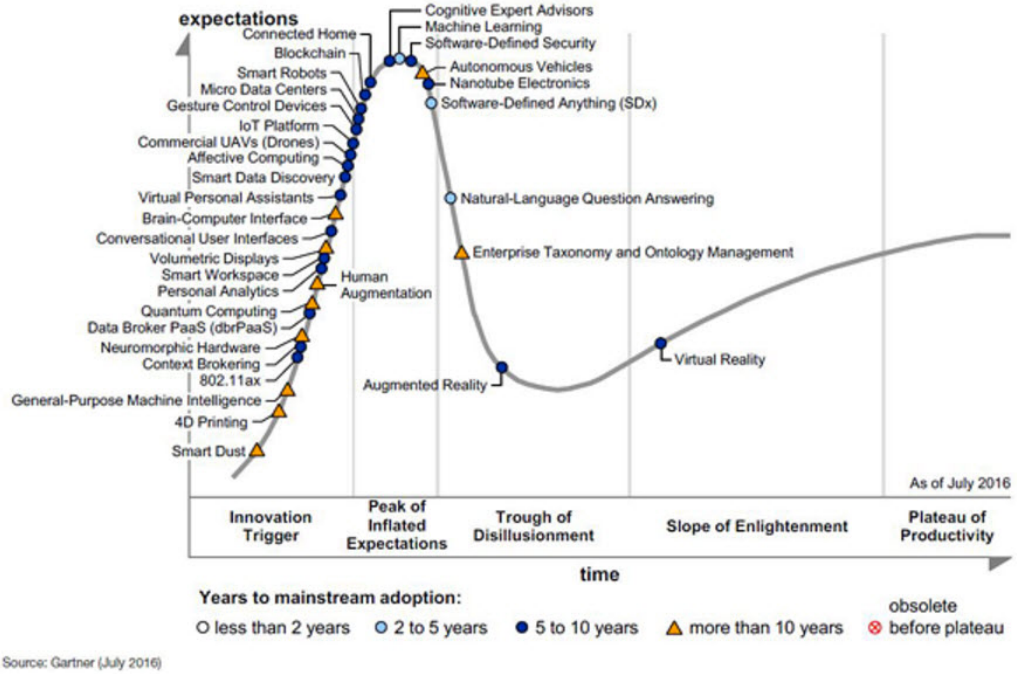
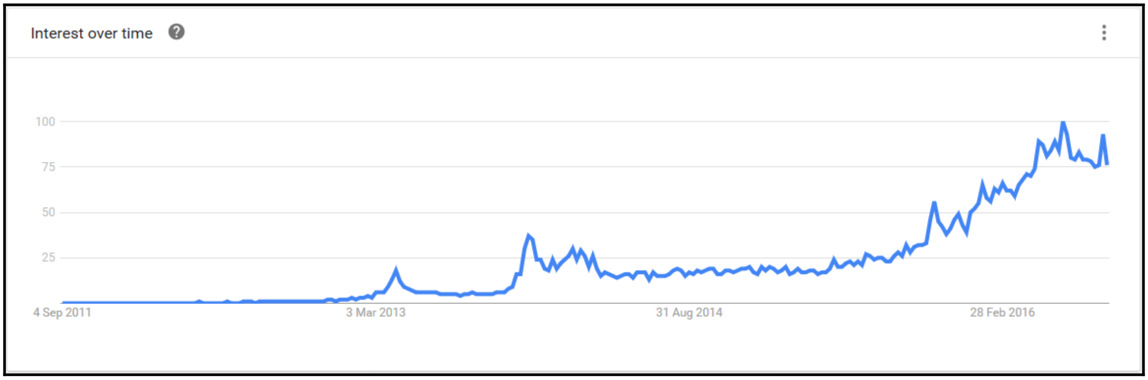
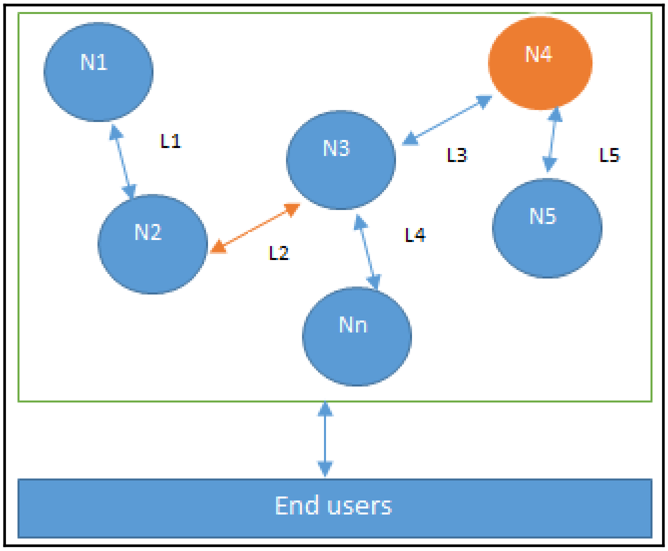
Chapter 1: Blockchain 101

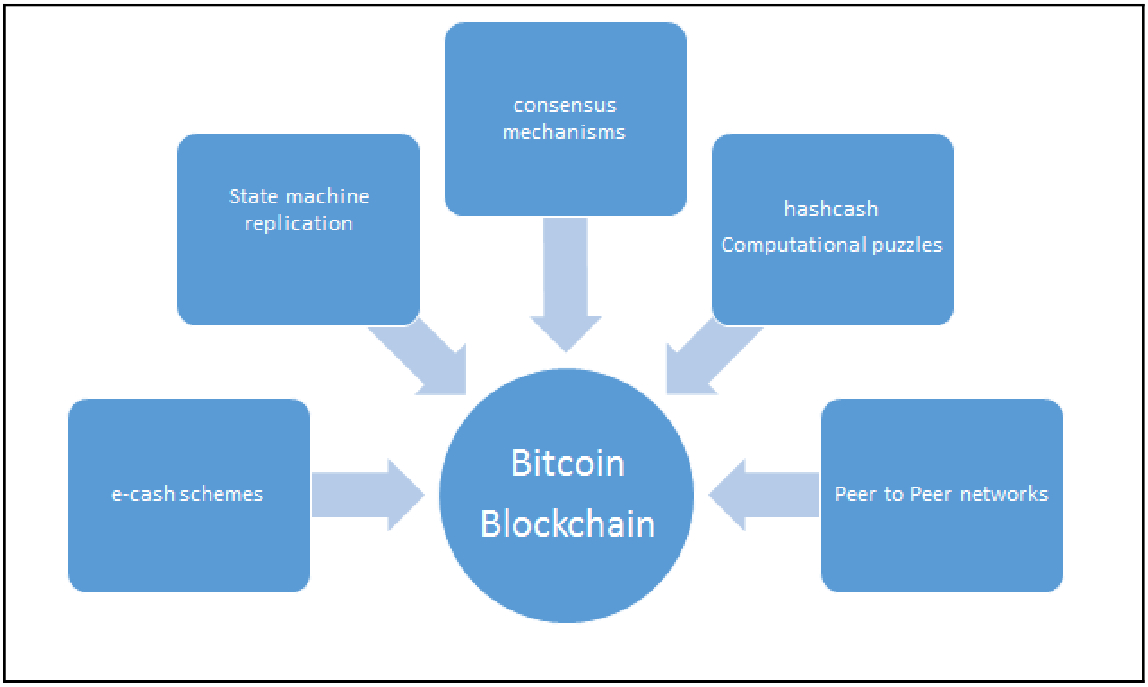
Figure 1. Hype Cycle for Emerging Technologies, 2016

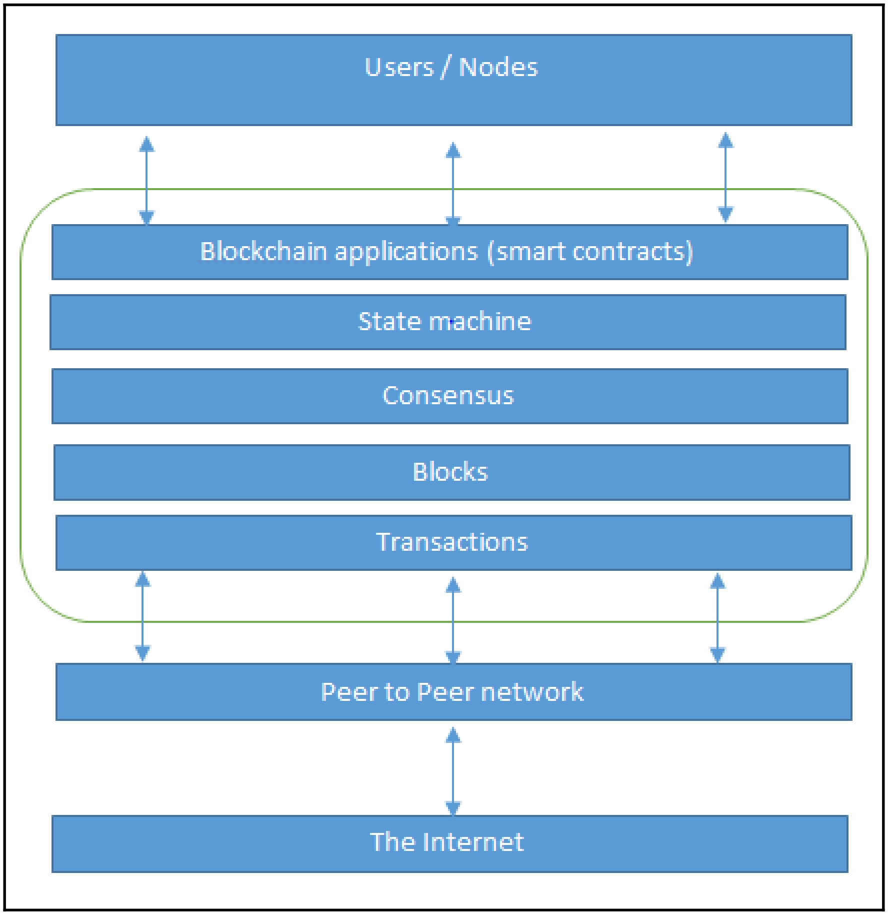


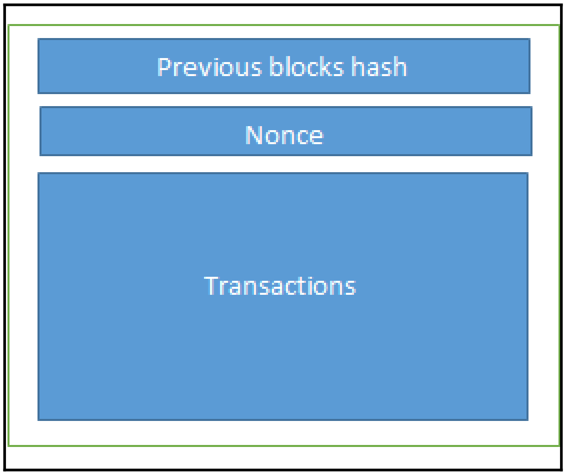
Source: Gartner (August 2016)

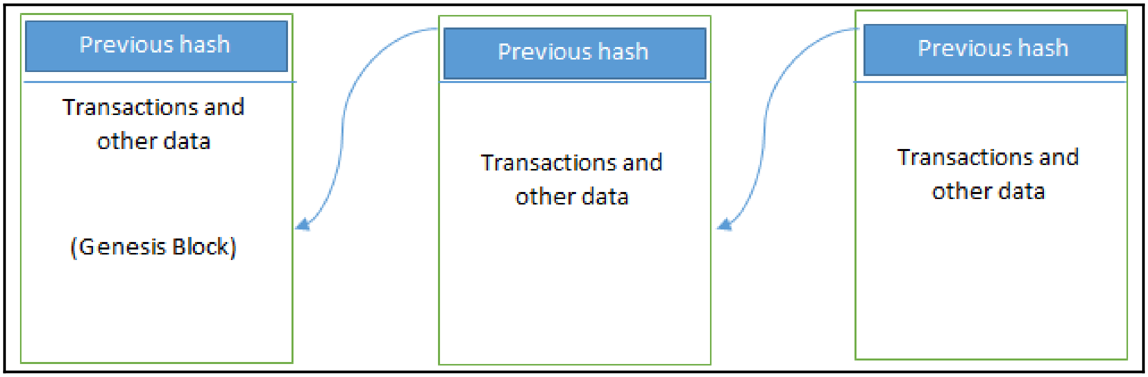

Interest over time
100
75
50
25
4 Sep 2011
3 Mar 2013
31 Aug 2014
28 Feb 2016


N1
N4
L1
N3
L3
L5
N2
N5
L4
L2
Nn
End users


consensus mechanisms
State machine replication
hashcash
Computational puzzles
e-cash schemes
Bitcoin
Blockchain
Peer to Peer networks

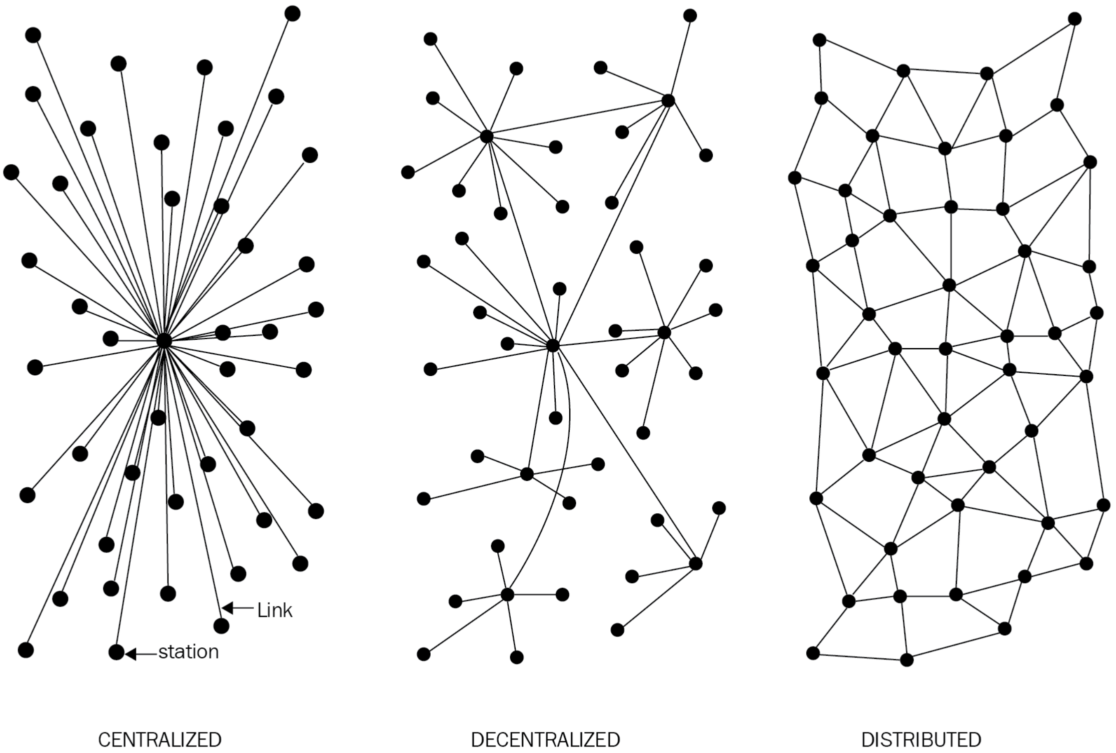

Users / Nodes
Blockchain applications (smart contracts)
State machine
Consensus
Blocks
Transactions
Peer to Peer network
The Internet

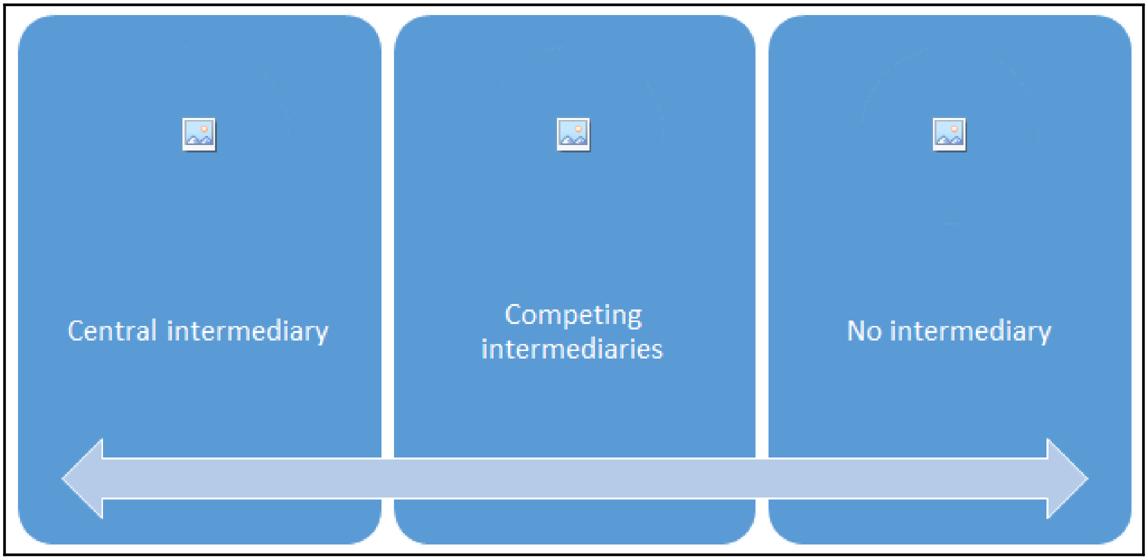

Previous blocks hash
Nonce
Transactions

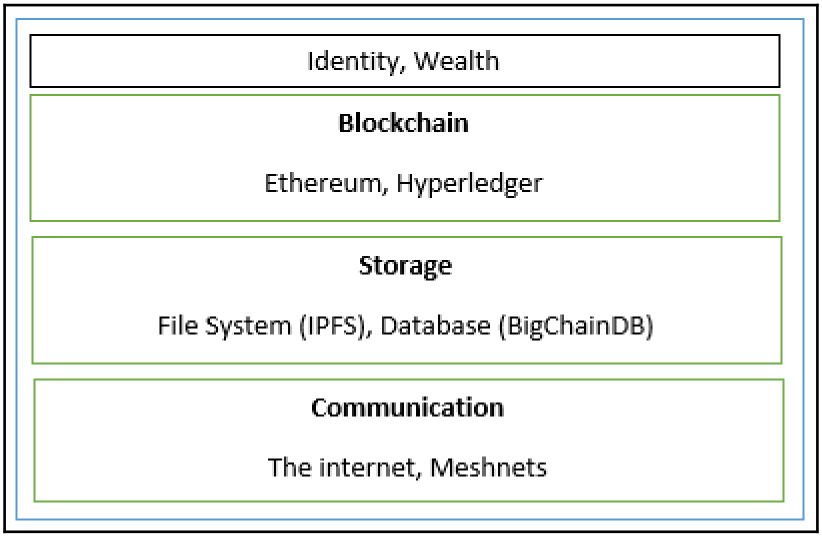

Previous hash
Transactions and other data
(Genesis Block)
Previous hash
Transactions and other data
Previous hash
Transactions and other data

Chapter 2: Decentralization

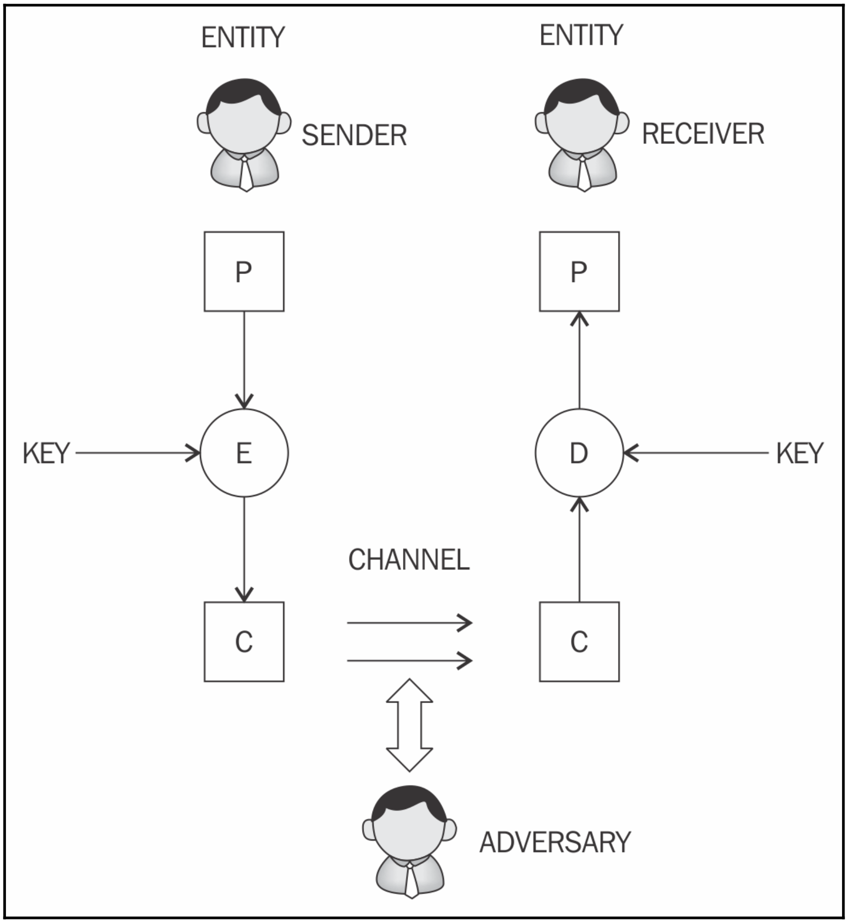
As appeared in paper by Paul Baran on distributed communication networks

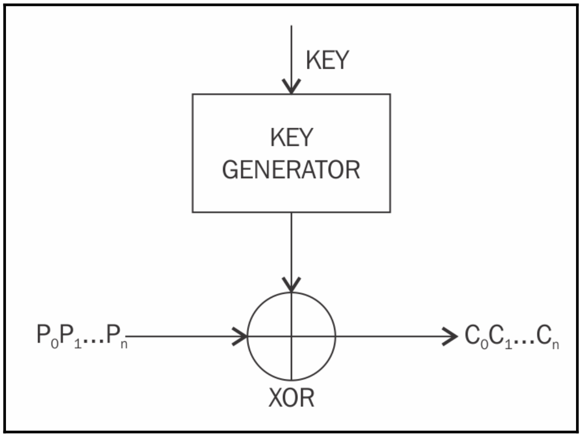


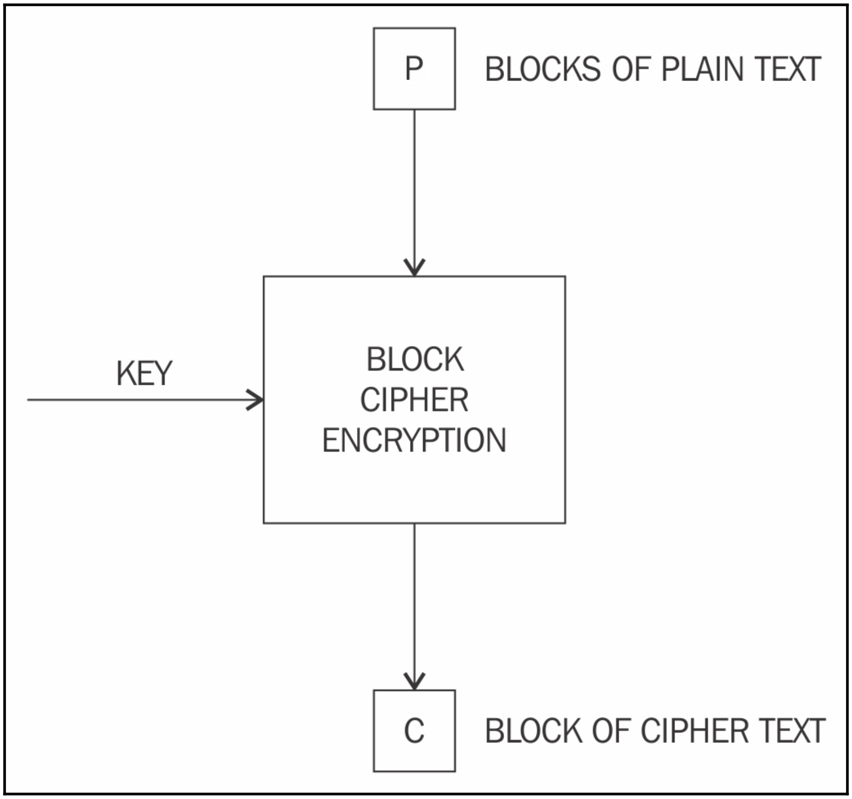

Central intermediary
Competing intermediaries
No intermediary

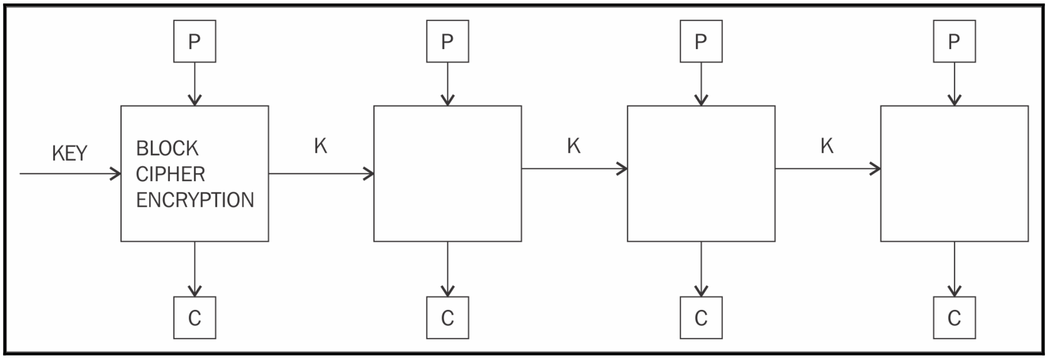

Identity, Wealth
Blockchain
Ethereum, Hyperledger
Storage
File System (IPFS), Database (BigChainDB)
Communication
The internet, Meshnets

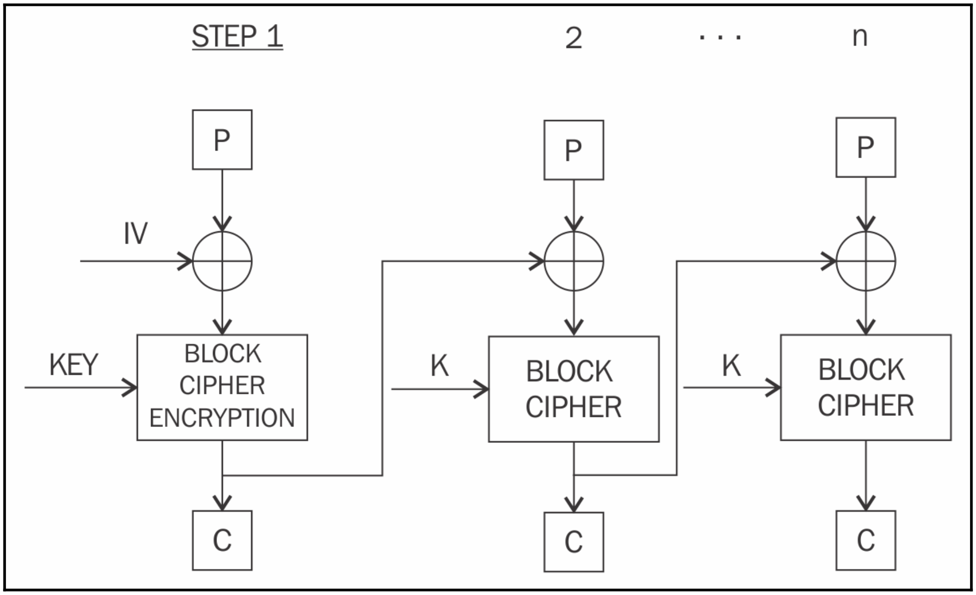
Chapter 3: Cryptography and technical foundations

