# Using Factom

**The Factom API  Version 0.2**

In the early Alpha version of Factom, the peer to peer network will be simulated with a centralized server.  As the project matures, the server will be replaced by a peer to peer network.  Data storage will eventually be provided by a separate DHT network, but is also currently simulated on the central server.

Users of Factom will interface with the system through a daemon program. The program is written in go and is called factomclient.  It is expected to be run on the user's computer, but could also be located elsewhere on the user's private network.  The factomclient program exposes a web services API which is called by user programs.  The data is encoded in JSON.

When the factomclient is updated from a client-server to P2P model, the base API calls from the user application will stay the same.  The change would be in what party orders the unanchored transactions.  Even in the temporary client-server model, Entries are protected by the blockchain after being anchored.  That being said, the system will be reset at various points during development.

## Quick Start

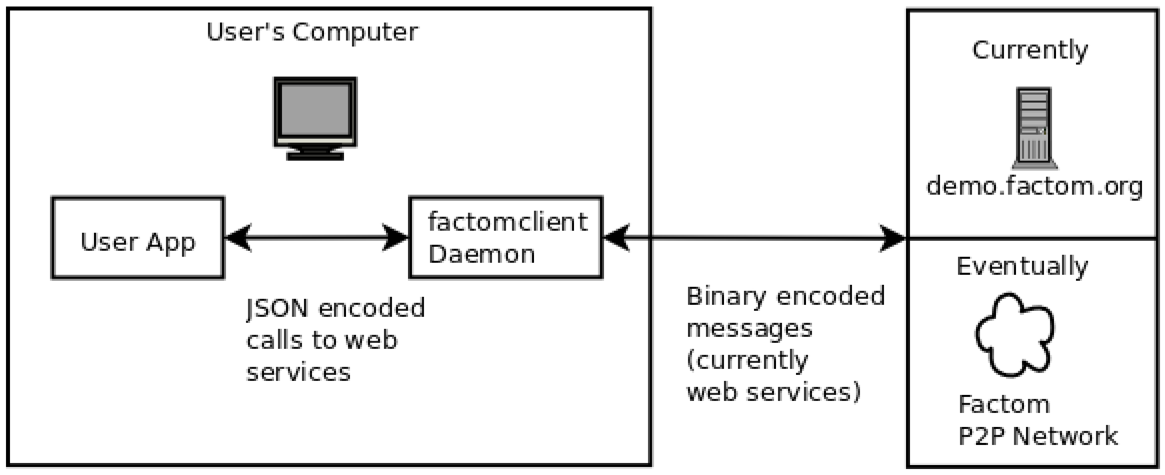
The easiest way to start experimenting in Facom is to use the factomexplorer instance running directly on the server.

Browse to: http://demo.factom.org:8087/

## Overview

Factom will eventually communicate via a P2P network, and a reference client is being developed to act as an interface for user applications.  It is expected that users will run the factomclient program, which exposes an API that applications can use.  Factom is useful for securing existing business processes.  Existing applications can call the API to make a system state not reversible without detection.

## Connection Diagram



The API between factomclient and the Factom network while interesting, is not detailed in this document. Some steps are converted from one JSON call to two Network calls. Factom uses two stage calls at several points. One reason is to prevent front-running by peers when exposing information that homesteads a namespace (similar to Namecoin's staged registration). Another reason is to allow for separation of the payment and data storage subsystems.

The nomenclature for the multiple stages is commit then reveal.

| | |
|---|---|
| Commit | Hash(es) of data is signed and broadcast. It is considered a payment for the revealed data. |
| Reveal | The committed data is broadcast and sorted by ChainID |
| Submit | A submit is a call which both commits and reveals. The Submit takes data, creates and broadcasts a commit. Shortly thereafter creates a reveal and broadcasts it.<br>Submit might make a transaction susceptible to front running attacks on P2P, because the timing of the two is very close. Front running is only a problem with a Chain reveal. |

This version of the API, factom will only expose the submit calls. The underlying commit and reveal will be exposed later.

Every Entry must be associated with some Chain, specified by its ChainID. Typically, a user will homestead some globally unique ChainID, and place their transactions in that Chain. The Chain is not exclusively theirs, so the application needs to be resistant to foreign data.

Before an Entry will be accepted, the Chain which it specifies must have been created.

Also, before any Chains can be created, factomclient's internal Entry Credit public key needs to have a positive balance on the server. Entry Credit balances are supposed to only be increased along with a Factoid balance decrease, but that functionality has not been written yet. Adding Entries into Factom is essentially free at this point. Factomclient has a temporary API call which asks for an increased balance of Entry Credits.

