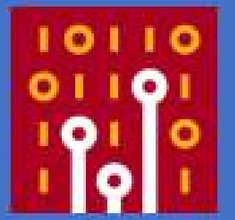
SharkFest '18 US



Traffic Analysis of Cryptocurrency and Blockchain Networks

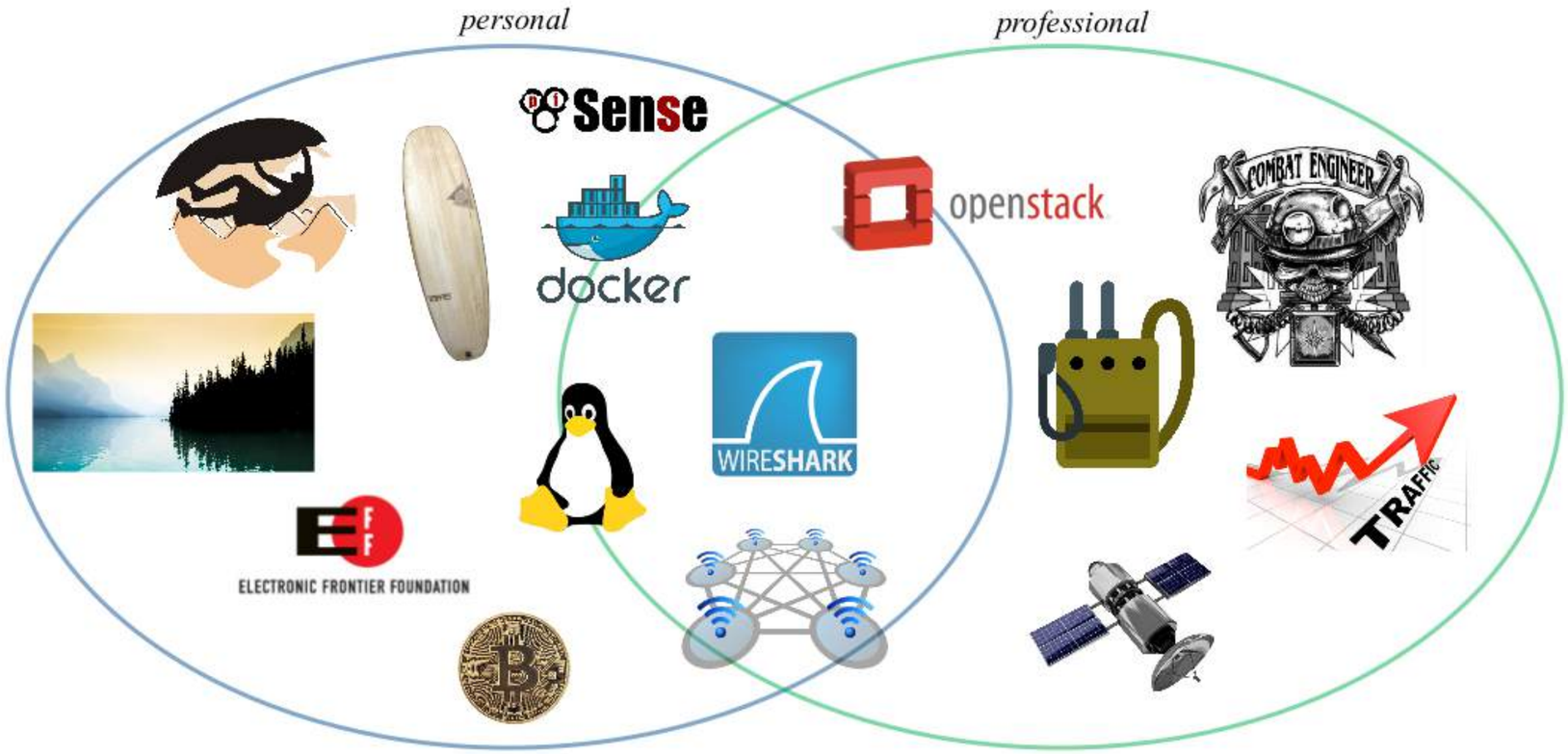
Brian Greunke
OpenOne Labs

&

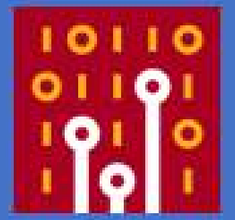
Brad Palm
BruteForce

#sf18us • Computer History Museum, Mountain View, CA • June 25-28

INTRODUCTION

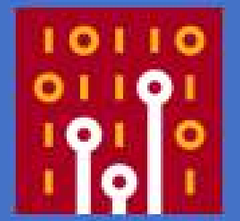


BUILDING IS FUN!

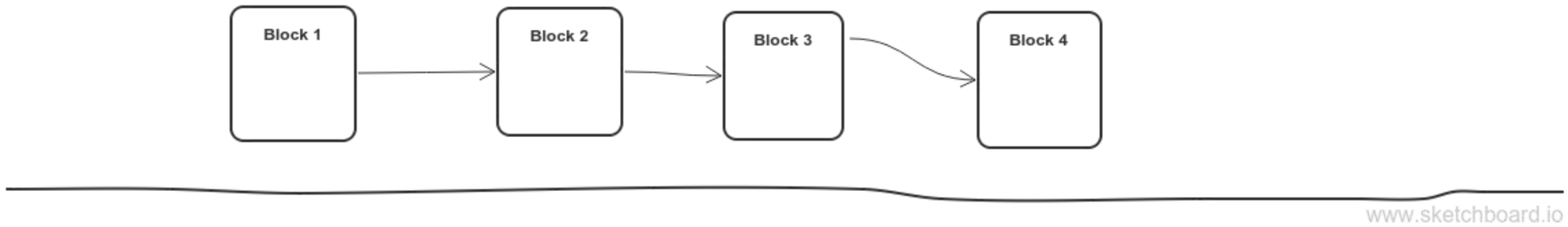


OUTLINE

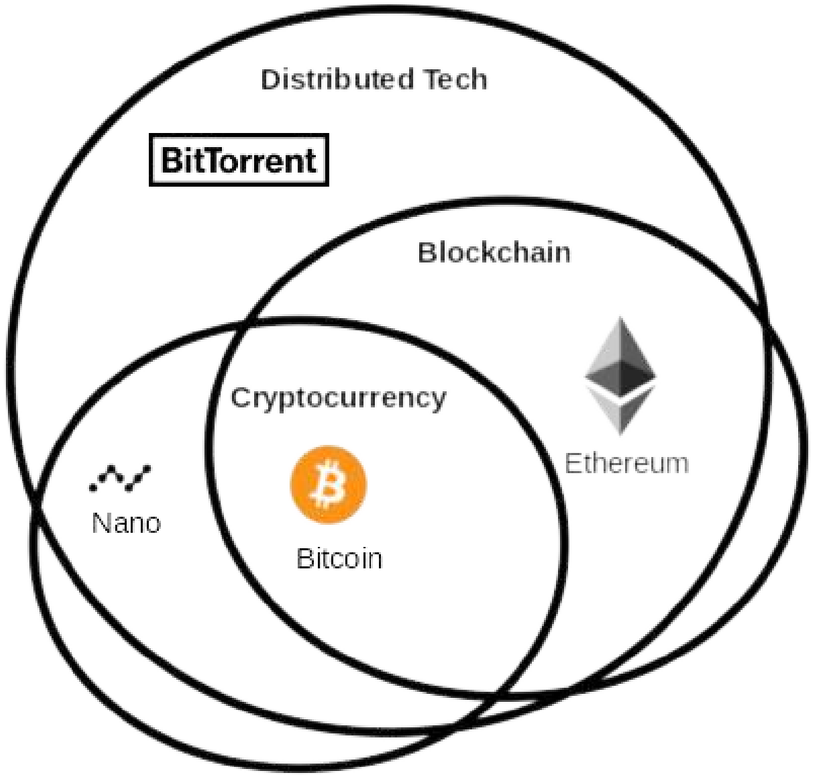
1. Block what? What chain? What what?
2. Traffic types and analysis
3. What is on your networks?

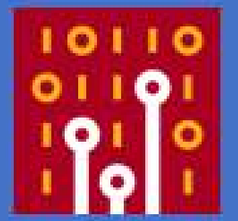


WHAT IS A BLOCKCHAIN?