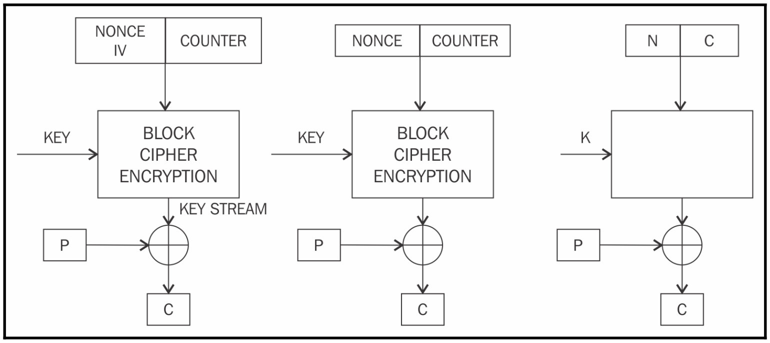


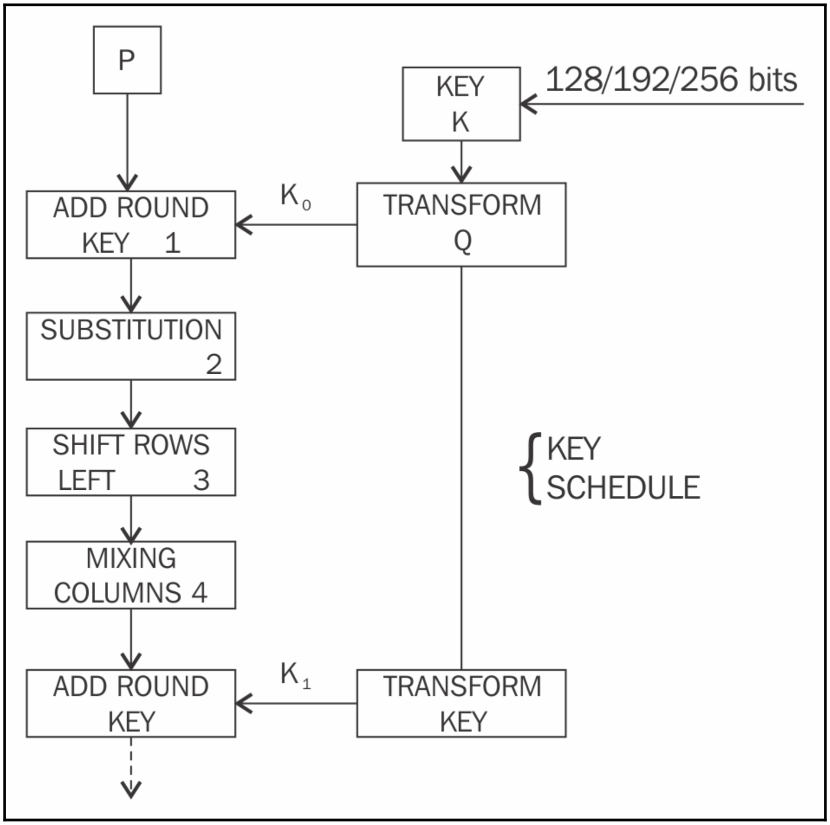

KEY
KEY GENERATOR
P0P1...Pn
C0C1...Cn
XOR

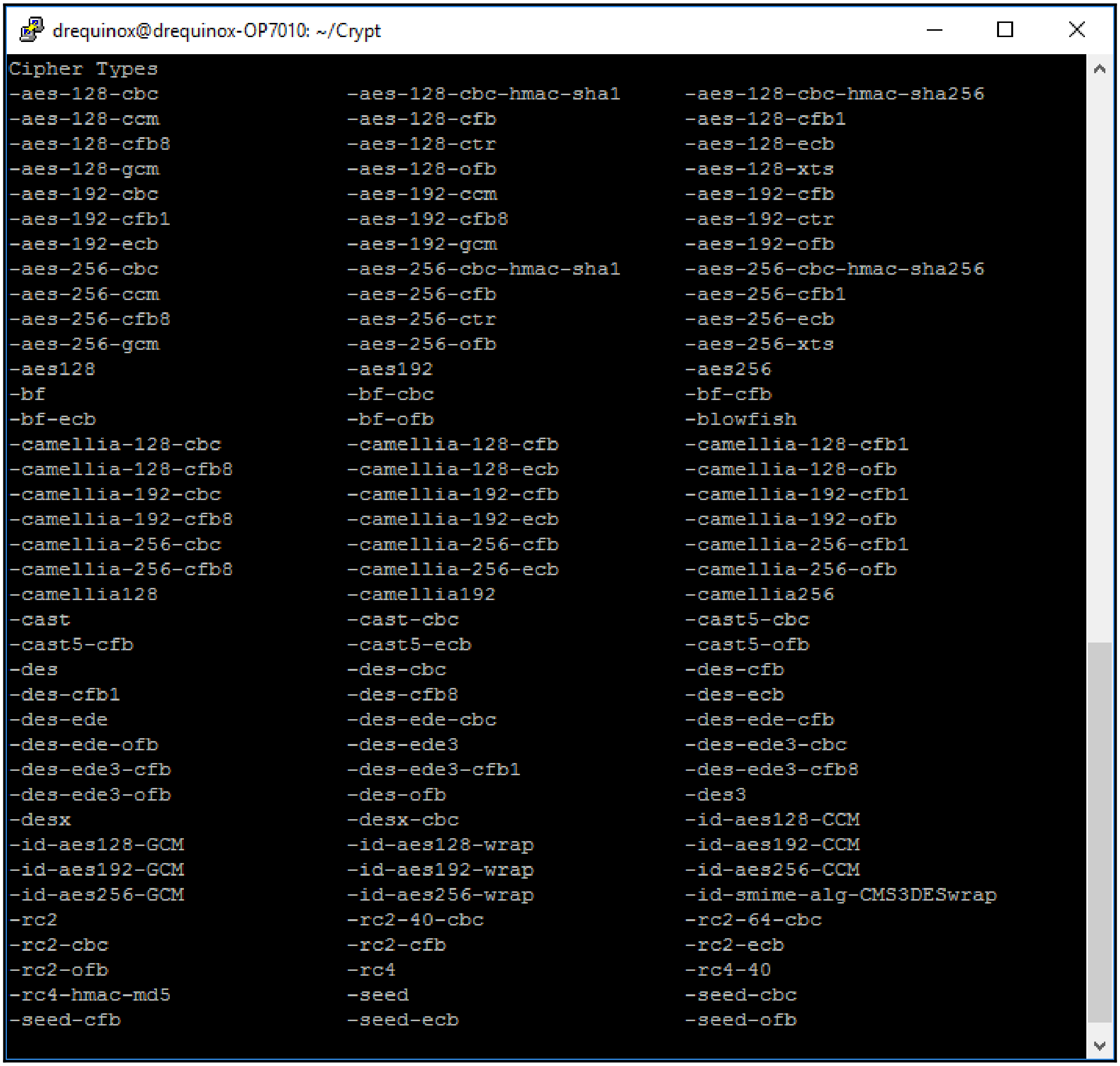

P
BLOCKS OF PLAIN TEXT
KEY
BLOCK CIPHER ENCRYPTION
C
BLOCK OF CIPHER TEXT


P
P
P
P
KEY
BLOCK
CIPHER
ENCRYPTION
K
K
K
C
C
C
C

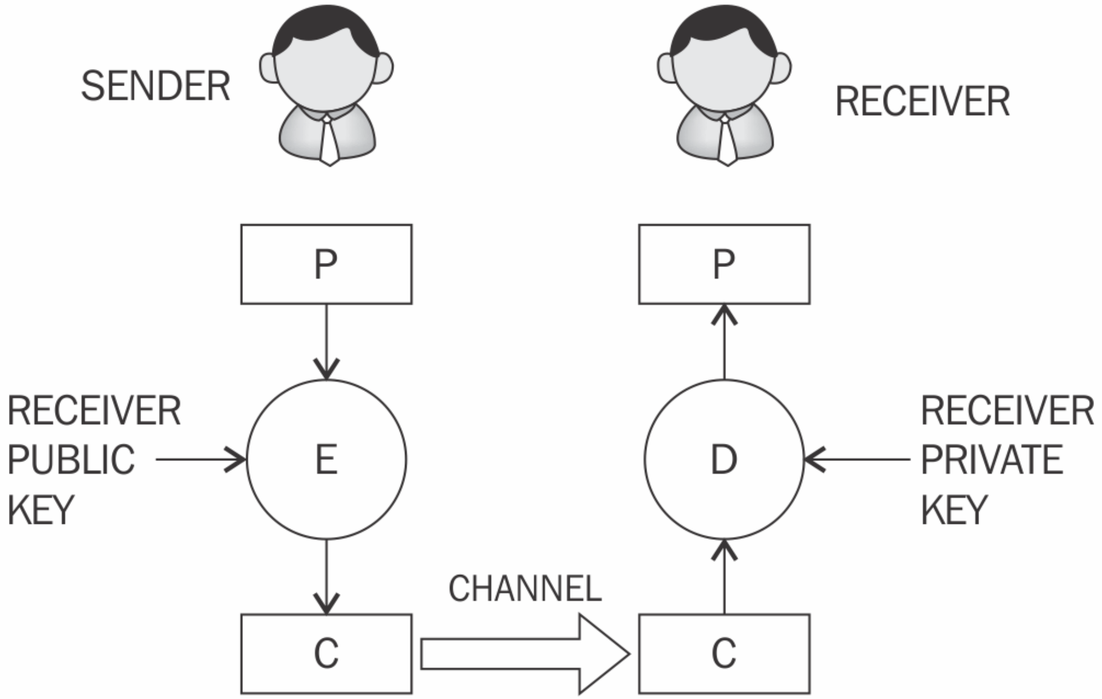

STEP 1
2
. . .
n
P
P
P
IV
KEY
BLOCK
CIPHER
ENCRYPTION
K
BLOCK
CIPHER
K
BLOCK
CIPHER
C
C
C


NONCE
IV
COUNTER
KEY
BLOCK
CIPHER
ENCRYPTION
KEY STREAM
P
C
NONCE
COUNTER
KEY
BLOCK
CIPHER
ENCRYPTION
P
C
N
C
K
P
C

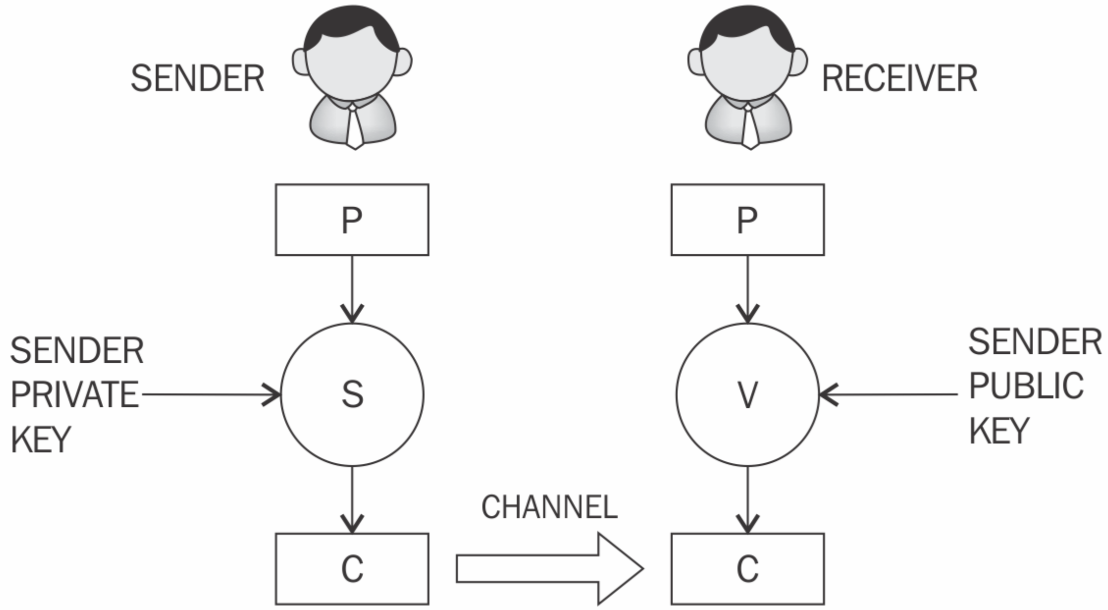

P
KEY
K
128/192/256 bits
ADD ROUND
KEY 1
K_0
TRANSFORM
Q
SUBSTITUTION
2
SHIFT ROWS
LEFT 3
KEY
SCHEDULE
MIXING
COLUMNS 4
ADD ROUND
KEY
K_1
TRANSFORM
KEY



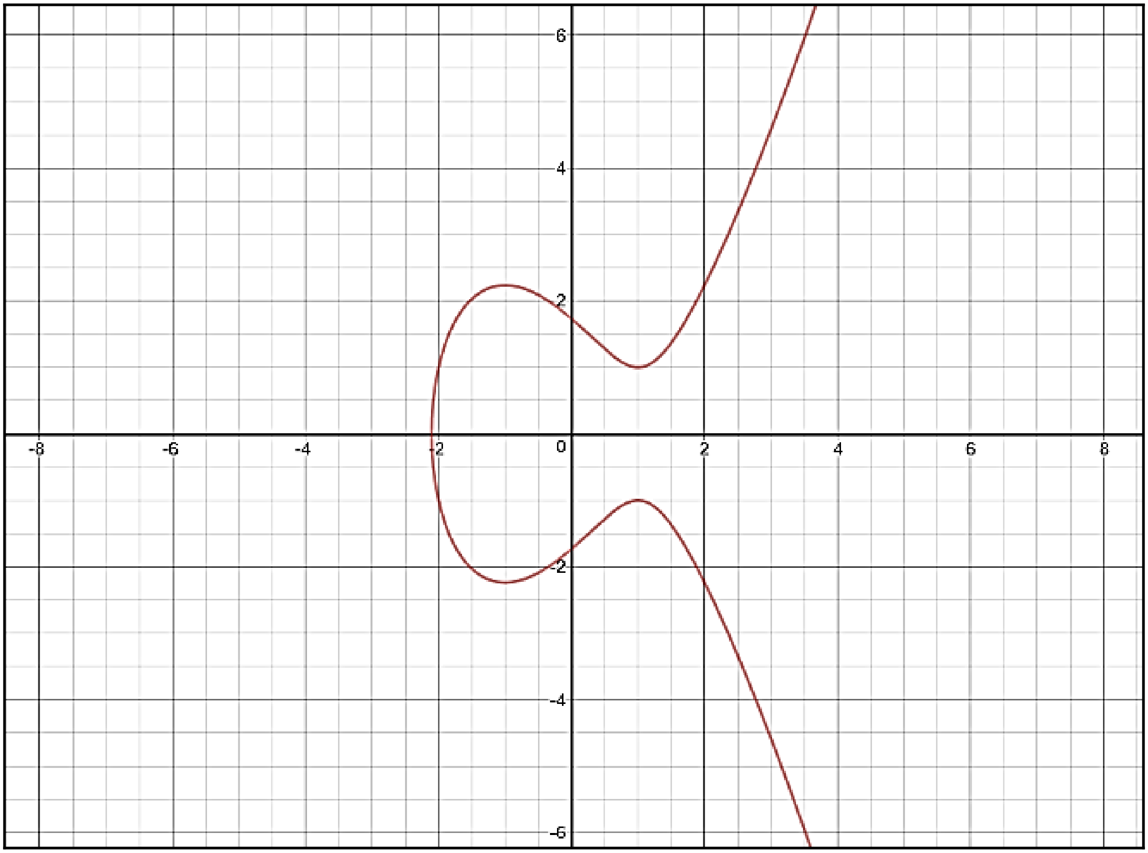
```
Cipher Types
-aes-128-cbc               -aes-128-cbc-hmac-sha1     -aes-128-cbc-hmac-sha256
-aes-128-ccm               -aes-128-cfb               -aes-128-cfb1
-aes-128-cfb8              -aes-128-ctr               -aes-128-ecb
-aes-128-gcm               -aes-128-ofb               -aes-128-xts
-aes-192-cbc               -aes-192-ccm               -aes-192-cfb
-aes-192-cfb1              -aes-192-cfb8              -aes-192-ctr
-aes-192-ecb               -aes-192-gcm               -aes-192-ofb
-aes-256-cbc               -aes-256-cbc-hmac-sha1     -aes-256-cbc-hmac-sha256
-aes-256-ccm               -aes-256-cfb               -aes-256-cfb1
-aes-256-cfb8              -aes-256-ctr               -aes-256-ecb
-aes-256-gcm               -aes-256-ofb               -aes-256-xts
-aes128                    -aes192                    -aes256
-bf                        -bf-cbc                    -bf-cfb
-bf-ecb                    -bf-ofb                    -blowfish
-camellia-128-cbc          -camellia-128-cfb          -camellia-128-cfb1
-camellia-128-cfb8         -camellia-128-ecb          -camellia-128-ofb
-camellia-192-cbc          -camellia-192-cfb          -camellia-192-cfb1
-camellia-192-cfb8         -camellia-192-ecb          -camellia-192-ofb
-camellia-256-cbc          -camellia-256-cfb          -camellia-256-cfb1
-camellia-256-cfb8         -camellia-256-ecb          -camellia-256-ofb
-camellia128               -camellia192               -camellia256
-cast                      -cast-cbc                  -cast5-cbc
-cast5-cfb                 -cast5-ecb                 -cast5-ofb
-des                       -des-cbc                   -des-cfb
-des-cfb1                  -des-cfb8                  -des-ecb
-des-ede                   -des-ede-cbc               -des-ede-cfb
-des-ede-ofb               -des-ede3                  -des-ede3-cbc
-des-ede3-cfb              -des-ede3-cfb1             -des-ede3-cfb8
-des-ede3-ofb              -des-ofb                   -des3
-desx                      -desx-cbc                  -id-aes128-CCM
-id-aes128-GCM             -id-aes128-wrap            -id-aes192-CCM
-id-aes192-GCM             -id-aes192-wrap            -id-aes256-CCM
-id-aes256-GCM             -id-aes256-wrap            -id-smime-alg-CMS3DESwrap
-rc2                       -rc2-40-cbc                -rc2-64-cbc
-rc2-cbc                   -rc2-cfb                   -rc2-ecb
-rc2-ofb                   -rc4                       -rc4-40
-rc4-hmac-md5              -seed                      -seed-cbc
-seed-cfb                  -seed-ecb                  -seed-ofb
```

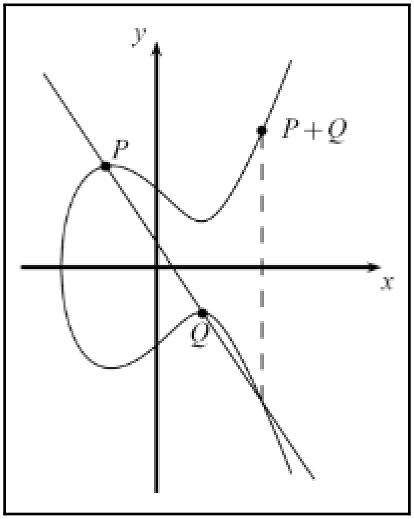


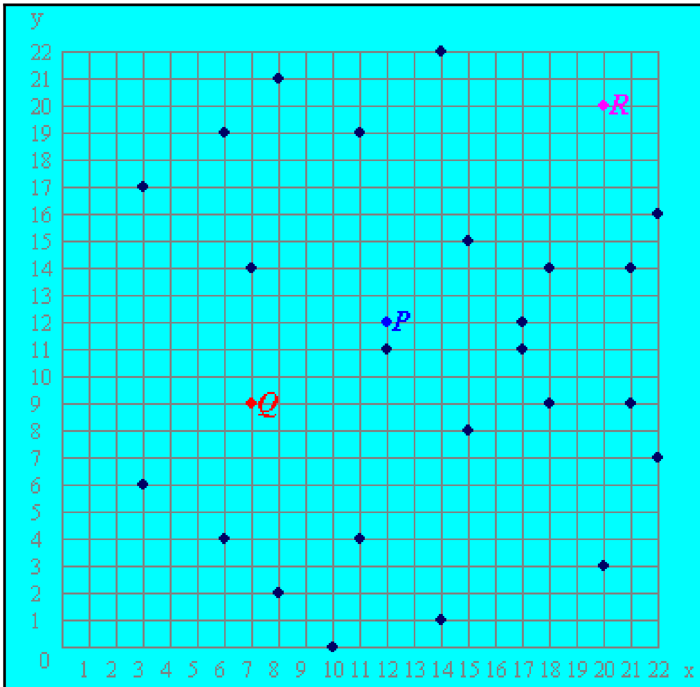
ENCRYPTION DECRYPTION USING PUBLIC / PRIVATE KEY



SIGNING & VERIFICATION USING PUBLIC / PRIVATE KEY


6
4
2
0
-2
-4
-6
-8
-6
-4
-2
2
4
6
8


y
P
P + Q
x
Q



$y^2 = x^3 + 7x + 11$ over F_{23}

27 solutions

P (12, 12)

Q (7, 9)

R (20, 20)

$l = (y_P - y_Q) * (x_P - x_Q)^{-1} \bmod p$

$= 3 * 5^{-1} \bmod 23$

$= 3 * 14 \bmod 23$

$= 19$

$x_R = l^2 - x_P - x_Q \bmod p$

$= 361 - 12 - 7 \bmod 23$

$= 20$

$y_R = -y_P + l * (x_P - x_R) \bmod p$

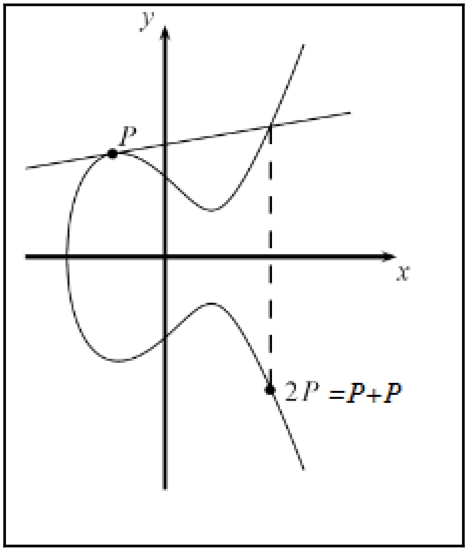
$= -12 + 19 * (12 - 20) \bmod 23$

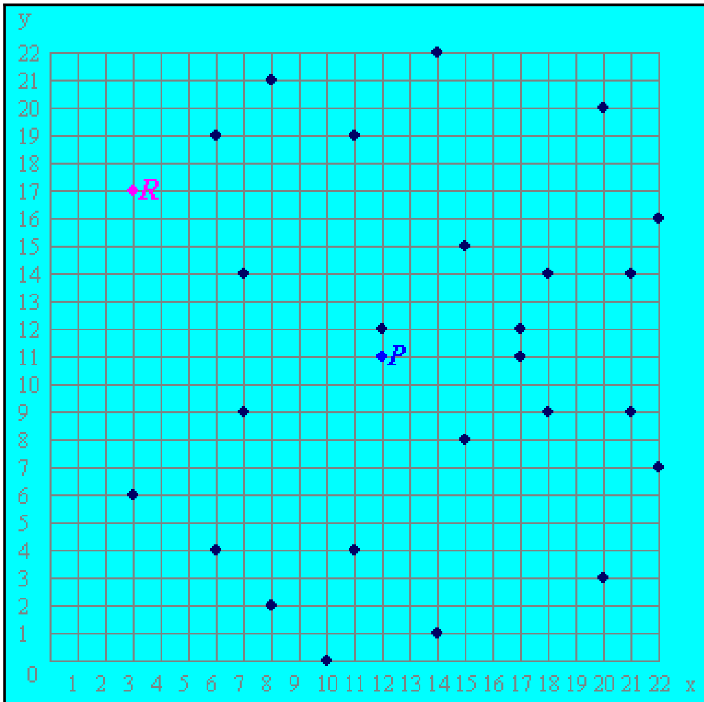
$= 11 + 19 * 15 \bmod 23$

$= 11 + 9 \bmod 23$

$= 20$

P + *Q* = *R* = (20, 20).


y
P
x
2P =P+P



$y^2 = x^3 + 7x + 11$ over F_{23}

27 solutions

P (12, 11)

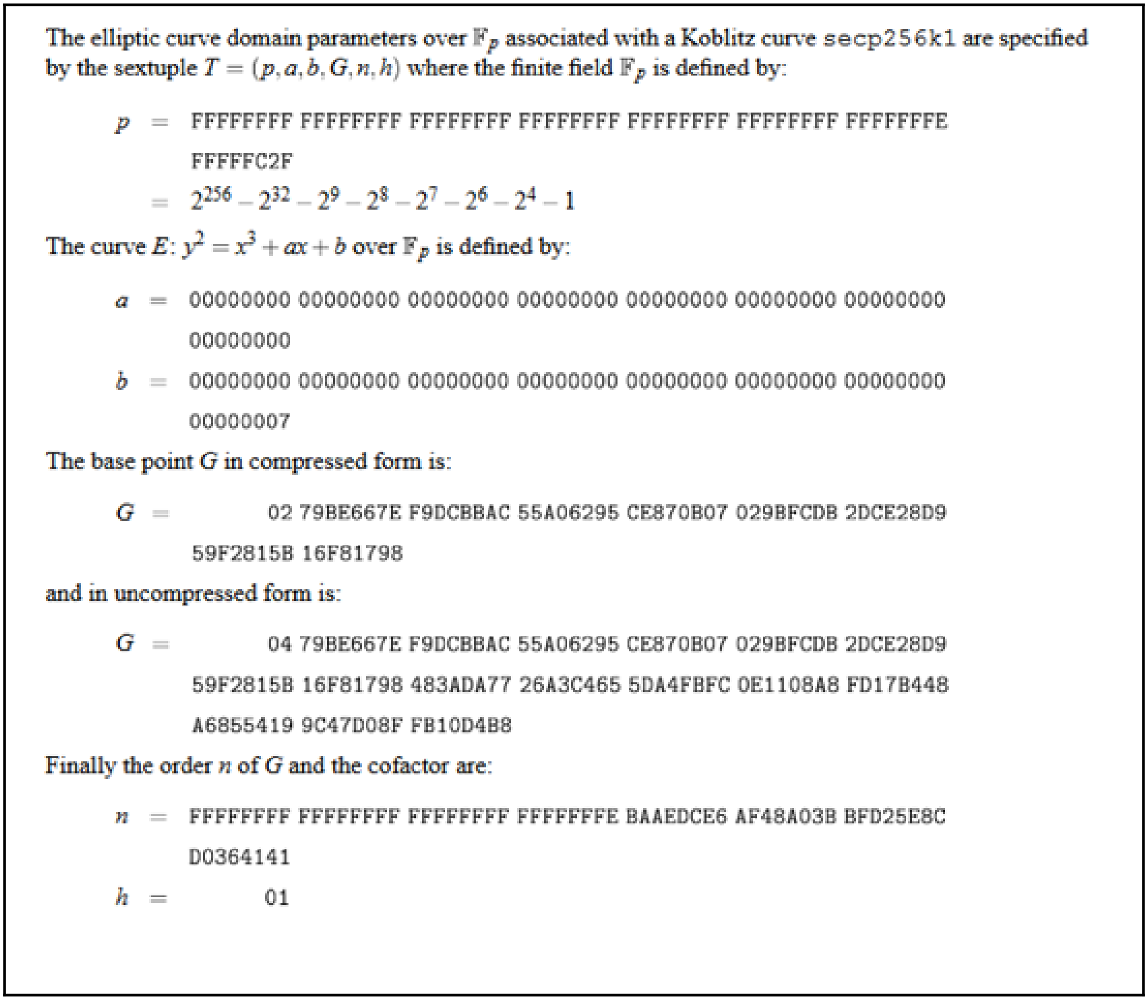
R (3, 17)

$$l = (3x_P^2 + a) * (2y_P)^{-1} \bmod p$$
$$= 439 * 22^{-1} \bmod 23$$
$$= 2 * 22 \bmod 23$$
$$= 21$$

$$x_R = l^2 - 2x_P \bmod p$$
$$= 441 - 24 \bmod 23$$
$$= 3$$

$$y_R = -y_P + l * (x_P - x_R) \bmod p$$
$$= -11 + 21 * (12 - 3) \bmod 23$$
$$= 12 + 21 * 9 \bmod 23$$
$$= 12 + 5 \bmod 23$$
$$= 17$$

$2P = R = (3, 17)$.



