CloudCoin Practical Project

Motivation

With the emergence of Dropbox 2008 and affordable prices for fast Internet connections storing data in the cloud became mainstream. Cloud storage services not only provide access to your data from all over the world on almost any devices but also data redundancy which prevents data loss by hardware failures and most of the time file revision control which lets you jump back in time or recover files which got lost through application or operator errors. But there are some non-technical problems: Cloud service providers are for-profit organization which work under jurisdiction of their home country and countries where they provide service which make them and the data of their users vulnerable to law enforcement. They could be forced to provide none or only weak cryptography to their costumers or to hand over, tamper, delete or restore user files or backtrack users respectively aid third parties to do so. They also could have interest in user data in terms of industrial espionage. Furthermore their access authority is usually hierarchically organized and centralized at a certain place which could be a problem if someone can influence the head of this hierarchy. The solution could be a protocol and software which provides the same service and benefits of centralized company driven cloud storage services extend by the benefits of decentralization to non-technical areas by its architecture and way of maintenance.

Concept

CloudCoin will be an open source maintained peer-to-peer protocol and network which provides IT resources to its members by using their own computation time and disc space as well as bandwidth, data volume and availability of their internet connection and securing data by delegating en- and decryption to the end-user. Members of this network could be anyone from an end-user with ISDN/aDSL connection and personal computer who wants to store or to compute date in the cloud as well as organizations with underutilized computing or server capacity right up to data center companies who want to earn money by renting out their machines. Because resources in this group are unequally distributed an incentive is needed to share resources with others. For this purpose we will use a new digital crypto-currency like Bitcoin[1] which can be used as payment. Furthermore the technology Bitcoin is based on can be used to store resource leasing contracts as well as ratings about contract fulfillment or any other data/communication between members of the network which should be made persistent in a forgery-proof, unalterable and way.

Milestones

The goals for the first practical phase are to
- develop the process of negotiating and signing contracts for CloudStorage
- extend the Bitcoin protocol by messages which are needed to negotiate, sign and rate contracts for CloudStorage
- build a CloudCoin prototype with CloudStorage extension which consists of
  - a daemon similar to bitcoind[2] (preferably multi-platform) extended with features described in the CloudCoin paper[3] which contains an interface for extensions like CloudStorage Negotiator
  - the CloudStorage Negotiator extension
  - a light CloudStorage file server which can be deployed at most web-hosting environments and can be connected to a local or remote CloudStorage Negotiator

---

1   http://bitcoin.org
2   https://en.bitcoin.it/wiki/Bitcoind
3   CloudCoin – Concept for a decentralized Cloud Service based on Bitcoin (Boehm 2013)