BLOCKCHAIN

TECHNOLOGY WORKSHOP

YESTERDAY'S MASTERCLASS:

http://neuroware.io/Blockchain-MasterClass-Q2-2017.pdf

presented by

neuroware

INTRODUCING THE NEUROWARE FOUNDERS

ONLY MSC BLOCKCHAIN COMPANY

MSC MALAYSIA Status Company

SUPPORTED BY MDEC & MOF

Mark Smalley - CEO

Living in Malaysia for the past 20 Years

Building FinTech Applications for 15 Years

Spent 10 Years Building Tech Communities

Building Blockchain Apps for 5 Years

Ruben Tan - CTO

Building Web Applications for 10 Years

Active Community Evangelist & Presenter

Early Developer at MyTeksi and OnApp

Studying Distributed Consensus for 5 Years

DISTRIBUTED CONSENSUS

HOW DO BLOCKCHAINS WORK?

BLOCKCHAINS ARE SIMPLY A NETWORK OF NODES

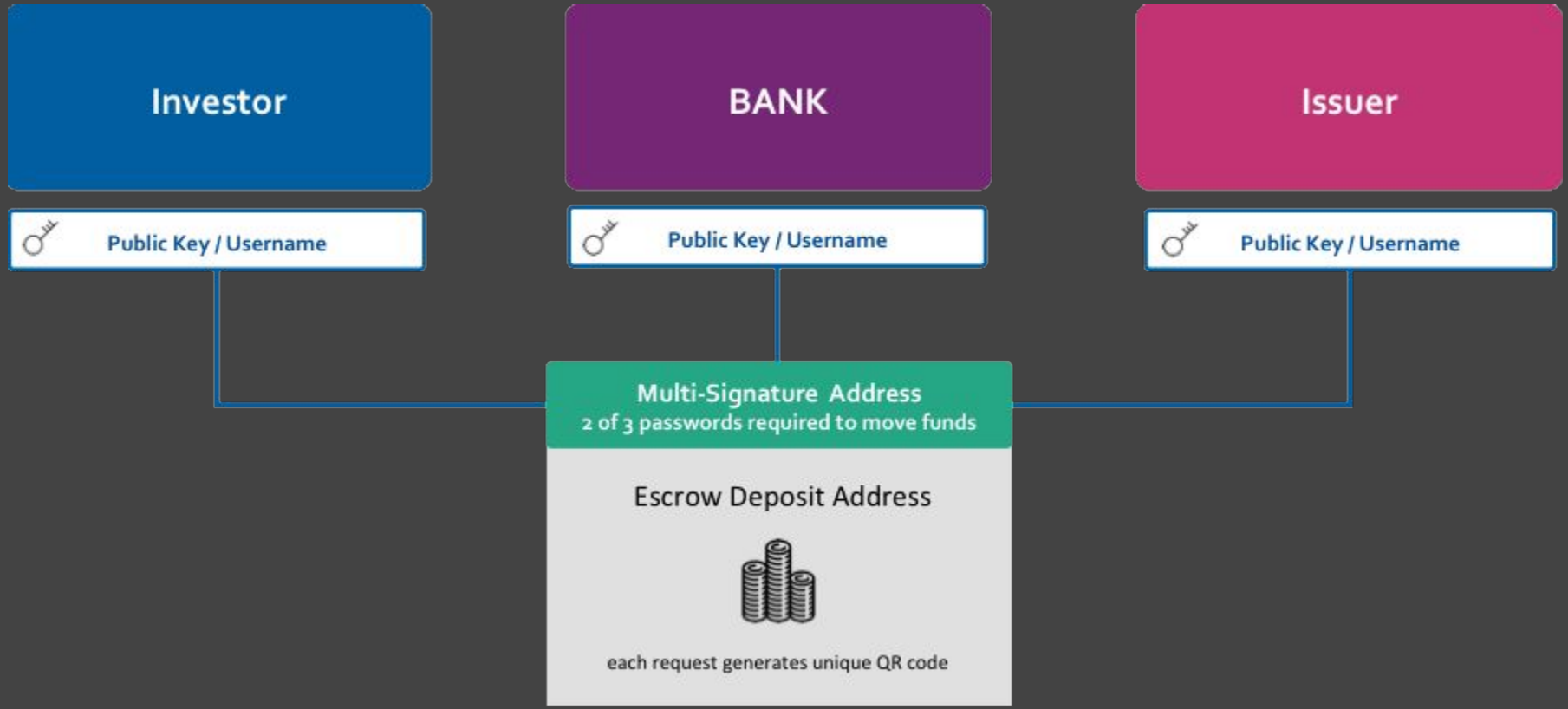
- Each member of the network runs their own node and all nodes are equal
- The blockchain becomes more secure as more nodes join the network
- All transactions across the entire network are tracked by each node
- There are no actual coins - there is only a ledger of who owns what
- On the blockchain - no one knows you're a fridge

ON THE BLOCKCHAINS EVERY ACCOUNT IS A SET OF KEYS

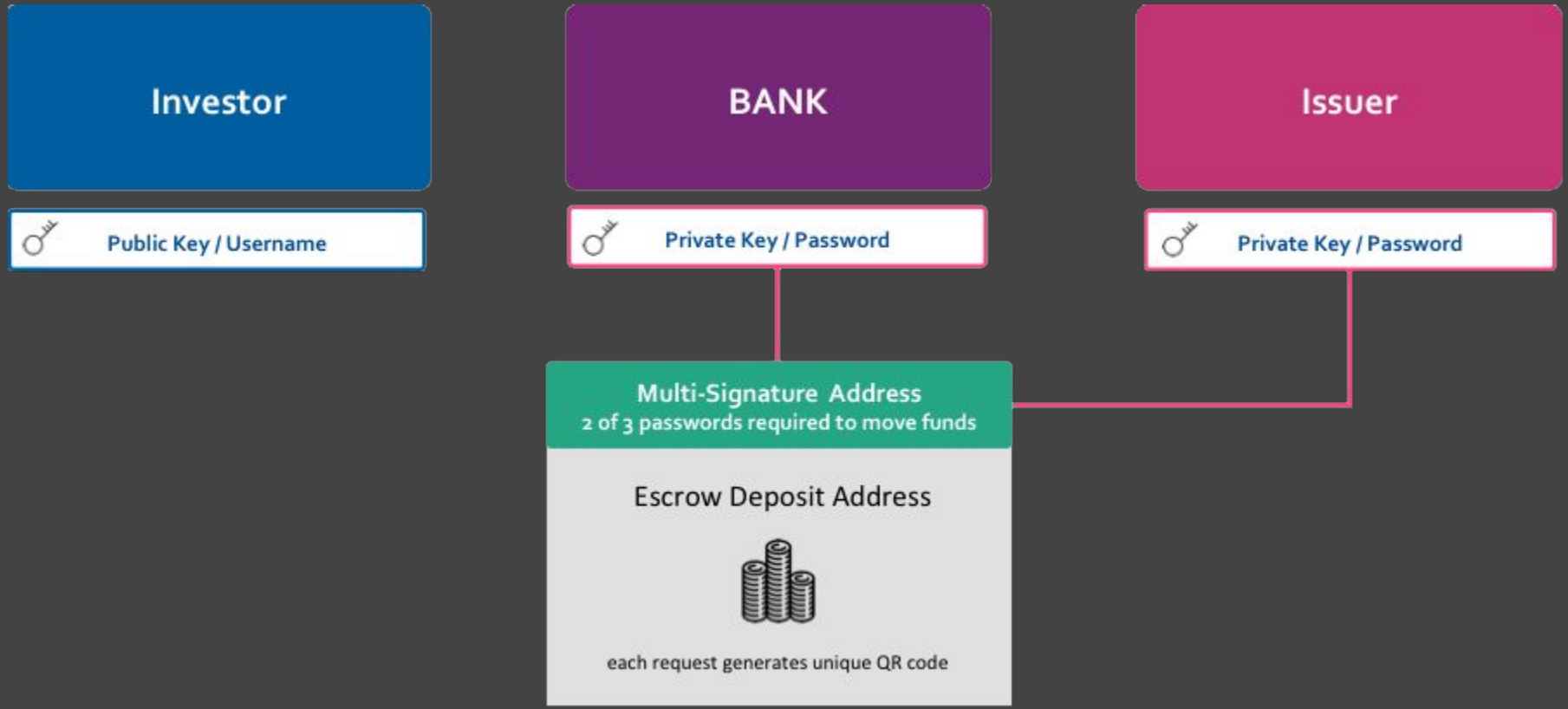
AND EACH “ADDRESS” REQUIRES A PRIVATE KEY TO ACCESS IT

SOME ADDRESSES EVEN REQUIRE MULTIPLE KEYS

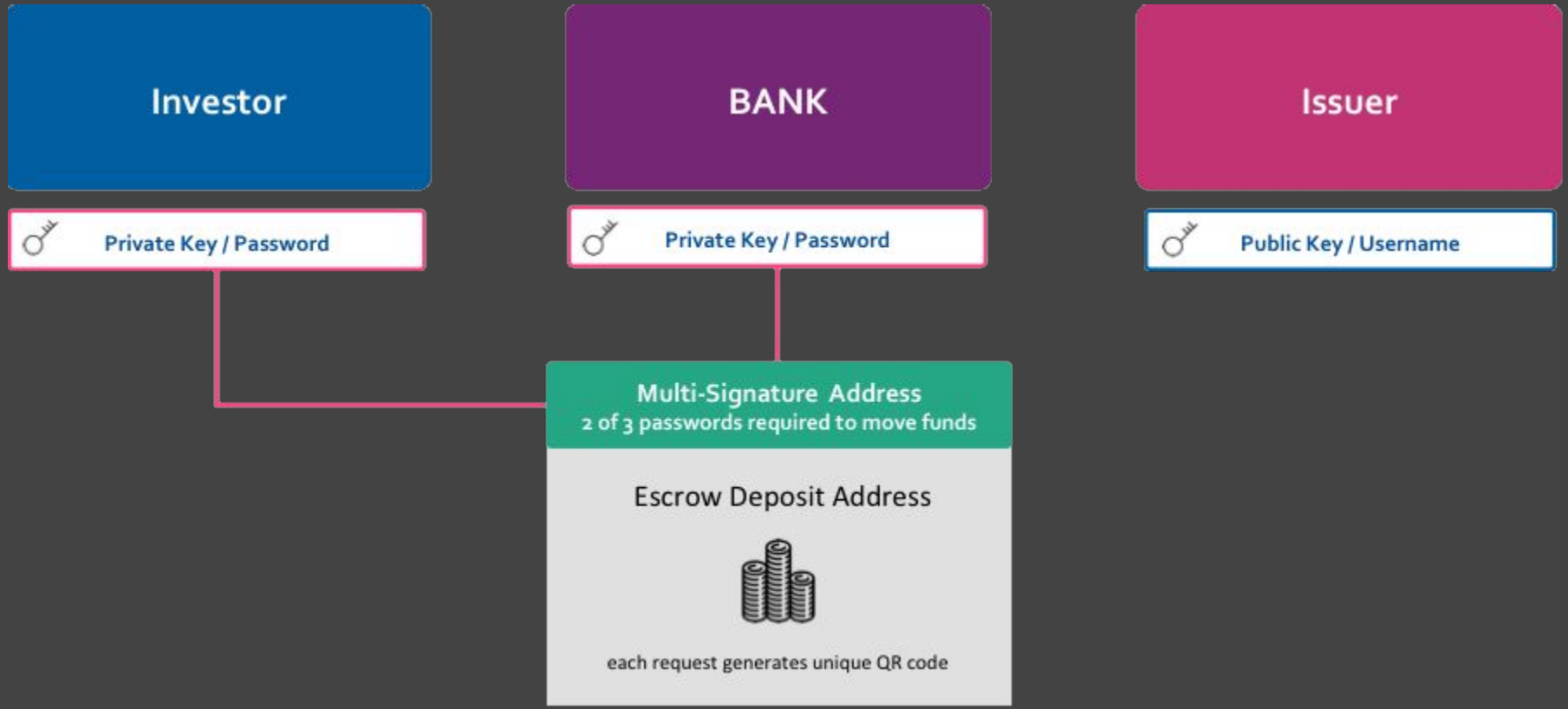
ECF CRYPTO ESCROW - NO ONE HOLDS OR MOVES FUNDS



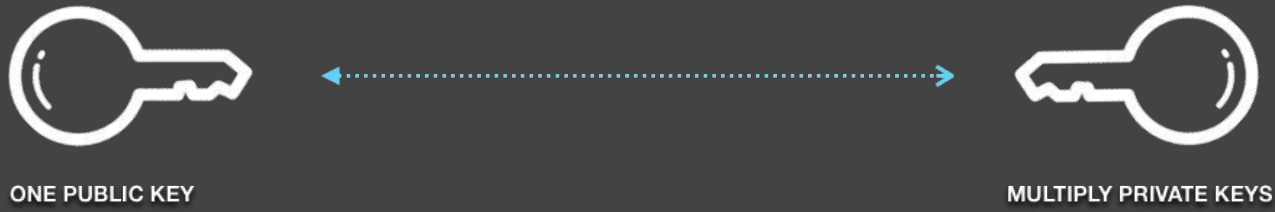
COMPLETING AN EQUITY CROWDFUNDED INVESTMENT PROCESS



REJECTING INVESTMENT OR RETURNING FUNDS TO INVESTORS



KEY PAIRS



- Example of a Bitcoin public address (derived from the public key):
  1GzBZ7eK6wzNjp1Wt6AxHo73kJL2tzoErq
- Example of a Bitcoin private key (used to transfer funds from address):
  L1winVkoRmxMdHKbwssx33Z9ZEuXeJ1eP9CVYvnNn4TdYA32GsWY
- Example of a Bitcoin extended private key (used by HD protocol):
  xprv9s21ZrQH143K2Ywhg9bhZ5nd31t3EbXsg8v28gkKjSm9PA3PiZ89d
  WW6YKxWZa2pgTuErQ65K46KGVfu1xCRBCK3Ppd465QGtH7TmxAEiLv