## Setup

This setup phase assumes you are running ubuntu linux 14.04. Windows may work but is untested.

install go:

```
sudo apt-get install golang git mercurial
```

create go directory in home `~/go/`
set go path. add to bottom of file ~/.profile

```
export GOPATH=$HOME/go
export PATH=$PATH:$GOPATH/bin
```

logout and login

Install factomclient with this command:
go get -v github.com/FactomProject/FactomCode/factomclient/…

copy `factomclient.conf` from
`~/go/src/github.com/FactomProject/FactomCode/factomclient/`
to home: `~/`
edit `factomclient.conf` and change `ServerAddr` to `"demo.factom.org:8083"`

Run factomclient from the commandline

You may need to clear the files `/tmp/factomclient/` if the demo.factom.org is reset.

## Add Entry Credits to your private key

Your public private keypair is autogenerated by the factomclient program.

Check balance of private key:

from command line:

```
      curl -X POST -H "application/json" -d 'pubkey=wallet'
      http://localhost:8088/v1/creditbalance
```

from web browser:

```
      http://localhost:8088/v1/creditbalance?&pubkey=wallet
```

should return public key and a zero balance like this:

```
      {"PublicKey":"NWNGhTqjv9rAxuxdpfsgjxmmFI6y8VMSgPm8+lOMmDc=","Cr
      edits":0}
```

### Increase the number of entry credits:

From web browser:

```
      http://localhost:8088/v1/buycredit?&to=wallet&value=100
```

### Add New Chain to Factom

Before adding Entries, a Chain must be created to put them in.  The easiest way to do this is to use the factomexplorer detailed below.  After installing it, open it’s interface in a web browser.  Next to the Chains menu item, there is a drop down arrow.  Click the + sign to create a new Chain.  Add a Chain Name and some data for a first Entry.  The Chain Name “`helloWorld`” corresponds to ChainID “`d5f39e4c4e041c37dfe0d65c7405d215924650891a689425c736e974c88d5ba0`”

## Other commands:

The metadata about the directory blocks can be retrieved with the URL:

```
http://localhost:8088/v1/dblocksbyrange/0/100
```

The first number is the start block and the second number is the end block.  This command gets the first 100 Directory Blocks' info.

This URL `http://localhost:8088/v1/dblocksbyrange/0/0` returns:

```
[{"Header":{"BlockID":0,"PrevBlockHash":"AAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAA=","MerkleRoot":"T90YoiF9prFQ2E315QYKvvTzrMxGZfyuhE4Lf
DJbaqs=","Version":1,"TimeStamp":1421361934,"BatchFlag":0,"EntryCount
":1},"DBEntries":[{"MerkleRoot":"MhSs/KSwRTfz4aWEFWh+67ms4gCo5XcO8SRX
Li2IvLc=","ChainID":"miTyxpen1v6D4Sr46otII3kqONChL/J0nztRB+skjt8="}]}
]
```

This URL `http://localhost:8088/v1/dblocksbyrange/4/4` returns:

```
[{"Header":{"BlockID":4,"PrevBlockHash":"f2O+qd8fTqi/fmnicH7b6TsEEEJI
JnE31OHiTBAeEoE=","MerkleRoot":"3/RkucLUFUNzNKW6CeFOYHKOrRdvV4KMvOmuU
8jeT5M=","Version":1,"TimeStamp":1421371497,"BatchFlag":0,"EntryCount
":2},"DBEntries":[{"MerkleRoot":"EqDqNN/H8ZaW+A9ysYStDuvFKw4BZzKckH23
03U3Drs=","ChainID":"1fOeTE4EHDff4NZcdAXSFZJGUIkaaJQlxzbpdMiNW6A="},{
"MerkleRoot":"u4mV1kw9o87+ukRCQt1NbyB2zaOy3+t2lS2tyrEXd3I=","ChainID"
:"AQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA="}]}]
```

This was the block which created the `helloWorld` Chain above.
`d5f39e4c4e041c37dfe0d65c7405d215924650891a689425c736e974c88d5ba0`
converted to base64 is `1fOeTE4EHDff4NZcdAXSFZJGUIkaaJQlxzbpdMiNW6A=`
which we see above as a ChainID.  The `AQAAA`… ChainID is the Entry Credit Chain, which keeps track of balances.

`http://localhost:8088/v1/creditbalance?&pubkey=wallet` at this point returns
`{"PublicKey":"NWNGhTqjv9rAxuxdpfsgjxmmFI6y8VMSgPm8+lOMmDc=","Credits":989}`, since we used 11 Entry Credits to make the Chain.  Earlier it was 1000.  10 were spent to make the Chain and 1 to pay for up to 1KiB of data used in the Entry.

## Submit Entries

factomclient takes json calls to itself and sends them out to demo.factom.org.  A command line application has been provided which takes command line arguments and makes a json call.

