

ビットコインとか勉強会

- コマンドラインで色々な暗号通貨を送金してみよう

目次

- 自己紹介
- 各通貨の特徴を簡単に説明
 - Bitcoin : SPV node
 - NEM : Full node
 - Zcash : Full node
- コマンドラインで色々な暗号通貨を送金してみよう

自己紹介

株式会社イーサセキュリティ

代表取締役 加門昭平

TW: @cameong

- セキュリティモニタリングツール `metstake.io` の開発運用
- NEM スーパーノードの構築 (国内シェア約20%, 世界シェア約5%)
- `bitdonation.org` の運用
- `coincheck api` のpython パッケージとか書いてます

用語

- `$abc` : 変数 `abc`
- Full node: フルノード. 全トランザクションを保有するノード.
- SPV node : いわゆるライトウォレット. トランザクションを自身では保有せず, 送金に特化したノード

注意事項

- 結構, python に偏ってます

各通貨の特徴

Bitcoin

- 特徴
 - PoW (SHA-256)
 - ブロック生成時間: 約10分
 - 単位は「BTC」
 - 最小単位は $10E-8$ BTC

1

¹ <https://upload.wikimedia.org/wikipedia/commons/thumb/4/46/Bitcoin.svg/240px-Bitcoin.svg.png>



NEM

- 特徴
 - PoI (EigenTrust++)
 - ブロック生成時間: 約1分
 - 単位は「XEM」
 - Bitcoin2.0
(ユーザー独自通貨発行(namespace/
Mosaic)/ メッセージ送信)



■ 特徴

- PoW (Equihash) (詳しくは【暗号通貨読書会#4】完全匿名コインZcashで採用されたPoWアルゴリズム「Equihash」を参照ください²⁾)
- ブロック生成時間: 150秒
- 採掘: マイニング
- 単位は「ZEC」
- 匿名性が高い。ゼロ知識証明。

²⁾ <https://cryptocurrency.connpass.com/event/43804/>
[^3]: <https://z.cash/press.html>



送金してみよう

Bitcoin



Bitcoin を送金

from : 18ef4syYvGd2K7MeYvbJ7LZ4x3kk5x4ufb

to : 15MMEVF6DM6RDdyaYeybEb9iKcv7uJwb36

volume: 10000 satoshi

エクスプローラ: <https://goo.gl/H2uFDb>

tool: pybitcointools⁵

エクスプローラが見れたら、demoに移ります

⁵ <https://github.com/vbuterin/pybitcointools>

Demo

```
# 送信用
# 秘密鍵(priv)からbitcoinアドレス(addr),取引履歴(h)を生成
:

# 受信用
# 秘密鍵(priv)からbitcoinアドレス(addr)を生成
:

# output 作成.
# 相手(addr2)に10000, 自分自身に39000 を送る. 残りはお釣り
:

# 署名するutxo の抽出
:

# sign
:

# broadcast tx
:
```

Bitcoin 関連ツール

- エクスプローラ
 - <http://blockr.io/>
 - <https://live.blockcypher.com/>
 - <https://www.blocktrail.com/BTC>
- トランザクションをdecode してエラー解析
 - <https://blockchain.info/decode-tx> (invalid だと解析結果を返さない)
 - <https://developer.indiesquare.me> (invalid でも結果を返す)

Bitcoin パッケージ, モジュール

- python
 - <https://github.com/petertodd/python-bitcoinlib>
 - <https://github.com/richardkiss/pycoin>
 - <https://github.com/jgarzik/python-bitcoinrpc>
- node
 - <https://bitcoinjs.org/>

NEM



XEM を送金

from : NB6X72-TE773V-QBAFL4-64VIJQ-EUWUIC-UMGYJS-GCRL
to : NCSR2E-CT3GVG-RVGKNP-0QJVD2-HMVOJM-ZB7RXX-VMUC
volume: 100 xem

エクスプローラ: <https://goo.gl/kEl6yP>

tool: nem-py

- 公式ツールだが、テスト用とのこと
- エクスプローラが見れたら、demoに移ります

ツールのインストール

> pip install nem-py

NCSR2E~~ に 0.01 xem 送金する

送金のためのデータ作成

- NEM epoch time

- 手数料

- メッセージ(もし必要なら)

- デッドライン

:

署名

:

ブロードキャスト

:

NEM 関連ツール

- エクスプローラ
 - <http://chain.nem.ninja/>
- nano wallet
 - <https://github.com/NemProject/NanoWallet>

NEM パッケージ, モジュール

- python
 - <https://github.com/NemProject/nem-py> (不十分)
- node
 - <https://www.npmjs.com/package/nem-api> (不十分)

資料

- <http://qiita.com/him0net/items/9052b59db7c16c3c5540>

Zcash



Zcash を送金

// zアドレスの生成

```
zcash-cli z_getnewaddress
```

// 保有しているzアドレスの一覧確認

```
zcash-cli z_listaddresses
```

```
// zcash-cli z_listreceivedbyaddress "$address"
```

Zcash の送金

- Poloniex からtアドレスに送金したら、self goxした(っぽい).
- ドキュメントにはzアドレスの送受金についての記載はあるが、tアドレスはほとんどない.
 - tアドレスはbitcoinと同じように操作できる、との記述があるので bitcoin力を上げてから再チャレンジしたい.

Zcash 関連ツール

- エクスプローラ
 - <https://explorer.zcha.in/>

Zcash パッケージ, モジュール

- python
 - みあたらない

まとめ

- Bitcoin

- 調べれば情報がわんさか出てくる。SPV の情報も豊富。
- 各言語のモジュール、パッケージが豊富にある。

- NEM 公式のツール以外、情報が古い。

- 各言語のモジュール、パッケージが殆どない。

- Zcash

- なんでもいいから、情報をください。

まとめ2

- 全部

- 開発者・翻訳者などコントリビュータが足りていない現状.
- とはいえ、コア開発はハードル高い...
- 周辺好きな言語のモジュール,パッケージ作成からでも、なにか作ってみよう!

ご静聴ありがとうございました