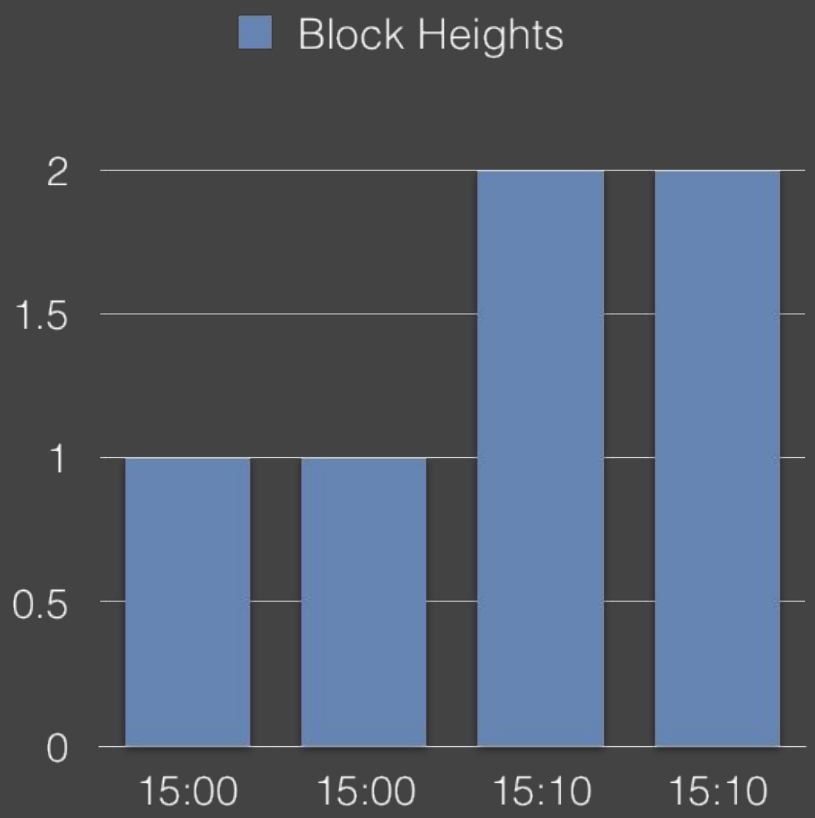
WHAT'S IN A BITCOIN TRANSACTION?

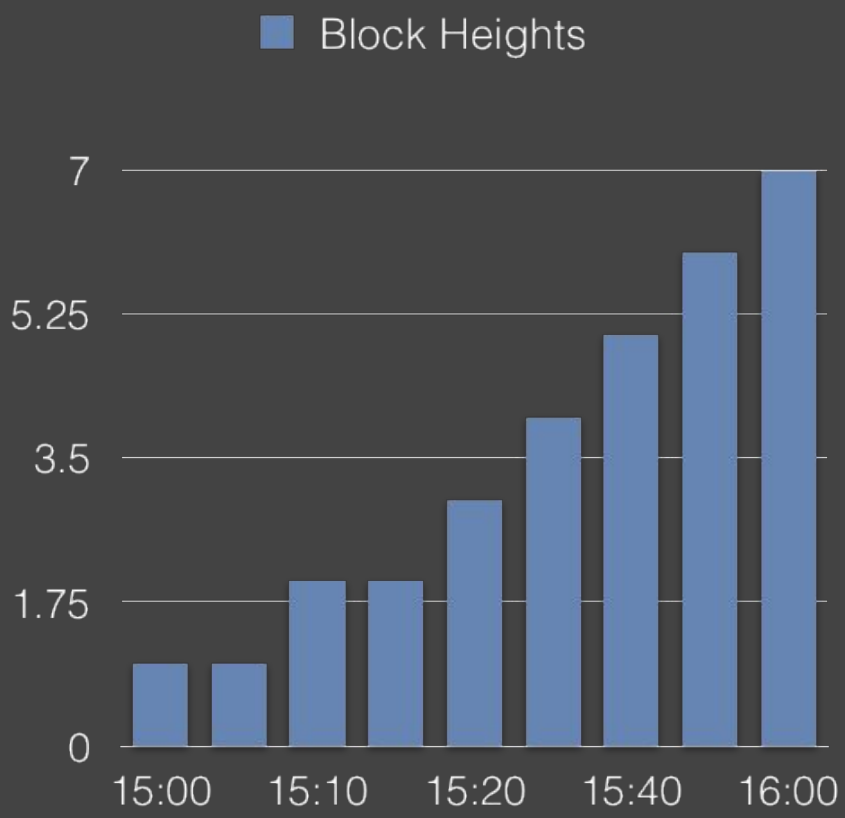
- Multiple unspent inputs are used in order to form the total value sent
- Cannot send proportions of inputs, must use all and send the change back
- Because a single transaction can send multiple values to multiple outputs
- Fees are based upon the total size (inputs and outputs) rather than value
- Paying these fees is done by forgetting to send some value to someone
- Transaction scripts can contain complex variables (multi-sig & timed locks)
- However, they can only contain one OP_Return (38 bytes of arbitrary data)

PUTTING THE BLOCK INTO BLOCKCHAINS

- Transactions are batched into blocks every ten minutes (with Bitcoin)
- The block is added to the chain with a link to the previous block
- With the block added to the chain, its transactions are then confirmed
- As soon as a new block has been added linking to that original block, the transactions from the first block then have 2 confirmations
- It is recommended that large physical transactions wait for 6 confirmations
- Whereas digital downloads may require no confirmations at all

REAL TIME Vs TRUTH

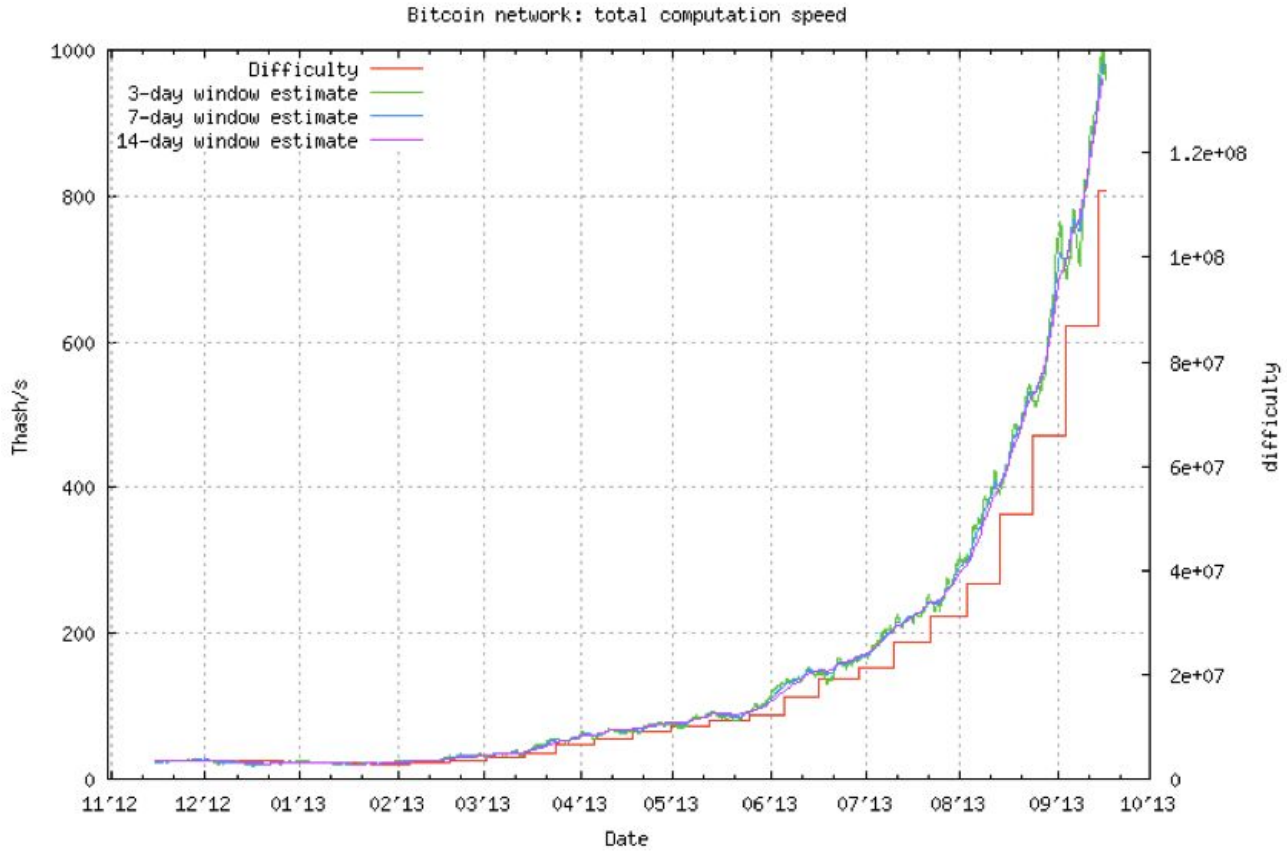




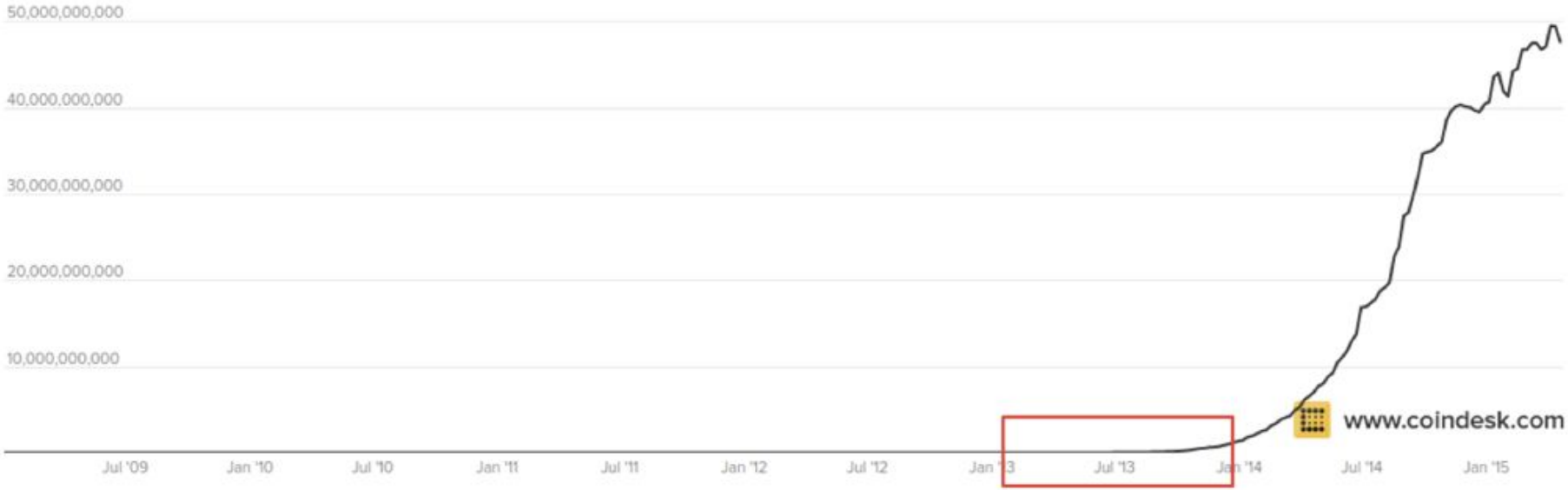
MINING FOR NUMBERS

- To reach consensus as to which node has the right to add the next block to the chain, miners compete in a race to solve cryptographic equations
- Miners gather and in-turn verify unconfirmed transactions into blocks
- They then add a nonce (one use number) to the block and hash it
- If the hash has X number of zeros at the beginning it becomes a valid block
- Otherwise the miners increase the nonce and they hash the block again
- Solving these cryptographic equations is becoming increasingly difficult