The elliptic curve domain parameters over $\mathbb{F}_p$ associated with a Koblitz curve `secp256k1` are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field $\mathbb{F}_p$ is defined by:

p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F

$= 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$

The curve E: $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$ is defined by:

a = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

b = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000007

The base point G in compressed form is:

G = 02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798

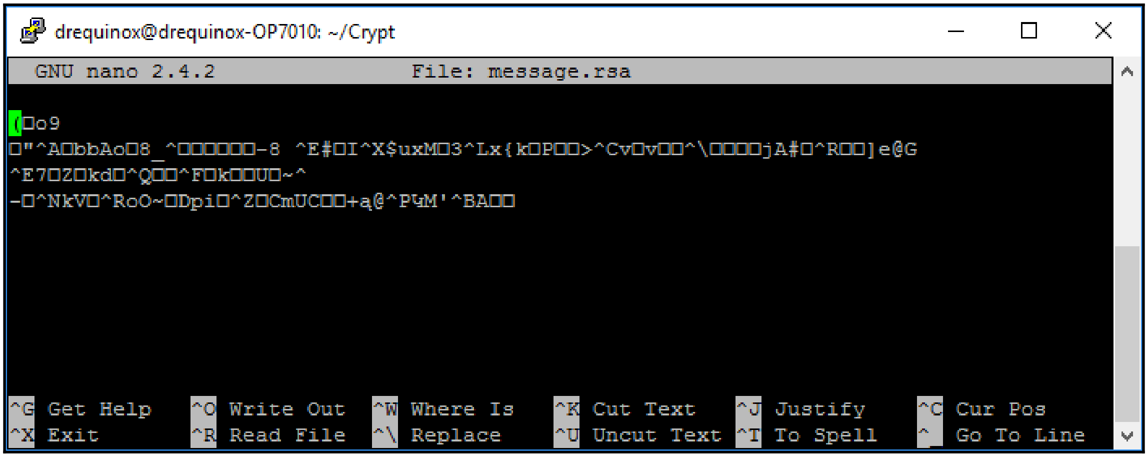
and in uncompressed form is:

G = 04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8

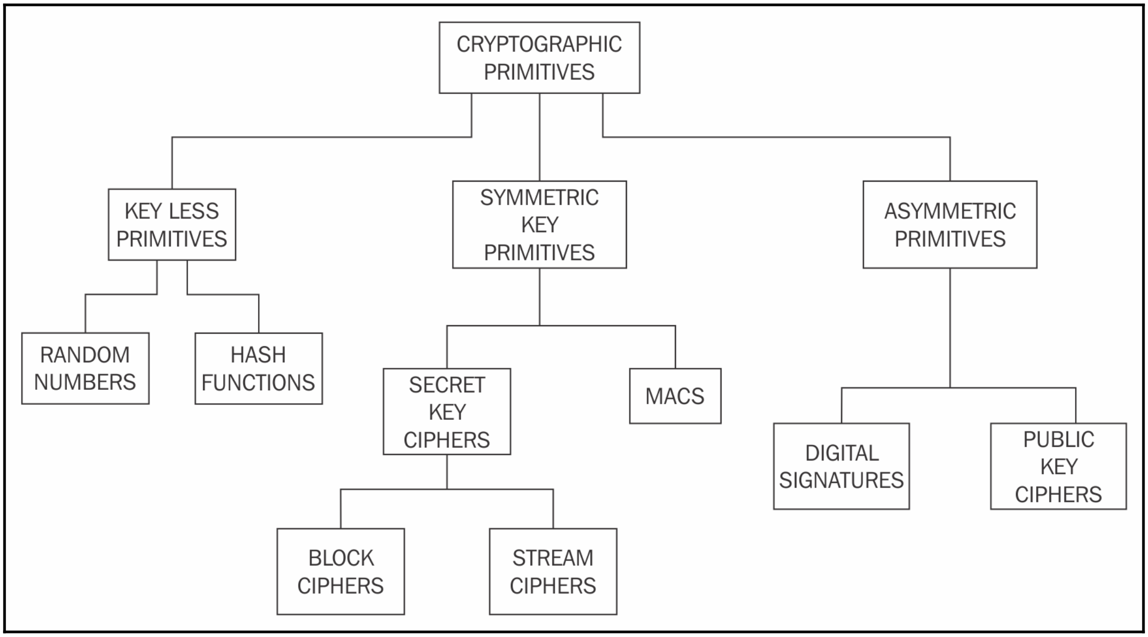
Finally the order n of G and the cofactor are:

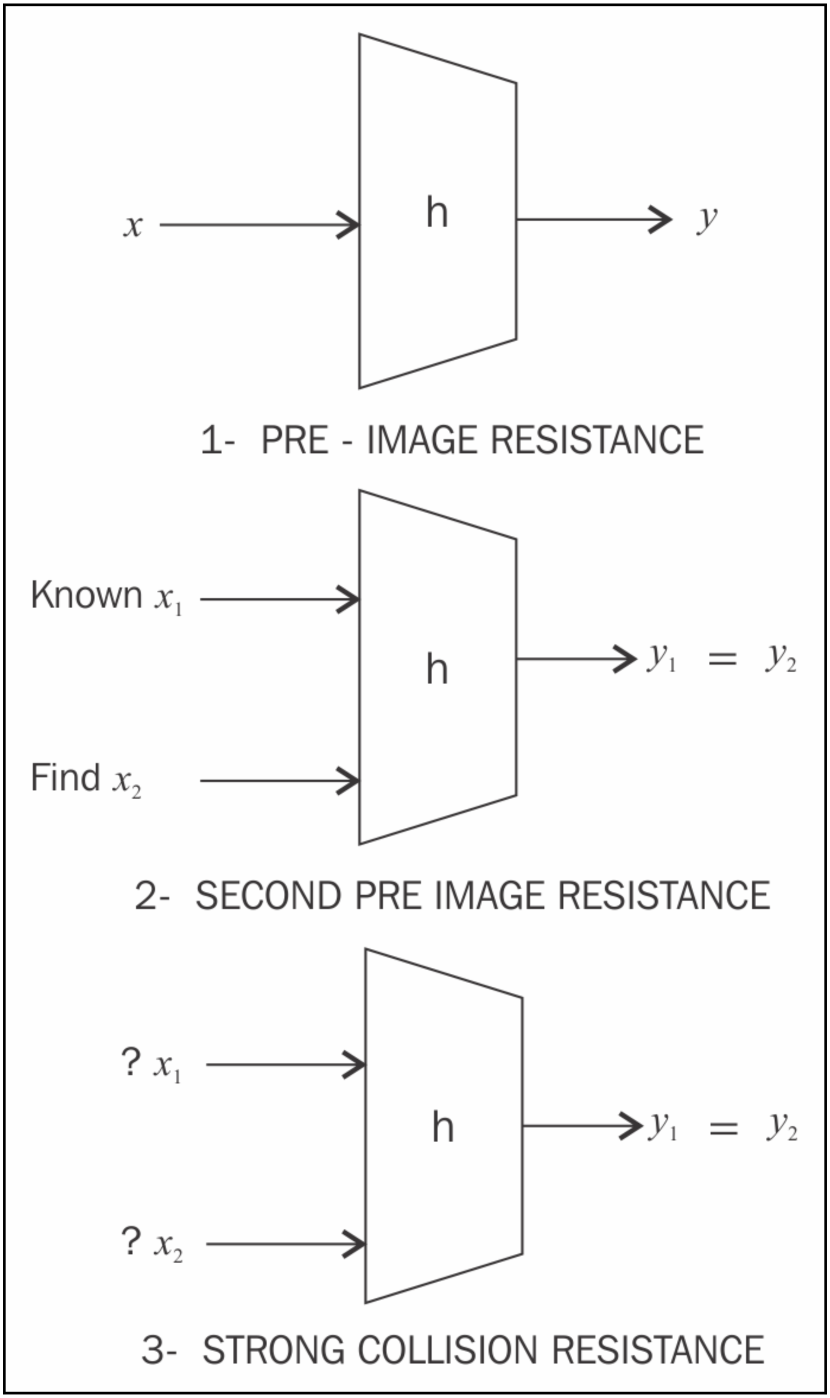
n = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141

h = 01



```
drequinox@drequinox-OP7010: ~/Crypt
  GNU nano 2.4.2                  File: message.rsa

(□o9
□"^A□bbAo□8_^□□□□□□□-8 ^E#□I^X$uxM□3^Lx{k□P□□>^Cv□v□□^\□□□□jA#□^R□□]e@G
^E7□Z□kd□^Q□□^F□k□□U□~^
-□^NkV□^RoO~□Dpi□^Z□CmUC□□+ą@^PЧM'^BA□□

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line
```

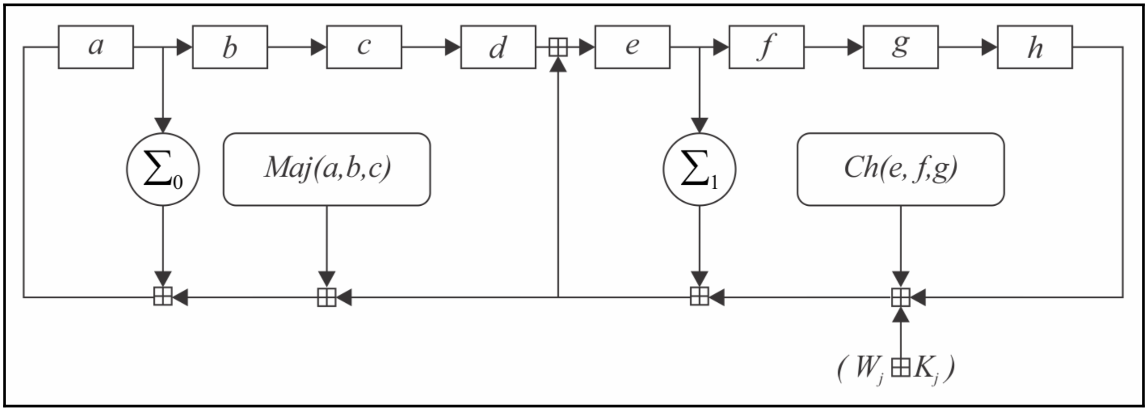


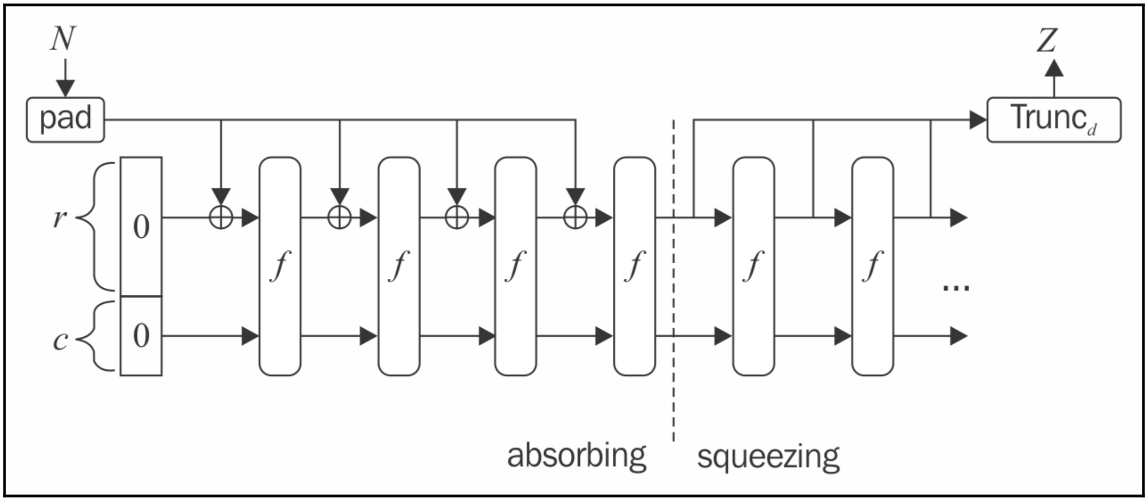


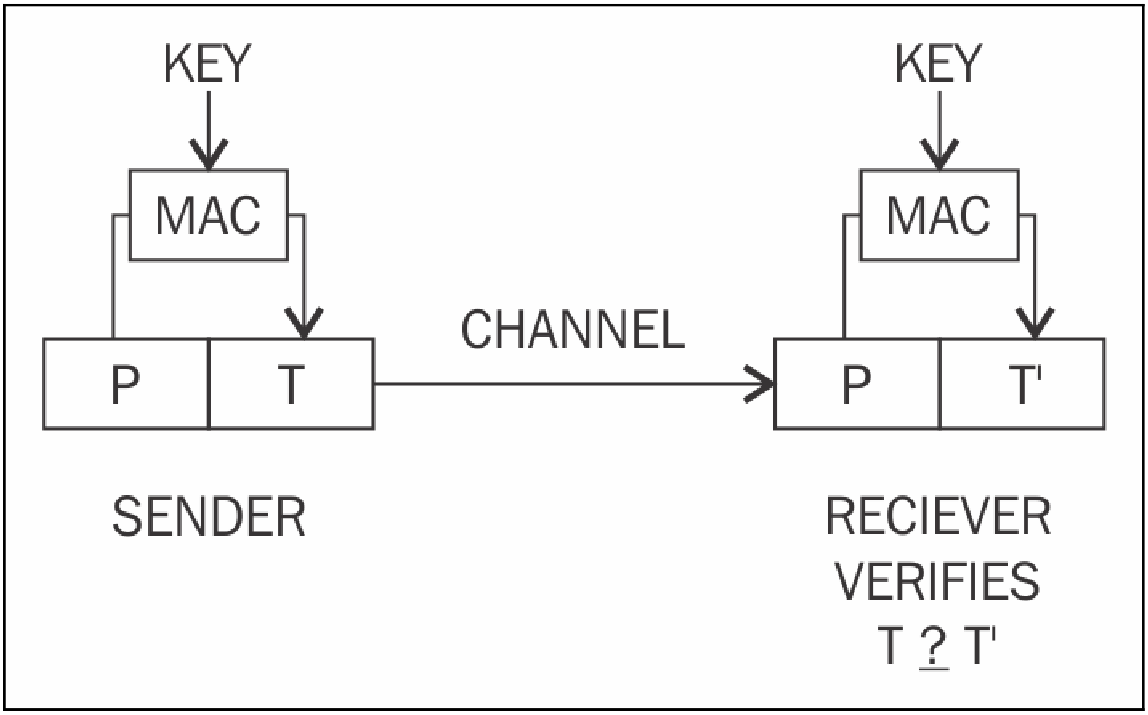
1- PRE - IMAGE RESISTANCE

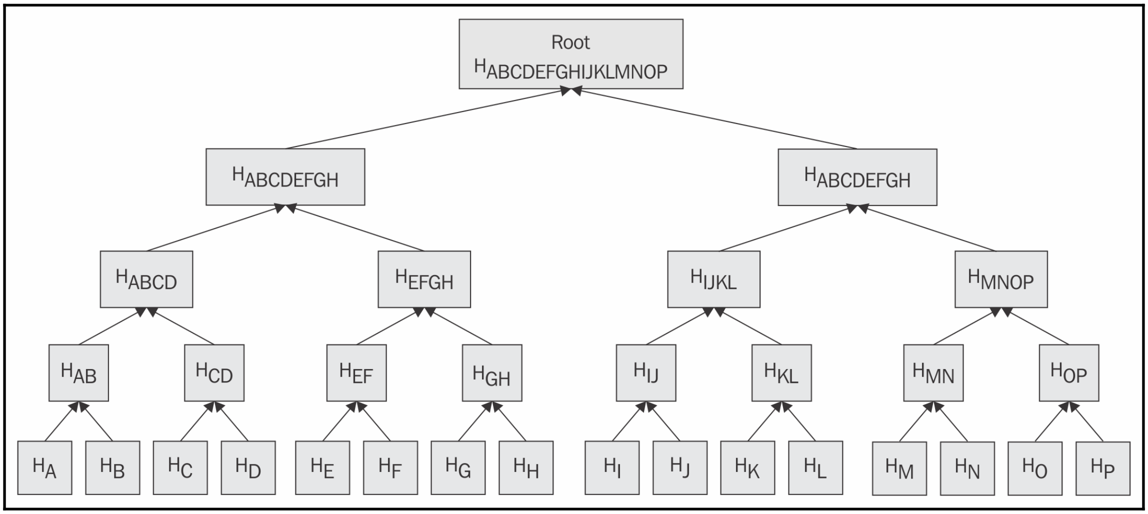
2- SECOND PRE IMAGE RESISTANCE

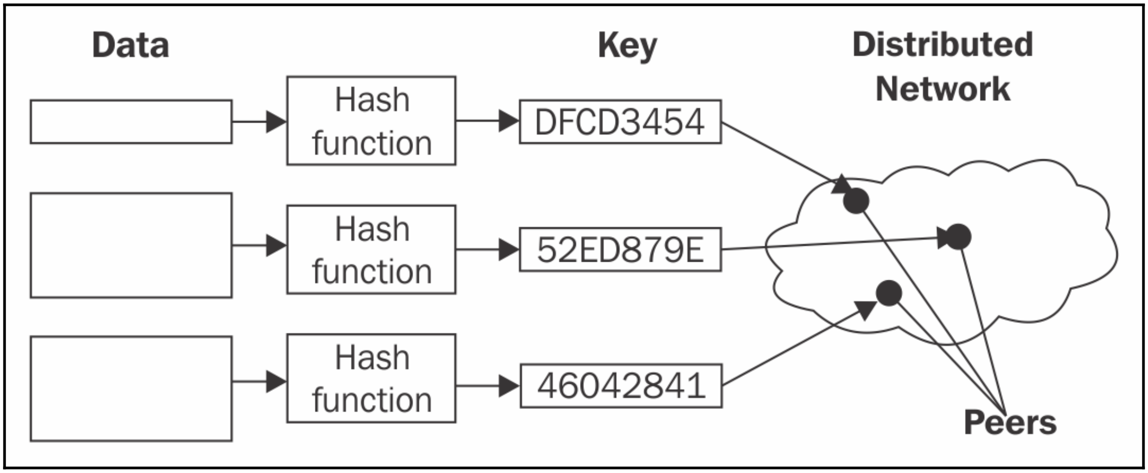
3- STRONG COLLISION RESISTANCE

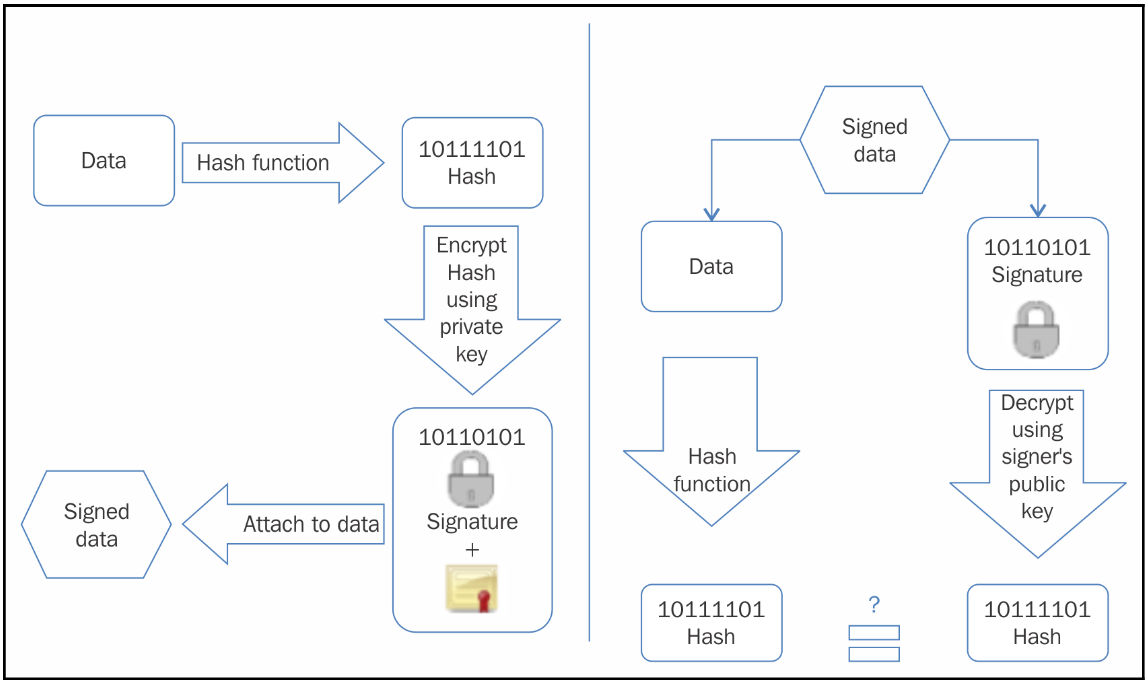

a
b
c
d
e
f
g
h
Σ0
Maj(a,b,c)
Σ1
Ch(e, f,g)
(Wj ⊞ Kj)

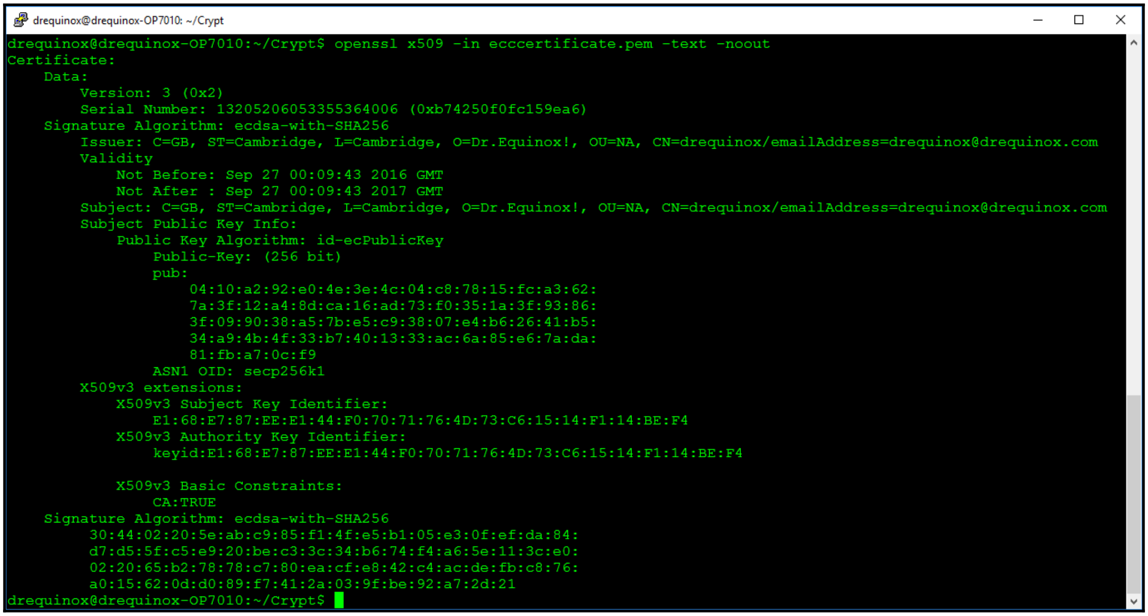

N
Z
pad
Truncd
r
c
0
0
f
f
f
f
f
f
...
absorbing
squeezing


KEY
MAC
P
T
CHANNEL
SENDER
KEY
MAC
P
T'
RECIEVER
VERIFIES
T ? T'

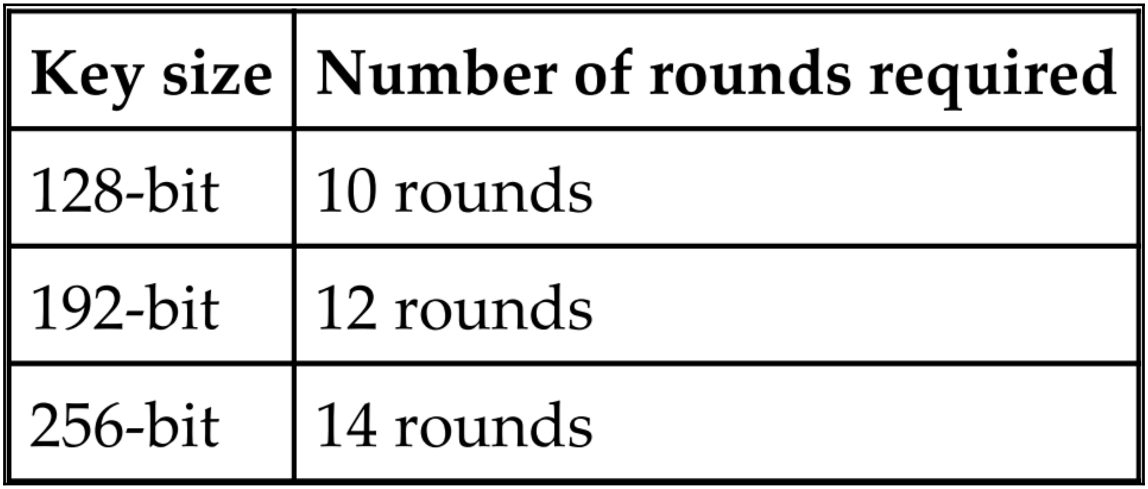

Root
$H_{ABCDEFGHIJKLMNOP}$
$H_{ABCDEFGH}$
$H_{ABCDEFGH}$
H_{ABCD}
H_{EFGH}
H_{IJKL}
H_{MNOP}
H_{AB}
H_{CD}
H_{EF}
H_{GH}
H_{IJ}
H_{KL}
H_{MN}
H_{OP}
H_A
H_B
H_C
H_D
H_E
H_F
H_G
H_H
H_I
H_J
H_K
H_L
H_M
H_N
H_O
H_P


Data
Key
Distributed Network
Hash function
Hash function
Hash function
DFCD3454
52ED879E
46042841
Peers


Data
Hash function
10111101
Hash
Encrypt Hash using private key
10110101
Signature
+
Attach to data
Signed data
Signed data
Data
10110101
Signature
Hash function
Decrypt using signer's public key
10111101
Hash
?
=
10111101
Hash

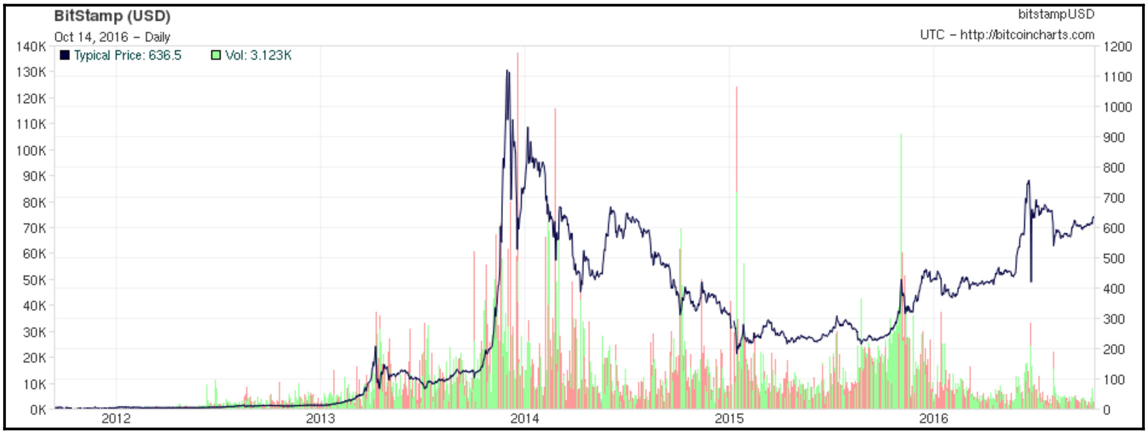


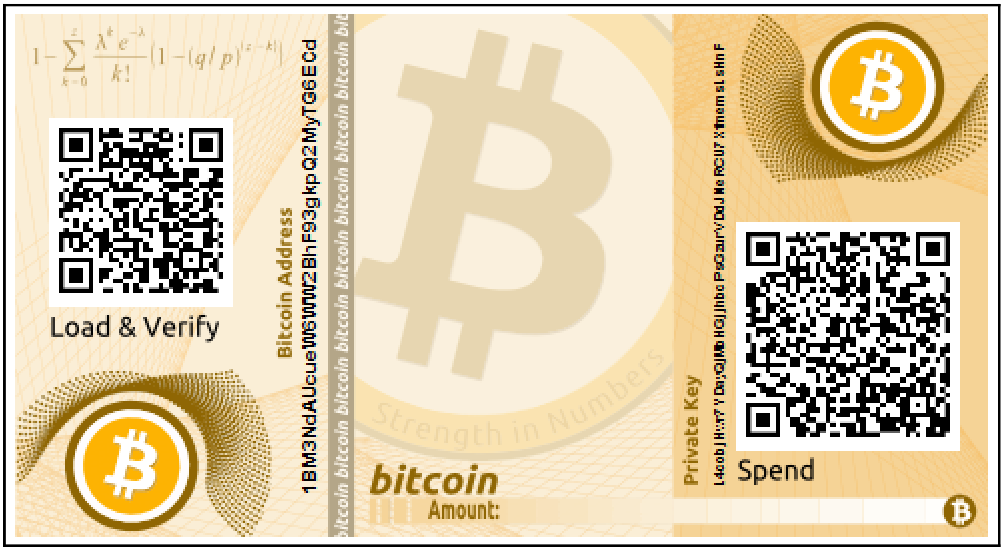
```
drequinox@drequinox-OP7010:~/Crypt$ openssl x509 -in ecccertificate.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 13205206053355364006 (0xb74250f0fc159ea6)
    Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=GB, ST=Cambridge, L=Cambridge, O=Dr.Equinox!, OU=NA, CN=drequinox/emailAddress=drequinox@drequinox.com
        Validity
            Not Before: Sep 27 00:09:43 2016 GMT
            Not After : Sep 27 00:09:43 2017 GMT
        Subject: C=GB, ST=Cambridge, L=Cambridge, O=Dr.Equinox!, OU=NA, CN=drequinox/emailAddress=drequinox@drequinox.com
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:10:a2:92:e0:4e:3e:4c:04:c8:78:15:fc:a3:62:
                    7a:3f:12:a4:8d:ca:16:ad:73:f0:35:1a:3f:93:86:
                    3f:09:90:38:a5:7b:e5:c9:38:07:e4:b6:26:41:b5:
                    34:a9:4b:4f:33:b7:40:13:33:ac:6a:85:e6:7a:da:
                    81:fb:a7:0c:f9
                ASN1 OID: secp256k1
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                E1:68:E7:87:EE:E1:44:F0:70:71:76:4D:73:C6:15:14:F1:14:BE:F4
            X509v3 Authority Key Identifier:
                keyid:E1:68:E7:87:EE:E1:44:F0:70:71:76:4D:73:C6:15:14:F1:14:BE:F4

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: ecdsa-with-SHA256
         30:44:02:20:5e:ab:c9:85:f1:4f:e5:b1:05:e3:0f:ef:da:84:
         d7:d5:5f:c5:e9:20:be:c3:3c:34:b6:74:f4:a6:5e:11:3c:e0:
         02:20:65:b2:78:78:c7:80:ea:cf:e8:42:c4:ac:de:fb:c8:76:
         a0:15:62:0d:d0:89:f7:41:2a:03:9f:be:92:a7:2d:21
drequinox@drequinox-OP7010:~/Crypt$
```



