller(NC)	Client
CPU	IntelCore i5(2.67 GHz)	IntelCore i5(2.67 GHz)	IntelCore i5(2.67 GHz)
Memory			
Disk Space	100 GB	100 GB	100 GB
Networking	100 Mbps	100 Mbps	100 Mbps

Table 1: Hardware Configuration

	Front−End Server	Node Controller(NC)
Functionality	LC, SC, CC and Walrus	NC
Network Interfaces	eth0-EucalyptusN/W	br0-EucalyptusN/W
IP Addresses	192.168.12.221 to 192.168.12.240	NA
Gateway IP	192.168.3.254	192.168.3.254

Table 2: Network Configuration

Storage and Storage Controller. The Node Controller comprises of virtual machine instances. The hardware configuration and the networking configuration of Front−End Server, Node Controller(NC) and the Client are shown in Tables 1 and 2.

5.4.1 Installation of Node Controllers:

1. Using the CentOS Fast Start image [reference website] select "Install Node Controller" as the cloud installation mode.

2. Node controller is installed before the Front End Server.

3. Use static networking rather than DHCP and provide the IP address as 192.168.12.161 and set the proxy information to 192.168.3.254.

References

[1] Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing, " 2011. [Online]. Available: csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System, " 2008. [Online]. Available: http://bitcoin.org/bitcoin.pdf.

[3] Graeme Philipson (July 2012), *Why cloud is important.* [Online]. Available: http://www.itwire.com/2012-06-01-13-40-03/browse/c-level/55713-why-cloud-computing-is-important.

[4] Ania Monaco (June 2012), *A view inside the cloud.* [Online]. Available: http://theinstitute.ieee.org/technology-focus/technology-topic/a-view-inside-the-cloud.

[5] Eucalyptus Systems. (2012, June 25). *User's Guide Enterprise Edition 2.0* [Online]. Available: http://www.eucalyptus.com/docs/2.0/ug-ee.pdf.

[6] Barrie Sosinsky, "Understanding Cloud Architecture," in *Cloud Computing Bible*, Indianapolis: Wiley, 2011, ch. 3,pp. 45-64.

[7] Eucalyptus Systems. (2012, June 25). *Eucalyptus 3.1.0 Installation Guide* . [Online]. Available: www.eucalyptus.com/docs/3.1/ig-3.1.0.pdf.