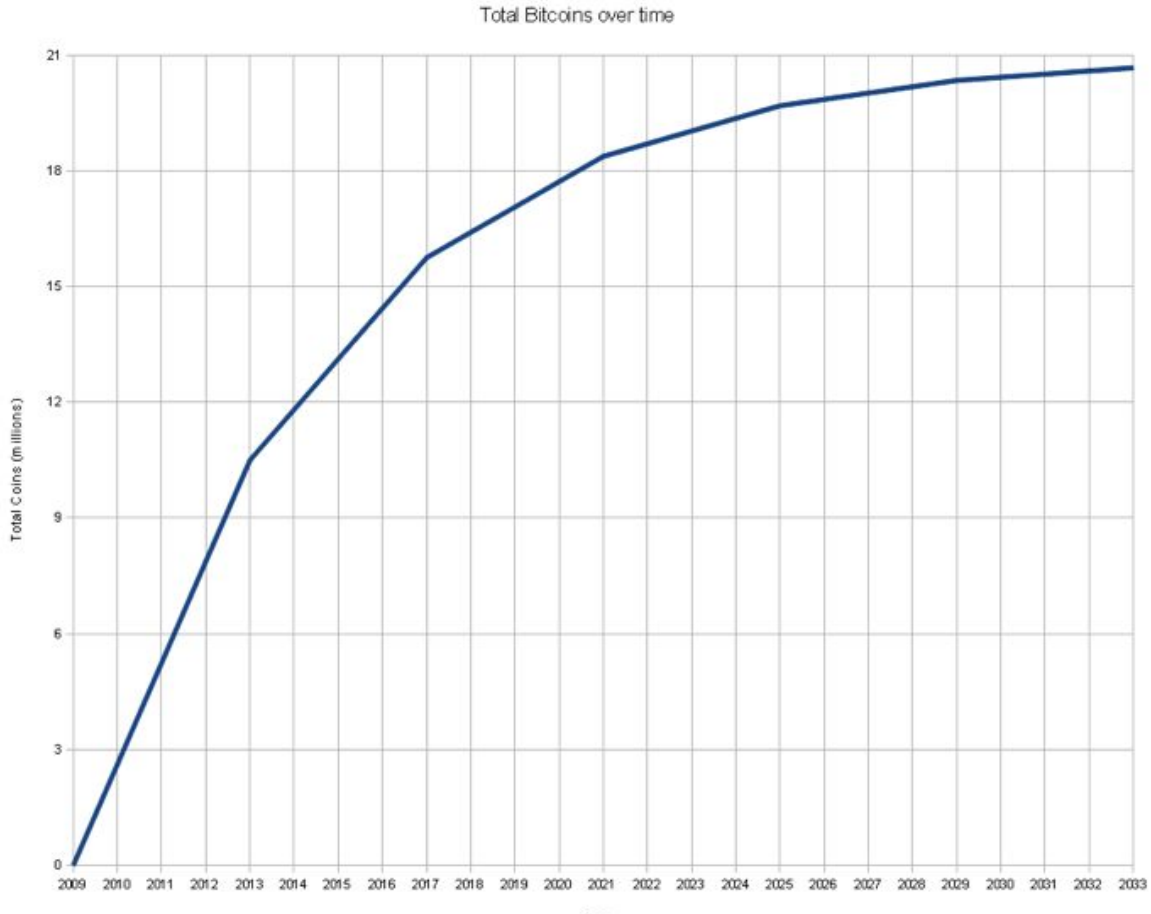
THIS IS THE HASHING POWER OF THE NETWORK IN 2013



MINING IS NOW A BILLION DOLLAR BUSINESS



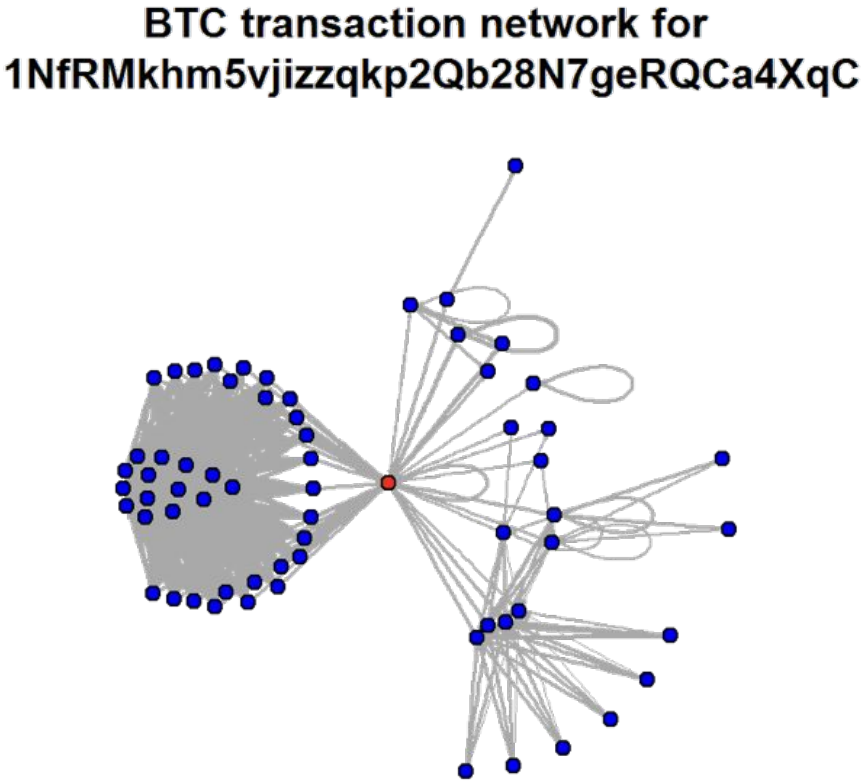
LONG TERM FUNCTION OF MINERS IS NOT TO MINE



TRUST IS SOLVED VIA TRANSPARENCY - IT'S OPEN TO ALL

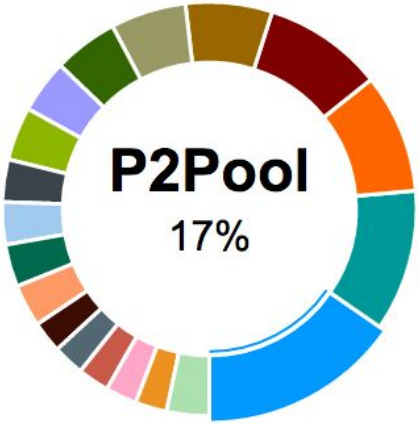

```
{
  "address": "DEHfgFYKL97gFFoYHM7UejXBGKjLFzD4za",
  "total_received": 1000000000,
  "total_sent": 800000000,
  "balance": 200000000,
  "unconfirmed_balance": 0,
  "final_balance": 200000000,
  "n_tx": 4,
  "unconfirmed_n_tx": 0,
  "final_n_tx": 4,
  "txs": [
    {
      "block_hash": "e9a38d8fa6b7abc1a35a2fad93bfa52e3eb9b1ca5cb2825692db0a3c2f054354",
      "block_height": 1213596,
      "block_index": 35,
      "hash": "3ebaecf042e0dbe20a35c0dd2700c83b13a5a1764e1882c2cc39e4bd81c326cf",
      "addresses": [
        "DEHfgFYKL97gFFoYHM7UejXBGKjLFzD4za",
        "DJHXpkQGcRydRvocWaeUtZir6c2pXHkUn4"
      ],
      "total": 400000000,
      "fees": 100000000,
      "size": 225,
      "preference": "high",
      "relayed_by": "",
      "confirmed": "2016-05-16T14:13:56Z",
      "received": "2016-05-16T14:13:56Z",
      "ver": 1,
      "lock_time": 0,
```

EVERYONE HAS A RECORD OF EVERYTHING - SO BE CAREFUL



TIME TO EXPLORE

SoChain. Networks Blockchain API Wallet API Blog



SoChain. Wow.

The Fastest Bitcoin Block Reader

Search for Addresses, Transactions, Blocks

Price	1,359.99 USD/฿
Hashrate	3610.96 PH/s
Activity	149 TX/min
Unconfirmed Txs	30,639
Fee Rate	0.00397766 BTC

29558.449 kb / 1000 kb

Transaction Ages (?)

28h 42m 0s

Latest TX	Size	Sent (฿)
...4de9030b	0.22 kb	0.003735
...933da4f7	0.22 kb	1.864657
...cfbe8c8d	0.22 kb	0.028045
...f9fa0dfe	0.22 kb	1.000000

Block #	Segwit?	Age	Miner	Transactions	Size
463,983	✓	about a minute	*BTCChina Pool*	1,862	998.10 kb
463,982		9 minutes	*1ERfGndG...*	1,974	998.21 kb
463,981		24 minutes	*ViaBTC*	1,996	999.16 kb
463,980		40 minutes	*P2Pool*	2,019	998.20 kb

TIPS & TRICKS

STORING & USING CRYPTO-CURRENCY

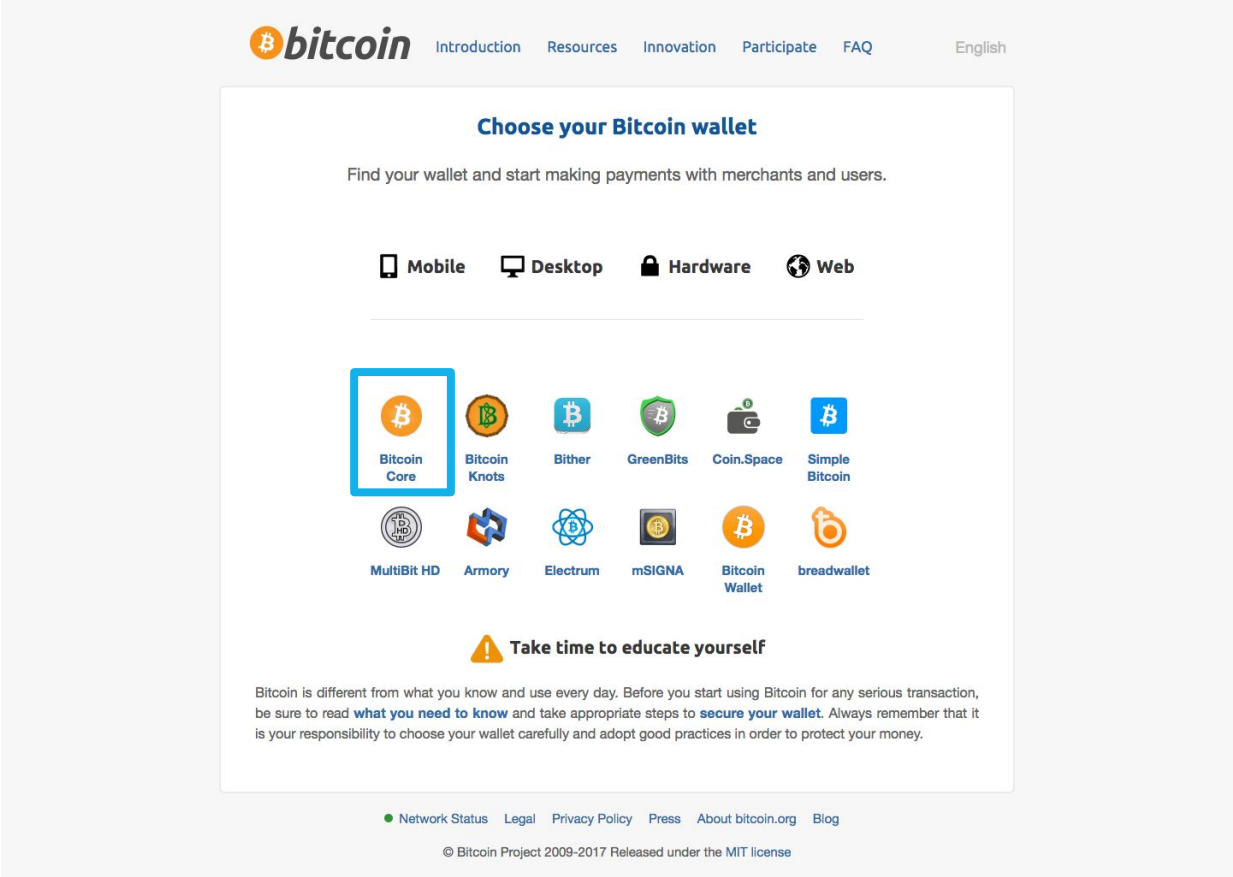
WHO OWNS WHAT? NOT TO MENTION MULTI-SIG

- Paper Vs Brain
- Hardware Vs Software
- Hard Drive Vs Web-Service
- Pseudo-Random Vs Deterministic