Key size	Number of rounds required
128-bit	10 rounds
192-bit	12 rounds
256-bit	14 rounds

Chapter 4: Bitcoin



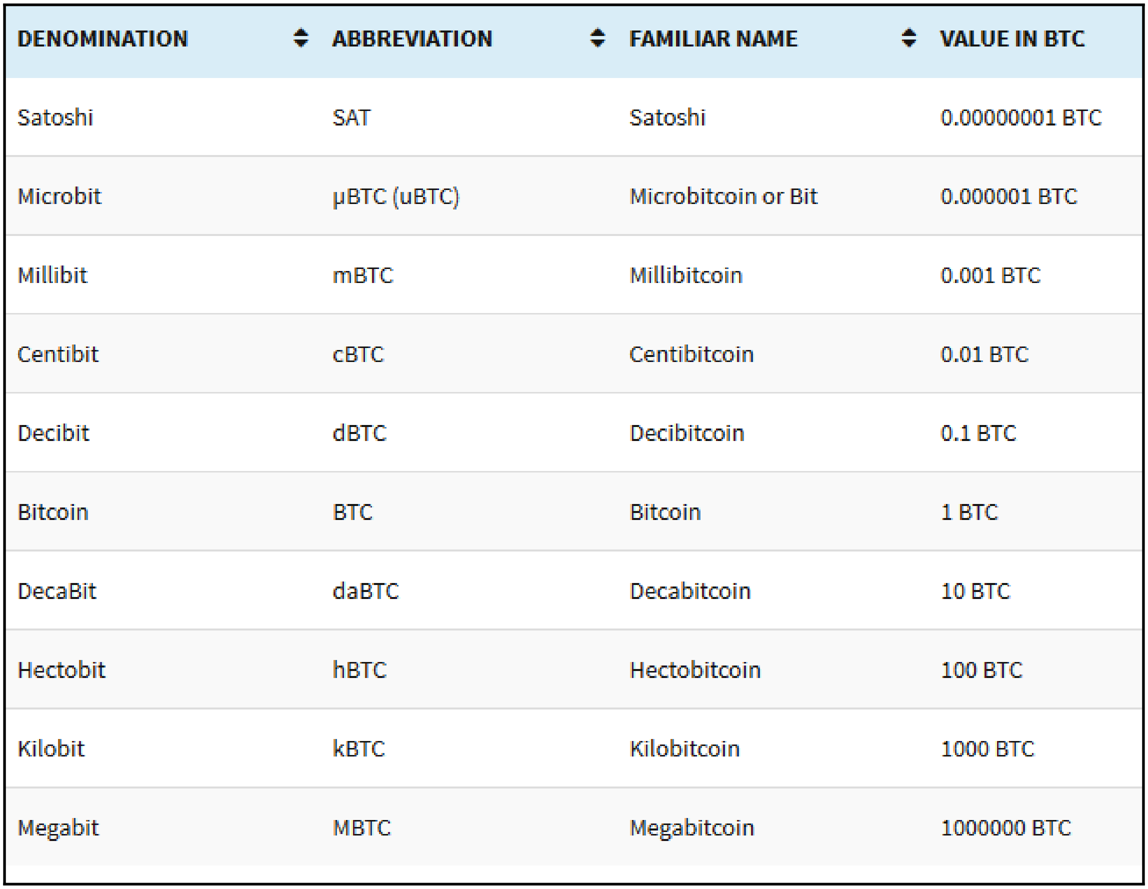

$1-\sum_{k=0}^{z}\frac{\lambda^k e^{-\lambda}}{k!}(1-(q/p)^{(z-k)})$
Load & Verify
bitcoin
Amount:
Strength in Numbers
Spend

Bitcoin Address

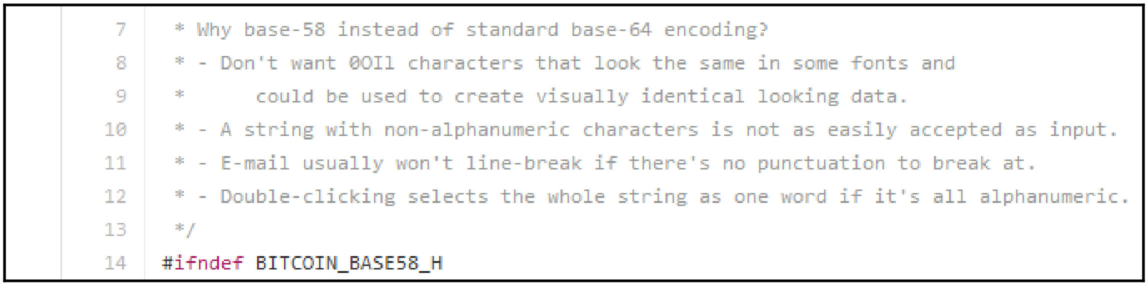
1BM3NdAUcueW6WW2BhF93gkpQ2MyTG6ECd

Private Key

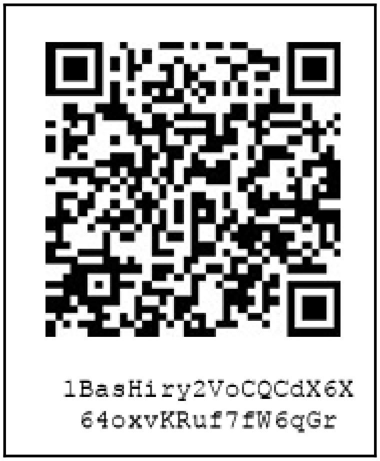
L4oobjHwr7YDayQjMbHGjjhbcPsGaurVDdJNeRCU7XfnemsLsHnF



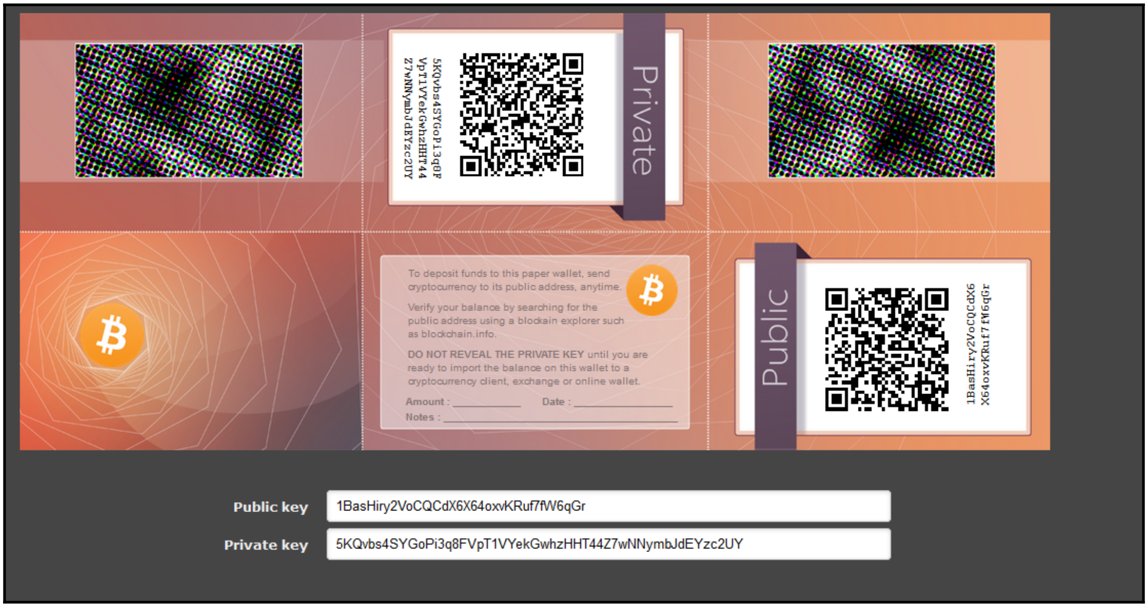
DENOMINATION	ABBREVIATION	FAMILIAR NAME	VALUE IN BTC
Satoshi	SAT	Satoshi	0.00000001 BTC
Microbit	µBTC (uBTC)	Microbitcoin or Bit	0.000001 BTC
Millibit	mBTC	Millibitcoin	0.001 BTC
Centibit	cBTC	Centibitcoin	0.01 BTC
Decibit	dBTC	Decibitcoin	0.1 BTC
Bitcoin	BTC	Bitcoin	1 BTC
DecaBit	daBTC	Decabitcoin	10 BTC
Hectobit	hBTC	Hectobitcoin	100 BTC
Kilobit	kBTC	Kilobitcoin	1000 BTC
Megabit	MBTC	Megabitcoin	1000000 BTC



```
 * Why base-58 instead of standard base-64 encoding?
 * - Don't want 0OIl characters that look the same in some fonts and
 *      could be used to create visually identical looking data.
 * - A string with non-alphanumeric characters is not as easily accepted as input.
 * - E-mail usually won't line-break if there's no punctuation to break at.
 * - Double-clicking selects the whole string as one word if it's all alphanumeric.
 */
#ifndef BITCOIN_BASE58_H
```



1BasHiry2VoCQCdX6X
64oxvKRuf7fW6qGr



5KQvbs4SYGoPi3q8F
VpT1VYekGwhzHHT44
Z7wNNymbJdEYzc2UY

To deposit funds to this paper wallet, send cryptocurrency to its public address, anytime.

Verify your balance by searching for the public address using a blockain explorer such as blockchain.info.

DO NOT REVEAL THE PRIVATE KEY until you are ready to import the balance on this wallet to a cryptocurrency client, exchange or online wallet.

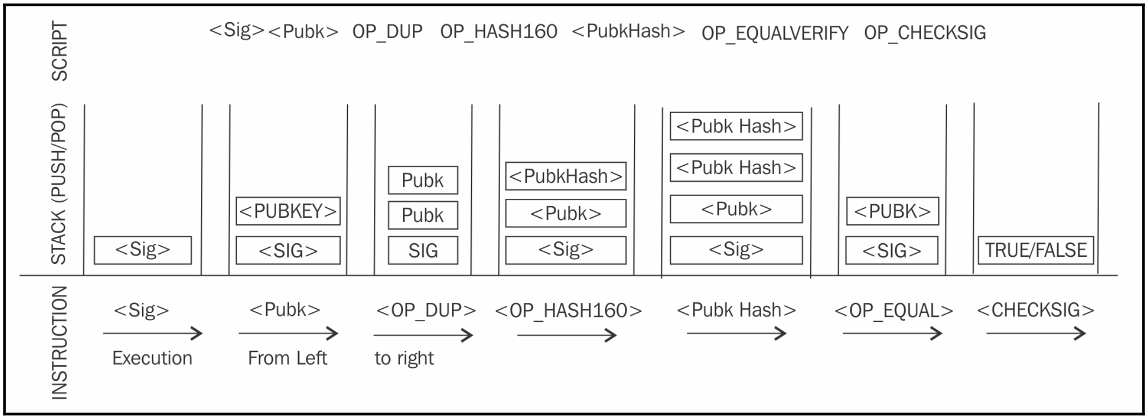
Amount : ____________ **Date :** ________________

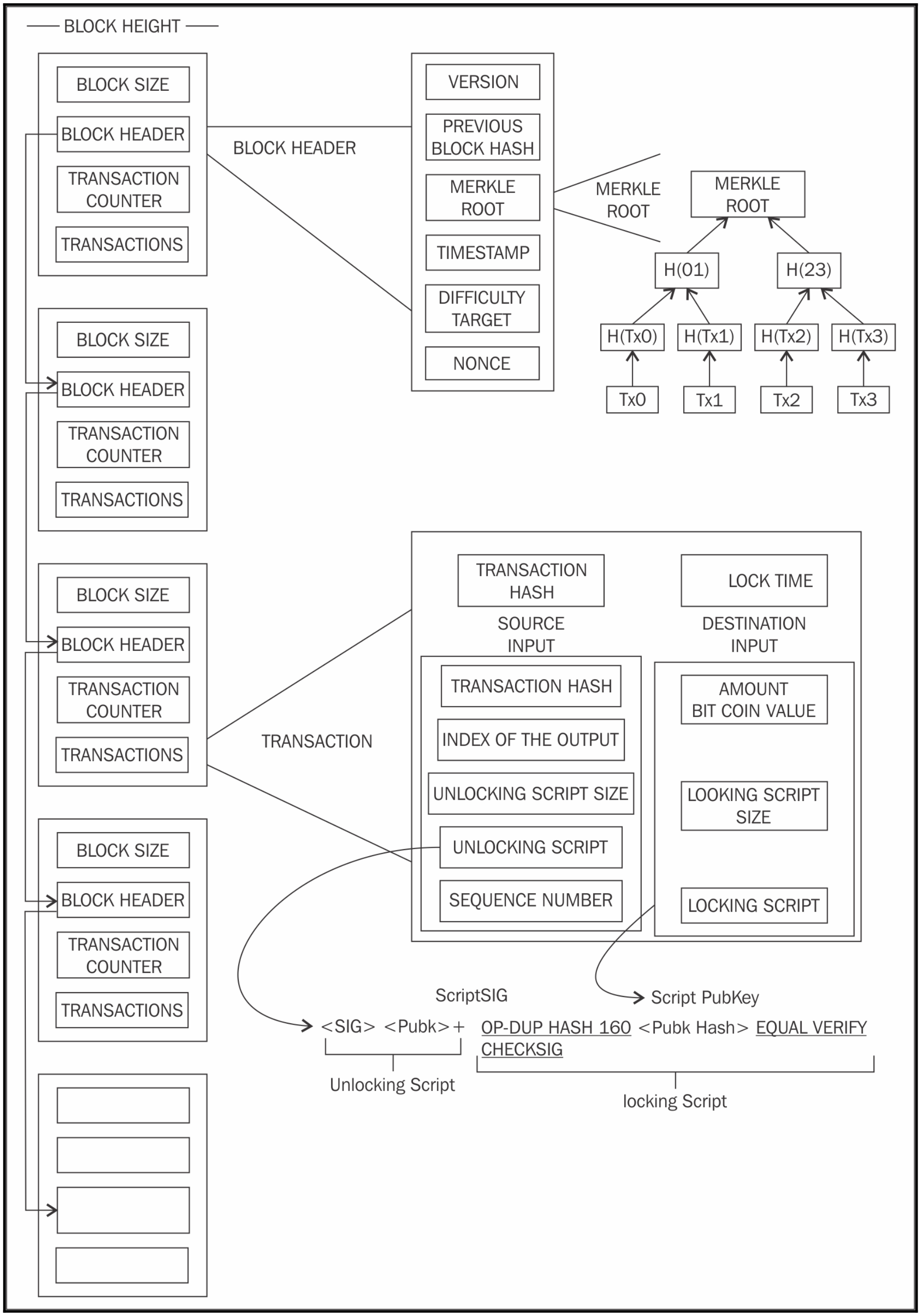
Notes : ________________________________

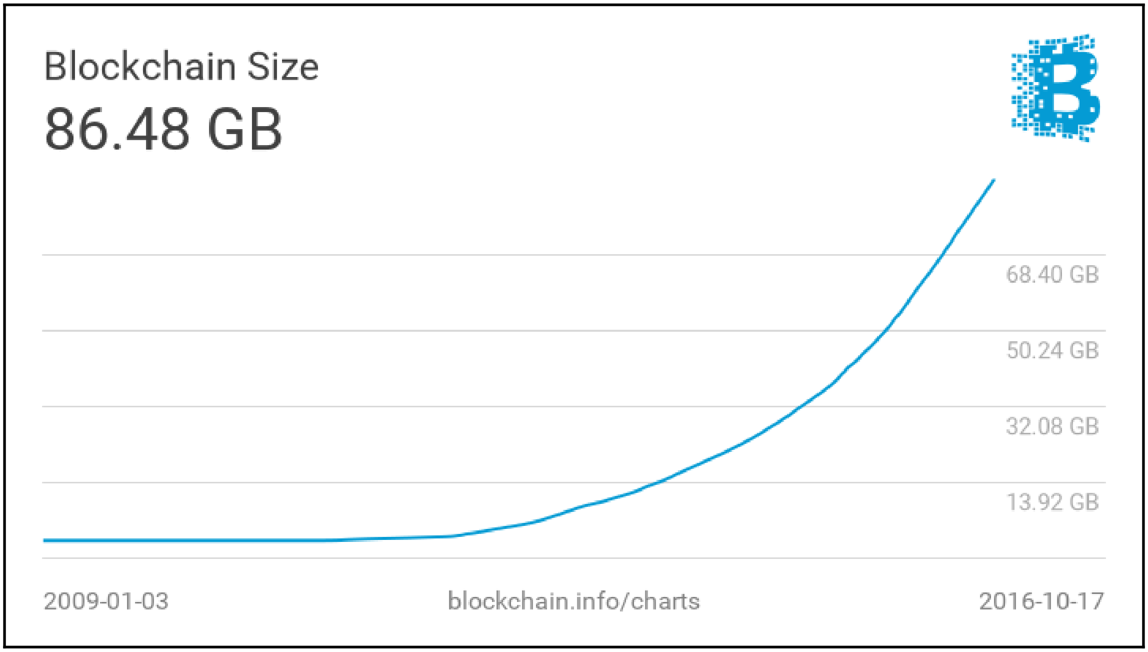
1BasHiry2VoCQCdX6
X64oxvKRuf7fW6qGr

Public key 1BasHiry2VoCQCdX6X64oxvKRuf7fW6qGr

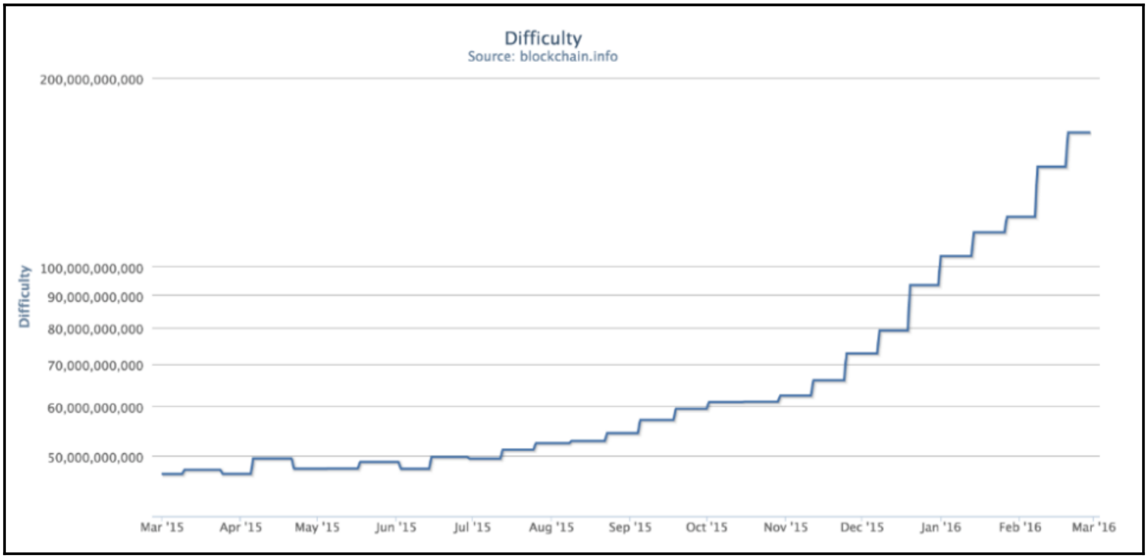
Private key 5KQvbs4SYGoPi3q8FVpT1VYekGwhzHHT44Z7wNNymbJdEYzc2UY

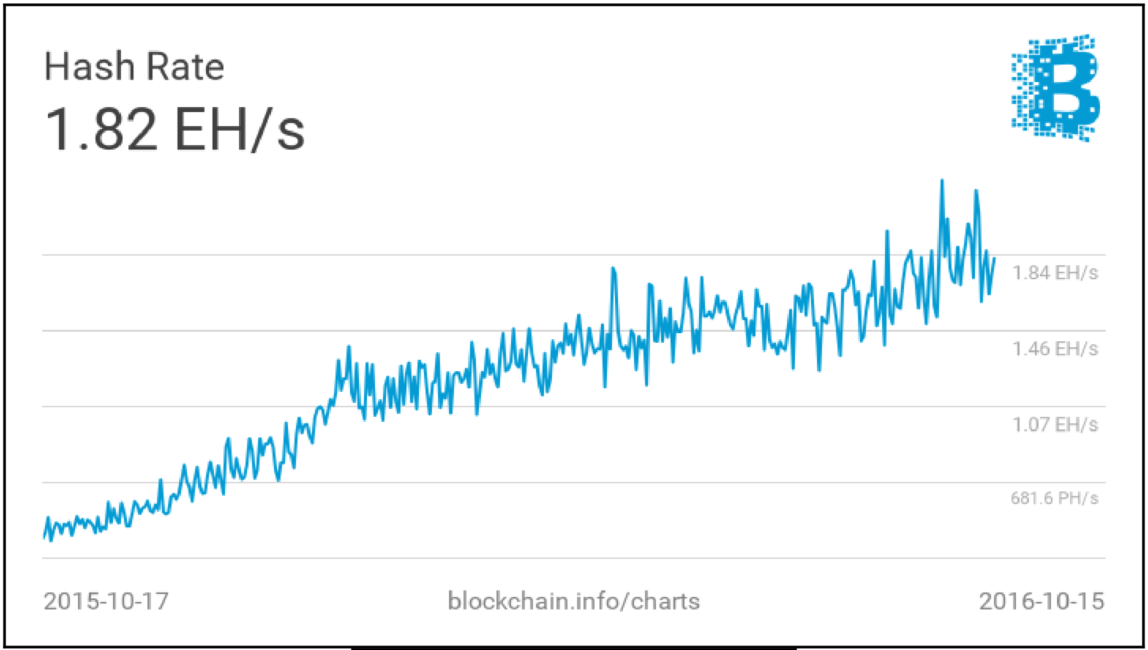

SCRIPT
<Sig><Pubk> OP_DUP OP_HASH160 <PubkHash> OP_EQUALVERIFY OP_CHECKSIG
STACK (PUSH/POP)
<Sig>
<PUBKEY>
<SIG>
Pubk
Pubk
SIG
<PubkHash>
<Pubk>
<Sig>
<Pubk Hash>
<Pubk Hash>
<Pubk>
<Sig>
<PUBK>
<SIG>
TRUE/FALSE
INSTRUCTION
<Sig>
Execution
<Pubk>
From Left
<OP_DUP>
to right
<OP_HASH160>
<Pubk Hash>
<OP_EQUAL>
<CHECKSIG>


BLOCK HEIGHT
BLOCK SIZE
BLOCK HEADER
TRANSACTION COUNTER
TRANSACTIONS
BLOCK SIZE
BLOCK HEADER
TRANSACTION COUNTER
TRANSACTIONS
BLOCK SIZE
BLOCK HEADER
TRANSACTION COUNTER
TRANSACTIONS
BLOCK SIZE
BLOCK HEADER
TRANSACTION COUNTER
TRANSACTIONS
BLOCK HEADER
VERSION
PREVIOUS BLOCK HASH
MERKLE ROOT
TIMESTAMP
DIFFICULTY TARGET
NONCE
MERKLE ROOT
MERKLE ROOT
H(01)
H(23)
H(Tx0)
H(Tx1)
H(Tx2)
H(Tx3)
Tx0
Tx1
Tx2
Tx3
TRANSACTION
TRANSACTION HASH
LOCK TIME
SOURCE INPUT
DESTINATION INPUT
TRANSACTION HASH
INDEX OF THE OUTPUT
UNLOCKING SCRIPT SIZE
UNLOCKING SCRIPT
SEQUENCE NUMBER
AMOUNT BIT COIN VALUE
LOOKING SCRIPT SIZE
LOCKING SCRIPT
ScriptSIG
Script PubKey
<SIG> <Pubk> + OP-DUP HASH 160 <Pubk Hash> EQUAL VERIFY CHECKSIG
Unlocking Script
locking Script

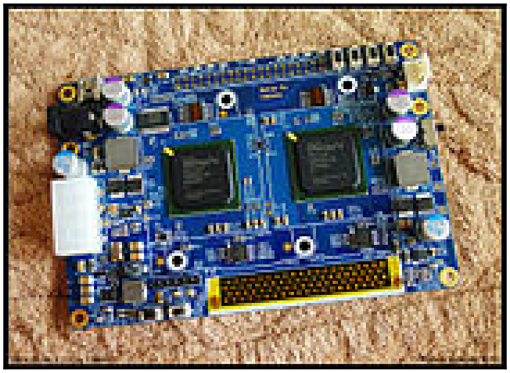

Blockchain Size

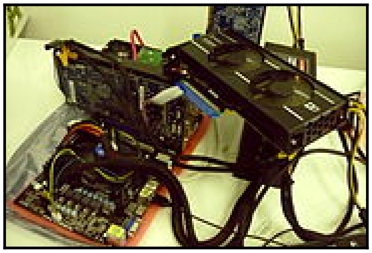
blockchain.info/charts

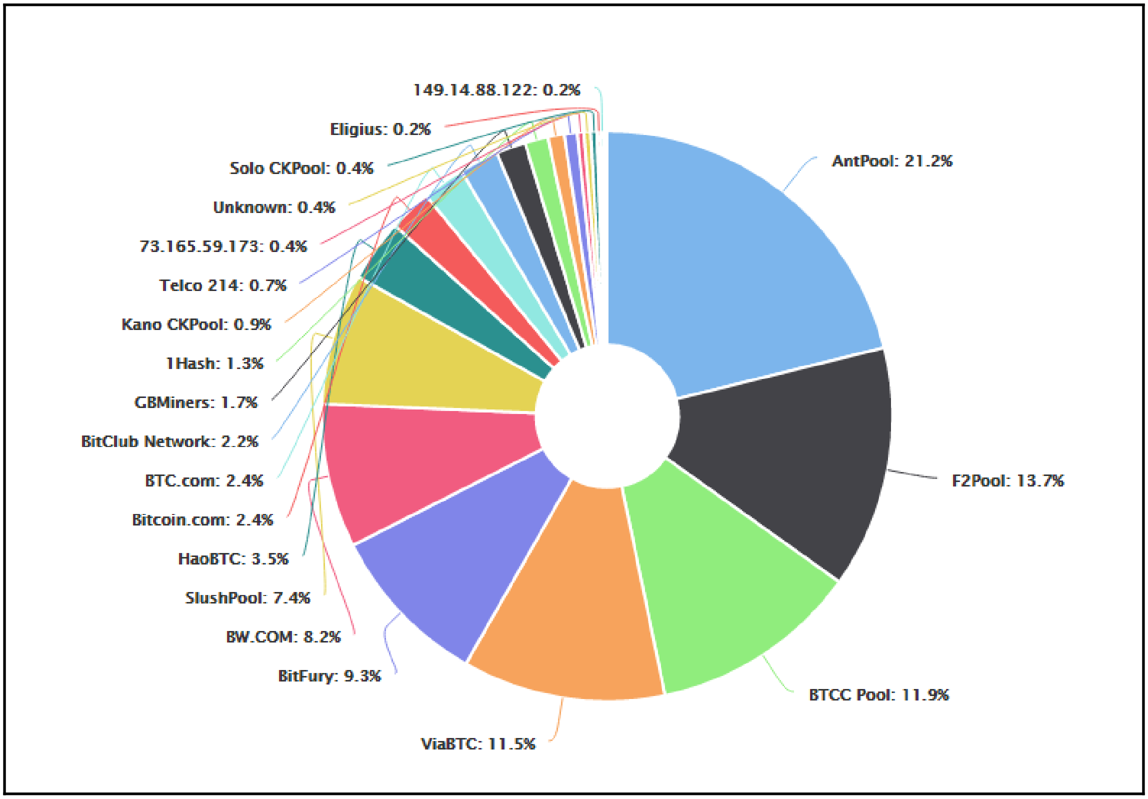

Difficulty
Source: blockchain.info

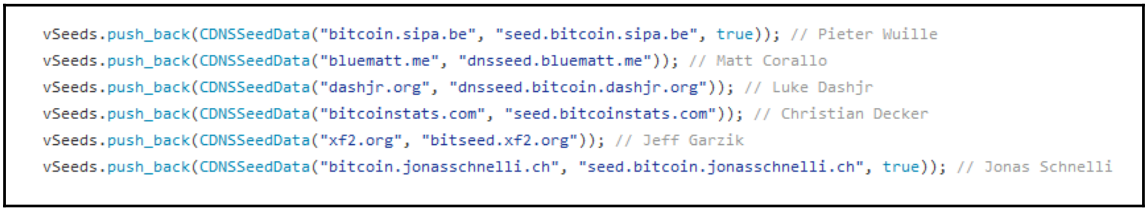

Hash Rate
1.82 EH/s
1.84 EH/s
1.46 EH/s
1.07 EH/s
681.6 PH/s
2015-10-17
blockchain.info/charts
2016-10-15