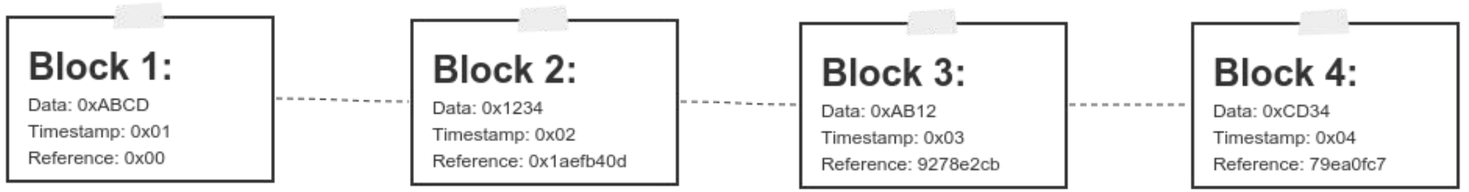


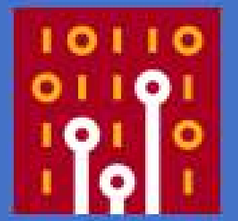
SEMANTICS


Distributed Tech
BitTorrent
Blockchain
Cryptocurrency
Ethereum
Nano
Bitcoin



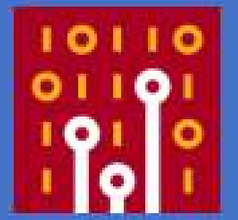
BLOCKCHAIN (HIGH LEVEL)





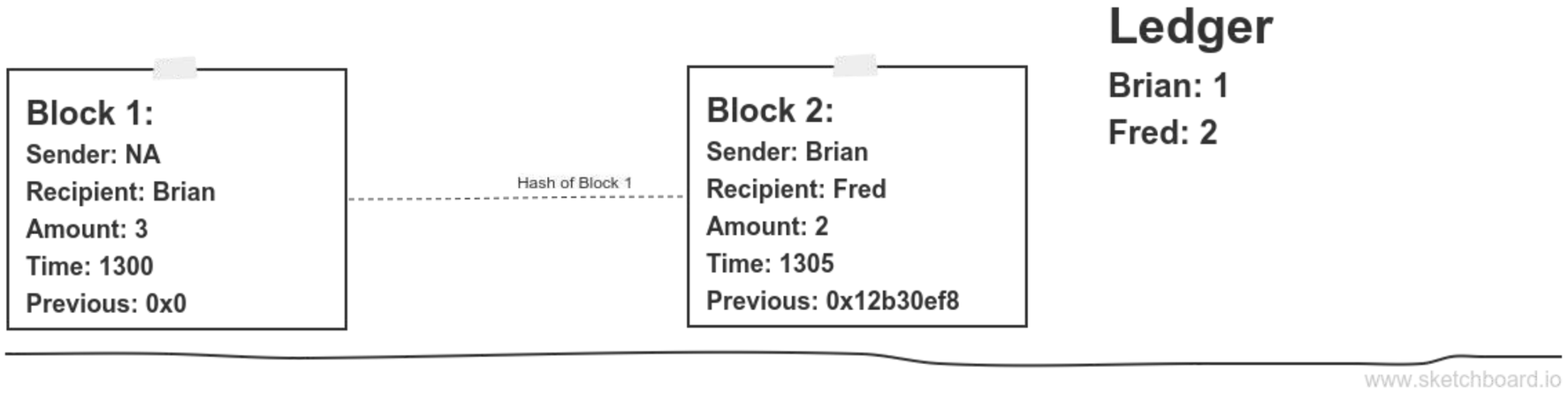
PROOF OF WORK

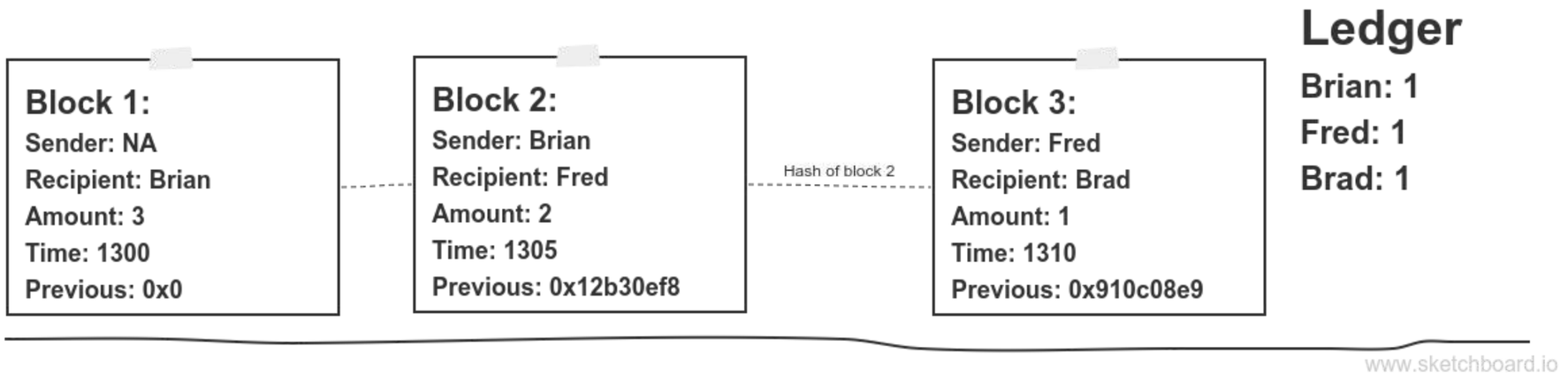
```
do while not hash_found:
  hash = sha256(block_info, nonce)
  if hash[0:2] == 00:
    hash_found

  nonce += 1
```

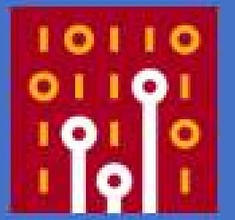


EXAMPLE

Block 1:
Sender: NA
Recipient: Brian
Amount: 3
Time: 1300
Previous: 0x0

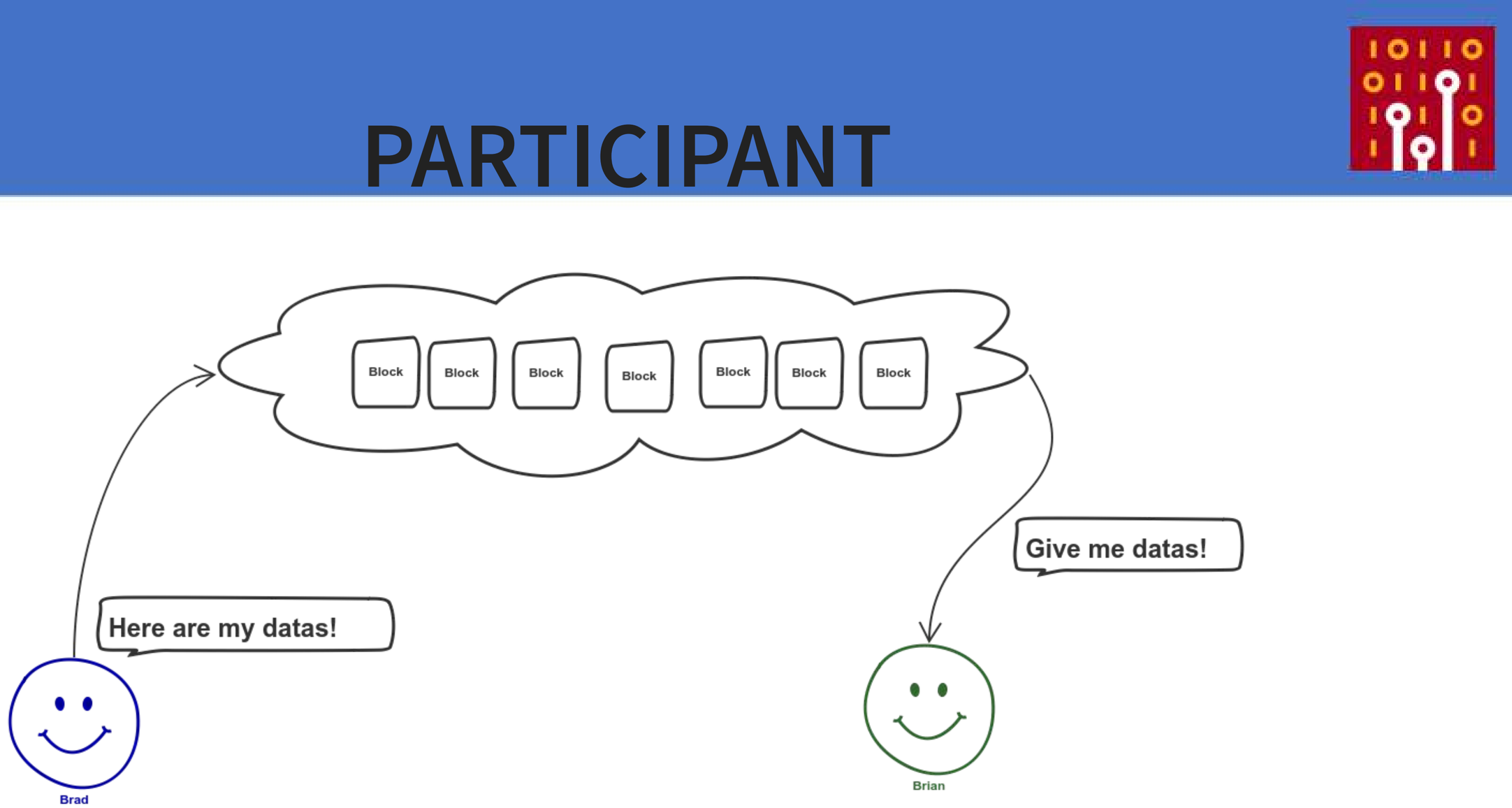

Block 1:
Sender: NA
Recipient: Brian
Amount: 3
Time: 1300
Previous: 0x0
Hash of Block 1
Block 2:
Sender: Brian
Recipient: Fred
Amount: 2
Time: 1305
Previous: 0x12b30ef8
Ledger
Brian: 1
Fred: 2
www.sketchboard.io