Install factom-cli:
go get -v github.com/FactomProject/factom-cli/…

Call factom-cli like this adding an Entry to our earlier example's ChainID:

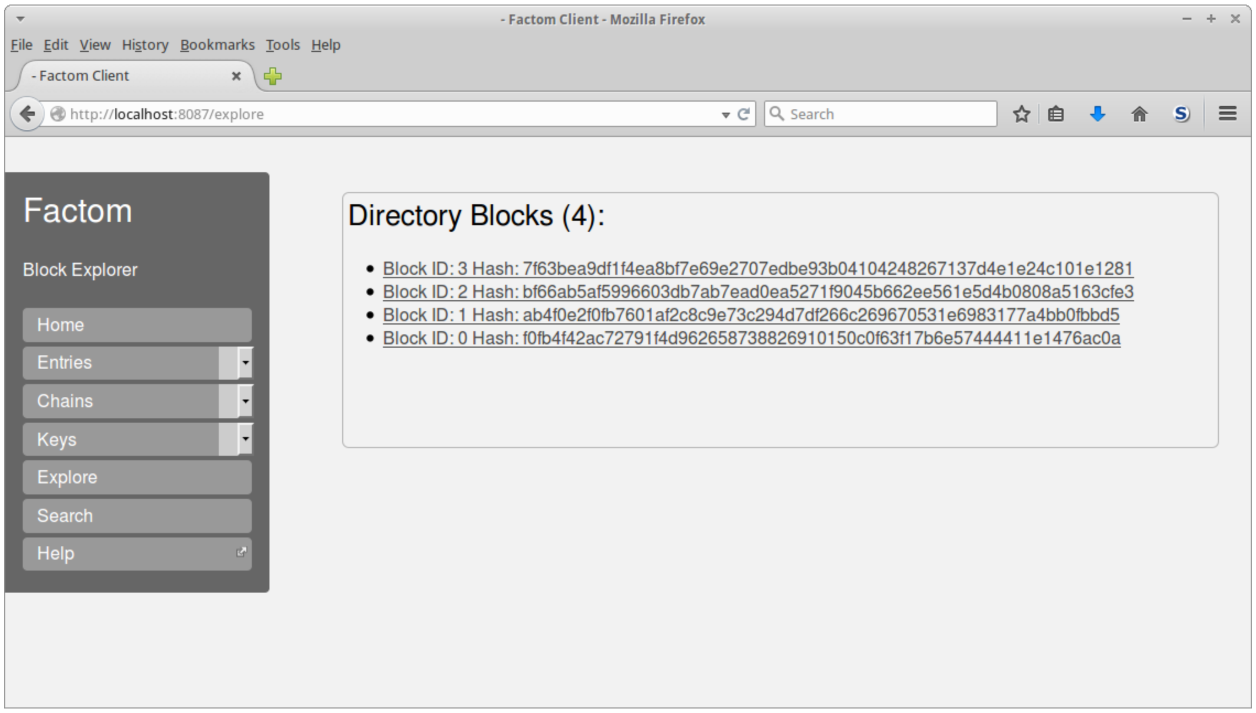
```
echo "Here is Entry data" | factom-cli -c
"d5f39e4c4e041c37dfe0d65c7405d215924650891a689425c736e974c88d5ba0" -e
"extIDforDB"
```

Install factomexplorer:
go get -v github.com/FactomProject/factomexplorer/…

make directory `~/.factom/client/data`
copy all files from
`~/go/src/github.com/FactomProject/factomexplorer/bundle/data/`
to:
`~/.factom/client/data/`

copy `client.conf` from:
`~/go/src/github.com/FactomProject/factomexplorer/`
to home:
`~/`
edit `client.conf` and change `ServerAddr` to `"demo.factom.org:8083"`
Some earlier data in `/tmp/client/` might need to be cleared out if the factom server is reset.