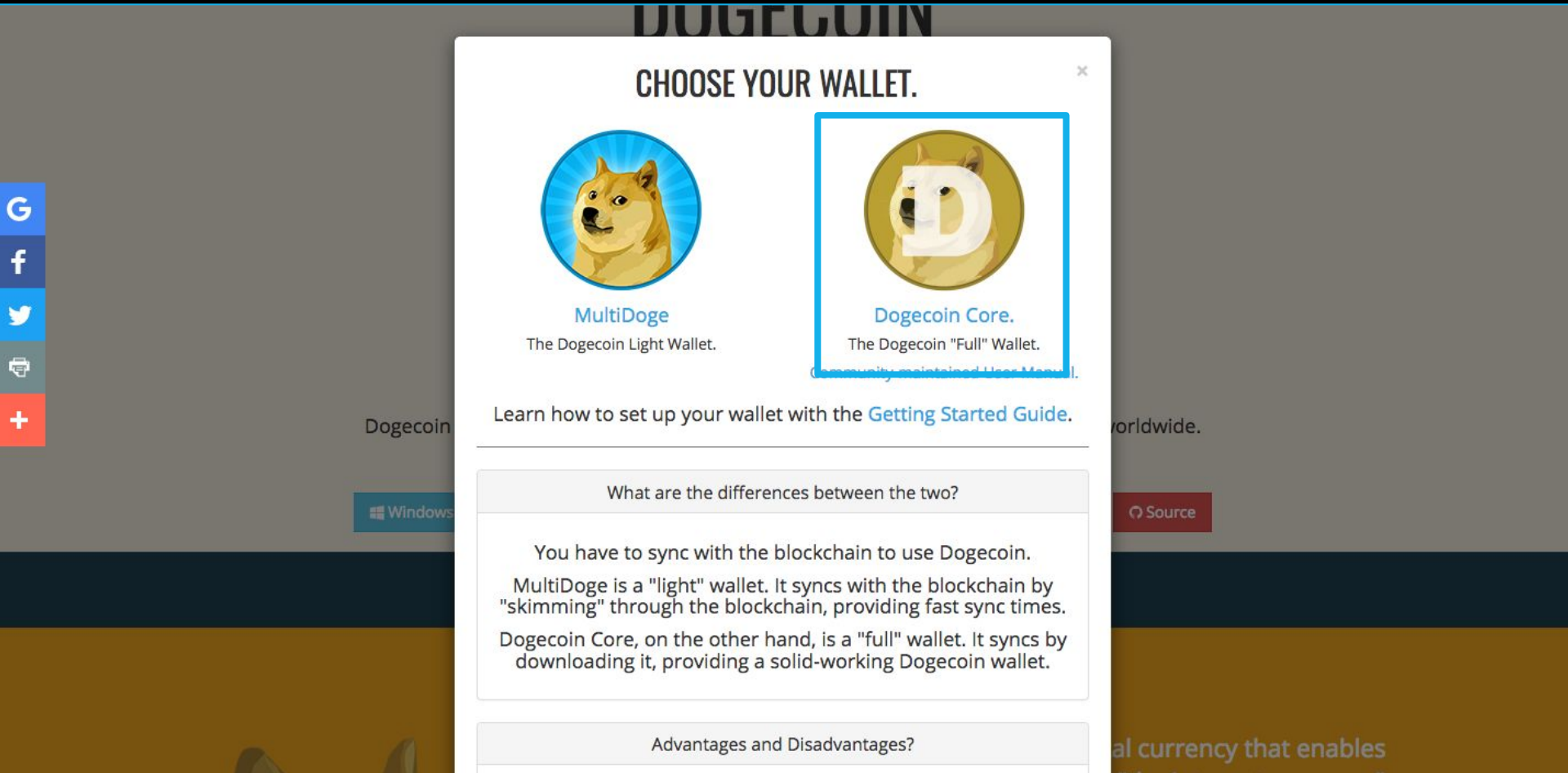
- Exchanges are **NOT** wallets …

  (1 exchange hacked every 3 months)

BITCOIN CORE = **FULL NODE** (RAW CHAIN = 120GB+)



DOGECOIN CORE = **FULL NODE** (RAW CHAIN = 20GB+)



JAXX.io = **NO NODE** (LOCAL STORAGE / APIs)

Support | View Source Code

Jaxx

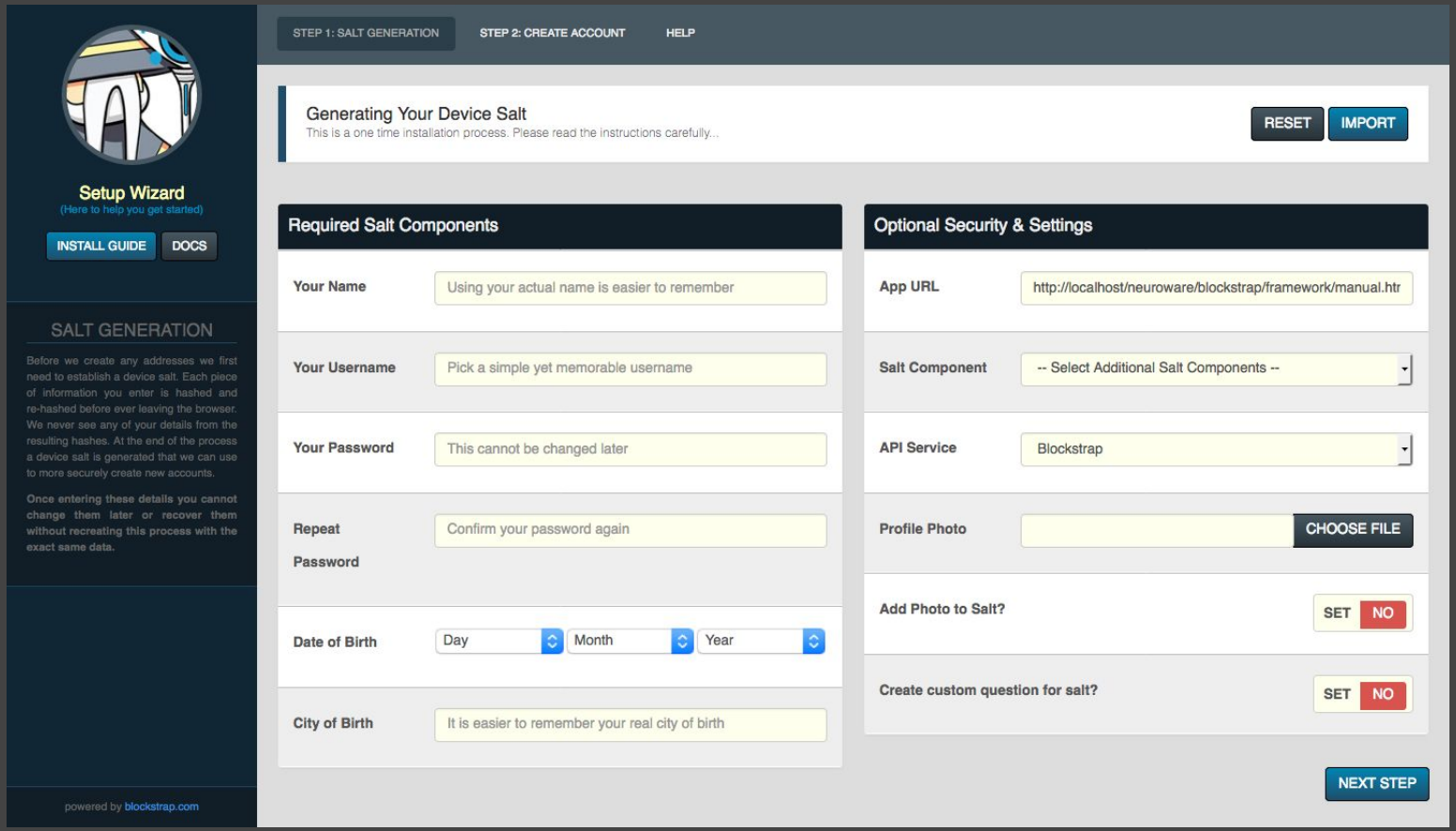
YOUR BLOCKCHAIN INTERFACE

Install Now

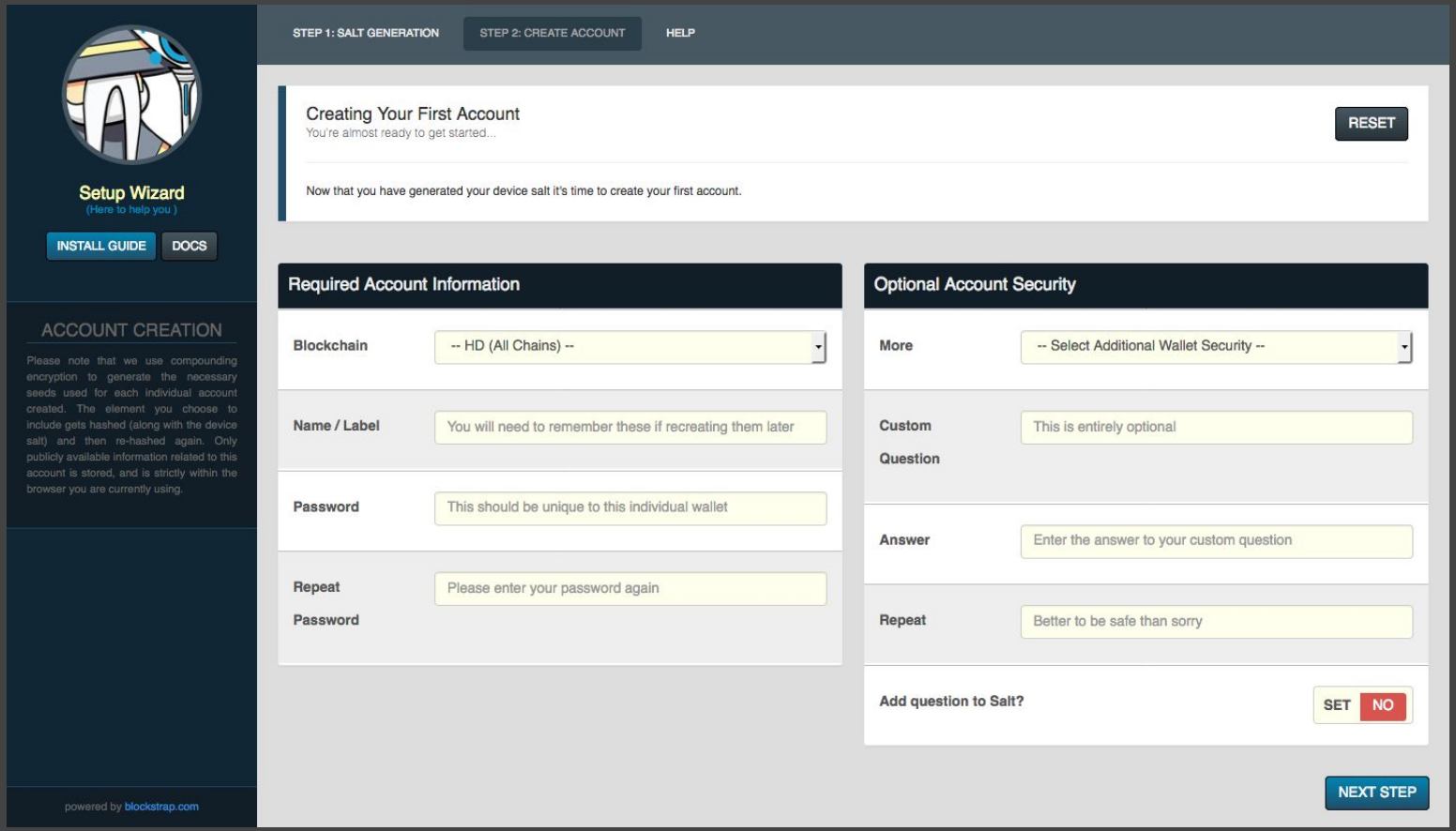
Android	iOS	OS X	Chrome
Mobile	Mobile	Desktop	Extension
Tablet	Tablet		