Block 1:
Sender: NA
Recipient: Brian
Amount: 3
Time: 1300
Previous: 0x0
Block 2:
Sender: Brian
Recipient: Fred
Amount: 2
Time: 1305
Previous: 0x12b30ef8
Hash of block 2
Block 3:
Sender: Fred
Recipient: Brad
Amount: 1
Time: 1310
Previous: 0x910c08e9
Ledger
Brian: 1
Fred: 1
Brad: 1
www.sketchboard.io



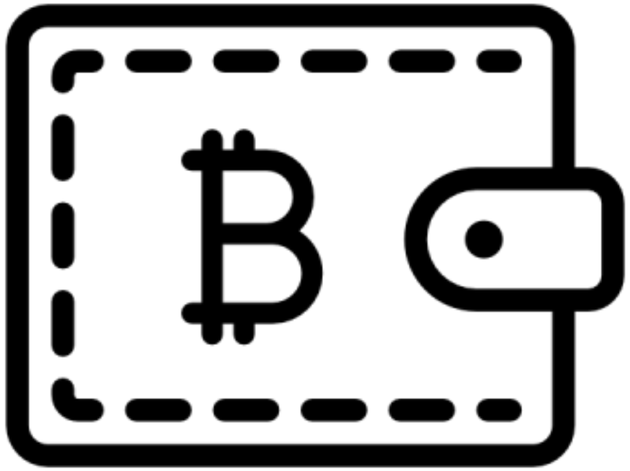
ROLES

- Participant
- Wallet
- Node
- Miner
- Pool


PARTICIPANT
Block
Block
Block
Block
Block
Block
Block
Give me datas!
Here are my datas!
Brad
Brian
www.sketchboard.io

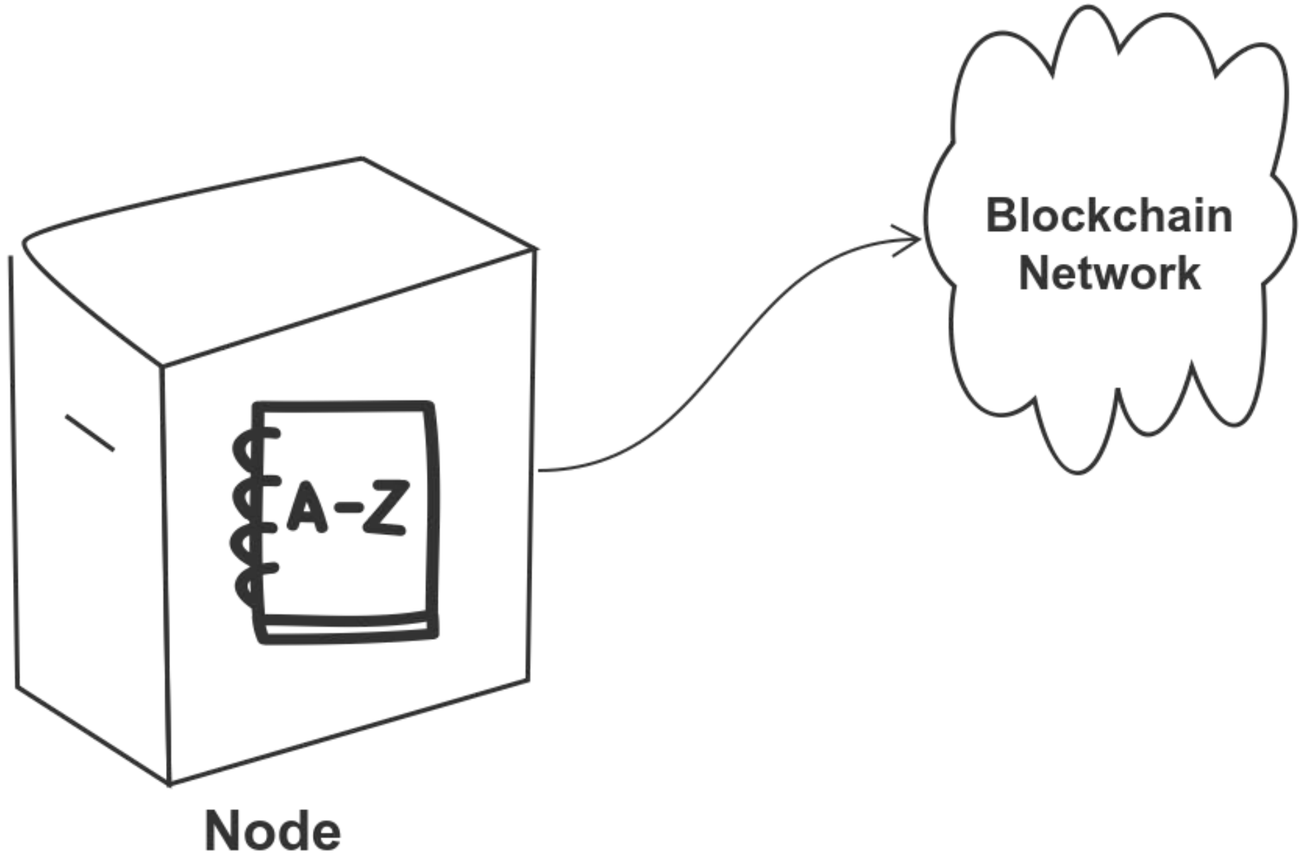
WALLET

Public Address:
13T4njyjqudTxut4U1J8rpaXJMxRK4BT6U



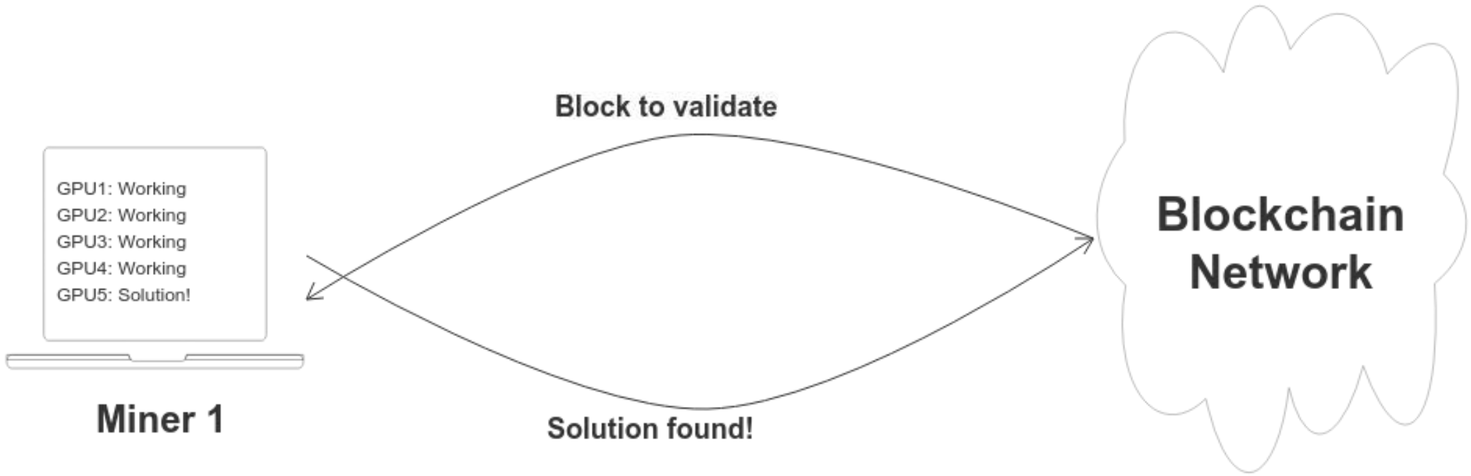
Private Address:
KyG4KsChWhfc5nHj1rSo3w5De7bUE1JQTxY6TbPNPvwxsdYw2K3L