INTEL© '05
INTEL® CORE™2 DUO
6300 SL9SA MALAY
1.86GHZ/2M/1066/06
L627A264

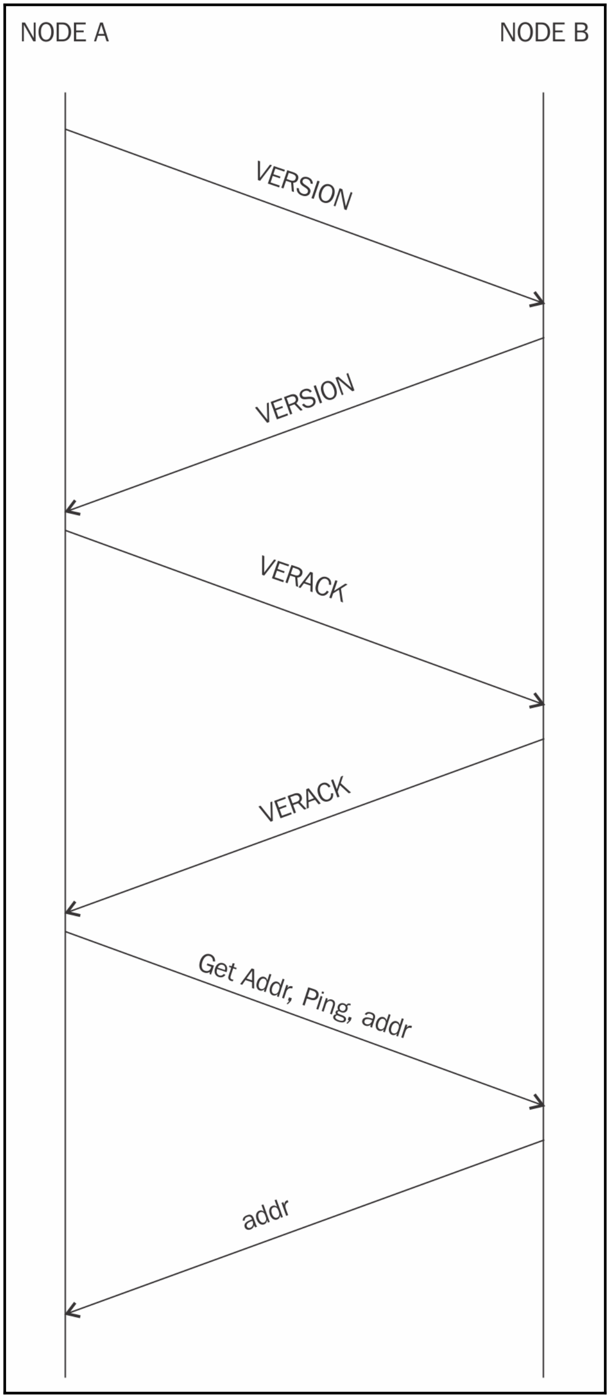




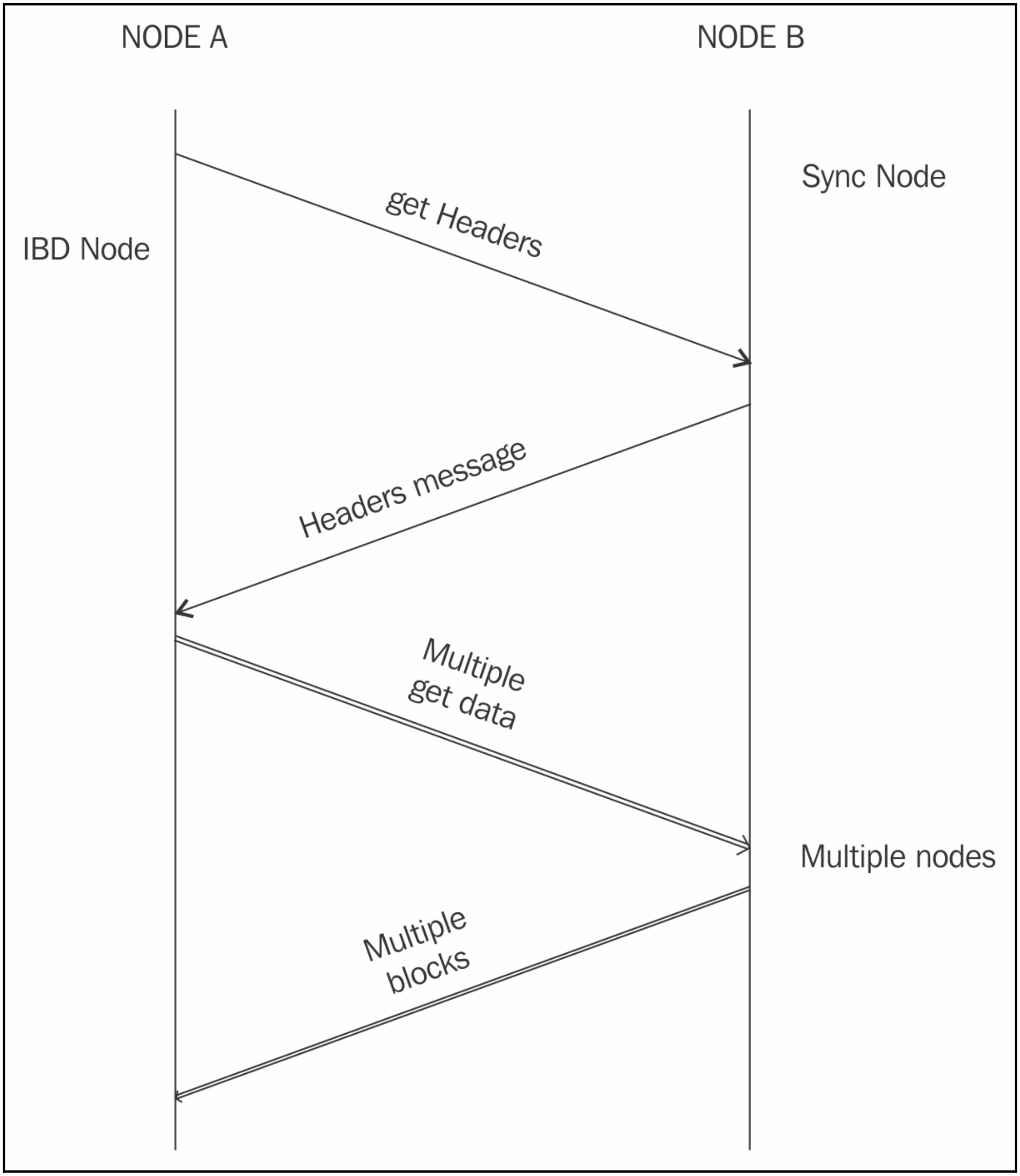


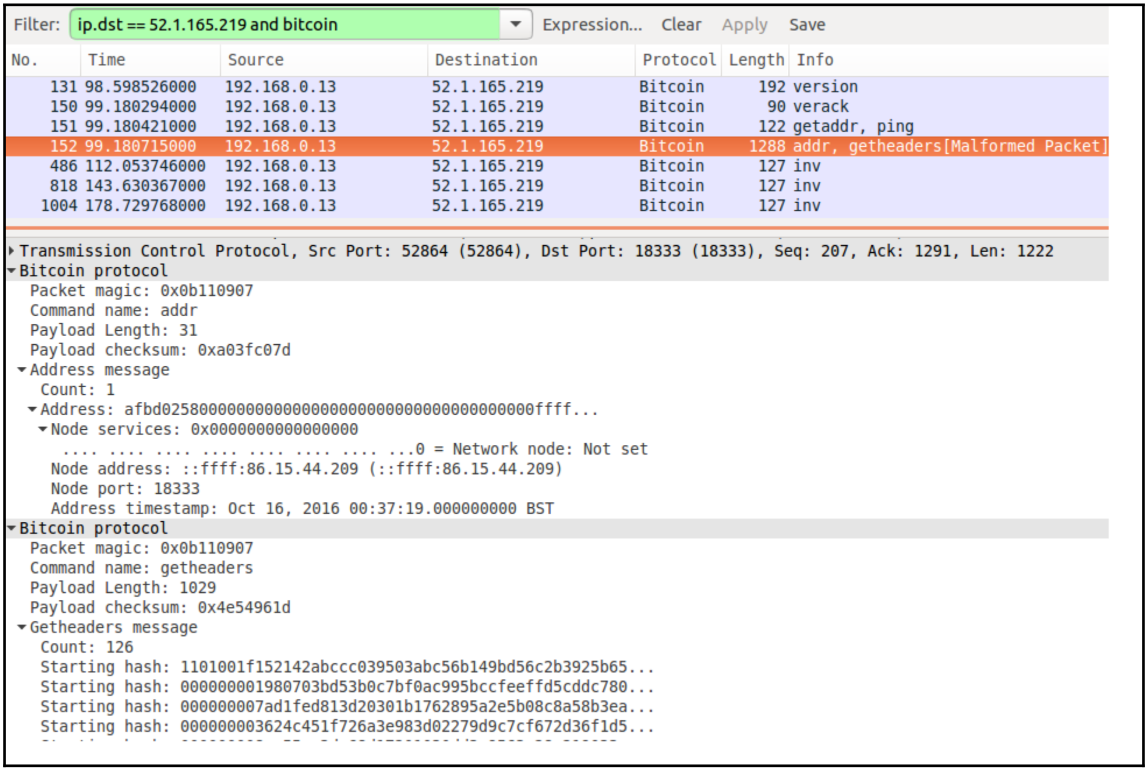


```
vSeeds.push_back(CDNSSeedData("bitcoin.sipa.be", "seed.bitcoin.sipa.be", true)); // Pieter Wuille
vSeeds.push_back(CDNSSeedData("bluematt.me", "dnsseed.bluematt.me")); // Matt Corallo
vSeeds.push_back(CDNSSeedData("dashjr.org", "dnsseed.bitcoin.dashjr.org")); // Luke Dashjr
vSeeds.push_back(CDNSSeedData("bitcoinstats.com", "seed.bitcoinstats.com")); // Christian Decker
vSeeds.push_back(CDNSSeedData("xf2.org", "bitseed.xf2.org")); // Jeff Garzik
vSeeds.push_back(CDNSSeedData("bitcoin.jonasschnelli.ch", "seed.bitcoin.jonasschnelli.ch", true)); // Jonas Schnelli
```



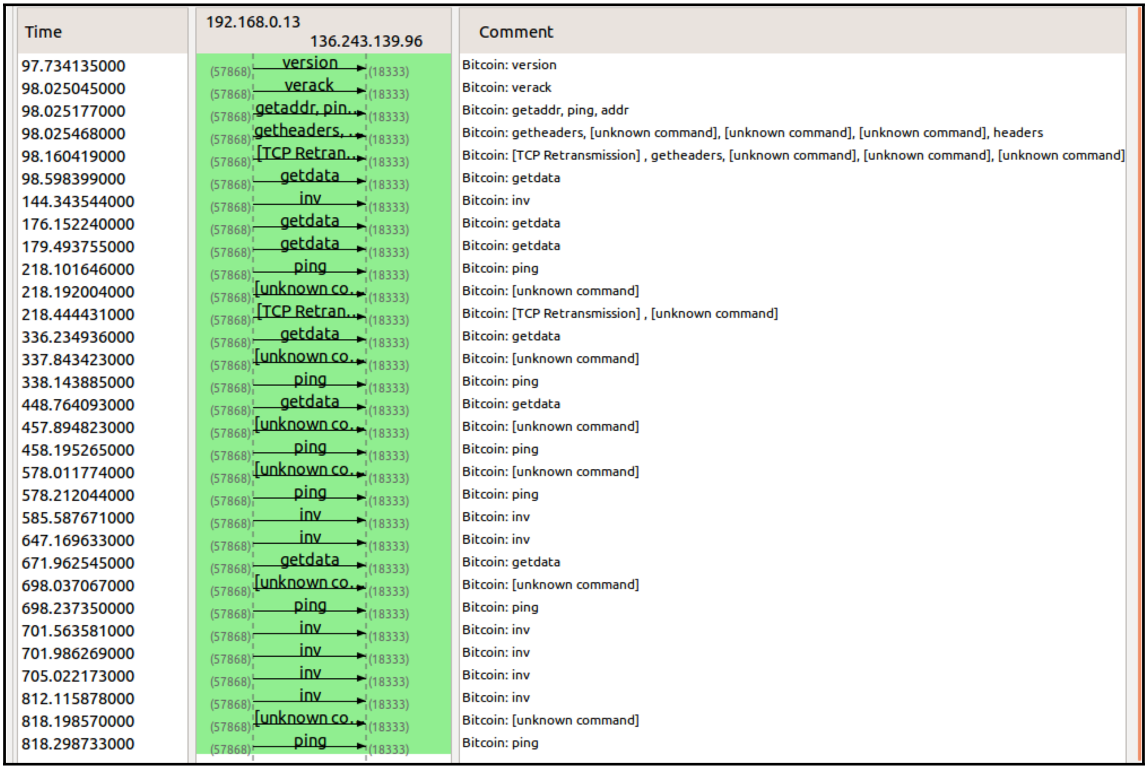
NODE A
NODE B
VERSION
VERSION
VERACK
VERACK
Get Addr, Ping, addr
addr


NODE A
NODE B
Sync Node
IBD Node
get Headers
Headers message
Multiple
get data
Multiple nodes
Multiple
blocks

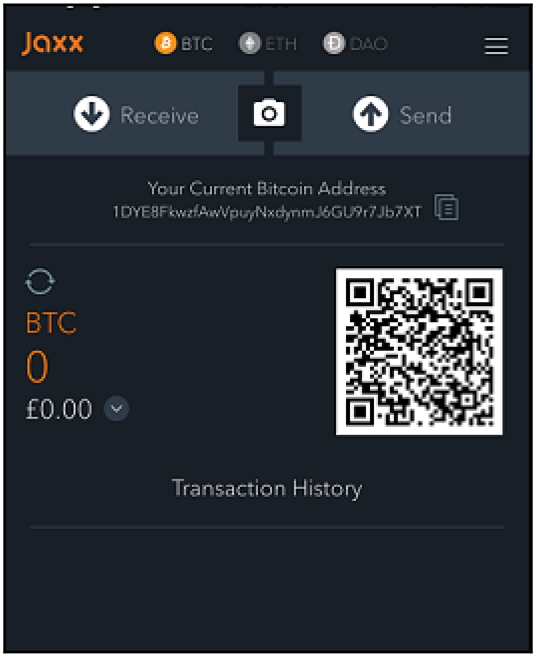


```
No.   Time            Source          Destination     Protocol Length Info
  131 98.598526000    192.168.0.13    52.1.165.219    Bitcoin     192 version
  150 99.180294000    192.168.0.13    52.1.165.219    Bitcoin      90 verack
  151 99.180421000    192.168.0.13    52.1.165.219    Bitcoin     122 getaddr, ping
  152 99.180715000    192.168.0.13    52.1.165.219    Bitcoin    1288 addr, getheaders[Malformed Packet]
  486 112.053746000   192.168.0.13    52.1.165.219    Bitcoin     127 inv
  818 143.630367000   192.168.0.13    52.1.165.219    Bitcoin     127 inv
 1004 178.729768000   192.168.0.13    52.1.165.219    Bitcoin     127 inv
```

```
▸ Transmission Control Protocol, Src Port: 52864 (52864), Dst Port: 18333 (18333), Seq: 207, Ack: 1291, Len: 1222
▾ Bitcoin protocol
    Packet magic: 0x0b110907
    Command name: addr
    Payload Length: 31
    Payload checksum: 0xa03fc07d
  ▾ Address message
      Count: 1
    ▾ Address: afbd0258000000000000000000000000000000000000ffff...
      ▾ Node services: 0x0000000000000000
          .... .... .... .... .... .... .... ...0 = Network node: Not set
        Node address: ::ffff:86.15.44.209 (::ffff:86.15.44.209)
        Node port: 18333
        Address timestamp: Oct 16, 2016 00:37:19.000000000 BST
▾ Bitcoin protocol
    Packet magic: 0x0b110907
    Command name: getheaders
    Payload Length: 1029
    Payload checksum: 0x4e54961d
  ▾ Getheaders message
      Count: 126
      Starting hash: 1101001f152142abccc039503abc56b149bd56c2b3925b65...
      Starting hash: 000000001980703bd53b0c7bf0ac995bccfeeffd5cddc780...
      Starting hash: 000000007ad1fed813d20301b1762895a2e5b08c8a58b3ea...
      Starting hash: 000000003624c451f726a3e983d02279d9c7cf672d36f1d5...
```

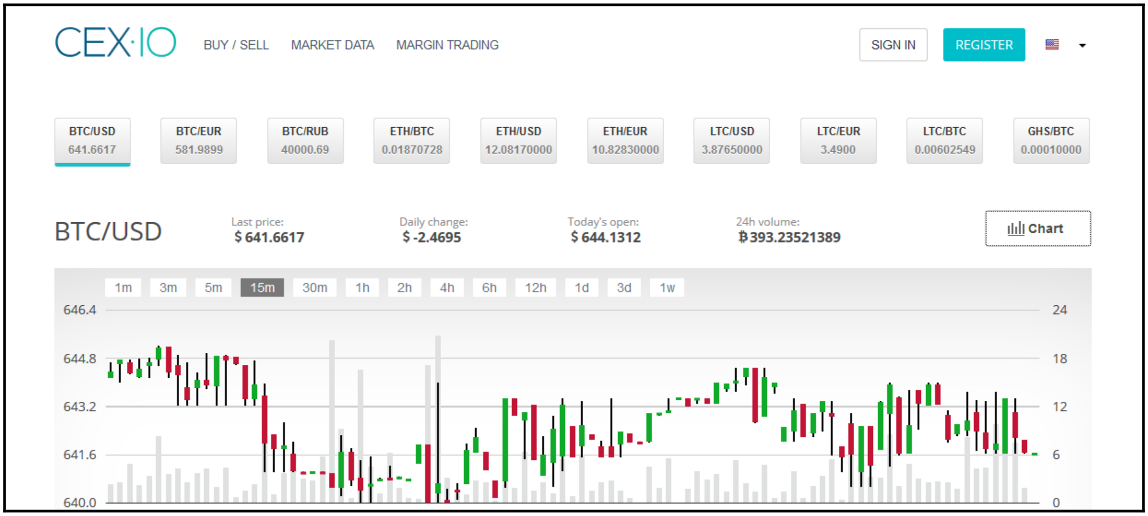


Time	192.168.0.13 136.243.139.96	Comment
97.734135000	(57868) version → (18333)	Bitcoin: version
98.025045000	(57868) verack → (18333)	Bitcoin: verack
98.025177000	(57868) getaddr, pin... → (18333)	Bitcoin: getaddr, ping, addr
98.025468000	(57868) getheaders, ... → (18333)	Bitcoin: getheaders, [unknown command], [unknown command], [unknown command], headers
98.160419000	(57868) [TCP Retran... → (18333)	Bitcoin: [TCP Retransmission] , getheaders, [unknown command], [unknown command], [unknown command]
98.598399000	(57868) getdata → (18333)	Bitcoin: getdata
144.343544000	(57868) inv → (18333)	Bitcoin: inv
176.152240000	(57868) getdata → (18333)	Bitcoin: getdata
179.493755000	(57868) getdata → (18333)	Bitcoin: getdata
218.101646000	(57868) ping → (18333)	Bitcoin: ping
218.192004000	(57868) [unknown co... → (18333)	Bitcoin: [unknown command]
218.444431000	(57868) [TCP Retran... → (18333)	Bitcoin: [TCP Retransmission] , [unknown command]
336.234936000	(57868) getdata → (18333)	Bitcoin: getdata
337.843423000	(57868) [unknown co... → (18333)	Bitcoin: [unknown command]
338.143885000	(57868) ping → (18333)	Bitcoin: ping
448.764093000	(57868) getdata → (18333)	Bitcoin: getdata
457.894823000	(57868) [unknown co... → (18333)	Bitcoin: [unknown command]
458.195265000	(57868) ping → (18333)	Bitcoin: ping
578.011774000	(57868) [unknown co... → (18333)	Bitcoin: [unknown command]
578.212044000	(57868) ping → (18333)	Bitcoin: ping
585.587671000	(57868) inv → (18333)	Bitcoin: inv
647.169633000	(57868) inv → (18333)	Bitcoin: inv
671.962545000	(57868) getdata → (18333)	Bitcoin: getdata
698.037067000	(57868) [unknown co... → (18333)	Bitcoin: [unknown command]
698.237350000	(57868) ping → (18333)	Bitcoin: ping
701.563581000	(57868) inv → (18333)	Bitcoin: inv
701.986269000	(57868) inv → (18333)	Bitcoin: inv
705.022173000	(57868) inv → (18333)	Bitcoin: inv
812.115878000	(57868) inv → (18333)	Bitcoin: inv
818.198570000	(57868) [unknown co... → (18333)	Bitcoin: [unknown command]
818.298733000	(57868) ping → (18333)	Bitcoin: ping



Your Current Bitcoin Address
1DYE8FkwzfAwVpuyNxdynmJ6GU9r7Jb7XT

BTC
0
£0.00



BTC/USD	BTC/EUR	BTC/RUB	ETH/BTC	ETH/USD	ETH/EUR	LTC/USD	LTC/EUR	LTC/BTC	GHS/BTC
641.6617	581.9899	40000.69	0.01870728	12.08170000	10.82830000	3.87650000	3.4900	0.00602549	0.00010000

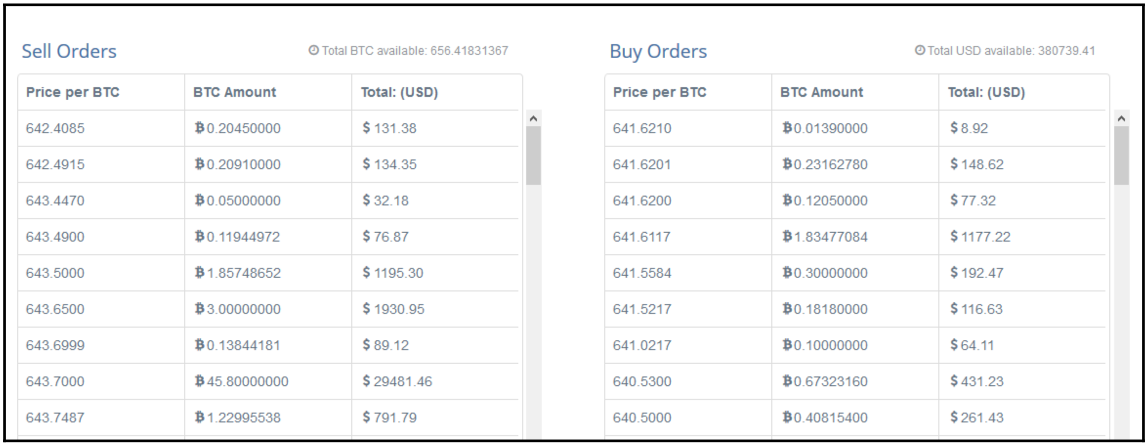
BTC/USD

Last price: $ 641.6617

Daily change: $ -2.4695

Today's open: $ 644.1312

24h volume: Ƀ393.23521389



Sell Orders

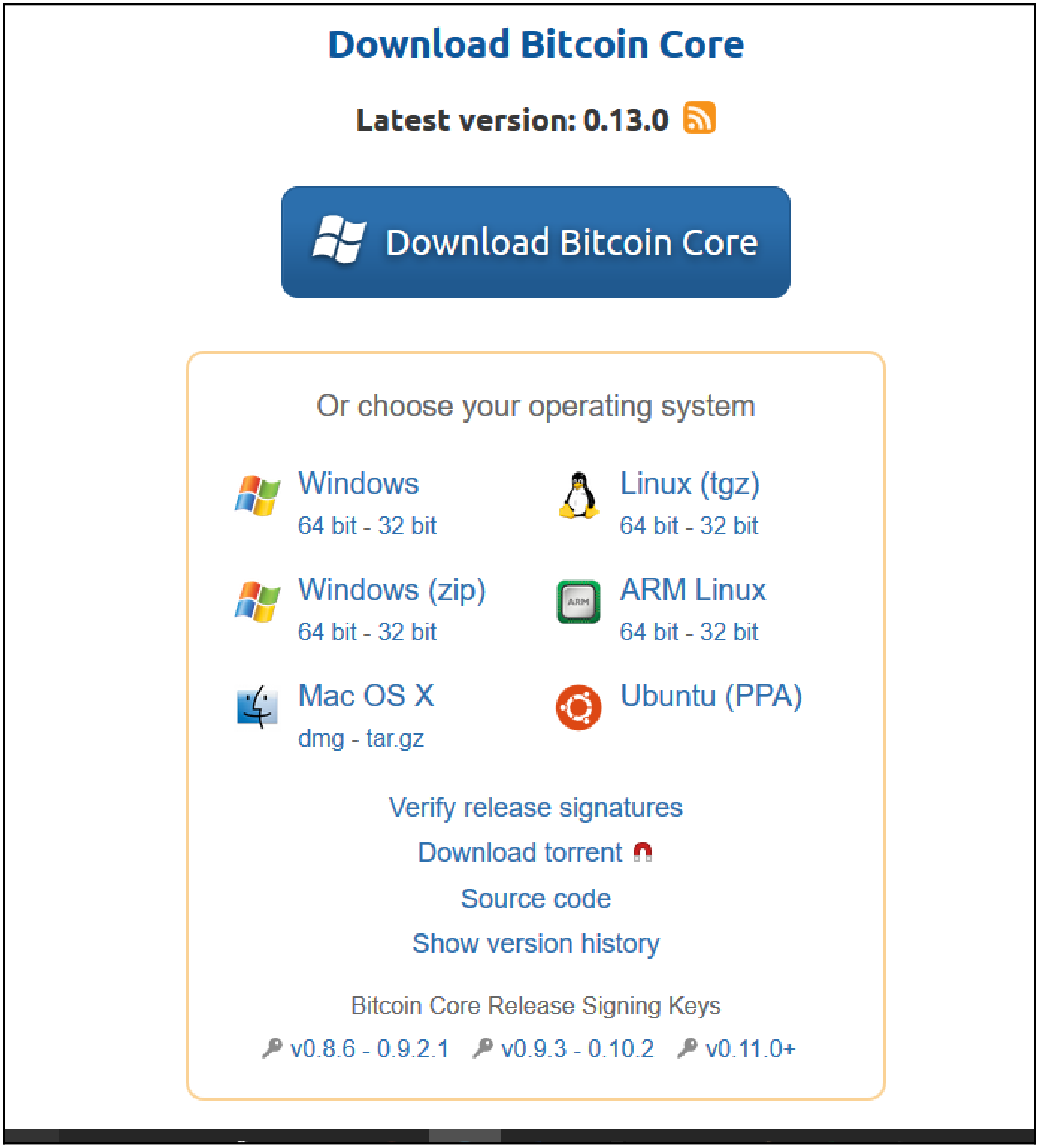
Total BTC available: 656.41831367

Price per BTC	BTC Amount	Total: (USD)
642.4085	₿0.20450000	$ 131.38
642.4915	₿0.20910000	$ 134.35
643.4470	₿0.05000000	$ 32.18
643.4900	₿0.11944972	$ 76.87
643.5000	₿1.85748652	$ 1195.30
643.6500	₿3.00000000	$ 1930.95
643.6999	₿0.13844181	$ 89.12
643.7000	₿45.80000000	$ 29481.46
643.7487	₿1.22995538	$ 791.79

Buy Orders

Total USD available: 380739.41

Price per BTC	BTC Amount	Total: (USD)
641.6210	₿0.01390000	$ 8.92
641.6201	₿0.23162780	$ 148.62
641.6200	₿0.12050000	$ 77.32
641.6117	₿1.83477084	$ 1177.22
641.5584	₿0.30000000	$ 192.47
641.5217	₿0.18180000	$ 116.63
641.0217	₿0.10000000	$ 64.11
640.5300	₿0.67323160	$ 431.23
640.5000	₿0.40815400	$ 261.43



Download Bitcoin Core

Latest version: 0.13.0

Or choose your operating system

Windows
64 bit - 32 bit

Linux (tgz)
64 bit - 32 bit

Windows (zip)
64 bit - 32 bit

ARM Linux
64 bit - 32 bit

Mac OS X
dmg - tar.gz

Ubuntu (PPA)