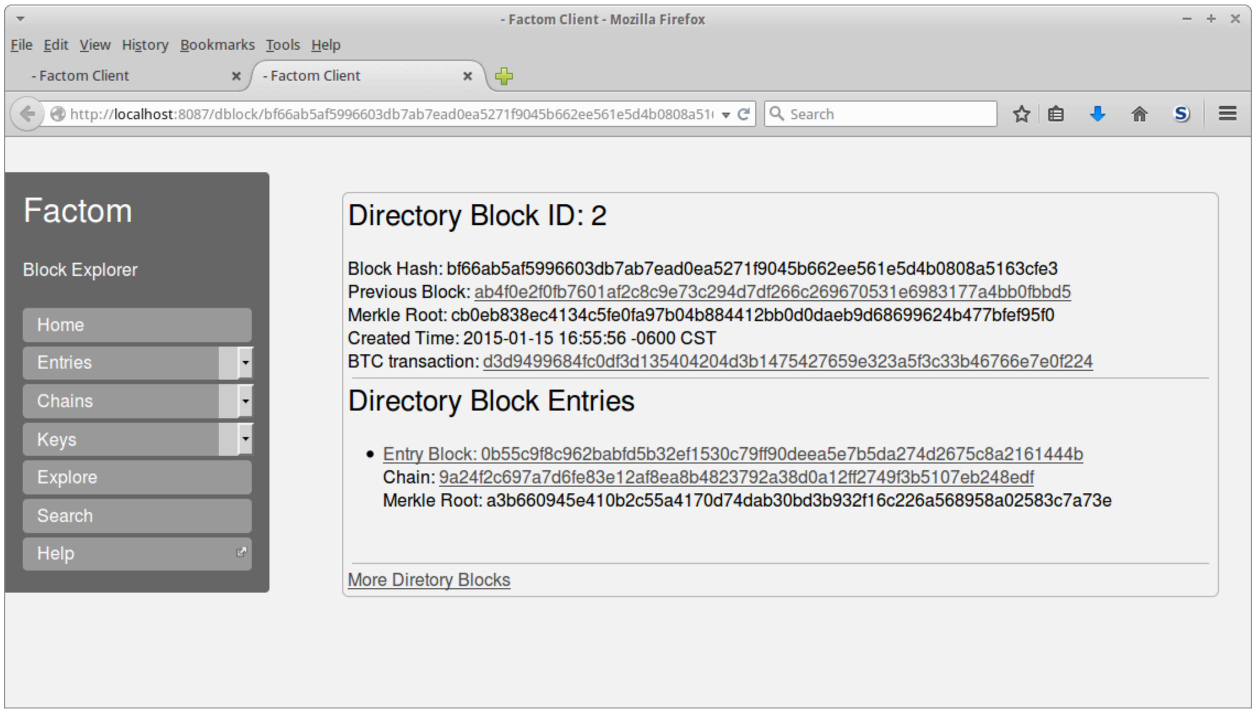
launch with the command `factomexplorer`
While it is running, it can be connected to with a web browser at the URL:
`http://localhost:8087/`


- Factom Client - Mozilla Firefox
File Edit View History Bookmarks Tools Help
- Factom Client
http://localhost:8087/explore
Search
Factom
Block Explorer
Home
Entries
Chains
Keys
Explore
Search
Help

Directory Blocks (4):

- Block ID: 3 Hash: 7f63bea9df1f4ea8bf7e69e2707edbe93b04104248267137d4e1e24c101e1281
- Block ID: 2 Hash: bf66ab5af5996603db7ab7ead0ea5271f9045b662ee561e5d4b0808a5163cfe3
- Block ID: 1 Hash: ab4f0e2f0fb7601af2c8c9e73c294d7df266c269670531e6983177a4bb0fbbd5
- Block ID: 0 Hash: f0fb4f42ac72791f4d962658738826910150c0f63f17b6e57444411e1476ac0a

Explore tab in factomexplorer. This shows all the available Directory Blocks, which are the highest level data structures in Factom.


- Factom Client - Mozilla Firefox
File Edit View History Bookmarks Tools Help
- Factom Client
- Factom Client
http://localhost:8087/dblock/bf66ab5af5996603db7ab7ead0ea5271f9045b662ee561e5d4b0808a51
Search
Factom
Block Explorer
Home
Entries
Chains
Keys
Explore
Search
Help