NODE



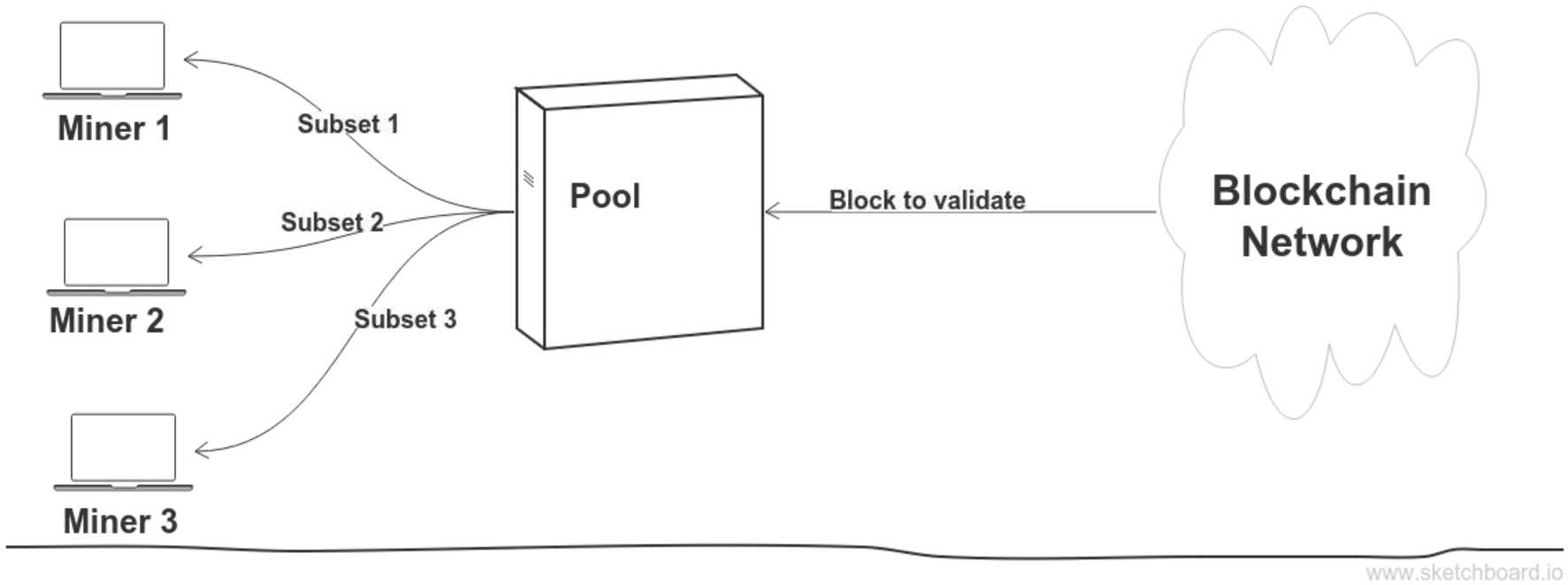
www.sketchboard.io

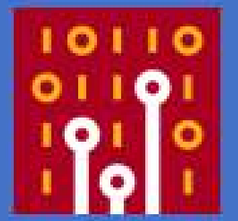
MINER



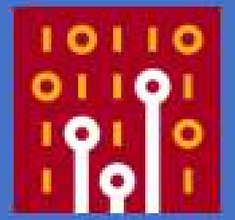
www.sketchboard.io

POOL


Miner 1
Miner 2
Miner 3
Subset 1
Subset 2
Subset 3
Pool
Block to validate
Blockchain Network
www.sketchboard.io



PROCESS

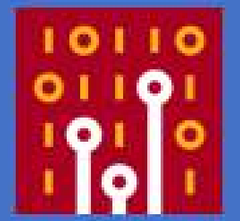


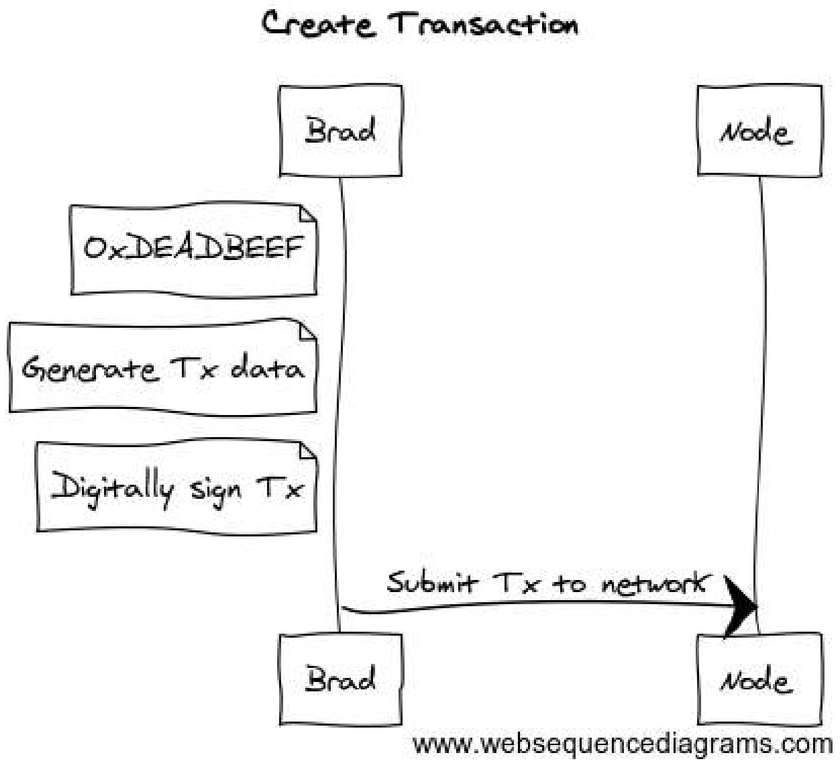
Brad wants to conduct a transaction with **Brian**

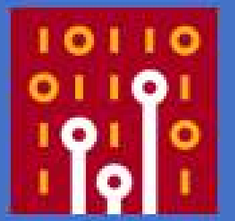
Ledger:

- Brad (0xCAFEBABE): 5
- Brian (0xDEADBEEF): 1

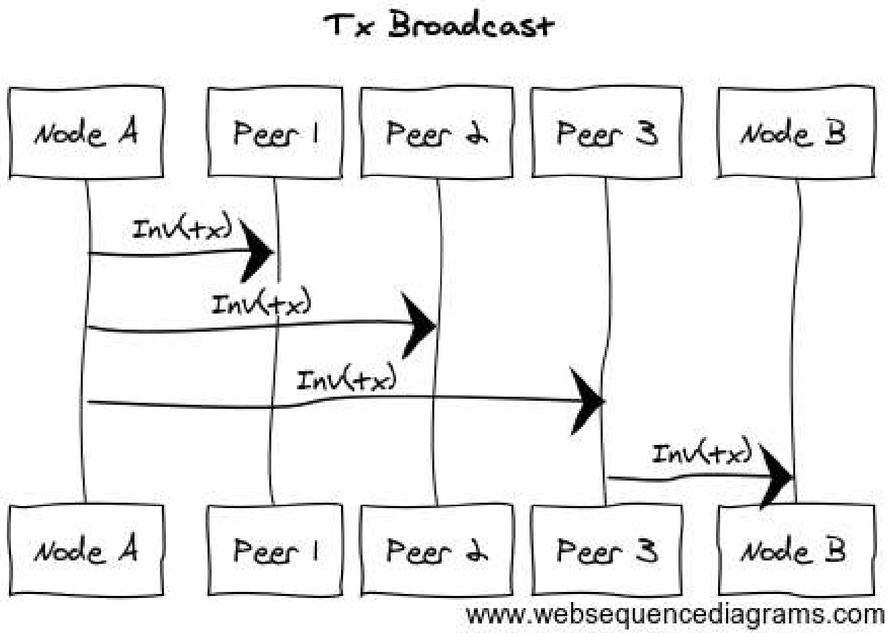
Brad creates a tx

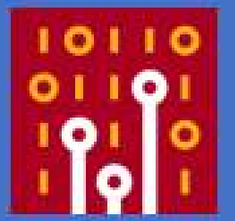




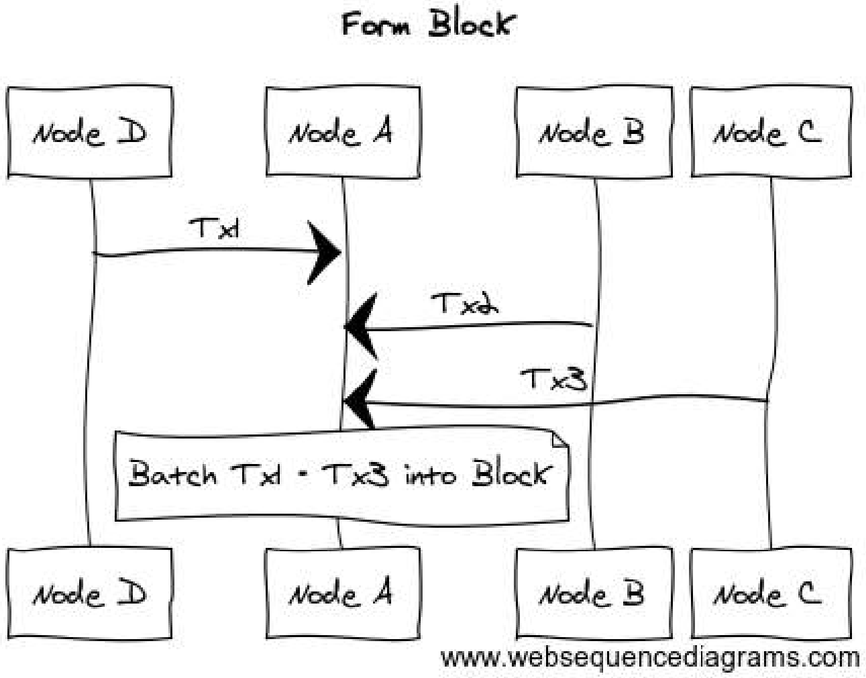


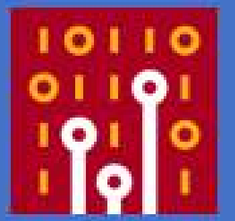
Transaction is broadcast to all **nodes** in the network





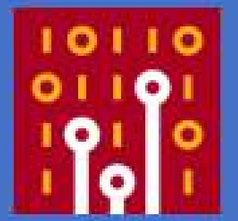
Multiple transactions form a **block**





Network determines how *hard* it is to validate (difficulty)

```
function calc_difficulty:
  tx_per_sec = num_tx / time_since_last_block
  hashrate = num_miners * avg_hashrate

  if hashrate / tx_per_sec > 10:
    increase_difficulty

  else
    decrease_difficulty
```



Miners (nodes) calculate a nonce to validate a block.

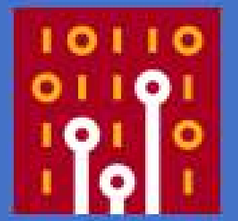
```
block = (all_txs_since_last_block,
         prev_block_hash,
         timestamp)
nonce = 0

do while not hash_found:
  hash = sha256(block, nonce)
  if hash < difficulty:
    hash_found

  nonce += 1
```

The miner is rewarded and ledger updated.

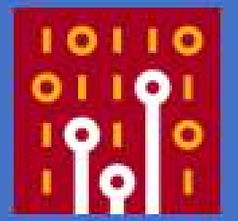
```
if nonce_is_valid:
  coinbase = new Coinbase
  miner_balance += coinbase

  sender_balance -= amount
  recipient_balance += amount
```

Ledger:

- Brad: 4
- Brian: 2
- Miner: 1



MISCONCEPTIONS

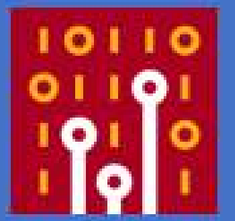


NOT INHERENTLY ANONYMOUS

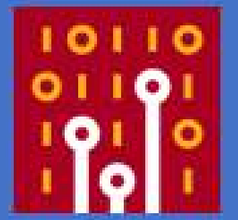
ANDY GREENBERG SECURITY 01.29.15 01:55 PM

PROSECUTORS TRACE $13.4M IN BITCOINS FROM THE SILK ROAD TO ULBRICHT'S LAPTOP

NOT INHERENTLY PRIVATE

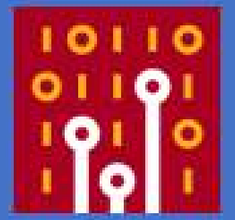


NOT INHERENTLY SECURE



TRAFFIC TYPES

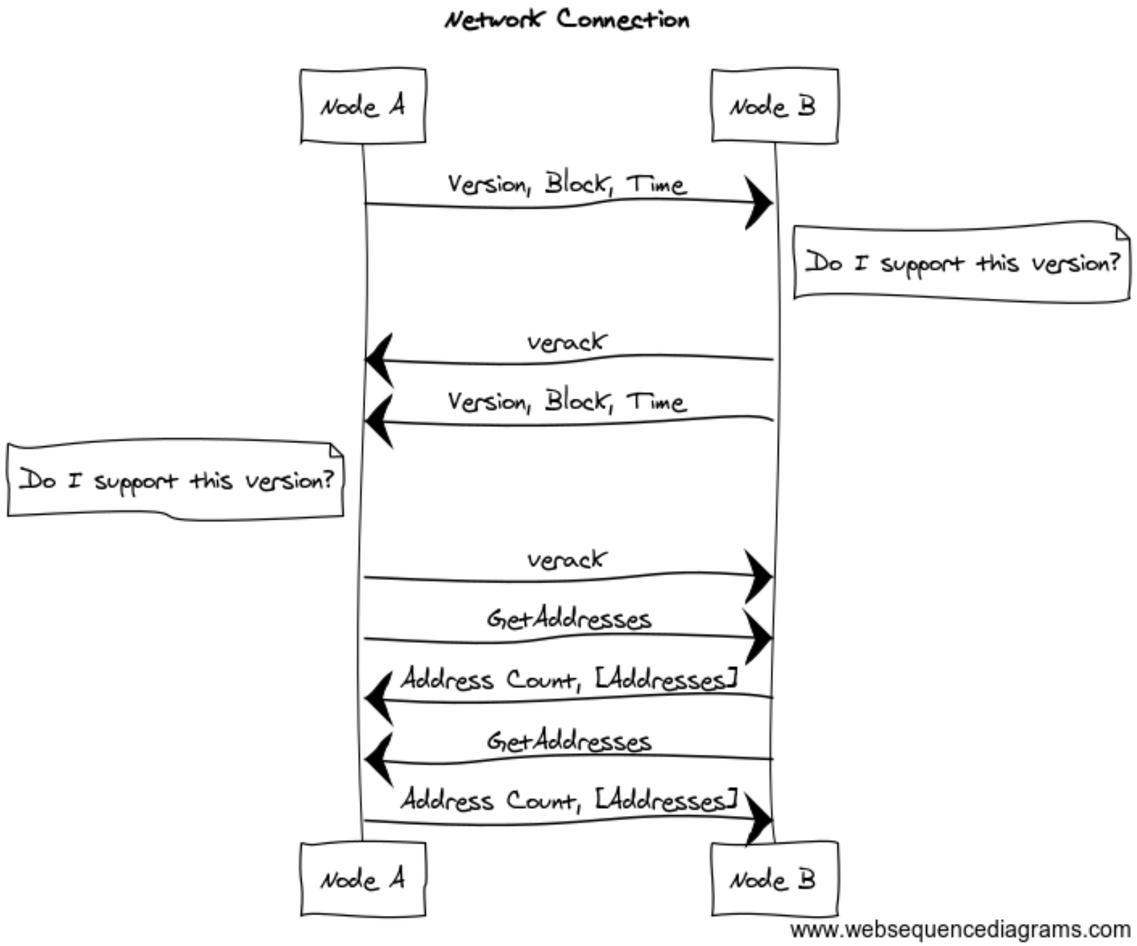
- P2P
- API
- Mining



P2P

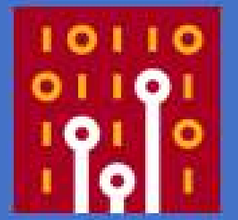
- Connect
- Initial Block Download
- Relay

CONNECT


Network Connection
Node A
Node B
Version, Block, Time
Do I support this version?
verack
Version, Block, Time
Do I support this version?
verack
GetAddresses
Address Count, [Addresses]
GetAddresses
Address Count, [Addresses]
Node A
Node B
www.websequencediagrams.com

VERSION MESSAGE

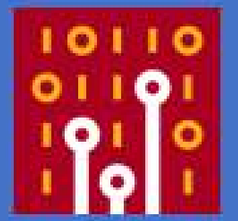
```
▾ Version message
    Protocol version: 70015
  ▾ Node services: 0x000000000000040d
      .... .... .... .... .... .... .... ...1 = Network node: Set
    Node timestamp: Jun 24, 2018 14:36:26.000000000 PDT
  ▾ Address as receiving node
    ▸ Node services: 0x0000000000000009
      Node address: ::ffff:67.169.94.193
      Node port: 8333
  ▾ Address of emmitting node
    ▸ Node services: 0x000000000000040d
      Node address: ::
      Node port: 0
    Random nonce: 0xcaab85c941ecd95f
  ▾ User agent
      Count: 16
      String value: /Satoshi:0.16.1/
    Block start height: 0
    Relay flag: 1
```



