Coinsy: An approach to anonymous decentralized crypto-currency exchange.

Abstract

In this document I propose a decentralized censorship and denial of service resistant, trust enabled crypto-currency exchange.

Background

The system utilizes a high performance decentralized database. The database acts as a short-term (up to 72 hours) storage mechanism for small objects. The database provides an effective complex query mechanism through the storage protocol. The database uses a single-hop architecture to achieve sub-second lookups regardless of network size. The database acts as a decentralized authenticated proxy mechanism to provide a layer of anonymity.

Getting Started

1. The client generates a 64-bit random username and password.
2. The client generates an N-bit PKCS#1 certificate.
3. The client generates a secret by calculating the HMAC-512 of the username and password.
4. The client sends it's DER encoded certificate to an authentication node along with it's username and secret.
5. The authentication node generates credentials by signing the certificate on behalf of the client and caches the username, secret and certificate for a period of 72 hours.

6. The client stores the credentials in the network.
7. The client must repeat steps 4 through 5 every 72 hours to retain it's username.

Storage Protocol

1. Ask

   Places an ask.

   Example:

   ```
   ask=LTC/BTC&__price=0.0123&__quantity=7
   &seller=abc&__address=192.168.1.1&__port=40028&id=123
   &__t=1394701668&__s=gHdeAJ0TIcj39%2BrMc...5y1aP8gax%2BNxiA%3D
   ```

2. Bid

   Places a bid.

   Example:

   ```
   bid=LTC/BTC&__price=0.0123&__quantity=7
   &buyer=xyz&__address=192.168.1.1&__port=40028&id=123
   &__t=1394701668&__s==gHdeAJ0TIcj39%2BrMc...5y1aP8gax%2BNxiA%3
   ```

3. Trade Reference

   A `trade reference` is similar to a `trade` but is much smaller and only contains the `price, quantity, buyer, seller, id, transaction id, timestamp` and the `signature` of the publisher. It is used as a reference to a `trade` and serves no other purpose.

   Example:

```
trade=LTC/BTC&__price=0.0123&__quantity=7
&buyer=xyz&seller=abc&id=123&tid=321&__t=1394701668
&__s==gHdeAJ0TIcj39%2BrMc...5y1aP8gax%2BNxiA%3D
```

Trading Protocol

1. Buy

   Performs a buy.

   Example:

   ```
   buy=LTC/BTC&buyer=xyz&seller=abc&__address=192.168.1.1&__port=
   &tid=321&__t=1394701668&__s==gHdeAJ0TIcj39%2BrMc...5y1aP8gax%2
   ```

2. Sell

   Performs a sell.

   Example:

   ```
   sell=LTC/BTC&buyer=xyz&seller=abc&__address=192.168.1.1&__port
   &tid=321&__t=1394701668&__s==gHdeAJ0TIcj39%2BrMc...5y1aP8gax%2
   ```

3. Trade

   Trades contain two parts, a buy and a sell.

   Buy Example:

   ```
   trade=LTC/BTC&__buy=YnV5PUxU...xFdVgzayUzRA%3D%3D
   &__sell=c2VsbD1MVEM...FY0tnbUJsUUNFJTNE&id=2570359900&tid=8233
   &__t=1397010942&__s=gHdeAJ0TIcj39%...1aP8gax%2BNxiA%3D
   ```

   Sell Example:

```
trade=LTC/BTC&__buy=YnV5PUxUQy9CVEM...NMV2Z2cmxFdVgzayUzRA%3D%
&__sell=c2VsbD1MVEMvQlRDJ...molMkJFY0tnbUJsUUNFJTNE&id=257035%
&__t=1397010942&__s=gHdeAJ0TIcj39%2BrMc...5y1aP8gax%2BNxiA%3D
```

Network Procedures

1. Buyer

   When a client wishes to place a buy order it stores a `bid` for 8 seconds, repeating every 7 seconds until the order is cancelled or a matching `ask` is found. The client performs a lookup every 4 seconds to find an `ask`. Once a client finds an `ask` it sends a `buy` to the seller. The `buy` MUST have the same `price, quantity, seller and id` as the `ask`.

   When the buyer receives a matching `sell` it MUST:

   1. Generate a trade.
   2. Store a trade reference in the system for 72 hours.
   3. Optionally store the trade in a block chain mechanism.

2. Seller

   When a client wishes to place a sell order it stores an `ask` for 8 seconds, repeating every 7 seconds until the order is cancelled or a `buy` is received. The `buy` MUST have the same `price, quantity, buyer and id` as the `bid`.

   When the seller receives a matching `buy` it MUST:

   1. Respond with a sell.
   2. Generate a trade.
   3. Store a trade reference in the system for 72 hours.
   4. Optionally store the trade in in a block chain mechanism.

3. Trades

   Trades are stored for a period of 72 hours. Trades are considered confirmed

when a valid pair is found. Long-term trade storage SHOULD utilize a block chain mechanism.

Order Fulfillment

The actual exchange of the crypto-currency is out of the scope of this document.

Author

Adudalesdi Ganiladisdi
adudalesdi@hmamail.com

References

None