Verify release signatures

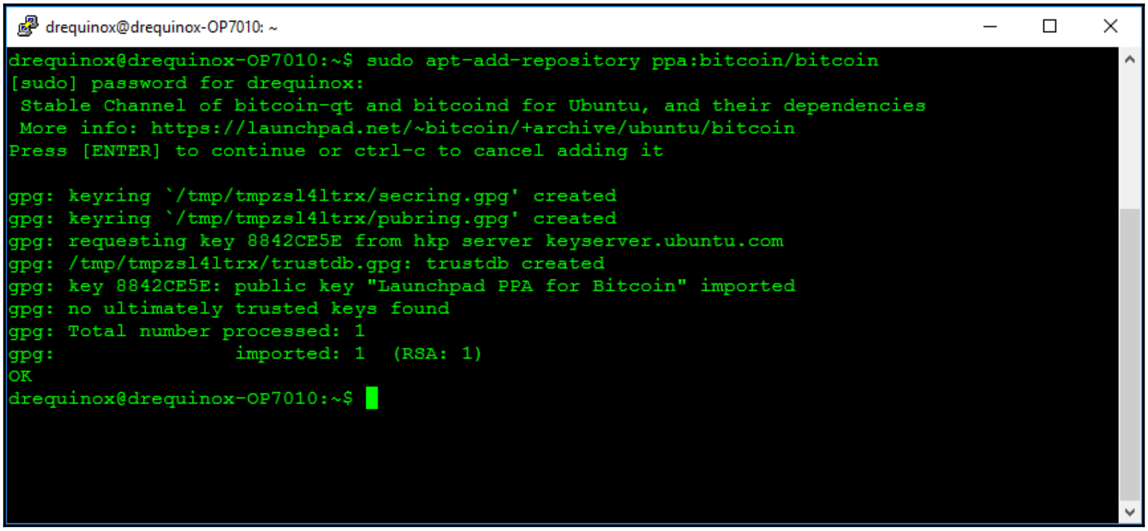
Download torrent

Source code

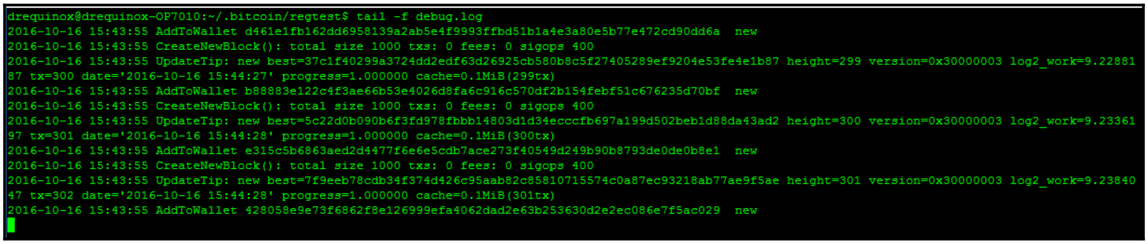
Show version history

Bitcoin Core Release Signing Keys

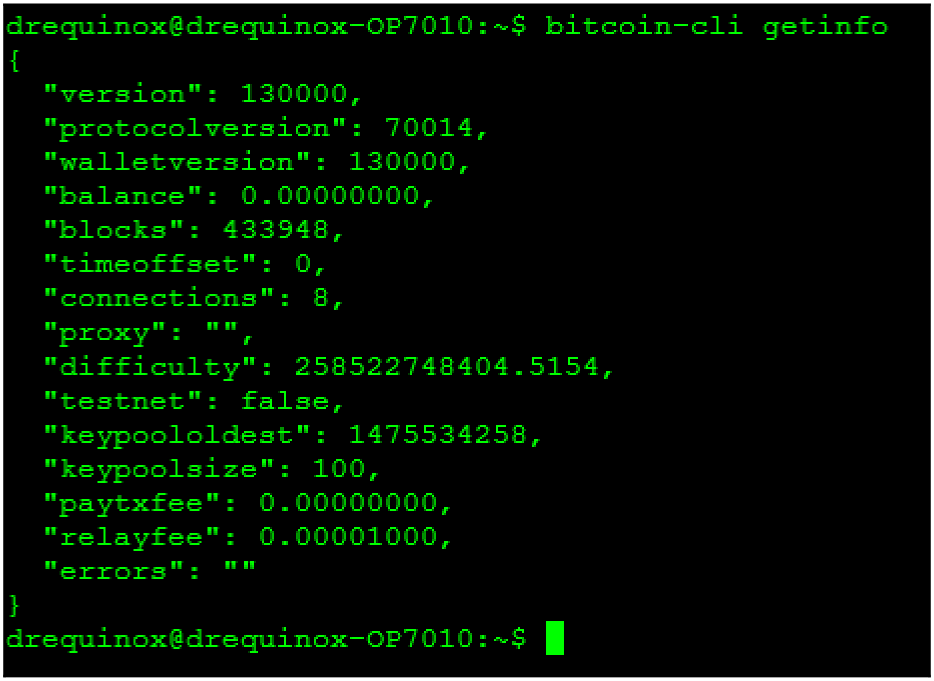
v0.8.6 - 0.9.2.1 v0.9.3 - 0.10.2 v0.11.0+



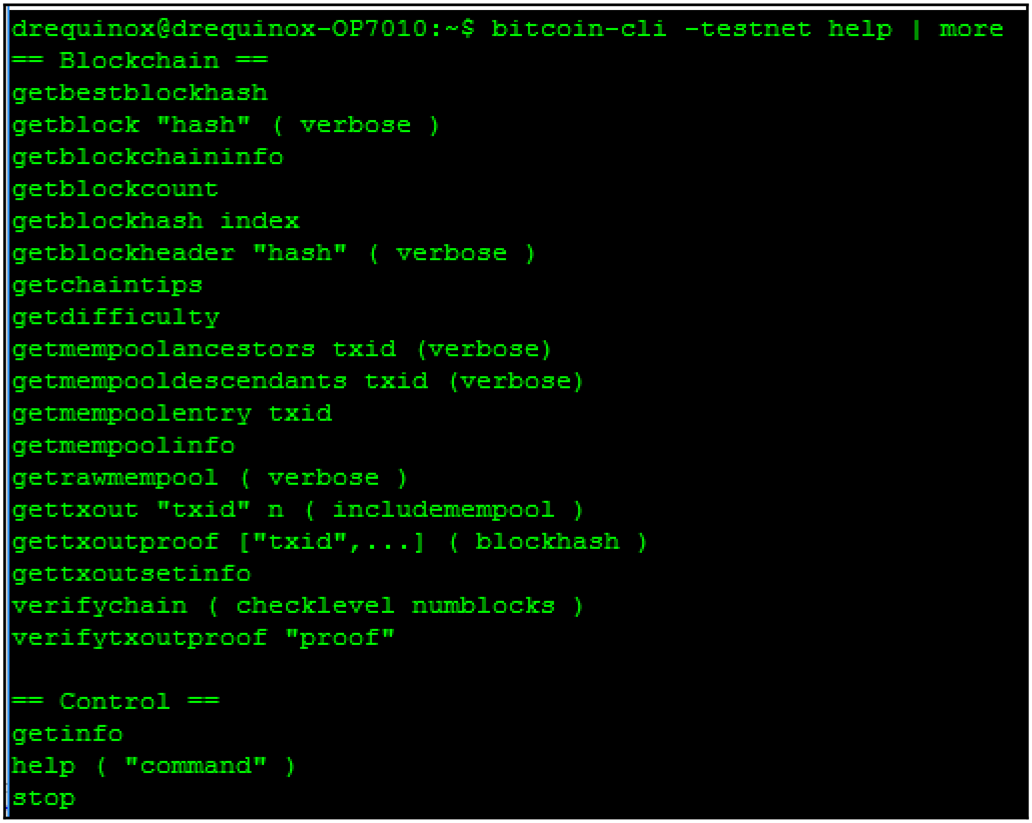
```
drequinox@drequinox-OP7010:~$ sudo apt-add-repository ppa:bitcoin/bitcoin
[sudo] password for drequinox:
 Stable Channel of bitcoin-qt and bitcoind for Ubuntu, and their dependencies
 More info: https://launchpad.net/~bitcoin/+archive/ubuntu/bitcoin
Press [ENTER] to continue or ctrl-c to cancel adding it

gpg: keyring `/tmp/tmpzsl4ltrx/secring.gpg' created
gpg: keyring `/tmp/tmpzsl4ltrx/pubring.gpg' created
gpg: requesting key 8842CE5E from hkp server keyserver.ubuntu.com
gpg: /tmp/tmpzsl4ltrx/trustdb.gpg: trustdb created
gpg: key 8842CE5E: public key "Launchpad PPA for Bitcoin" imported
gpg: no ultimately trusted keys found
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
OK
drequinox@drequinox-OP7010:~$
```



```
drequinox@drequinox-OP7010:~/.bitcoin/regtest$ tail -f debug.log
2016-10-16 15:43:55 AddToWallet d461e1fb162dd6958139a2ab5e4f9993ffbd51b1a4e3a80e5b77e472cd90dd6a  new
2016-10-16 15:43:55 CreateNewBlock(): total size 1000 txs: 0 fees: 0 sigops 400
2016-10-16 15:43:55 UpdateTip: new best=37c1f40299a3724dd2edf63d26925cb580b8c5f27405289ef9204e53fe4e1b87 height=299 version=0x30000003 log2_work=9.22881
87 tx=300 date='2016-10-16 15:44:27' progress=1.000000 cache=0.1MiB(299tx)
2016-10-16 15:43:55 AddToWallet b88883e122c4f3ae66b53e4026d8fa6c916c570df2b154febf51c676235d70bf  new
2016-10-16 15:43:55 CreateNewBlock(): total size 1000 txs: 0 fees: 0 sigops 400
2016-10-16 15:43:55 UpdateTip: new best=5c22d0b090b6f3fd978fbbb14803d1d34ecccfb697a199d502beb1d88da43ad2 height=300 version=0x30000003 log2_work=9.23361
97 tx=301 date='2016-10-16 15:44:28' progress=1.000000 cache=0.1MiB(300tx)
2016-10-16 15:43:55 AddToWallet e315c5b6863aed2d4477f6e6e5cdb7ace273f40549d249b90b8793de0de0b8e1  new
2016-10-16 15:43:55 CreateNewBlock(): total size 1000 txs: 0 fees: 0 sigops 400
2016-10-16 15:43:55 UpdateTip: new best=7f9eeb78cdb34f374d426c95aab82c85810715574c0a87ec93218ab77ae9f5ae height=301 version=0x30000003 log2_work=9.23840
47 tx=302 date='2016-10-16 15:44:28' progress=1.000000 cache=0.1MiB(301tx)
2016-10-16 15:43:55 AddToWallet 428058e9e73f6862f8e126999efa4062dad2e63b253630d2e2ec086e7f5ac029  new
```

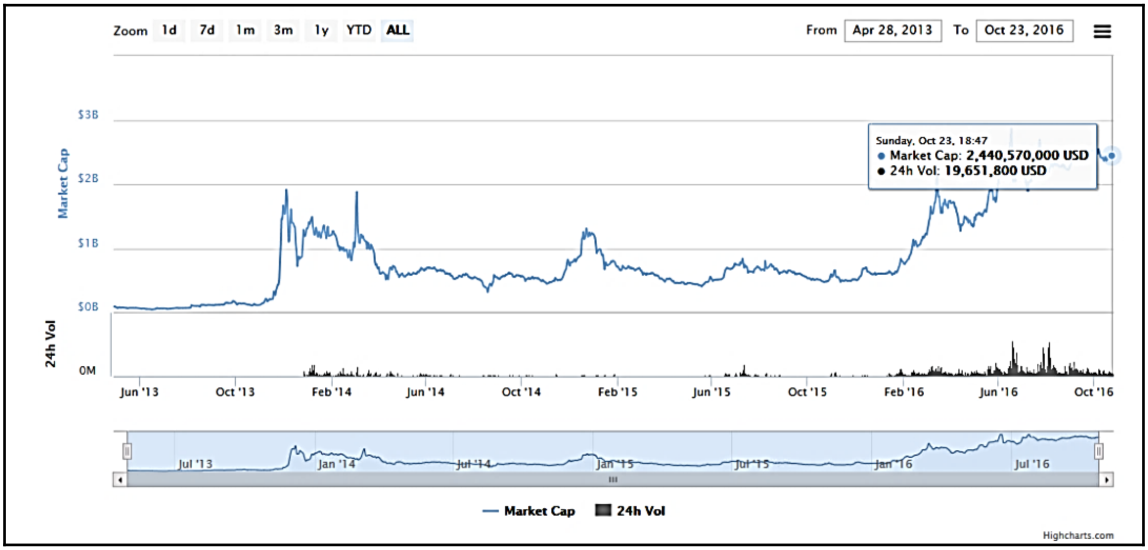


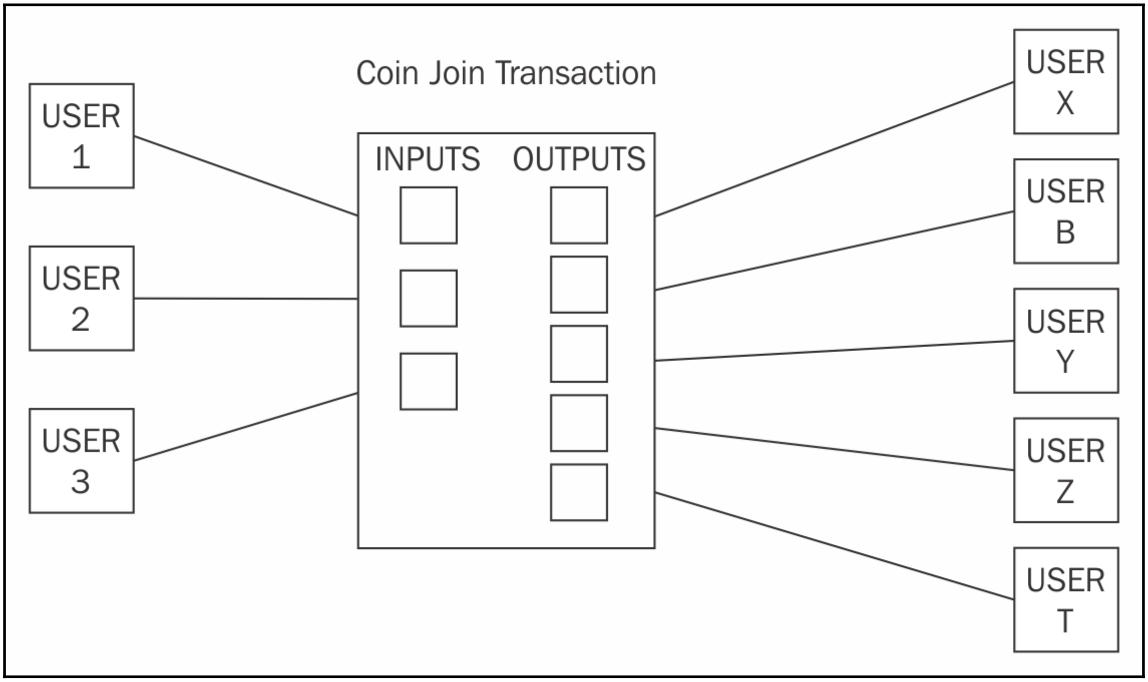
```
drequinox@drequinox-OP7010:~$ bitcoin-cli getinfo
{
  "version": 130000,
  "protocolversion": 70014,
  "walletversion": 130000,
  "balance": 0.00000000,
  "blocks": 433948,
  "timeoffset": 0,
  "connections": 8,
  "proxy": "",
  "difficulty": 258522748404.5154,
  "testnet": false,
  "keypoololdest": 1475534258,
  "keypoolsize": 100,
  "paytxfee": 0.00000000,
  "relayfee": 0.00001000,
  "errors": ""
}
drequinox@drequinox-OP7010:~$
```

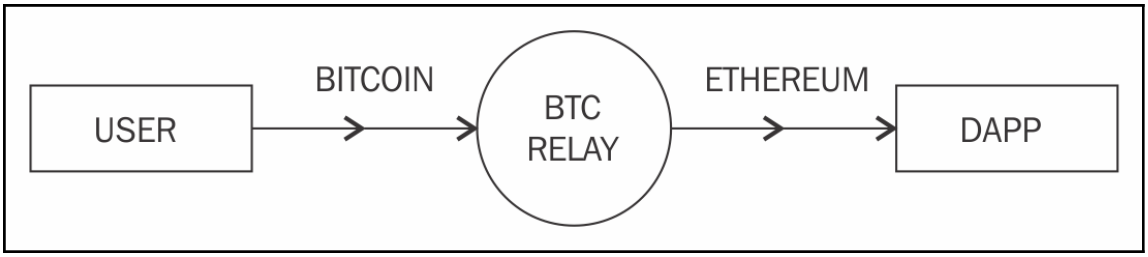


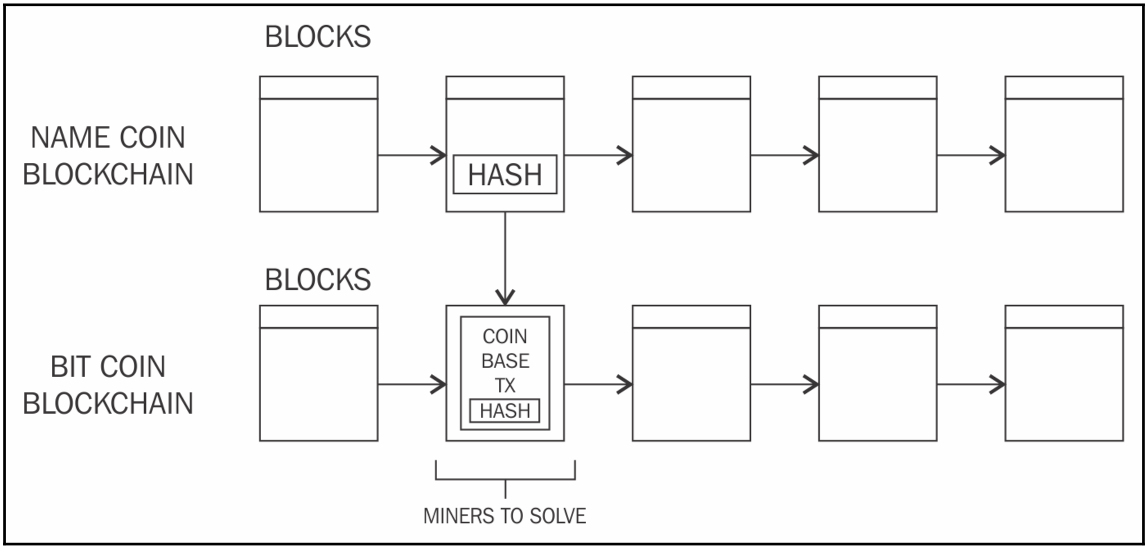
```
drequinox@drequinox-OP7010:~$ bitcoin-cli -testnet help | more
== Blockchain ==
getbestblockhash
getblock "hash" ( verbose )
getblockchaininfo
getblockcount
getblockhash index
getblockheader "hash" ( verbose )
getchaintips
getdifficulty
getmempoolancestors txid (verbose)
getmempooldescendants txid (verbose)
getmempoolentry txid
getmempoolinfo
getrawmempool ( verbose )
gettxout "txid" n ( includemempool )
gettxoutproof ["txid",...] ( blockhash )
gettxoutsetinfo
verifychain ( checklevel numblocks )
verifytxoutproof "proof"

== Control ==
getinfo
help ( "command" )
stop
```

Chapter 5: Alternative Coins

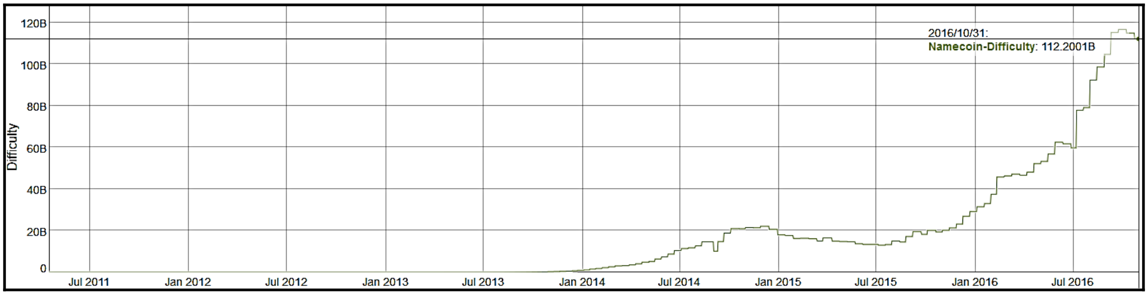



Coin Join Transaction
USER 1
USER 2
USER 3
INPUTS
OUTPUTS
USER X
USER B
USER Y
USER Z
USER T

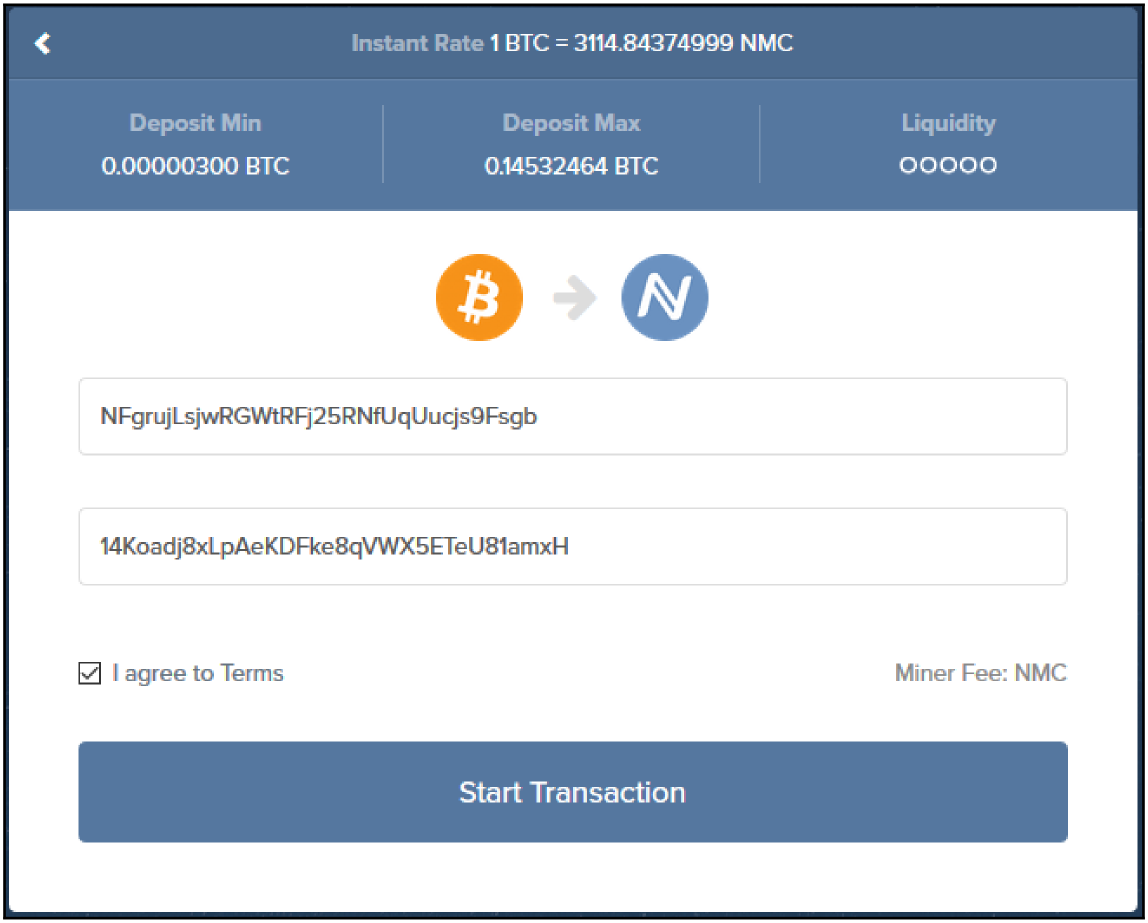

USER
BITCOIN
BTC RELAY
ETHEREUM
DAPP



BLOCKS
NAME COIN BLOCKCHAIN
HASH
BLOCKS
BIT COIN BLOCKCHAIN
COIN BASE TX
HASH
MINERS TO SOLVE



120B
100B
80B
60B
40B
20B
0
Difficulty
Jul 2011
Jan 2012
Jul 2012
Jan 2013
Jul 2013
Jan 2014
Jul 2014
Jan 2015
Jul 2015
Jan 2016
Jul 2016
2016/10/31:
Namecoin-Difficulty: 112.2001B



Instant Rate 1 BTC = 3114.84374999 NMC

Deposit Min 0.00000300 BTC

Deposit Max 0.14532464 BTC

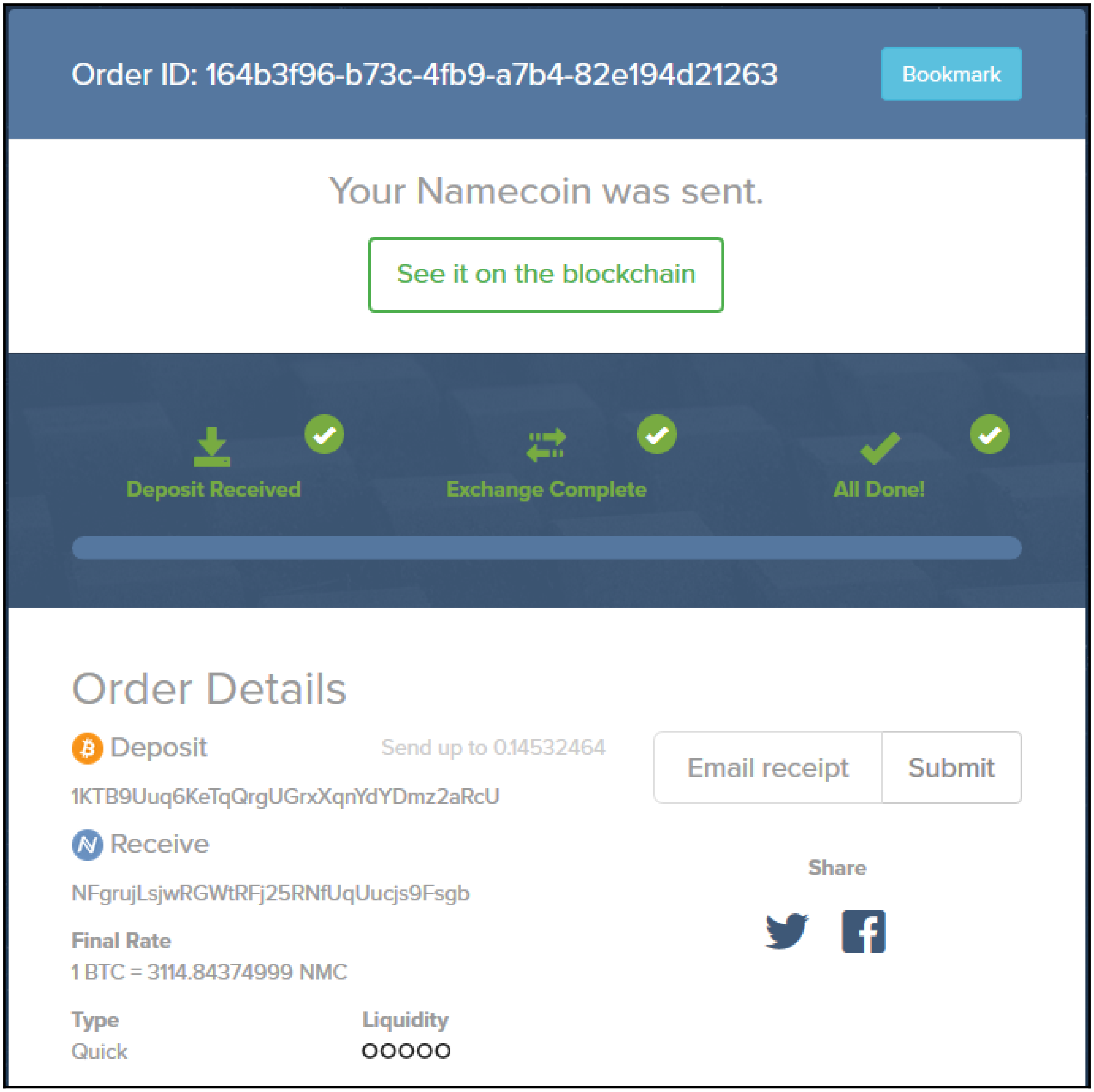
Liquidity ○○○○○

NFgrujLsjwRGWtRFj25RNfUqUucjs9Fsgb

14Koadj8xLpAeKDFke8qVWX5ETeU81amxH

☑ I agree to Terms

Miner Fee: NMC



Order ID: 164b3f96-b73c-4fb9-a7b4-82e194d21263

Your Namecoin was sent.