GET ADDRESS MESSAGE

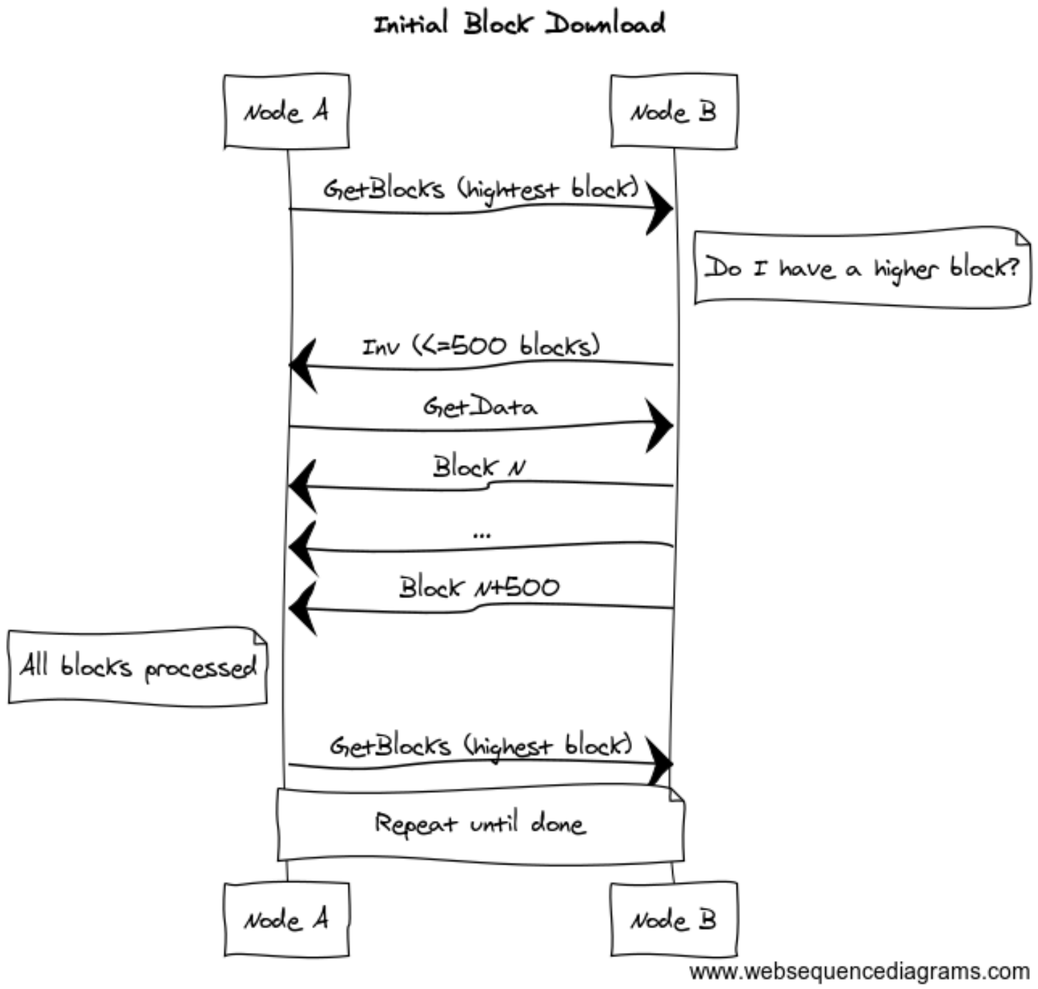
```
▾ Bitcoin protocol
    Packet magic: 0xf9beb4d9
    Command name: getaddr
    Payload Length: 0
    Payload checksum: 0x5df6e0e2
```

ADDRESS MESSAGE

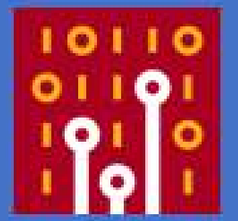


```
▾ Bitcoin protocol
    Packet magic: 0xf9beb4d9
    Command name: addr
    Payload Length: 31
    Payload checksum: 0x01c7697d
  ▾ Address message
      Count: 1
    ▾ Address: d90e305b0d040000000000002601064580033d7000000000...
      ▾ Node services: 0x000000000000040d
          .... .... .... .... .... .... .... ...1 = Network node: Set
        Node address: 2601:645:8003:3d70::bd9d
        Node port: 8333
        Address timestamp: Jun 24, 2018 14:36:25.000000000 PDT
```

INITIAL BLOCK DOWNLOAD (SYNC)

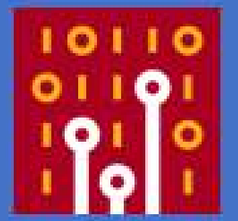


INVENTORY VECTOR MESSAGE



(Here's what I have)

```
▾ Bitcoin protocol
    Packet magic: 0xf9beb4d9
    Command name: inv
    Payload Length: 73
    Payload checksum: 0xb2009f0b
  ▾ Inventory message
      Count: 2
    ▾ Inventory vector
        Type: MSG_TX (1)
        Data hash: 805503b08790b17ea701fa5fa878793658ffadab0a53de84...
    ▾ Inventory vector
        Type: MSG_TX (1)
        Data hash: 9d0d039b1fbd495889899104ea3d78b27d3f6cc85f0b443c...
```