Firefox	Windows	Linux	Hardware
Extension	Desktop	Desktop	Coming soon

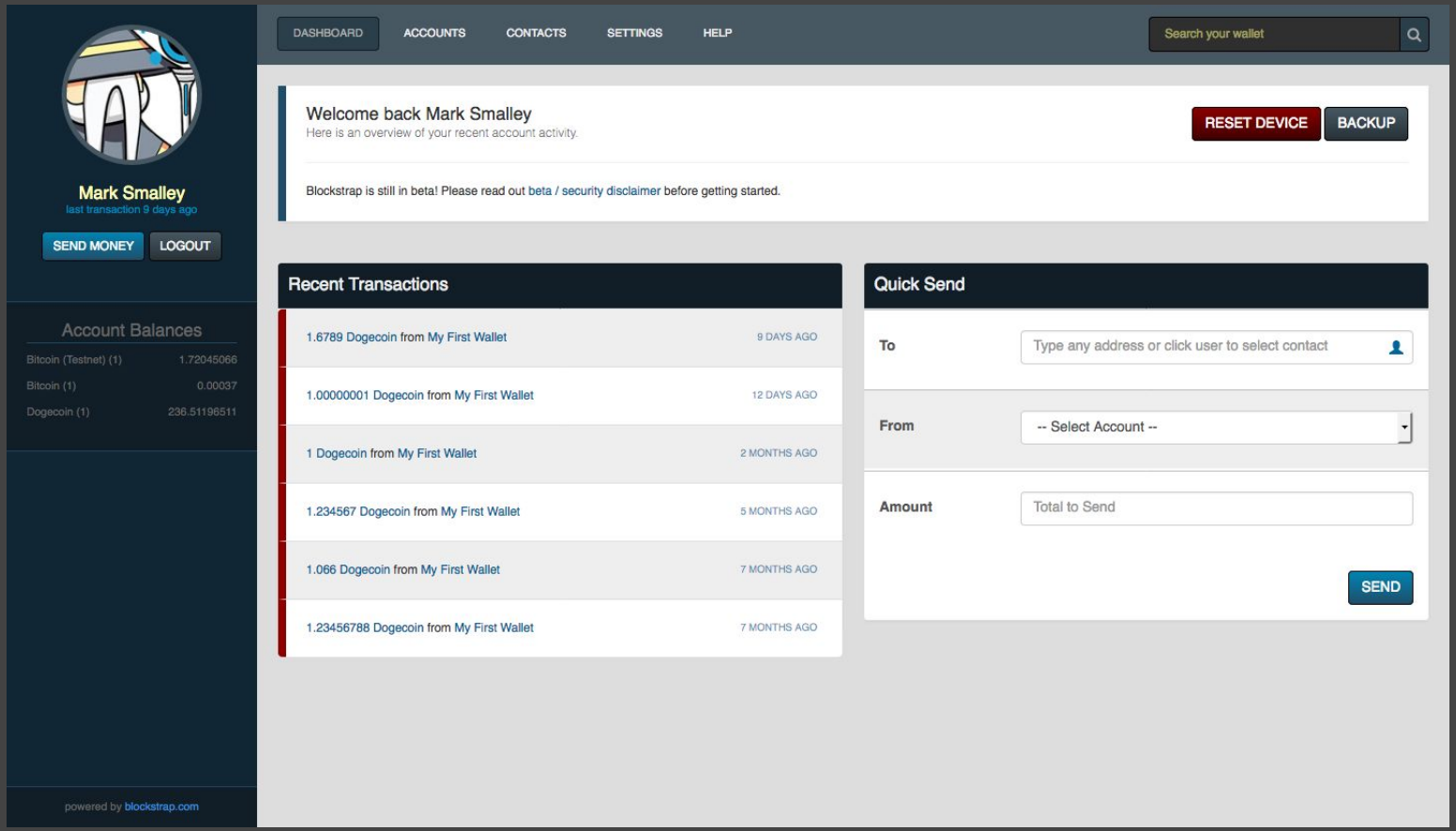
LET'S CREATE A DETERMINISTIC SALT FOR THE DEVICE FIRST



THEN WE CAN CREATE SECURE BRAIN WALLETS



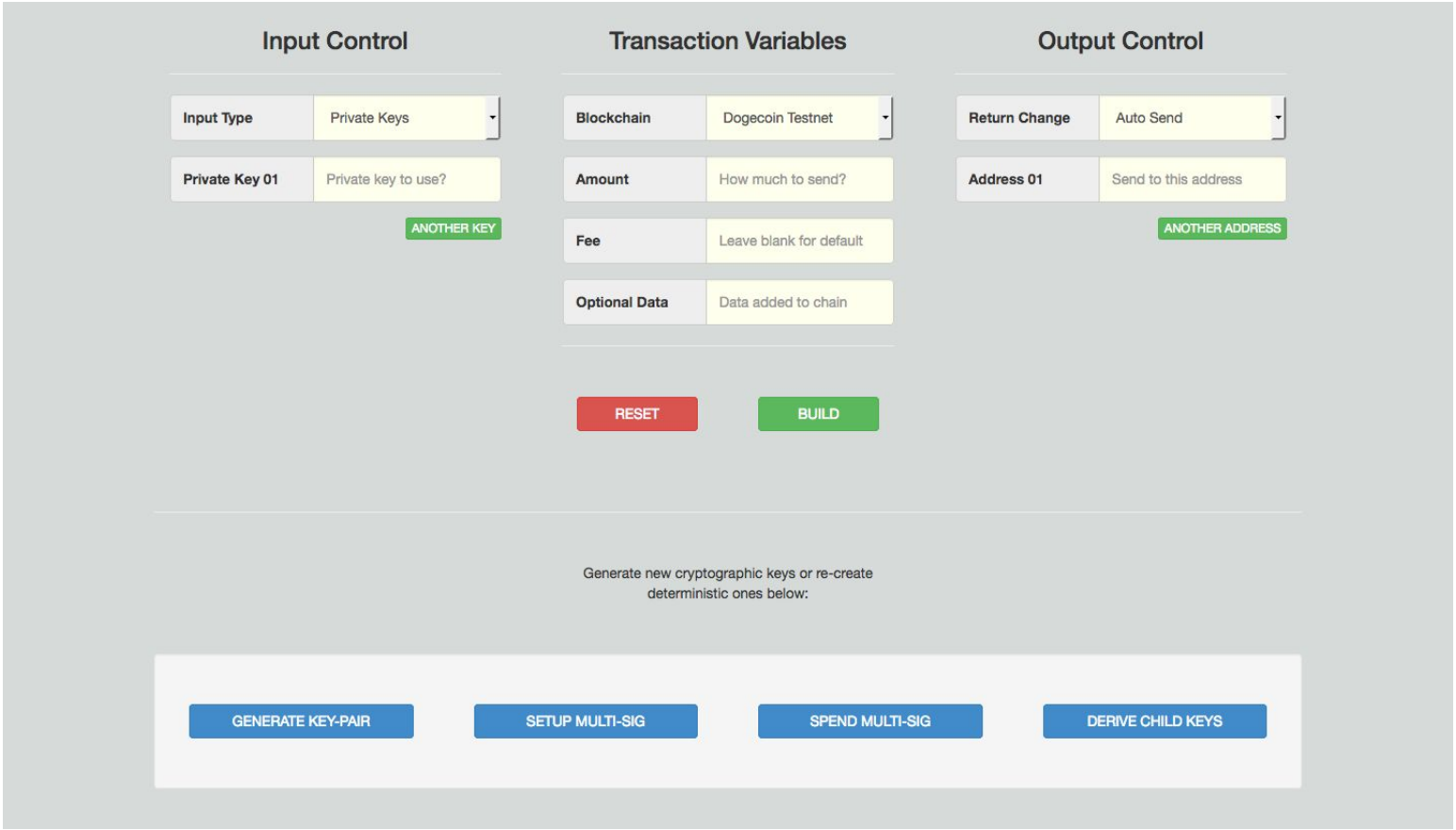
LET'S SEND YOU SOME COINS