Order Details

Deposit Send up to 0.14532464

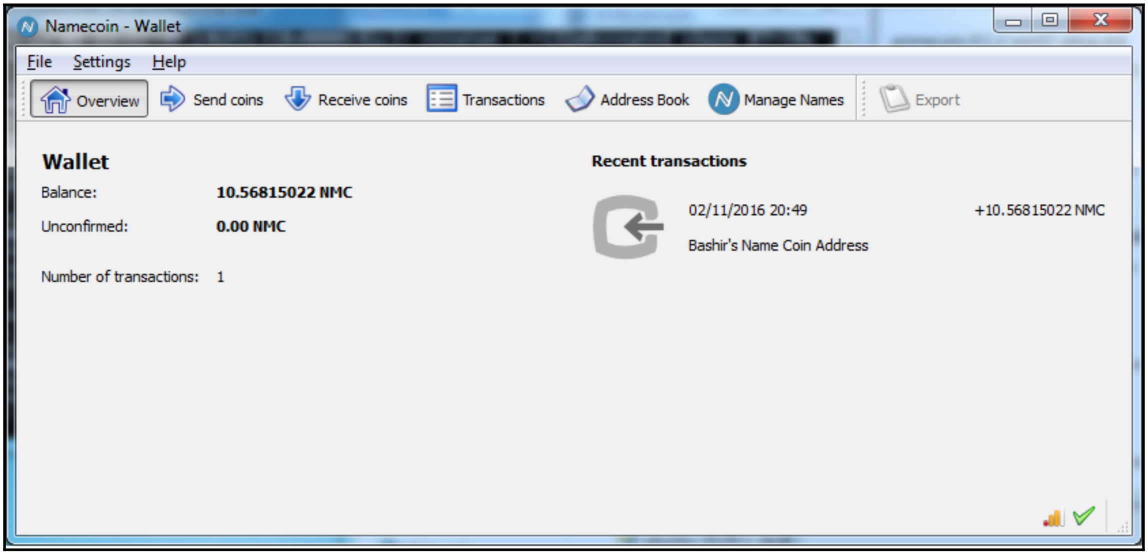
1KTB9Uuq6KeTqQrgUGrxXqnYdYDmz2aRcU

Receive

NFgrujLsjwRGWtRFj25RNfUqUucjs9Fsgb

Final Rate
1 BTC = 3114.84374999 NMC

Type	**Liquidity**
Quick	○○○○○



Wallet

Balance: 10.56815022 NMC

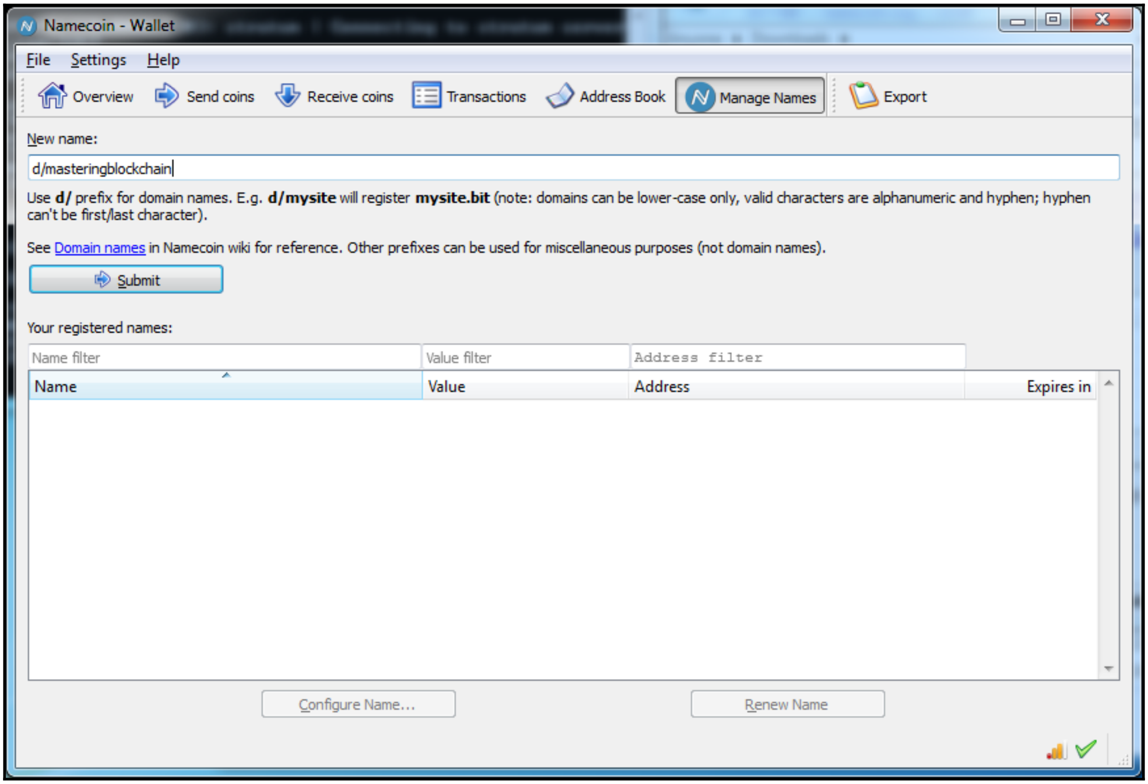
Unconfirmed: 0.00 NMC

Number of transactions: 1

Recent transactions

02/11/2016 20:49 +10.56815022 NMC

Bashir's Name Coin Address



New name:

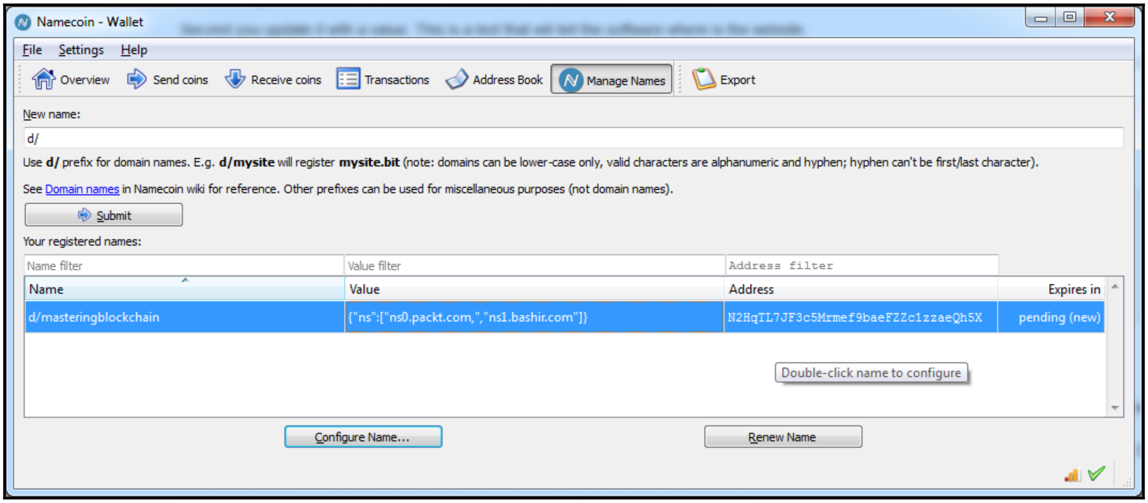
d/masteringblockchain

Use **d/** prefix for domain names. E.g. **d/mysite** will register **mysite.bit** (note: domains can be lower-case only, valid characters are alphanumeric and hyphen; hyphen can't be first/last character).

See Domain names in Namecoin wiki for reference. Other prefixes can be used for miscellaneous purposes (not domain names).

Your registered names:

Name	Value	Address	Expires in
Name filter	Value filter	Address filter	



New name:

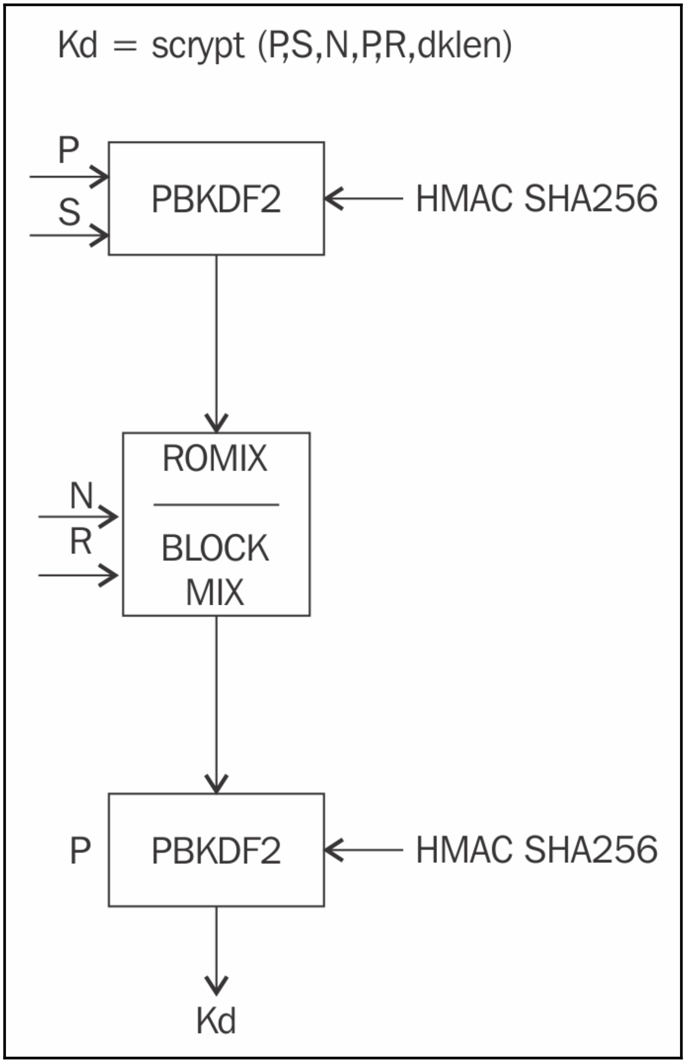
d/

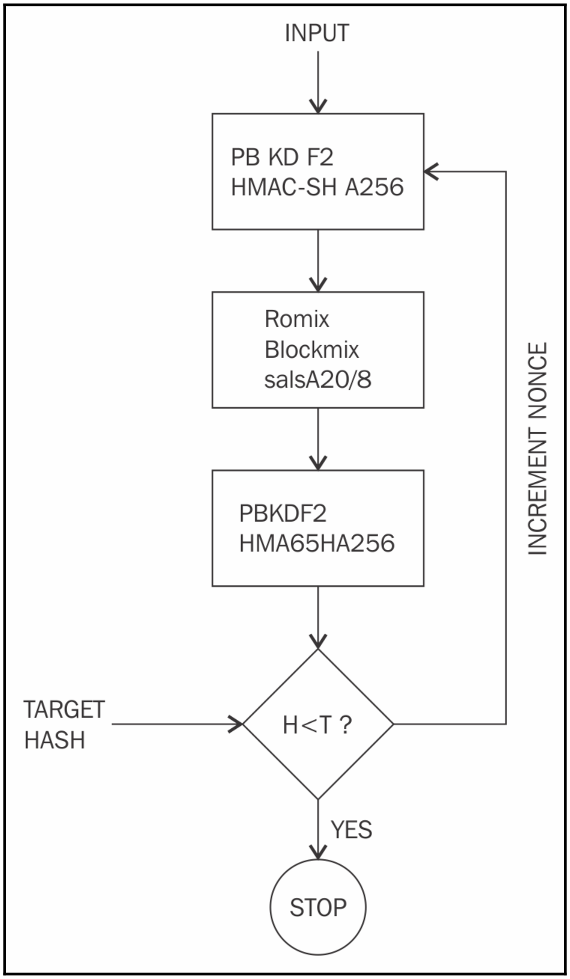
Use **d/** prefix for domain names. E.g. **d/mysite** will register **mysite.bit** (note: domains can be lower-case only, valid characters are alphanumeric and hyphen; hyphen can't be first/last character).

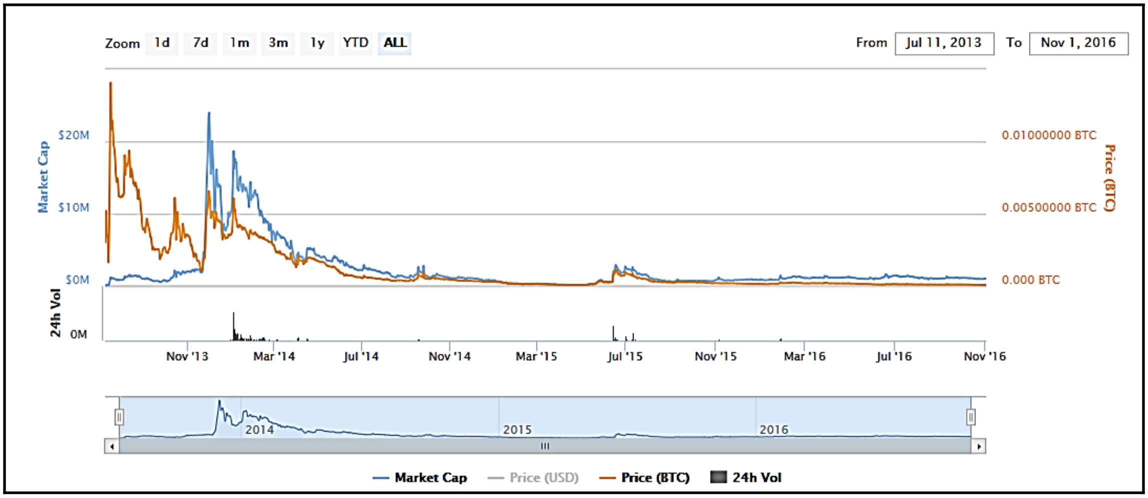
See Domain names in Namecoin wiki for reference. Other prefixes can be used for miscellaneous purposes (not domain names).

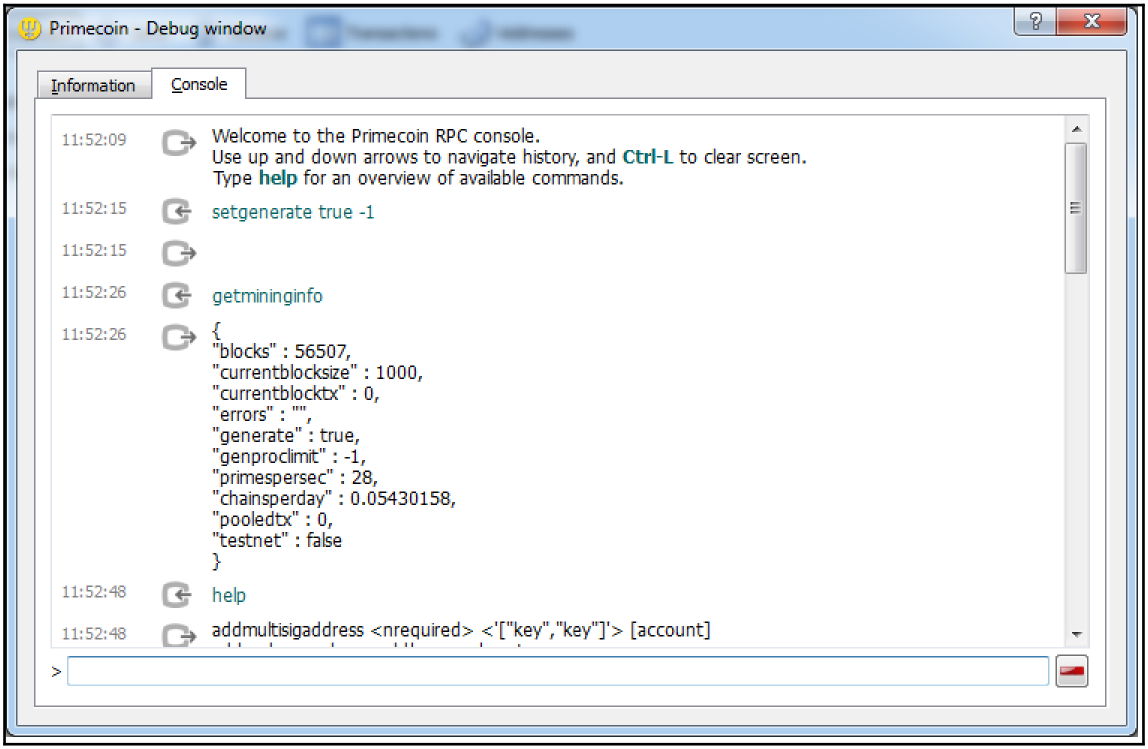
Your registered names:

Name	Value	Address	Expires in
d/masteringblockchain	{"ns":["ns0.packt.com,","ns1.bashir.com"]}	N2HqTL7JF3c5Mrmef9baeFZZc1zzaeQh5X	pending (new)

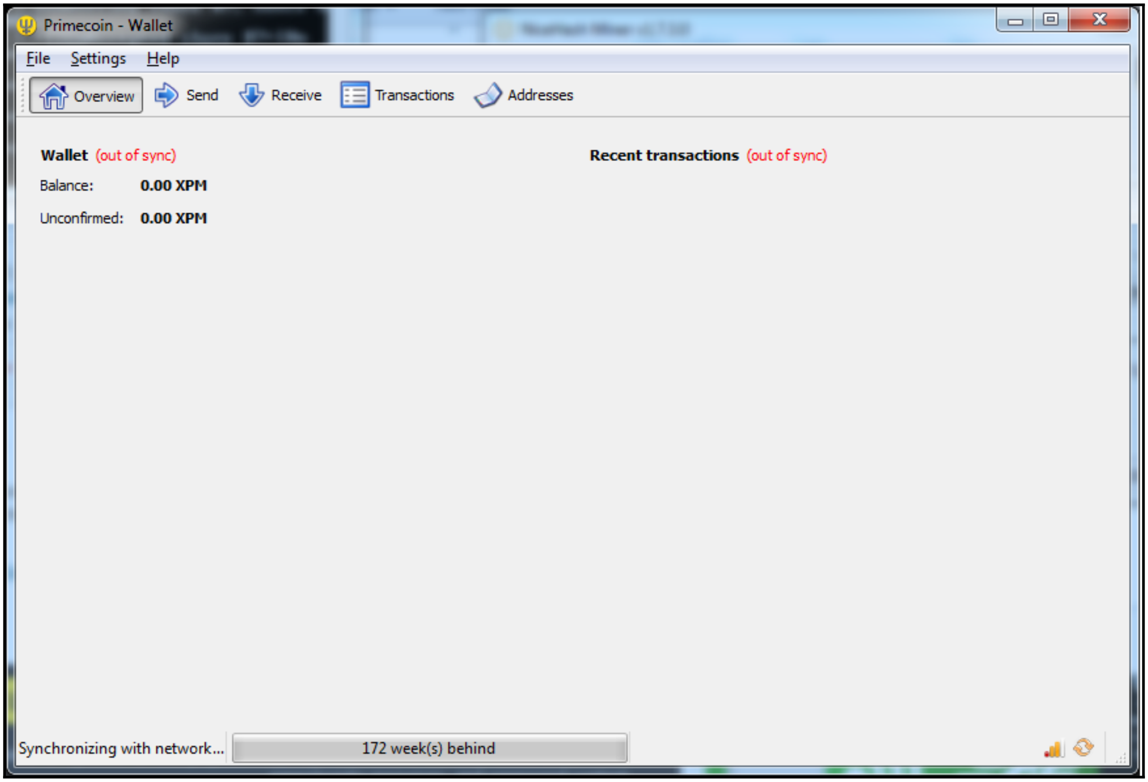

Kd = scrypt (P,S,N,P,R,dklen)
P
S
PBKDF2
HMAC SHA256
ROMIX
N
R
BLOCK
MIX
P
PBKDF2
HMAC SHA256
Kd


INPUT
PB KD F2
HMAC-SH A256
Romix
Blockmix
salsA20/8
PBKDF2
HMA65HA256
INCREMENT NONCE
TARGET
HASH
H<T ?
YES
STOP





```
11:52:09    Welcome to the Primecoin RPC console.
            Use up and down arrows to navigate history, and Ctrl-L to clear screen.
            Type help for an overview of available commands.
11:52:15    setgenerate true -1
11:52:15
11:52:26    getmininginfo
11:52:26    {
            "blocks" : 56507,
            "currentblocksize" : 1000,
            "currentblocktx" : 0,
            "errors" : "",
            "generate" : true,
            "genproclimit" : -1,
            "primespersec" : 28,
            "chainsperday" : 0.05430158,
            "pooledtx" : 0,
            "testnet" : false
            }
11:52:48    help
11:52:48    addmultisigaddress <nrequired> <'["key","key"]'> [account]
```



Primecoin - Wallet

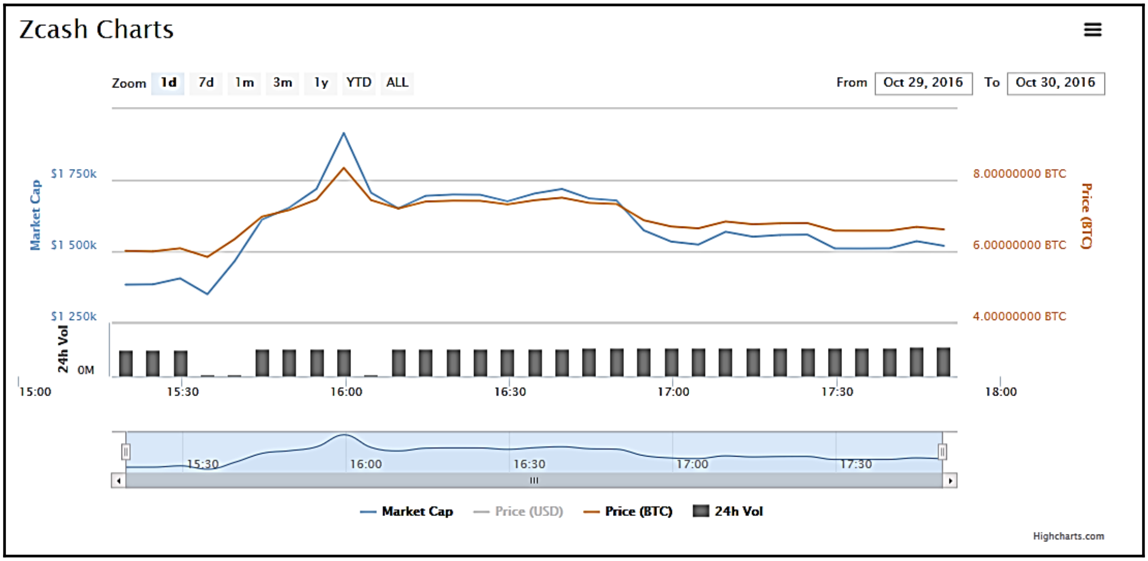
Wallet (out of sync)

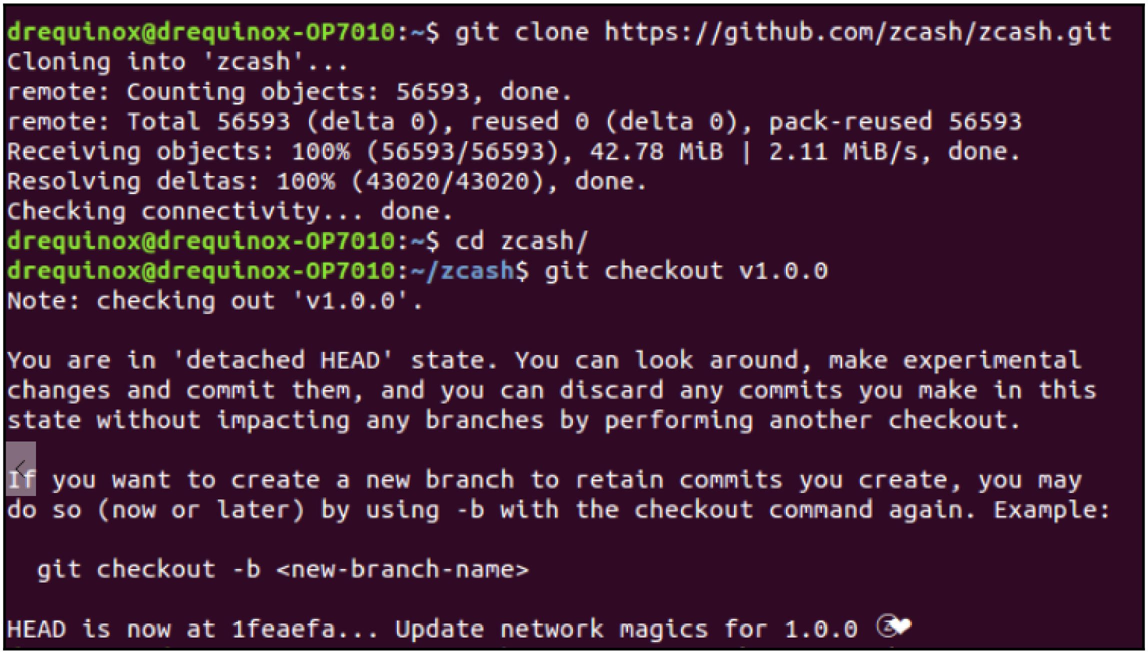
Balance: **0.00 XPM**

Unconfirmed: **0.00 XPM**

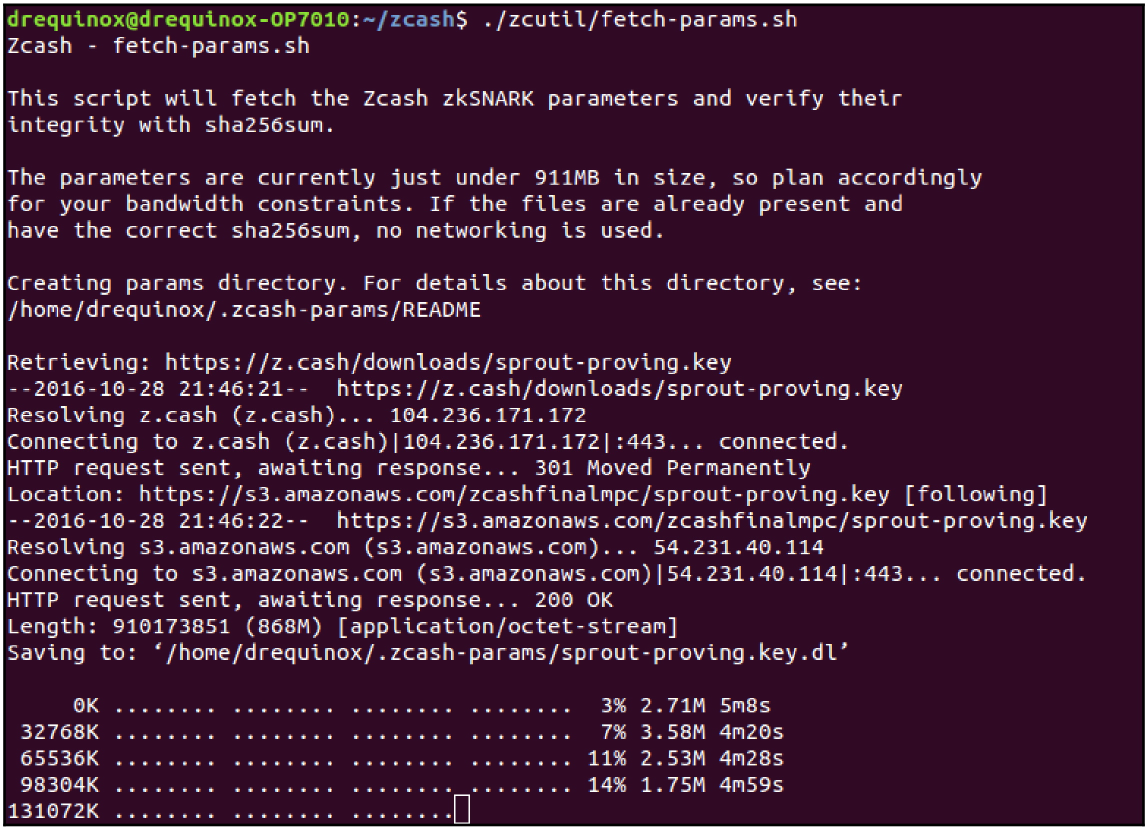
Recent transactions (out of sync)

Synchronizing with network... 172 week(s) behind

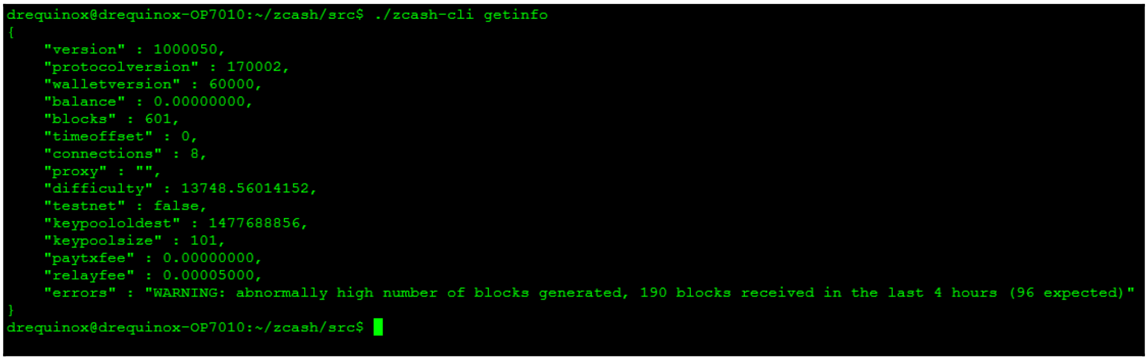




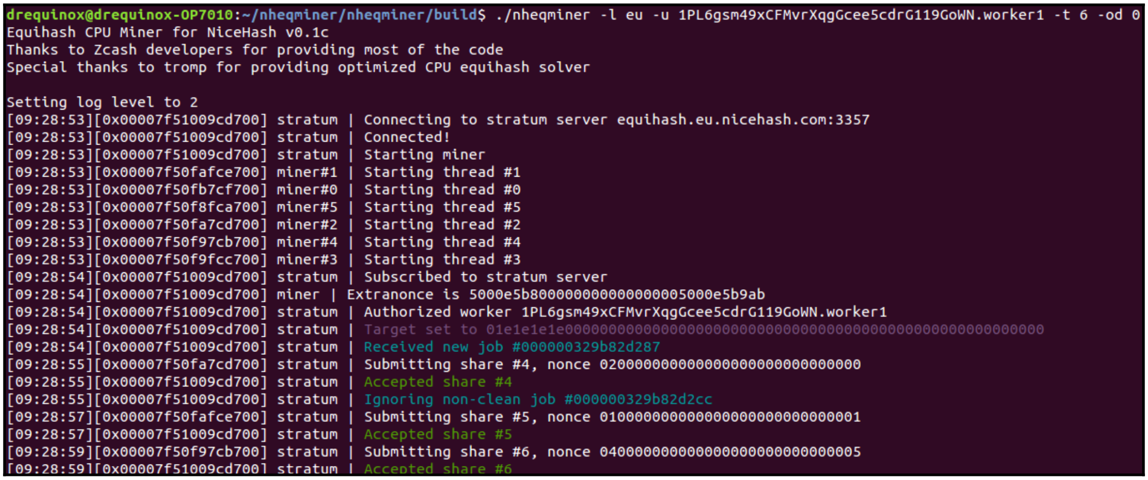
```
drequinox@drequinox-OP7010:~$ git clone https://github.com/zcash/zcash.git
Cloning into 'zcash'...
remote: Counting objects: 56593, done.
remote: Total 56593 (delta 0), reused 0 (delta 0), pack-reused 56593
Receiving objects: 100% (56593/56593), 42.78 MiB | 2.11 MiB/s, done.
Resolving deltas: 100% (43020/43020), done.
Checking connectivity... done.
drequinox@drequinox-OP7010:~$ cd zcash/
drequinox@drequinox-OP7010:~/zcash$ git checkout v1.0.0
Note: checking out 'v1.0.0'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by performing another checkout.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -b with the checkout command again. Example:

  git checkout -b <new-branch-name>

HEAD is now at 1feaefa... Update network magics for 1.0.0
```



