**Title**: Multisig Escrow of Funds

**Summary**: Building a platform & iOS client to deposit and then distribute funds using M of N signatures to create transactions.

**Team**: Huang Pan, Dan Perez, Hans Gill, Travis Giggy

**Github**: https://github.com/huang-pan/multisig-escrow

**Slack Room**: https://thechain.slack.com/home

WHY MULTISIG ESCROW?

* A Building Block for many applications
  + Use Case 1: Investment Club Fund Management
  + Use Case 2: Insurance
* Application considerations
  + Resilient to key people dying
  + Policies:
    - Daily & per user spending limits
    - Time of day constraints
    - Emergency stop
  + Prediction markets as oracle?
* Some MultiSig websites
  + <https://www.linkedin.com/company/pavilion-io>
  + Bitgo – multisig wallet, API
  + Smartcontract.com – already implemented escrow services

TO DO:

* Finish web page
* Debug iOs app

STATUS:

* Here's a video showing what i've got workin so far. I can't get the CoreBitcoin sdk to work yet, so no multi sig.
  + [**https://www.youtube.com/watch?v=-z3ozehbT\_I&feature=youtu.be**](https://www.youtube.com/watch?v=-z3ozehbT_I&feature=youtu.be)
* Its ugly and bare bones but it can:
  + create a new address & key pair using blockcypher api
  + download 10 most recent blocks (but not transactions details)
  + send bitcoin from/to addresses that are in the apps db.
  + scan a QR code
  + display QR code for an address

NOTES:

* Using the Core Protocol
  + Local Node:
    - Takes too long to download bitcoin blockchain (2-3 days, 30 GB)
    - Bitcoin reference client (C++, most up to date)
      * Need to download entire to run wallet
    - Nodejs: bitcore.io (js version of bitcoin reference client; may not be updated, easier to learn than C++)
    - Ruby: toshi.io
    - Python: python bitcoin lib
  + API service (run reference code for you, allows you to interact with reference code):
    - free
      * Blockchain.info
        + Blockchain explorer
      * Chain.so
      * Blockr.io
        + Acquired by coinbase
      * We found [block.io](http://block.io) and chain.so's testnet APIs really helpful:
        + <https://www.block.io/api>
        + <https://chain.so/api>
    - Not free
      * Chain.com
      * Blockcypher.com
    - If you need some inspiration for a MultiSig/Escrow API, take a look at Distributed Trust by Block.io. Here are some example scripts that create 4 of 5 MultiSig addresses:
      * <https://github.com/BlockIo/block_io-python/blob/master/examples/dtrust.py>
      * <https://github.com/BlockIo/block_io-php/blob/master/examples/dtrust.php>
      * <https://github.com/BlockIo/gem-block-io/blob/master/examples/dtrust.rb>
    - What if third party APIs go away?
* Generating a website:
  + Tutorial
    - part1 : <http://cwbuecheler.com/web/tutorials/2013/node-express-mongo/>
    - part2: <http://cwbuecheler.com/web/tutorials/2014/restful-web-app-node-express-mongodb/>
    - <http://dev.blockcypher.com/samples/multisig-tx.html>
    - <http://dev.blockcypher.com/#multisig>
  + The Express Generator on express js page also help us get a site up and running faster
    - <http://expressjs.com/starter/generator.html>
  + building a bitcoin payment site w/node.js
    - <https://www.youtube.com/watch?v=5ROp9Ac3UqE>
    - <https://github.com/BlockIo/blockgarage/blob/master/onsite_projects.txt>