Directory Block ID: 2

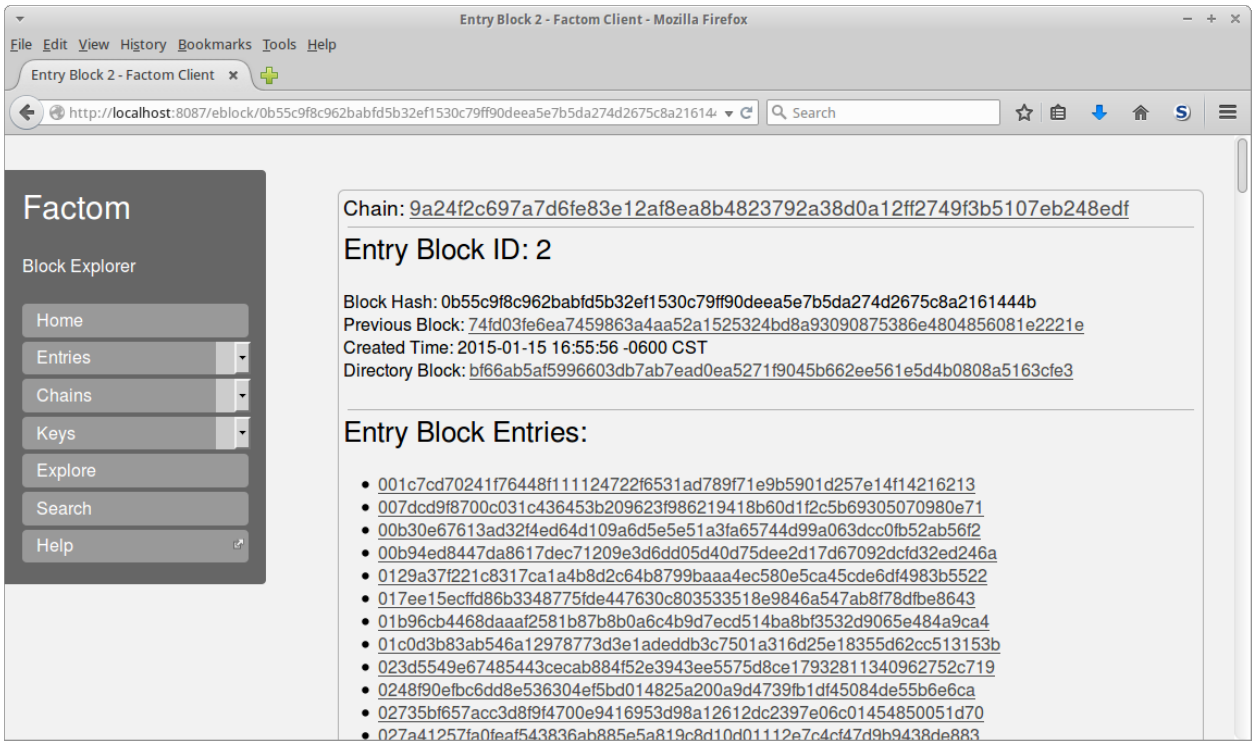
Block Hash: bf66ab5af5996603db7ab7ead0ea5271f9045b662ee561e5d4b0808a5163cfe3
Previous Block: ab4f0e2f0fb7601af2c8c9e73c294d7df266c269670531e6983177a4bb0fbbd5
Merkle Root: cb0eb838ec4134c5fe0fa97b04b884412bb0d0daeb9d68699624b477bfef95f0
Created Time: 2015-01-15 16:55:56 -0600 CST
BTC transaction: d3d9499684fc0df3d135404204d3b1475427659e323a5f3c33b46766e7e0f224

Directory Block Entries

- Entry Block: 0b55c9f8c962babfd5b32ef1530c79ff90deea5e7b5da274d2675c8a2161444b
  Chain: 9a24f2c697a7d6fe83e12af8ea8b4823792a38d0a12ff2749f3b5107eb248edf
  Merkle Root: a3b660945e410b2c55a4170d74dab30bd3b932f16c226a568958a02583c7a73e

More Diretory Blocks

Directory Blocks are composed of a header and a paired list of Entry Blocks and the Chain which the Entry Block is associated with.


Entry Block 2 - Factom Client - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Entry Block 2 - Factom Client
http://localhost:8087/eblock/0b55c9f8c962babfd5b32ef1530c79ff90deea5e7b5da274d2675c8a21614
Search
Factom
Block Explorer
Home
Entries
Chains
Keys
Explore
Search
Help