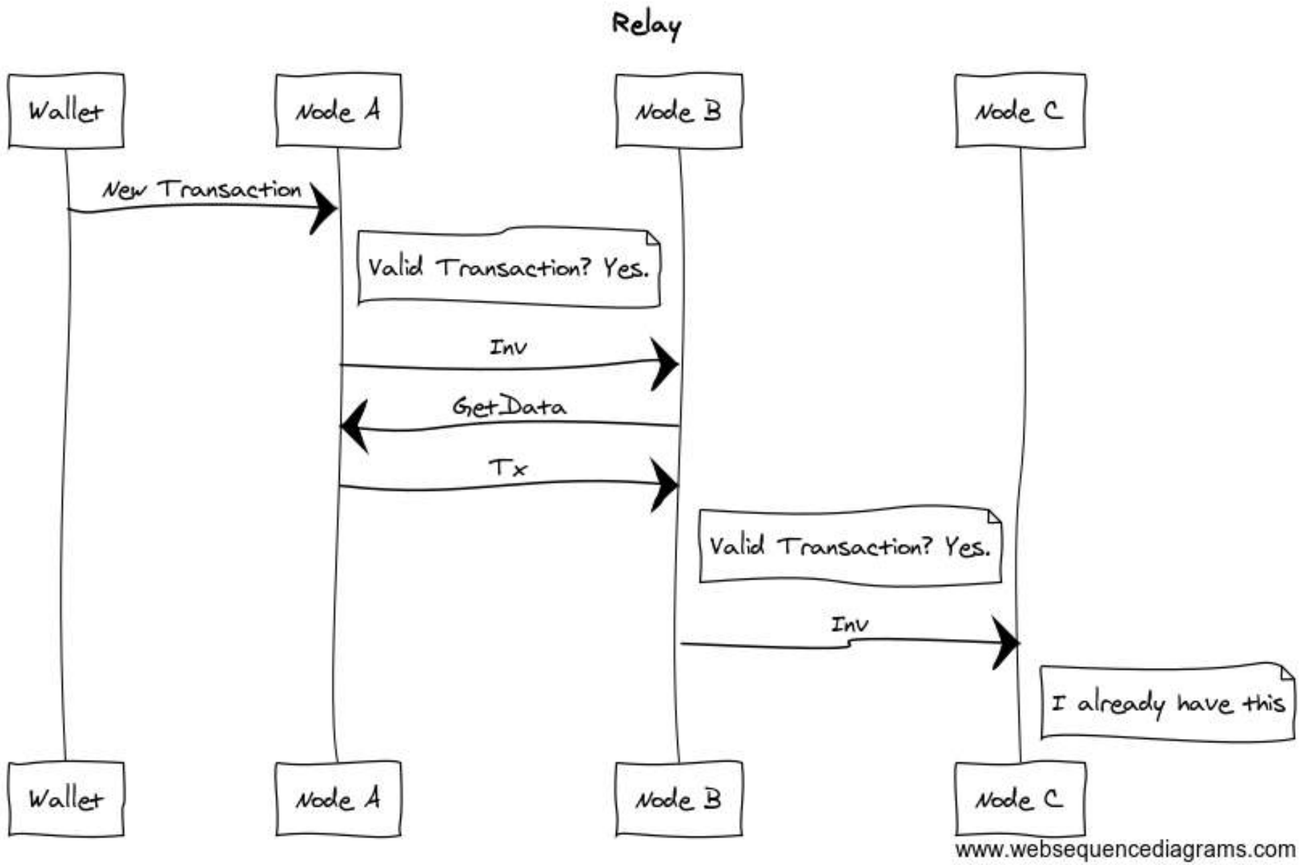


GET HEADERS

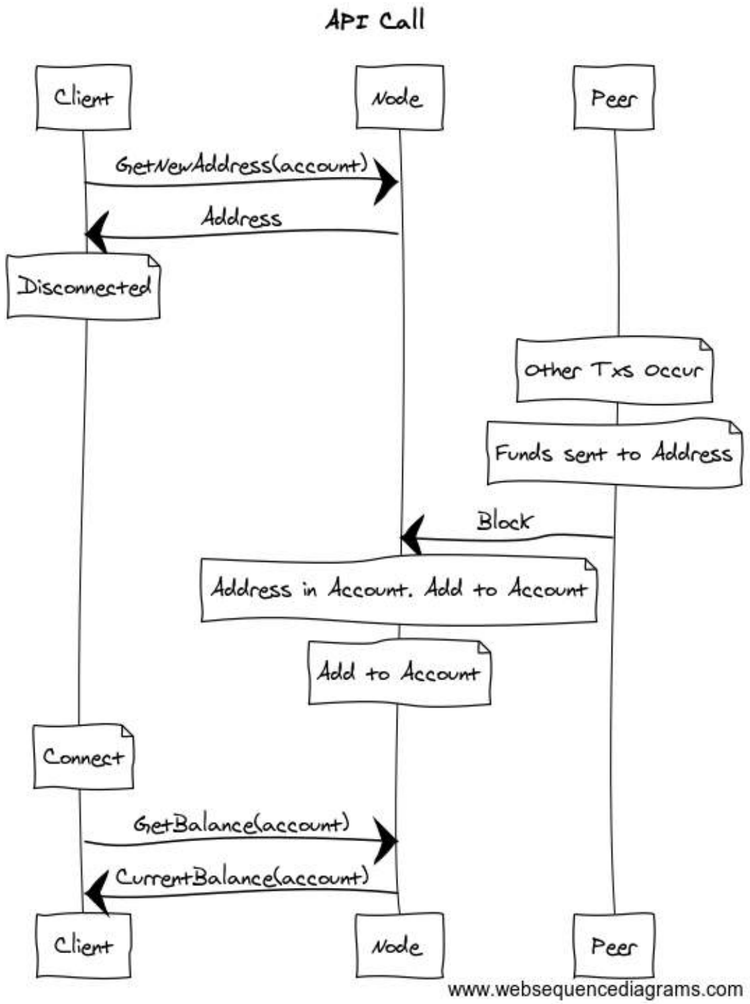
(Update me)

```
▾ Bitcoin protocol
    Packet magic: 0xf9beb4d9
    Command name: getheaders
    Payload Length: 69
    Payload checksum: 0x84f4958d
  ▾ Getheaders message
      Block version: 70015
      Count: 1
      Starting hash: 6fe28c0ab6f1b372c1a6a246ae63f74f931e8365e15a089c...
      Stopping hash: 0000000000000000000000000000000000000000000000000...
```

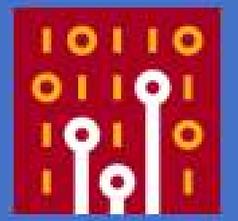
RELAY


Relay
Wallet
Node A
Node B
Node C
New Transaction
Valid Transaction? Yes.
Inv
GetData
Tx
Valid Transaction? Yes.
Inv
I already have this
Wallet
Node A
Node B
Node C
www.websequencediagrams.com

API

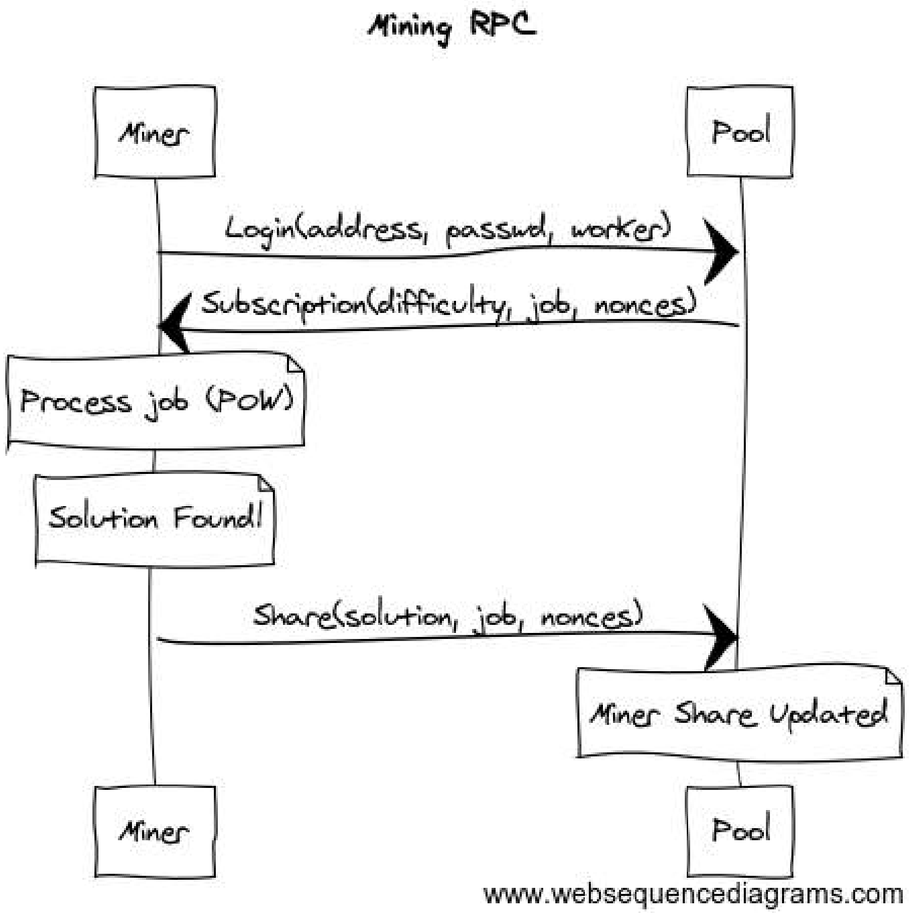

API Call
Client
Node
Peer
GetNewAddress(account)
Address
Disconnected
Other Txs occur
Funds sent to Address
Block
Address in Account. Add to Account
Add to Account
Connect
GetBalance(account)
CurrentBalance(account)
Client
Node
Peer
www.websequencediagrams.com

API CAPTURE

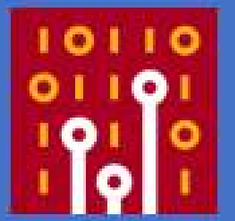


```
POST / HTTP/1.1
Host: 127.0.0.1
Connection: close
Authorization: Basic X19jb29raWVfXzo2OWE5OGQxMWU1YTMyMzg4MjNiM
Content-Length: 61

{"method":"getnewaddress","params":["sharkfest2018"],"id":1}
HTTP/1.1 200 OK
Content-Type: application/json
Date: Mon, 25 Jun 2018 04:21:12 GMT
Content-Length: 68
Connection: close

{"result":"3KWrA6cuQK2CgEPqQFBTvBuMLMKCr8HqEx","error":null,"i
```

MINING

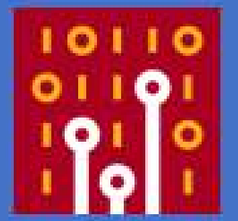

Mining RPC
Miner
Pool
Login(address, passwd, worker)
Subscription(difficulty, job, nonces)
Process job (POW)
Solution Found!
Share(solution, job, nonces)
Miner Share Updated
Miner
Pool
www.websequencediagrams.com