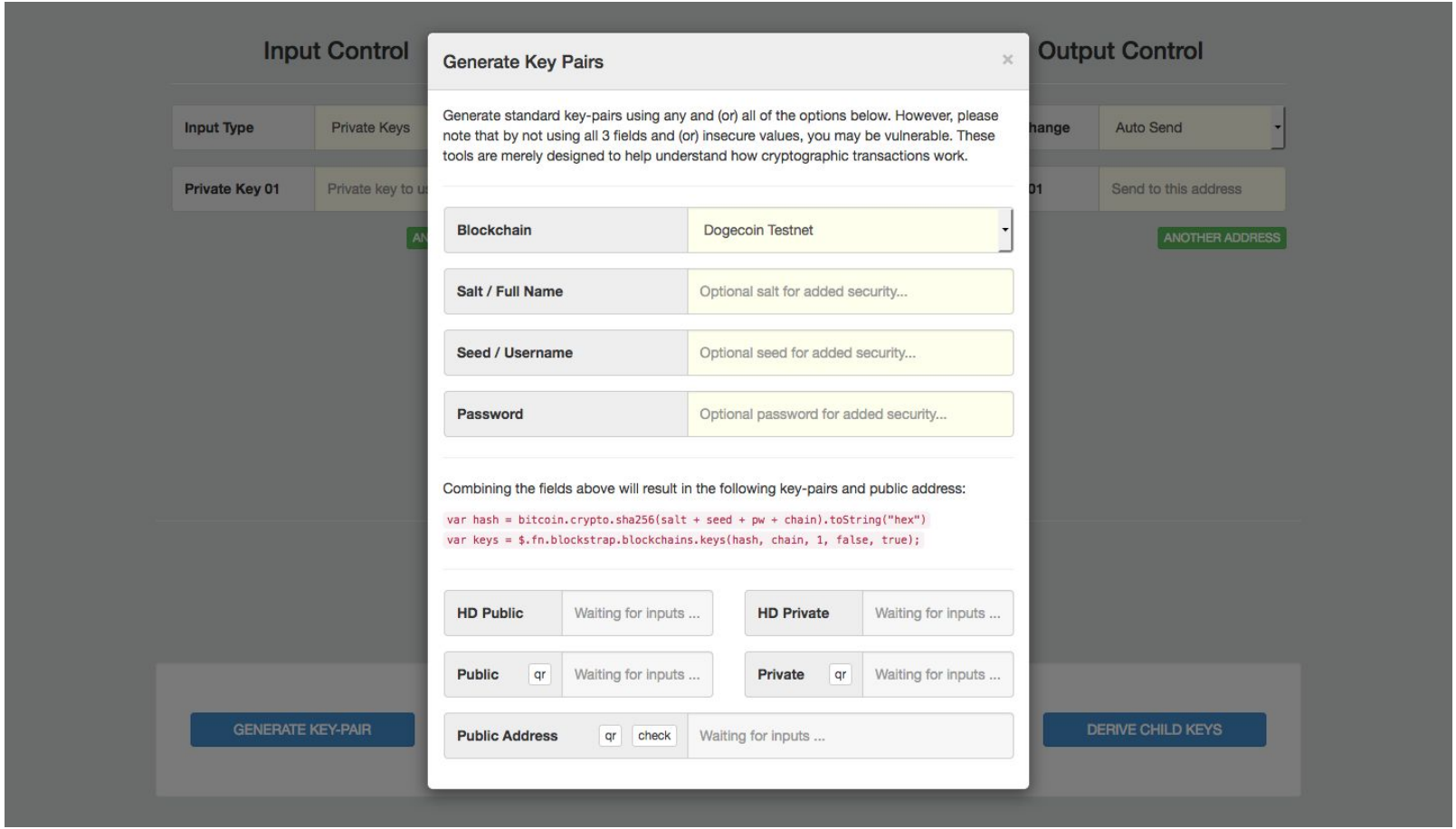
KEY MANAGEMENT

GENERATING & USING CRYPTOGRAPHIC KEYS

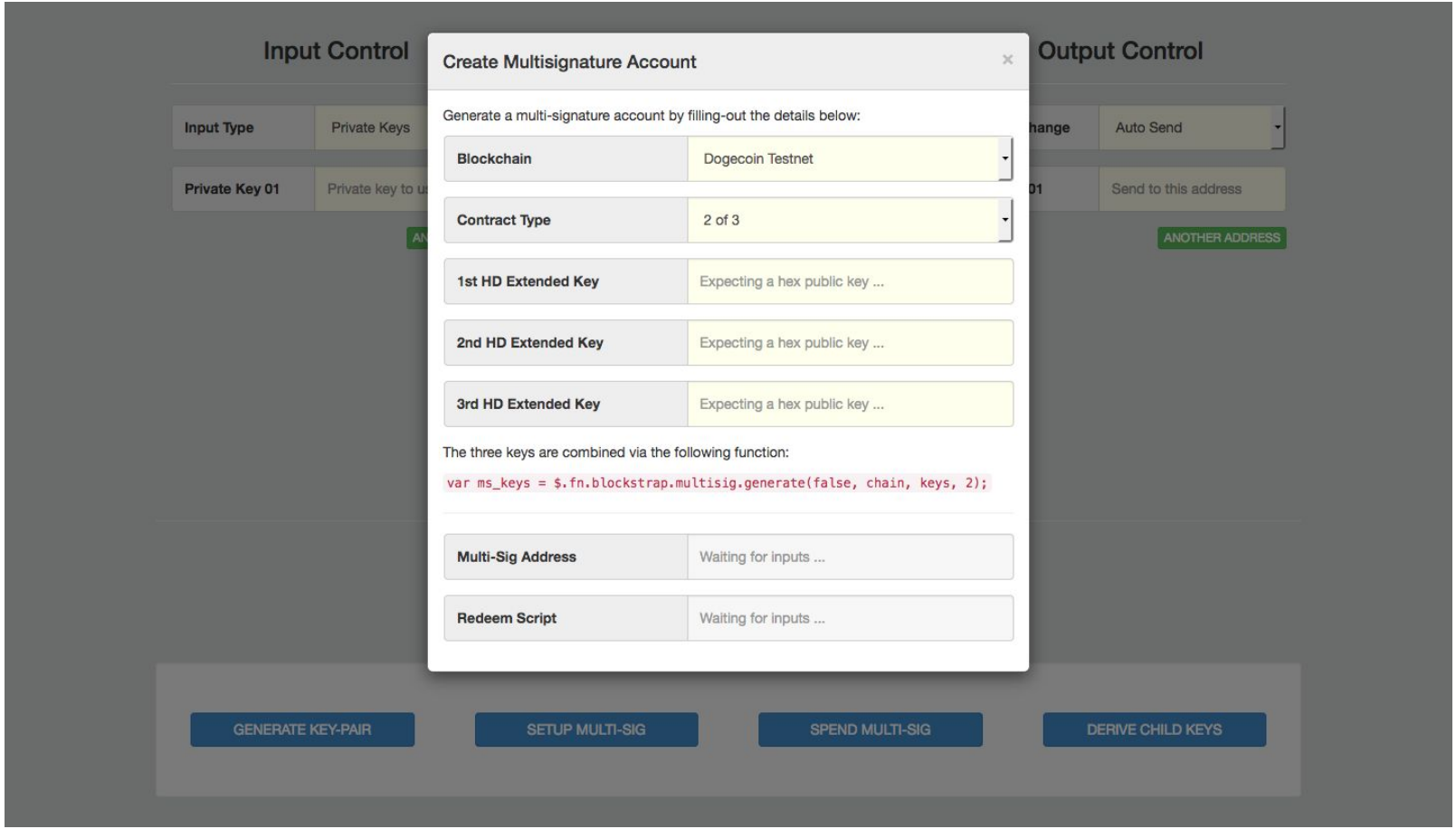
LET'S PLAY WITH THE TOOLBOX



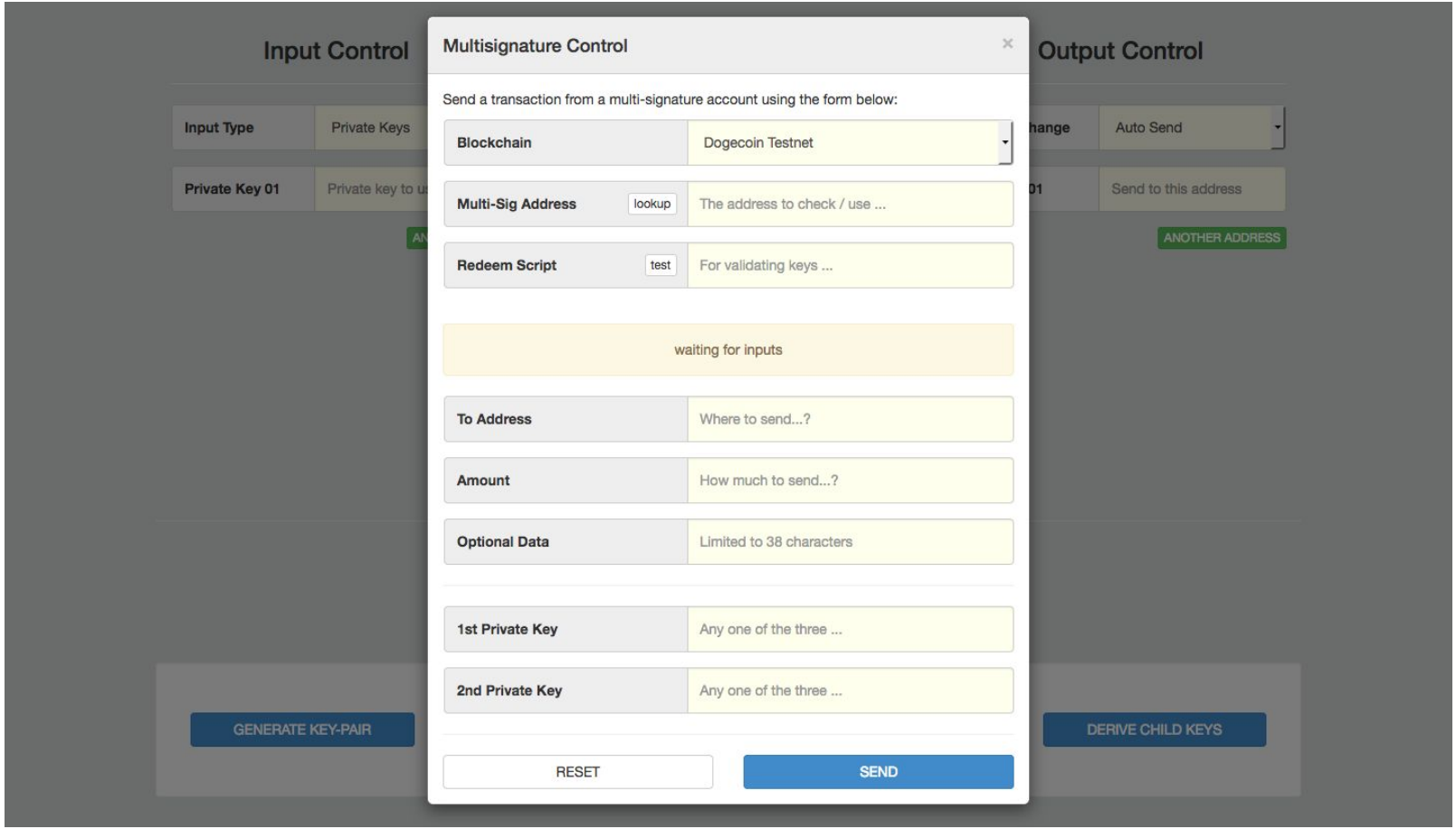
PUBLIC KEYS Vs ADDRESSES Vs PRIVATE KEYS Vs HD KEYS