Chain: 9a24f2c697a7d6fe83e12af8ea8b4823792a38d0a12ff2749f3b5107eb248edf

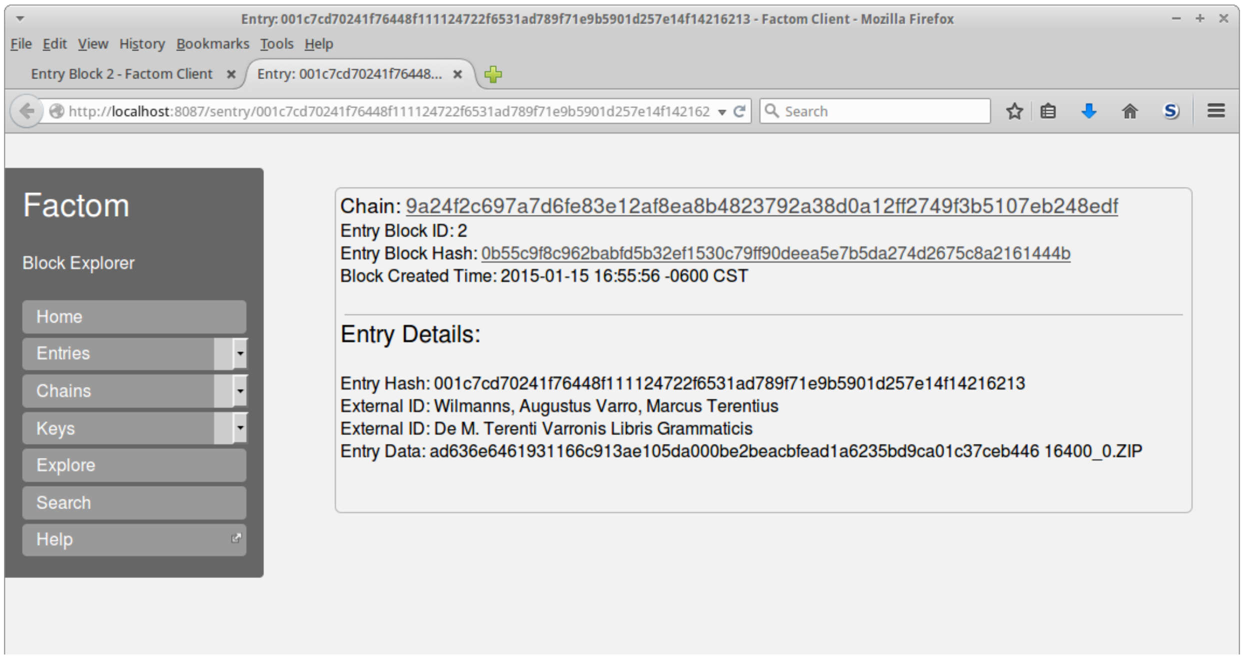
Entry Block ID: 2

Block Hash: 0b55c9f8c962babfd5b32ef1530c79ff90deea5e7b5da274d2675c8a2161444b
Previous Block: 74fd03fe6ea7459863a4aa52a1525324bd8a93090875386e4804856081e2221e
Created Time: 2015-01-15 16:55:56 -0600 CST
Directory Block: bf66ab5af5996603db7ab7ead0ea5271f9045b662ee561e5d4b0808a5163cfe3

Entry Block Entries:

- 001c7cd70241f76448f111124722f6531ad789f71e9b5901d257e14f14216213
- 007dcd9f8700c031c436453b209623f986219418b60d1f2c5b69305070980e71
- 00b30e67613ad32f4ed64d109a6d5e5e51a3fa65744d99a063dcc0fb52ab56f2
- 00b94ed8447da8617dec71209e3d6dd05d40d75dee2d17d67092dcfd32ed246a
- 0129a37f221c8317ca1a4b8d2c64b8799baaa4ec580e5ca45cde6df4983b5522
- 017ee15ecffd86b3348775fde447630c803533518e9846a547ab8f78dfbe8643
- 01b96cb4468daaaf2581b87b8b0a6c4b9d7ecd514ba8bf3532d9065e484a9ca4
- 01c0d3b83ab546a12978773d3e1adeddb3c7501a316d25e18355d62cc513153b
- 023d5549e67485443cecab884f52e3943ee5575d8ce1793281134096275 2c719
- 0248f90efbc6dd8e536304ef5bd014825a200a9d4739fb1df45084de55b6e6ca
- 02735bf657acc3d8f9f4700e9416953d98a12612dc2397e06c01454850051d70
- 027a41257fa0feaf543836ab885e5a819c8d10d01112e7c4cf47d9b9438de883

Entry Blocks are composed of a header and a list of Entries. All the Entries referenced in a specific Entry Block have the same ChainID.