MINING CAPTURE




```
{"method":"login","params":
{"login":"47oXJPtiqdjc3Dm7U8HWRt5jaCfVn1vD1iWptGcj7oEvQDMm2mwi3REXFWPhe7YcTrjXuiu2fw61tbjduxgEt3c2
7UjGedC","pass":"x","rigid":"sharkfest2018","agent":"xmr-stak/2.4.5/b3f79de/master/lin/cpu/aeon-
cryptonight-monero/20"},"id":1}
{"id":1,"jsonrpc":"2.0","error":null,"result":{"id":"6daf6419-c290-4e28-a49d-b486ff610d96","job":
{"blob":"0707dc8eb0d9053835eef85a228e398876a095ccd1fca8541170f381ebf2c5bc147444682ab23e00000000f28
f1abe51e0298e696f2d37d5deafd4a4299f684a13ff60dc78aa373ba36ede02","job_id":"rFD94RL/61pxfdf8G1cmigj
wMUrX","target":"711b0d00","id":"6daf6419-c290-4e28-a49d-b486ff610d96"},"status":"OK"}}
{"method":"submit","params":{"id":"6daf6419-c290-4e28-a49d-
b486ff610d96","job_id":"rFD94RL/61pxfdf8G1cmigjwMUrX","nonce":"d3120000","result":"381dad5f4194b92
d386d262e798d4749bd1c812e1c71a2692a405c3650260300"},"id":1}
{"id":1,"jsonrpc":"2.0","error":null,"result":{"status":"OK"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"0707dc8eb0d9053835eef85a228e398876a095ccd1fca8541170f381ebf2c5bc147444682ab23e000000004db
f3706ea02c415daec09f1b79bade3214eaf4e99710b2055be2fab7b6d809702","job_id":"ZpDmTztAEu7xtXWa0Ol0QQB
DbFUo","target":"b6600b00","id":"6daf6419-c290-4e28-a49d-b486ff610d96"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"0707a88fb0d905d55f3ef40bdec0efd83b3d5b9233fb38ccf9b32cec95f18d471f330ab201b20500000000a8f
3b2dd2205d06b978b1c569795f9fe3c3d6e872b3ea2b99925b86cd50379e705","job_id":"yL6suvdS0R8pbmQ02dMBXxA
IRGEb","target":"b6600b00","id":"6daf6419-c290-4e28-a49d-b486ff610d96"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"0707a88fb0d905d55f3ef40bdec0efd83b3d5b9233fb38ccf9b32cec95f18d471f330ab201b205000000000dc
86e4bfabf4350d1855d972dd65f02fb31bd8007e28dc51148245999b7d5ad05","job_id":"hrGEvxG/+Tw18Z5vY6sJSfL
oK24t","target":"711b0d00","id":"6daf6419-c290-4e28-a49d-b486ff610d96"}}
```

INDICATORS



P2P

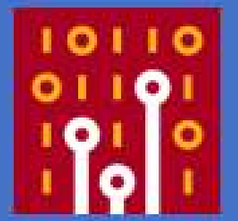
```
tcp.port == 18080
tcp.port == 8333
```

API

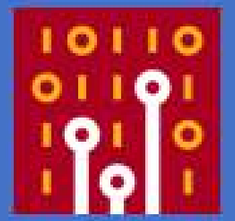
```
tcp.port == 18081
tcp.port == 8332
```

MINING

```
tcp.port==3333
frame matches "jsonrpc"
frame matches "xmr"
frame matches "pool"
dns.qry.name matches coinhive
```



WHAT IS ON YOUR NETWORK?



FOLLOW THE $$$

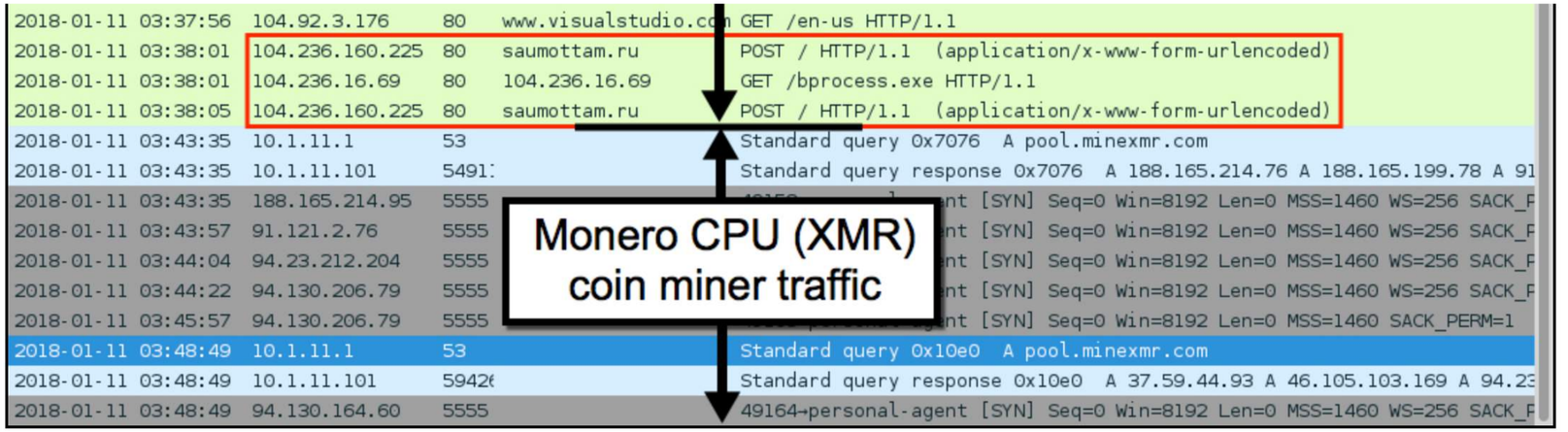
-In 2017 cryptocurrency market grew 20 fold - $18B to more than $600B (USD)

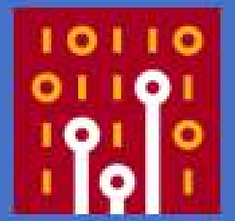
-Became lucrative to compromise systems and access computing resources to mine

-Impact of cryptocurrecy mining on a host is often viewed as more of a nuisance

CRYPTOJACKING

2018-01-11 - RIG EK SENDS SMOKE LOADER AND MONERO COIN MINER



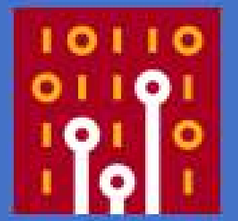


CRYPTOJACKING 2

Malware Delivery/Exploit method

The malware is delivered by way of a standard 1x1 iFRAME that will attempt to load the binary file, "Photo.SCR" upon visiting the website. The following is the iframe:

```
<iframe src=Photo.scr width=1 height=1 frameborder=0> </iframe>
```



CRYPTOJACKING 3

ADYLKUZZ CRYPTOCURRENCY MINING MALWARE SPREADING FOR WEEKS VIA ETERNALBLUE/DOUBLEPULSAR

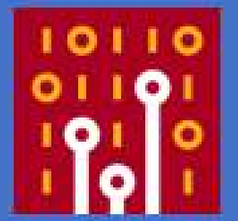
...shadow who?...

CRYPTOJACKING 4

ARTICLE / DEC 15, 2017

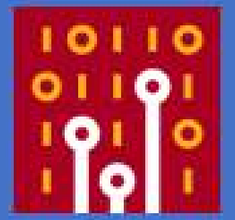
ZEALOT: NEW APACHE STRUTS CAMPAIGN USES ETERNALBLUE AND ETERNALSYNERGY TO MINE MONERO ON INTERNAL NETWORKS

BY MAXIM ZAVODCHIK, LIRON SEGAL



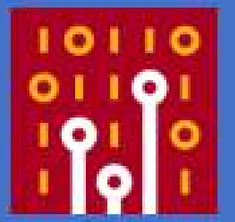
DRIVE BY MINING

```
<script src="https://authedmine.com/lib/authedmine.min.js">
</script>
<script>
    var miner = new CoinHive.Anonymous('YOUR_SITE_KEY',
                                       {throttle: 0.3});

    // Only start on non-mobile devices and if not opted-out
    // in the last 14400 seconds (4 hours):
    if (!miner.isMobile() && !miner.didOptOut(14400)) {
        miner.start();
    }
</script>
```



DRIVE BY MINING

```
DNS          94 Standard query response 0xdfa7 A ws007.coinhive.com A 37.187.165.207
DNS         106 Standard query response 0xfcb0 AAAA ws007.coinhive.com AAAA 2607:7700:0:13::25bb:a5cf
DNS          78 Standard query 0x2871 A ws007.coinhive.com
DNS          78 Standard query 0xda8a AAAA ws007.coinhive.com
DNS          94 Standard query response 0x2871 A ws007.coinhive.com A 37.187.165.207
DNS         106 Standard query response 0xda8a AAAA ws007.coinhive.com AAAA 2607:7700:0:13::25bb:a5cf
```



SOURCES

- http://www.righto.com/2014/02/bitcoin-mining-hard-way-algorithms.html
- https://en.bitcoin.it/wiki/Network
- https://en.bitcoin.it/wiki/Protocol_documentation
- https://slushpool.com/help/manual/stratum-protocol
- Bitcoin Logo: https://commons.wikimedia.org/w/index.php?curid=30202095
- Etereum Logo By Ethereum Foundation - https://camo.githubusercontent.com/1b3d0063d6a8bcd56ca07b0ea2ef0f71b17a0fa8/687474703a2f2f737667706f726e2e636f6
  CC BY 3.0, Link
- Wallet Icon made by Tomas Knop from www.flaticon.com is licensed by CC 3.0 BY