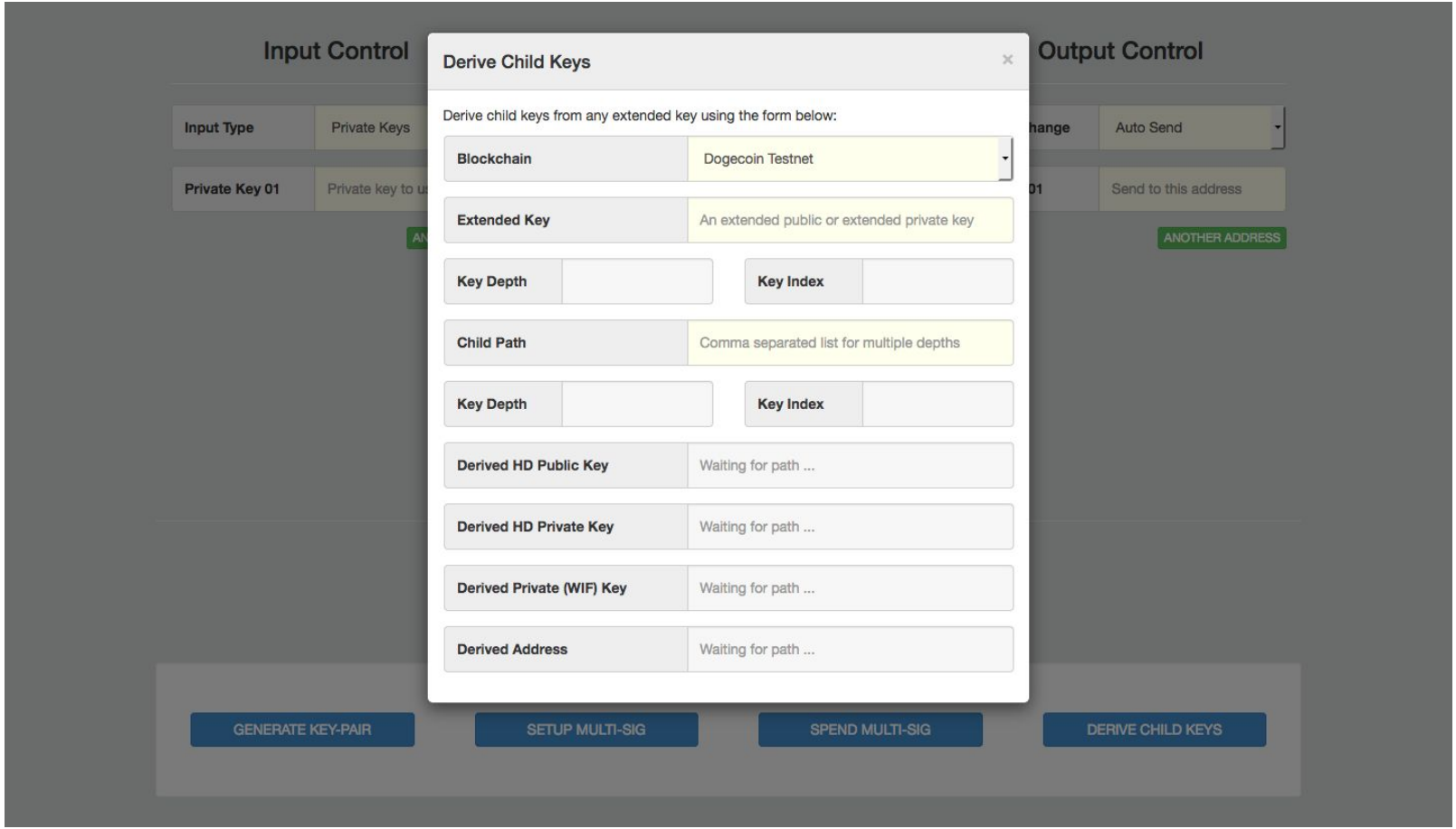
CREATING MULTI-SIGNATURE ACCOUNTS



MOVING FUNDS FROM A MULTI-SIGNATURE ACCOUNT



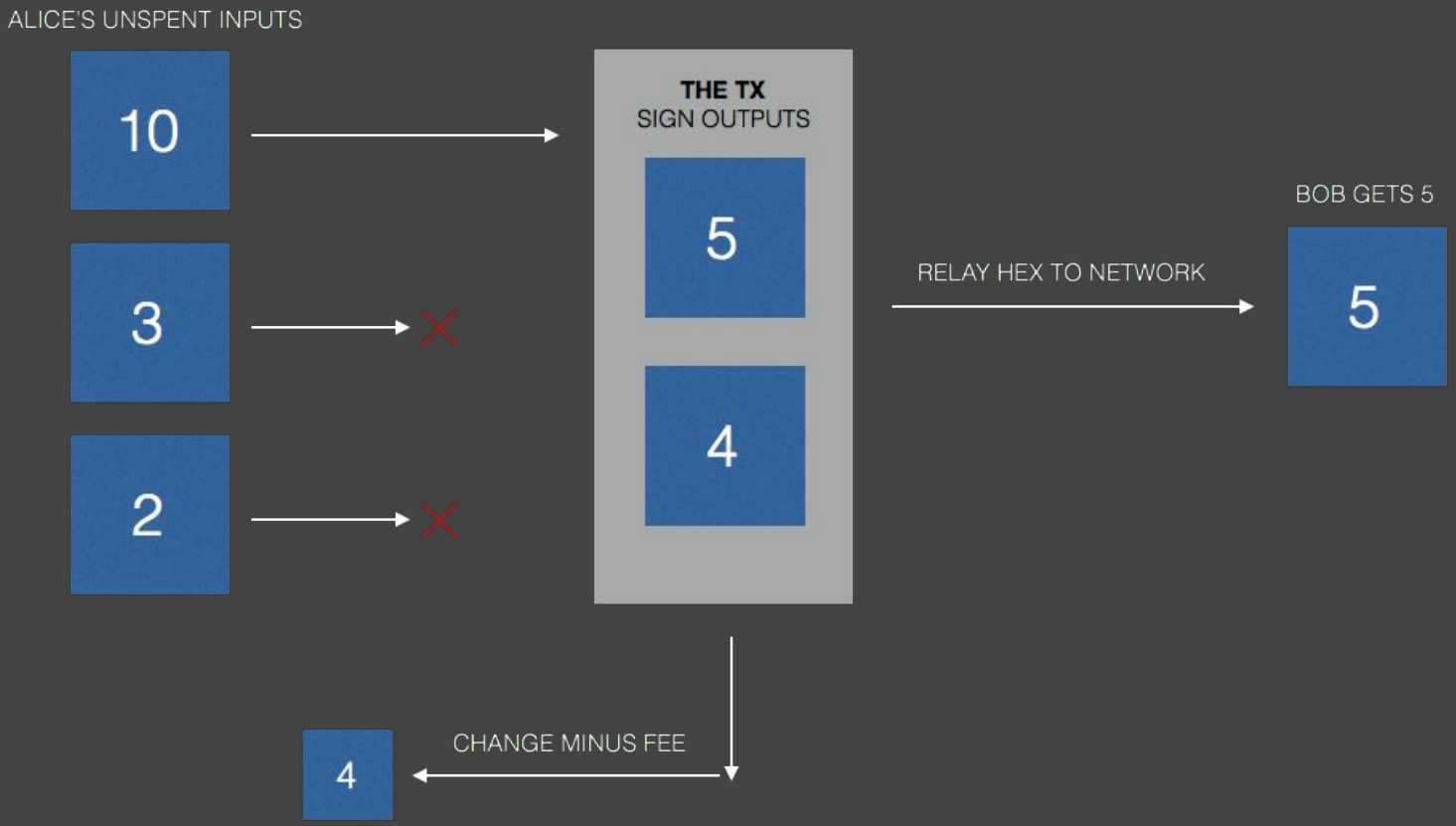
HIERARCHICALLY DETERMINISTIC KEYS



CRYPTO TRANSACTIONS

HOW TO SEND UNSPENTS?

ALICE CAN'T SEND WHAT SHE DOESN'T HAVE AND BOB WANTS 5



TIME FOR SOME CODE

```
$inputs = [ ];
$bitcoind = new jsonRPCClient("http://un:pw@localhost:8585/");
$unspents = $bitcoind->listunspent(1, 9999999, [$address_to_check]);

foreach($unspents as $unspent)
{
	if($balance >= ($amount_to_send + $required_fee)
	{
	$balance = $balance + intval($unspent['amount'] * 100000000);
	$inputs[ ] = $unspent;
	}
}
```

TIME FOR SOME CODE

```
$outputs = [ {
    address: $address_to_send_to,
    value: intval($amount_to_send * 100000000)
},
{
    address: $address_to_send_change_to,
    value: $total_amount_of_inputs - ($amount_to_send + $fee)
}];

foreach($outputs as $key => $output)
{
    $outputs[$key] = sign_tx($output, $private_key);
}
```

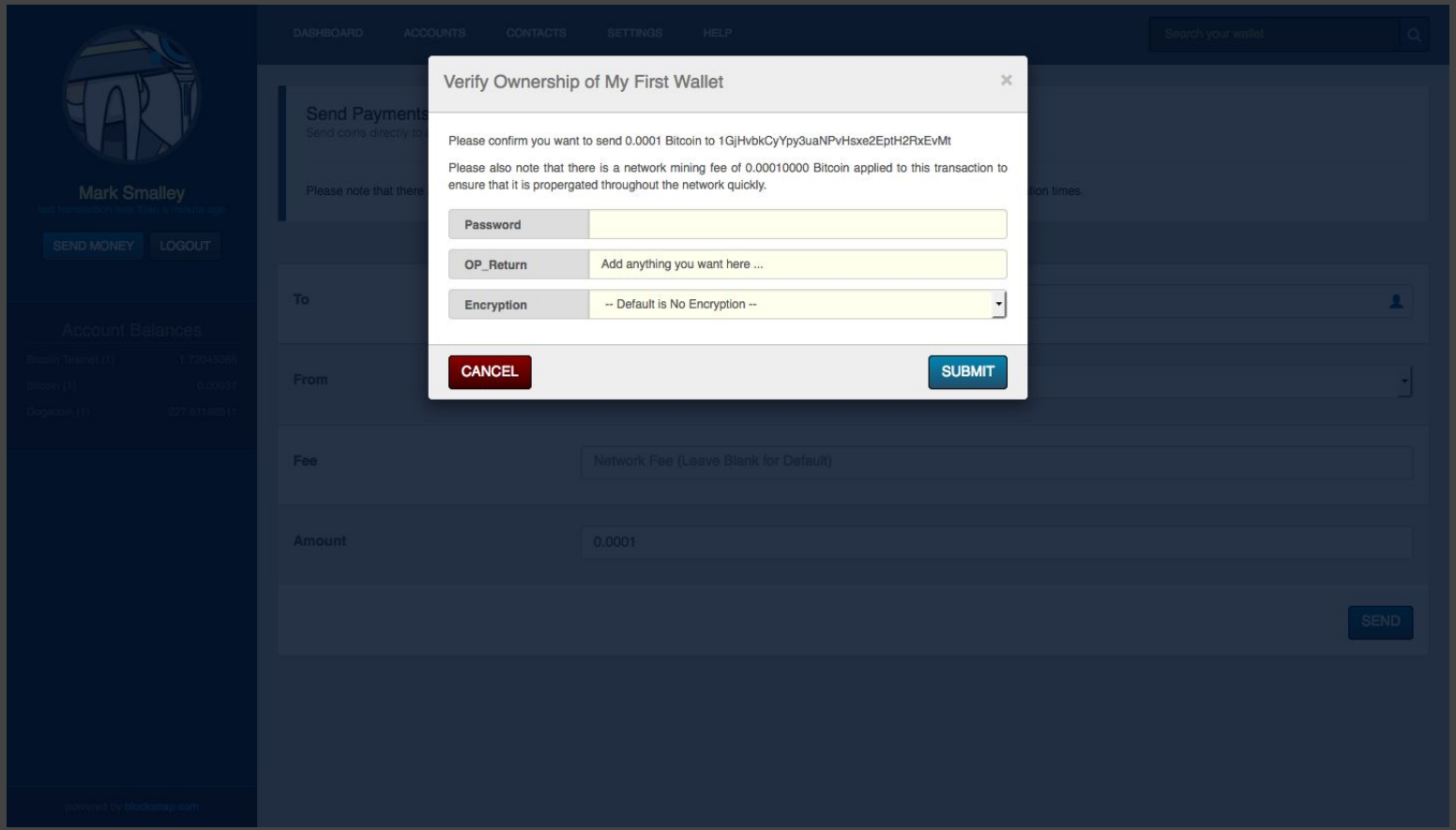
TIME FOR SOME CODE

```
$raw_transaction = transaction_to_hex($inputs, $outputs);

// $raw_transaction_should_equal =
“0100000001484d40d45b9ea0d652fca8
258ab7caa42541eb52975857f96fb50cd732c8b481000000008a47304402
202cb265bf10707bf49346c3515dd3d16fc454618c58ec0a0ff448a676c54ff
71302206c6624d762a1fcef4618284ead8f08678ac05b13c84235f1654e6a
d168233e8201410414e301b2328f17442c0b8310d787bf3d8a404cfbd070
4f135b6ad4b2d3ee751310f981926e53a6e8c39bd7d3fefd576c543cce493
cbac06388f2651d1aacbfcdffffffff0162640100000000001976a914c8e9099
6c7c6080ee06284600c684ed904d14c5c88ac00000000”;

$txid = relay_raw_transaction($raw_transaction);
```