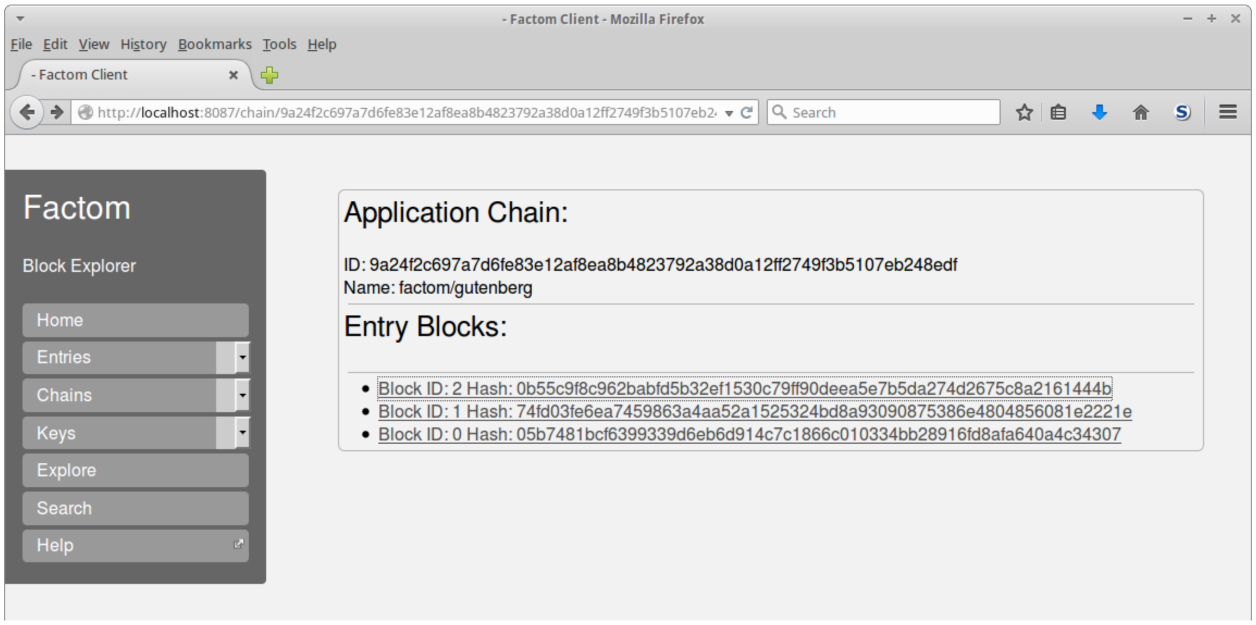

Entry: 001c7cd70241f76448f111124722f6531ad789f71e9b5901d257e14f14216213 - Factom Client - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Entry Block 2 - Factom Client
Entry: 001c7cd70241f76448...
http://localhost:8087/sentry/001c7cd70241f76448f111124722f6531ad789f71e9b5901d257e14f142162
Search
Factom
Block Explorer
Home
Entries
Chains
Keys
Explore
Search
Help

Chain: 9a24f2c697a7d6fe83e12af8ea8b4823792a38d0a12ff2749f3b5107eb248edf
Entry Block ID: 2
Entry Block Hash: 0b55c9f8c962babfd5b32ef1530c79ff90deea5e7b5da274d2675c8a2161444b
Block Created Time: 2015-01-15 16:55:56 -0600 CST

Entry Details:

Entry Hash: 001c7cd70241f76448f111124722f6531ad789f71e9b5901d257e14f14216213
External ID: Wilmanns, Augustus Varro, Marcus Terentius
External ID: De M. Terenti Varronis Libris Grammaticis
Entry Data: ad636e6461931166c913ae105da000be2beacbfead1a6235bd9ca01c37ceb446 16400_0.ZIP

Entries are a packet of data including a ChainID (required), External IDs (optional), and a payload. The External IDs are essentially part of the payload, but are tagged to be keys into a database.


- Factom Client - Mozilla Firefox
File Edit View History Bookmarks Tools Help
- Factom Client
http://localhost:8087/chain/9a24f2c697a7d6fe83e12af8ea8b4823792a38d0a12ff2749f3b5107eb2
Search
Factom
Block Explorer
Home
Entries
Chains
Keys
Explore
Search
Help

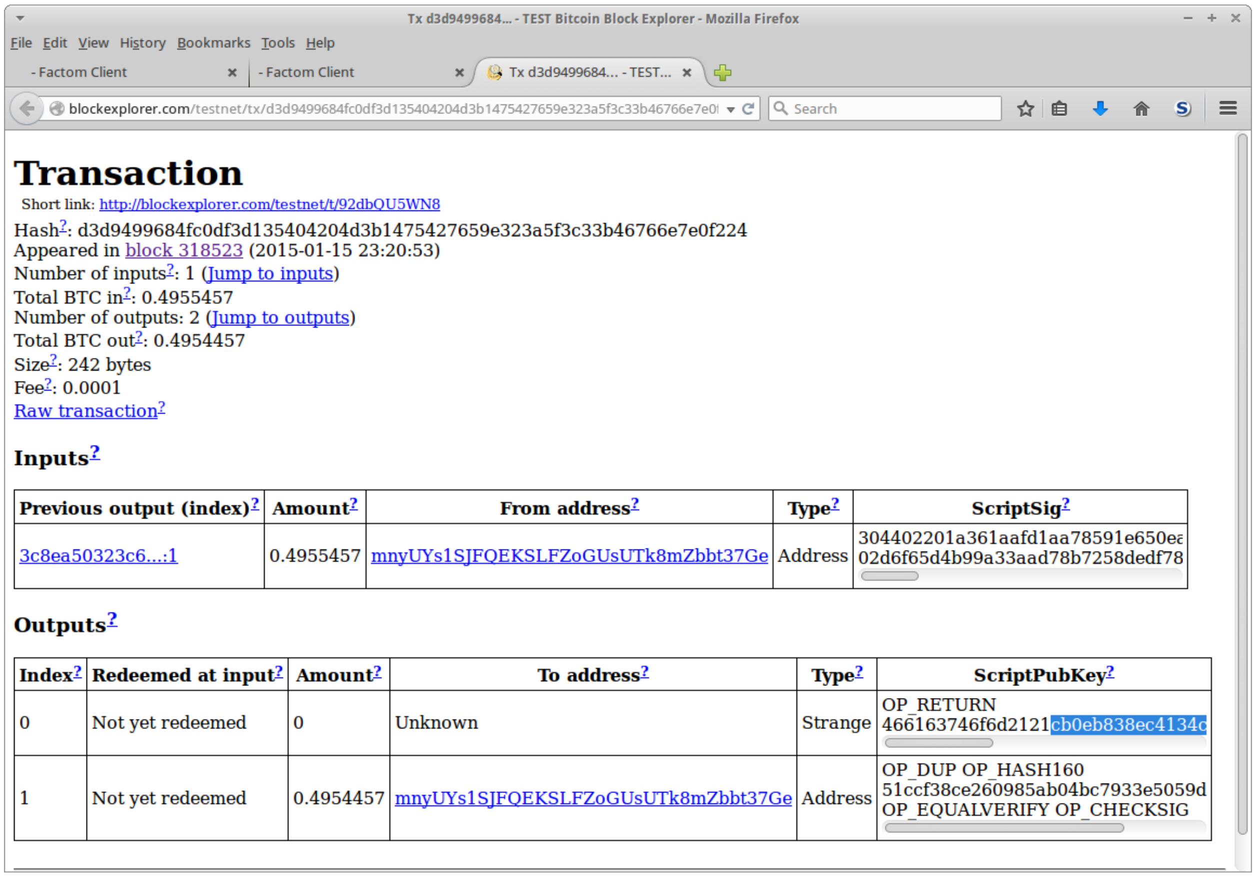
## Application Chain:

ID: 9a24f2c697a7d6fe83e12af8ea8b4823792a38d0a12ff2749f3b5107eb248edf
Name: factom/gutenberg

## Entry Blocks:

- Block ID: 2 Hash: 0b55c9f8c962babfd5b32ef1530c79ff90deea5e7b5da274d2675c8a2161444b
- Block ID: 1 Hash: 74fd03fe6ea7459863a4aa52a1525324bd8a93090875386e4804856081e2221e
- Block ID: 0 Hash: 05b7481bcf6399339d6eb6d914c7c1866c010334bb28916fd8afa640a4c34307

The Factom system keeps track of the Entry Blocks by ChainID. ChainID is a hash of the Chain Name.


Tx d3d9499684... - TEST Bitcoin Block Explorer - Mozilla Firefox
File Edit View History Bookmarks Tools Help
- Factom Client
- Factom Client
Tx d3d9499684... - TEST...
blockexplorer.com/testnet/tx/d3d9499684fc0df3d135404204d3b1475427659e323a5f3c33b46766e7e0
Search

## Transaction

Short link: http://blockexplorer.com/testnet/t/92dbQU5WN8
Hash?: d3d9499684fc0df3d135404204d3b1475427659e323a5f3c33b46766e7e0f224
Appeared in block 318523 (2015-01-15 23:20:53)
Number of inputs?: 1 (Jump to inputs)
Total BTC in?: 0.4955457
Number of outputs: 2 (Jump to outputs)
Total BTC out?: 0.4954457
Size?: 242 bytes
Fee?: 0.0001
Raw transaction?

### Inputs?

| Previous output (index)? | Amount? | From address? | Type? | ScriptSig? |
|---|---|---|---|---|
| 3c8ea50323c6...:1 | 0.4955457 | mnyUYs1SJFQEKSLFZoGUsUTk8mZbbt37Ge | Address | 304402201a361aafd1aa78591e650ea<br>02d6f65d4b99a33aad78b7258dedf78 |

### Outputs?

| Index? | Redeemed at input? | Amount? | To address? | Type? | ScriptPubKey? |
|---|---|---|---|---|---|
| 0 | Not yet redeemed | 0 | Unknown | Strange | OP_RETURN<br>466163746f6d2121cb0eb838ec4134c |
| 1 | Not yet redeemed | 0.4954457 | mnyUYs1SJFQEKSLFZoGUsUTk8mZbbt37Ge | Address | OP_DUP OP_HASH160<br>51ccf38ce260985ab04bc7933e5059d<br>OP_EQUALVERIFY OP_CHECKSIG |

The Merkle root of each Directory Block is anchored in the blockchain.

## Relevant Code:

Here are some places to look in Factom to see how the APIs are handled.

https://github.com/FactomProject/FactomCode/blob/development/factomclient/serve.go

https://github.com/FactomProject/FactomCode/blob/development/factomapi/wsapi.go

https://github.com/FactomProject/FactomCode/blob/development/factomapi/wsapi_test.go

https://github.com/FactomProject/factom-cli/blob/mk2/put.go