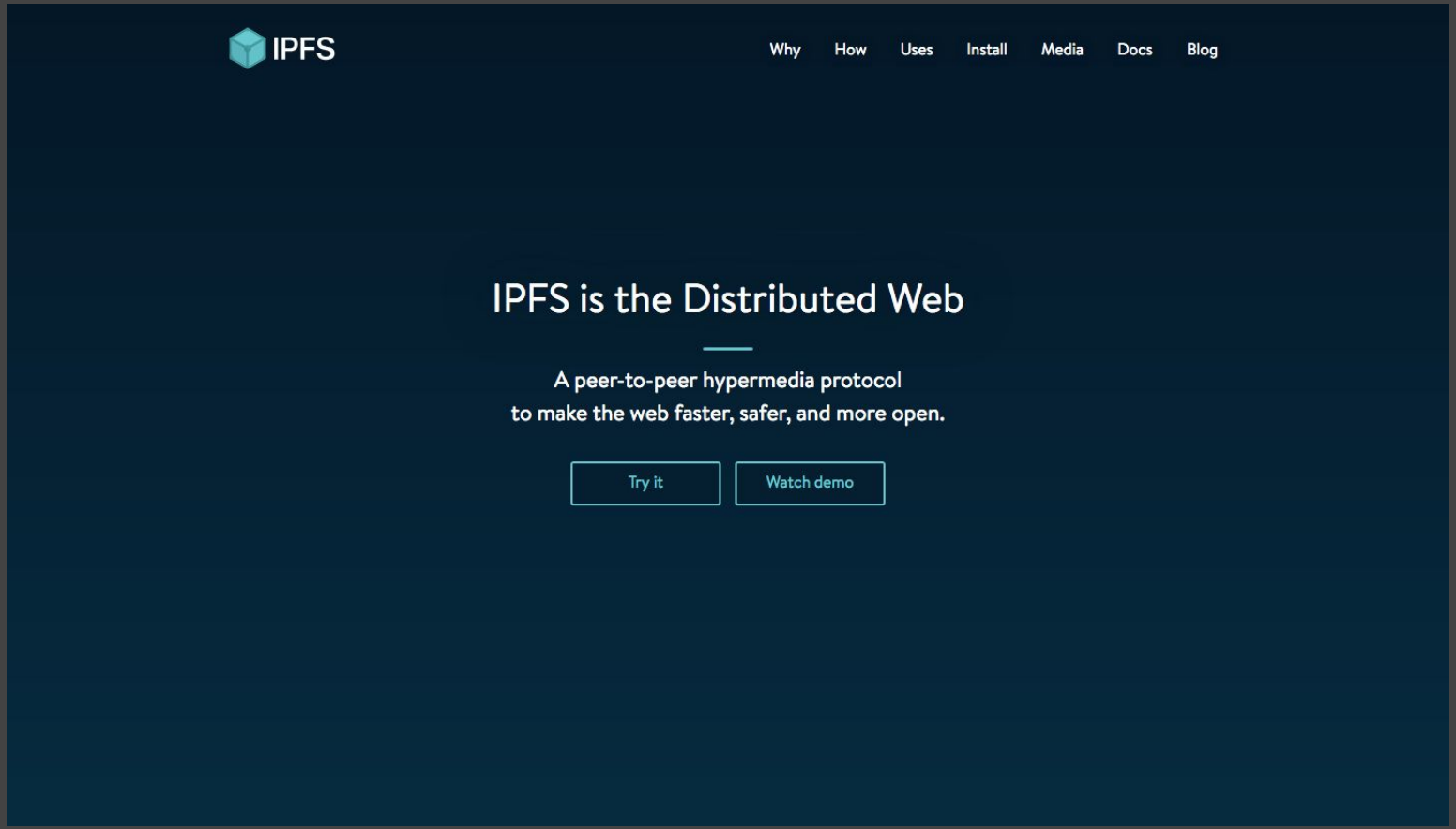
IMMUTABLE DATA

USING THE BLOCKCHAINS FOR STORAGE

STORING DATA IN OP_RETURNS



IPFS = INTERPLANETARY FILE SYSTEM = HTTP REPLACEMENT



SMART CONTRACTS

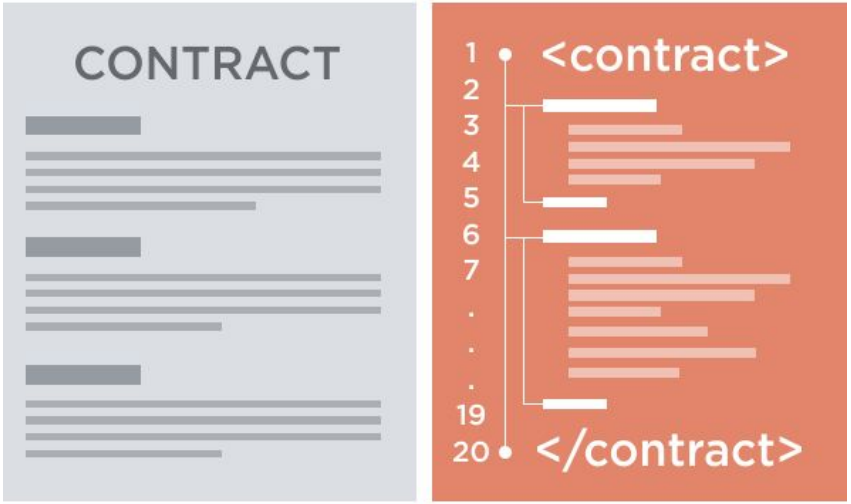
PROGRAMMABLE MONEY & AUTOMATION

SMART CONTRACTS WERE POPULARIZED BY ETHEREUM

THE WORLD'S SUPER COMPUTER...?

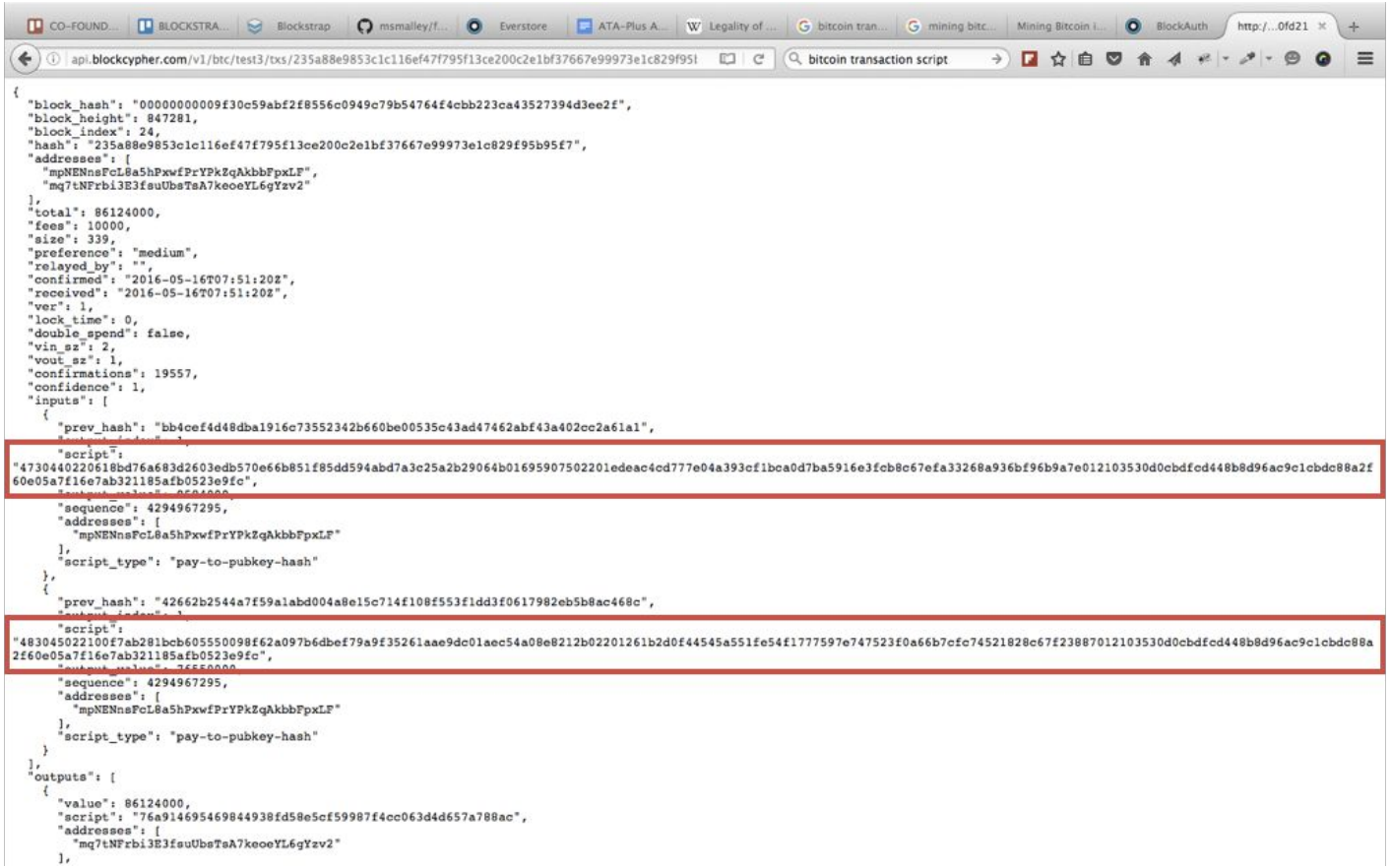
- Raised US$15 Million in crowd-funding when launching their Ether currency
- Aiming to be the first turing complete blockchain, they have almost achieved it
- Heavily supported by Microsoft and also used by IBM for their IoT platform
- Recently raised US$150 Million in crowd-funding their own venture fund
- However, the more moving parts a system has - the more likely it is to break

IN REALITY - SMART CONTRACTS ARE EVERYWHERE



- Even Bitcoin utilizes basic smart contracts (with over 100 script functions)
- Smart contracts are snippets of code stored and executed by the network
- They can perform transactional based events if defined conditions are met

WHAT'S REALLY IN A TRANSACTION?



DECODING SCRIPT HEXES

- 80% of transactions are known as standard transactions

  OP_DUP OP_HASH160 <pubKeyHash>

  OP_EQUALVERIFY OP_CHECKSIG

- Approximately 1% of transactions contain OP_Returns

  OP_RETURN <hexedData>

- There are even a few hidden puzzles on the blockchain…

  OP_HASH256

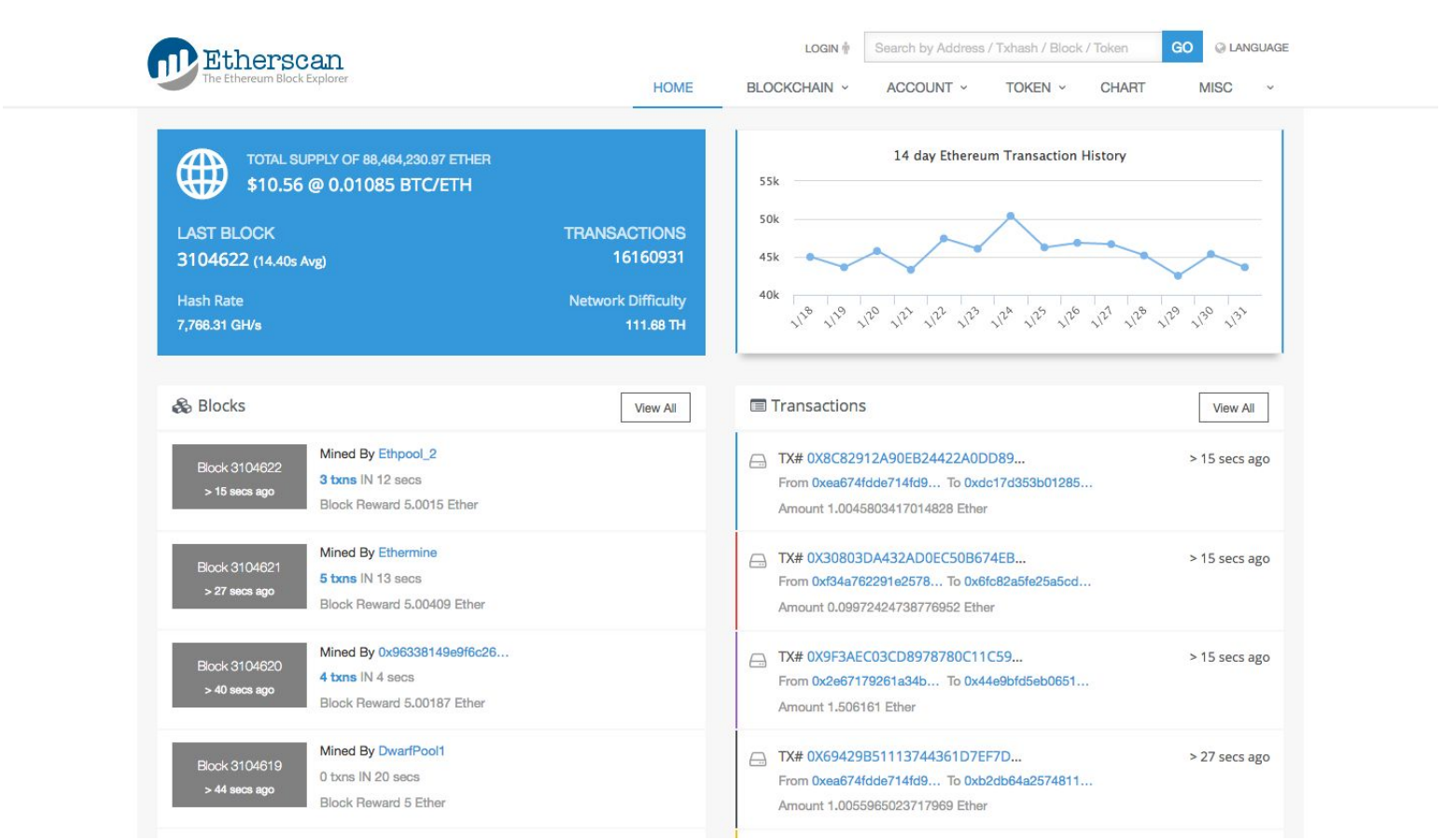
  6fe28c0ab6f1b372c1a6a246ae63f74f931e8365e15a089c68d6190000000000

  OP_EQUAL

ETHEREUM TAKES THINGS ONE STEP FURTHER

```
contract MyToken {

    string public standard = 'Token 0.1';
    string public name;
    string public symbol;
    uint8 public decimals;
    uint256 public totalSupply;

    function MyToken( … )
    function transfer( … )
    function approveAndCall( … )
    function transferFrom( … )

}
```

LET'S EXPLORE



neuroware

THANK YOU FOR YOUR TIME

please email us for more information - founders@neuroware.io