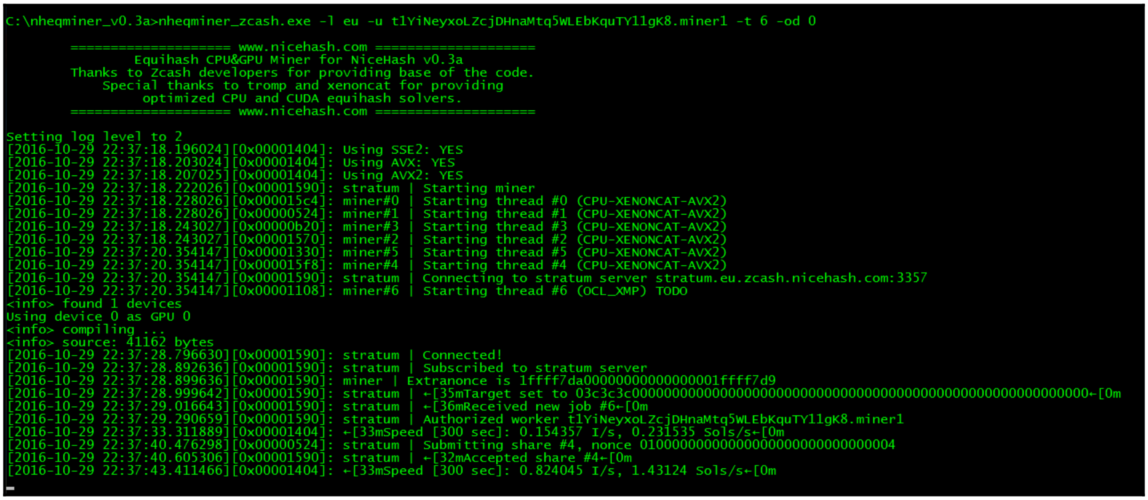
```
drequinox@drequinox-OP7010:~/zcash$ ./zcutil/fetch-params.sh
Zcash - fetch-params.sh

This script will fetch the Zcash zkSNARK parameters and verify their
integrity with sha256sum.

The parameters are currently just under 911MB in size, so plan accordingly
for your bandwidth constraints. If the files are already present and
have the correct sha256sum, no networking is used.

Creating params directory. For details about this directory, see:
/home/drequinox/.zcash-params/README

Retrieving: https://z.cash/downloads/sprout-proving.key
--2016-10-28 21:46:21--  https://z.cash/downloads/sprout-proving.key
Resolving z.cash (z.cash)... 104.236.171.172
Connecting to z.cash (z.cash)|104.236.171.172|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://s3.amazonaws.com/zcashfinalmpc/sprout-proving.key [following]
--2016-10-28 21:46:22--  https://s3.amazonaws.com/zcashfinalmpc/sprout-proving.key
Resolving s3.amazonaws.com (s3.amazonaws.com)... 54.231.40.114
Connecting to s3.amazonaws.com (s3.amazonaws.com)|54.231.40.114|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 910173851 (868M) [application/octet-stream]
Saving to: ‘/home/drequinox/.zcash-params/sprout-proving.key.dl’

     0K ........ ........ ........ ........  3% 2.71M 5m8s
 32768K ........ ........ ........ ........  7% 3.58M 4m20s
 65536K ........ ........ ........ ........ 11% 2.53M 4m28s
 98304K ........ ........ ........ ........ 14% 1.75M 4m59s
131072K ........ ........ ........
```



```
drequinox@drequinox-OP7010:~/zcash/src$ ./zcash-cli getinfo
{
    "version" : 1000050,
    "protocolversion" : 170002,
    "walletversion" : 60000,
    "balance" : 0.00000000,
    "blocks" : 601,
    "timeoffset" : 0,
    "connections" : 8,
    "proxy" : "",
    "difficulty" : 13748.56014152,
    "testnet" : false,
    "keypoololdest" : 1477688856,
    "keypoolsize" : 101,
    "paytxfee" : 0.00000000,
    "relayfee" : 0.00005000,
    "errors" : "WARNING: abnormally high number of blocks generated, 190 blocks received in the last 4 hours (96 expected)"
}
drequinox@drequinox-OP7010:~/zcash/src$
```

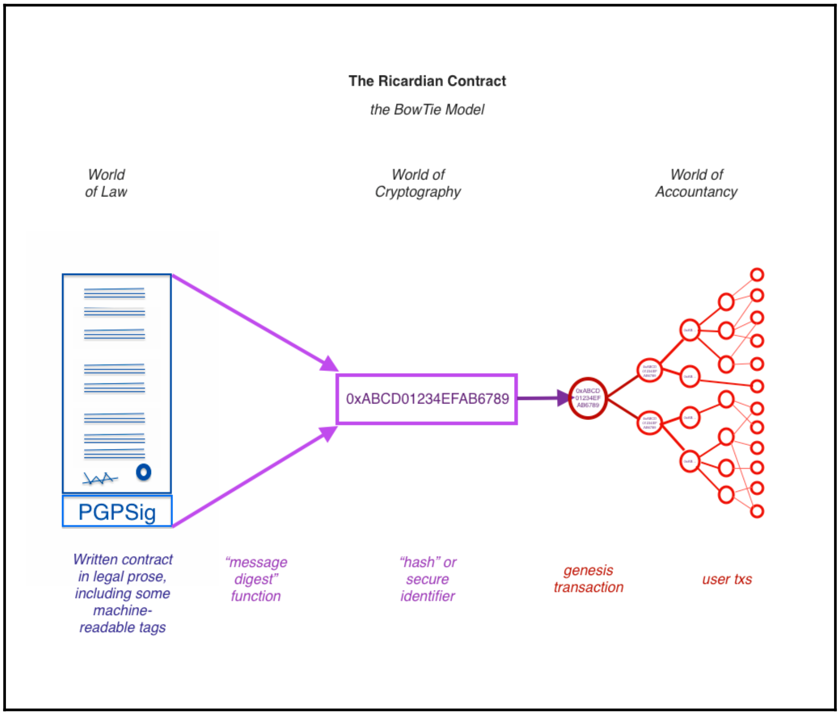


```
drequinox@drequinox-OP7010:~/nheqminer/nheqminer/build$ ./nheqminer -l eu -u 1PL6gsm49xCFMvrXqgGcee5cdrG119GoWN.worker1 -t 6 -od 0
Equihash CPU Miner for NiceHash v0.1c
Thanks to Zcash developers for providing most of the code
Special thanks to tromp for providing optimized CPU equihash solver

Setting log level to 2
[09:28:53][0x00007f51009cd700] stratum | Connecting to stratum server equihash.eu.nicehash.com:3357
[09:28:53][0x00007f51009cd700] stratum | Connected!
[09:28:53][0x00007f51009cd700] stratum | Starting miner
[09:28:53][0x00007f50fafce700] miner#1 | Starting thread #1
[09:28:53][0x00007f50fb7cf700] miner#0 | Starting thread #0
[09:28:53][0x00007f50f8fca700] miner#5 | Starting thread #5
[09:28:53][0x00007f50fa7cd700] miner#2 | Starting thread #2
[09:28:53][0x00007f50f97cb700] miner#4 | Starting thread #4
[09:28:53][0x00007f50f9fcc700] miner#3 | Starting thread #3
[09:28:54][0x00007f51009cd700] stratum | Subscribed to stratum server
[09:28:54][0x00007f51009cd700] miner | Extranonce is 5000e5b800000000000000005000e5b9ab
[09:28:54][0x00007f51009cd700] stratum | Authorized worker 1PL6gsm49xCFMvrXqgGcee5cdrG119GoWN.worker1
[09:28:54][0x00007f51009cd700] stratum | Target set to 01e1e1e1e0000000000000000000000000000000000000000000000000000000
[09:28:54][0x00007f51009cd700] stratum | Received new job #000000329b82d287
[09:28:55][0x00007f50fa7cd700] stratum | Submitting share #4, nonce 020000000000000000000000000000
[09:28:55][0x00007f51009cd700] stratum | Accepted share #4
[09:28:55][0x00007f51009cd700] stratum | Ignoring non-clean job #000000329b82d2cc
[09:28:57][0x00007f50fafce700] stratum | Submitting share #5, nonce 010000000000000000000000000001
[09:28:57][0x00007f51009cd700] stratum | Accepted share #5
[09:28:59][0x00007f50f97cb700] stratum | Submitting share #6, nonce 040000000000000000000000000005
[09:28:59][0x00007f51009cd700] stratum | Accepted share #6
```



```
C:\nheqminer_v0.3a>nheqminer_zcash.exe -l eu -u t1YiNeyxoLZcjDHnaMtq5WLEbKquTY11gK8.miner1 -t 6 -od 0

        ==================== www.nicehash.com ====================
                Equihash CPU&GPU Miner for NiceHash v0.3a
        Thanks to Zcash developers for providing base of the code.
            Special thanks to tromp and xenoncat for providing
                 optimized CPU and CUDA equihash solvers.
        ==================== www.nicehash.com ====================

Setting log level to 2
[2016-10-29 22:37:18.196024][0x00001404]: Using SSE2: YES
[2016-10-29 22:37:18.203024][0x00001404]: Using AVX: YES
[2016-10-29 22:37:18.207025][0x00001404]: Using AVX2: YES
[2016-10-29 22:37:18.222026][0x00001590]: stratum | Starting miner
[2016-10-29 22:37:18.228026][0x000015c4]: miner#0 | Starting thread #0 (CPU-XENONCAT-AVX2)
[2016-10-29 22:37:18.228026][0x00000524]: miner#1 | Starting thread #1 (CPU-XENONCAT-AVX2)
[2016-10-29 22:37:18.243027][0x00000b20]: miner#3 | Starting thread #3 (CPU-XENONCAT-AVX2)
[2016-10-29 22:37:18.243027][0x00001570]: miner#2 | Starting thread #2 (CPU-XENONCAT-AVX2)
[2016-10-29 22:37:20.354147][0x00001330]: miner#5 | Starting thread #5 (CPU-XENONCAT-AVX2)
[2016-10-29 22:37:20.354147][0x000015f8]: miner#4 | Starting thread #4 (CPU-XENONCAT-AVX2)
[2016-10-29 22:37:20.354147][0x00001590]: stratum | Connecting to stratum server stratum.eu.zcash.nicehash.com:3357
[2016-10-29 22:37:20.354147][0x00001108]: miner#6 | Starting thread #6 (OCL_XMP) TODO
<info> found 1 devices
Using device 0 as GPU 0
<info> compiling ...
<info> source: 41162 bytes
[2016-10-29 22:37:28.796630][0x00001590]: stratum | Connected!
[2016-10-29 22:37:28.892636][0x00001590]: stratum | Subscribed to stratum server
[2016-10-29 22:37:28.899636][0x00001590]: miner | Extranonce is 1ffff7da00000000000000001ffff7d9
[2016-10-29 22:37:28.999642][0x00001590]: stratum | ←[35mTarget set to 03c3c3c000000000000000000000000000000000000000000000000000000000←[0m
[2016-10-29 22:37:29.016643][0x00001590]: stratum | ←[36mReceived new job #6←[0m
[2016-10-29 22:37:29.290659][0x00001590]: stratum | Authorized worker t1YiNeyxoLZcjDHnaMtq5WLEbKquTY11gK8.miner1
[2016-10-29 22:37:33.311889][0x00001404]: ←[33mSpeed [300 sec]: 0.154357 I/s, 0.231535 Sols/s←[0m
[2016-10-29 22:37:40.476298][0x00000524]: stratum | Submitting share #4, nonce 01000000000000000000000000000004
[2016-10-29 22:37:40.605306][0x00001590]: stratum | ←[32mAccepted share #4←[0m
[2016-10-29 22:37:43.411466][0x00001404]: ←[33mSpeed [300 sec]: 0.824045 I/s, 1.43124 Sols/s←[0m
```

Chapter 6: Smart Contracts



The Ricardian Contract

the BowTie Model

World of Law

World of Cryptography

World of Accountancy

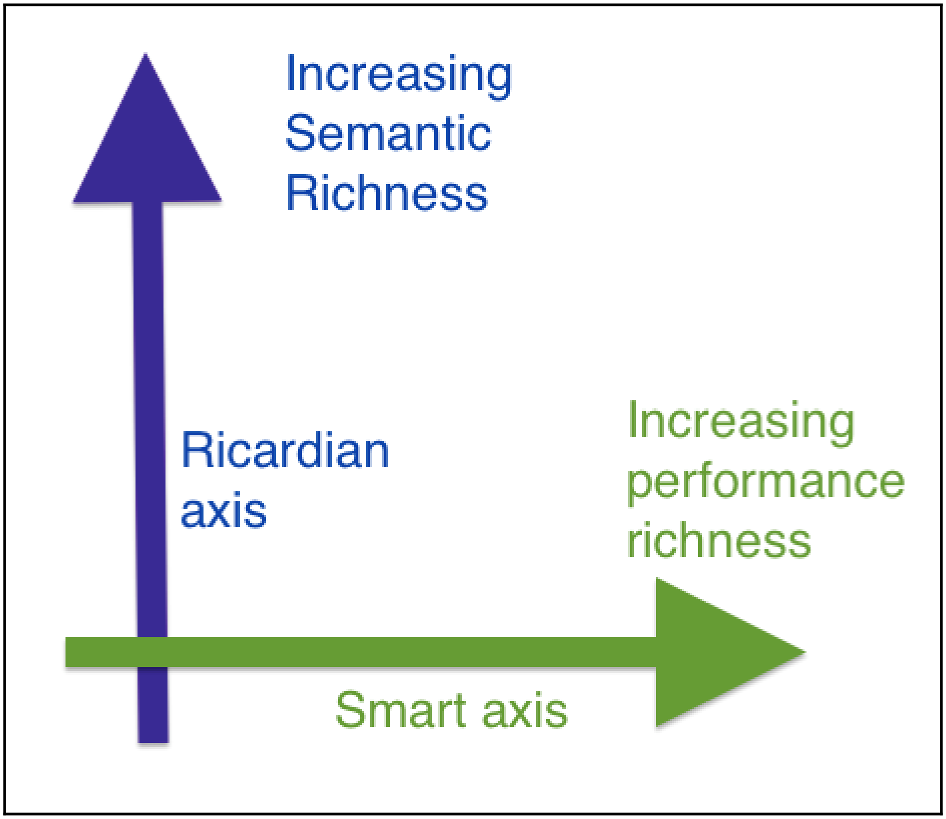
Written contract in legal prose, including some machine-readable tags

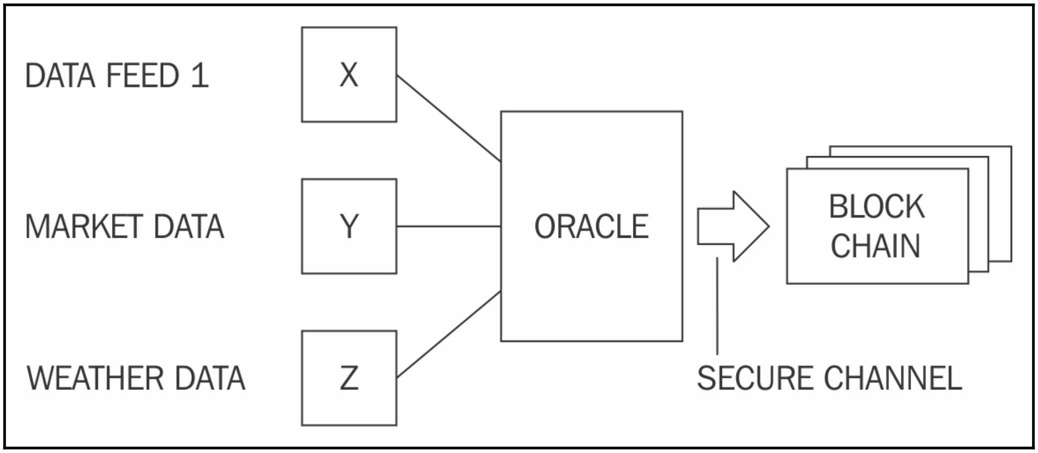
"message digest" function

"hash" or secure identifier

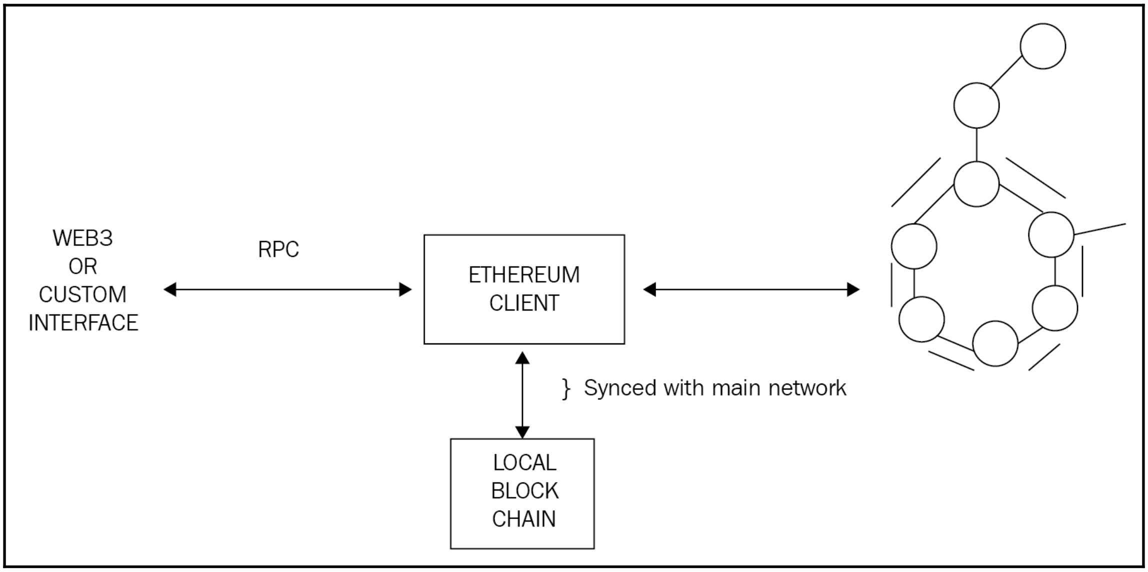
genesis transaction

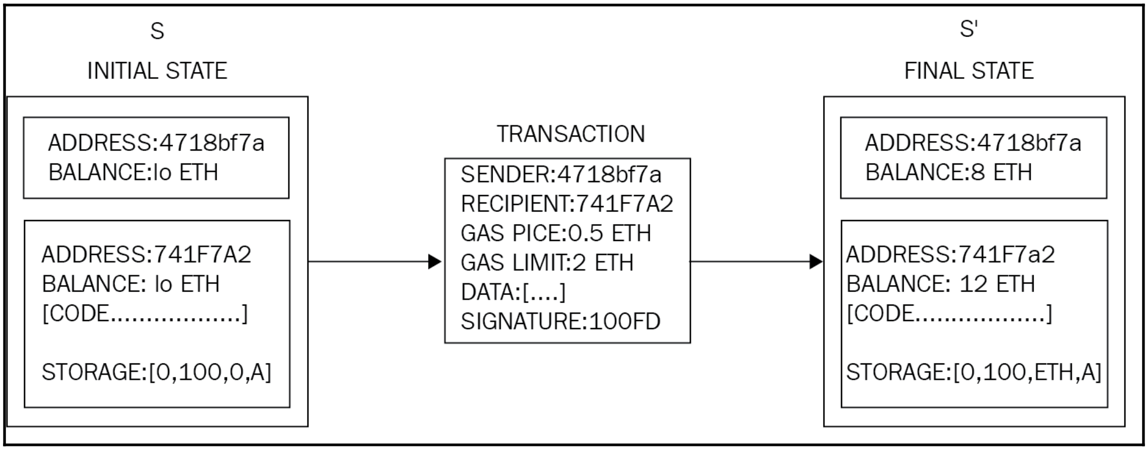
user txs


Increasing
Semantic
Richness
Ricardian
axis
Increasing
performance
richness
Smart axis


DATA FEED 1
X
MARKET DATA
Y
WEATHER DATA
Z
ORACLE
BLOCK
CHAIN
SECURE CHANNEL

Chapter 7: Ethereum 101





ADDRESS:4718bf7a
BALANCE:lo ETH

ADDRESS:741F7A2
BALANCE: lo ETH
[CODE..................]

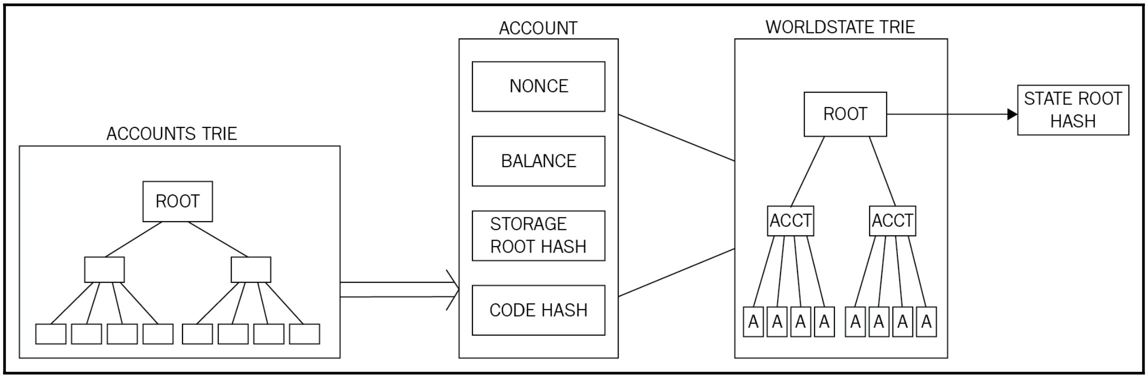
STORAGE:[0,100,0,A]

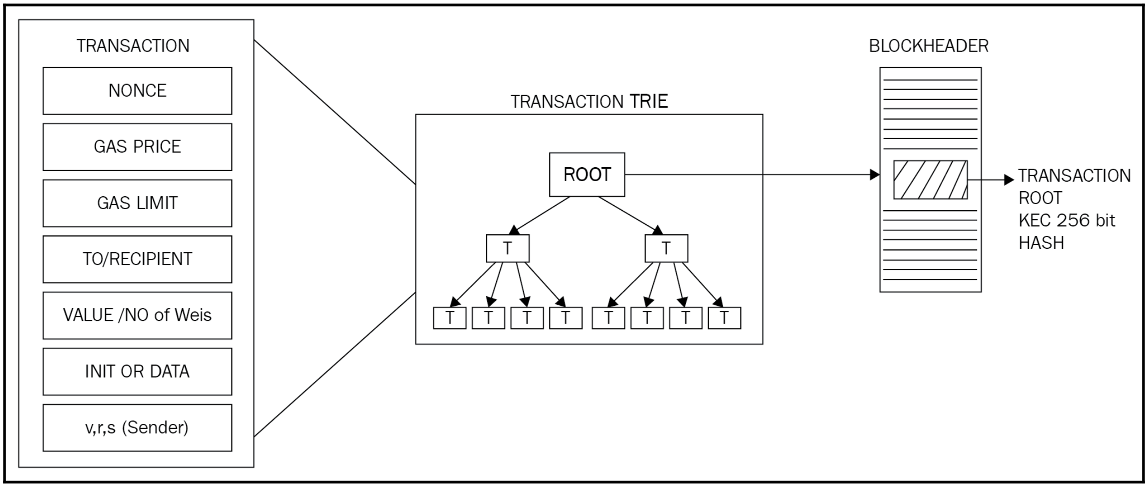
SENDER:4718bf7a
RECIPIENT:741F7A2
GAS PICE:0.5 ETH
GAS LIMIT:2 ETH
DATA:[....]
SIGNATURE:100FD

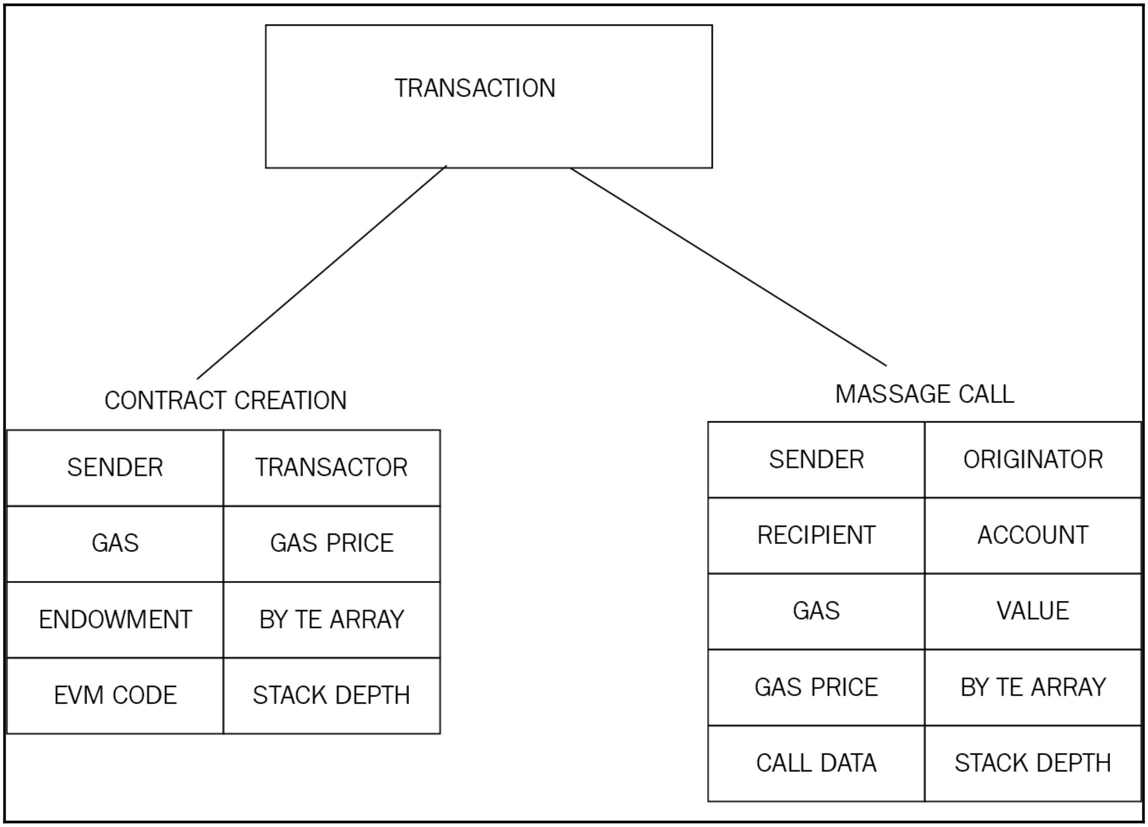
ADDRESS:4718bf7a
BALANCE:8 ETH

ADDRESS:741F7a2
BALANCE: 12 ETH
[CODE..................]

STORAGE:[0,100,ETH,A]


ACCOUNTS TRIE
ROOT
ACCOUNT
NONCE
BALANCE
STORAGE ROOT HASH
CODE HASH
WORLDSTATE TRIE
ROOT
ACCT
ACCT
A
A
A
A
A
A
A
A
STATE ROOT HASH


TRANSACTION
NONCE
GAS PRICE
GAS LIMIT
TO/RECIPIENT
VALUE /NO of Weis
INIT OR DATA
v,r,s (Sender)
TRANSACTION TRIE
ROOT
T
T
T
T
T
T
T
T
T
T
BLOCKHEADER
TRANSACTION ROOT KEC 256 bit HASH



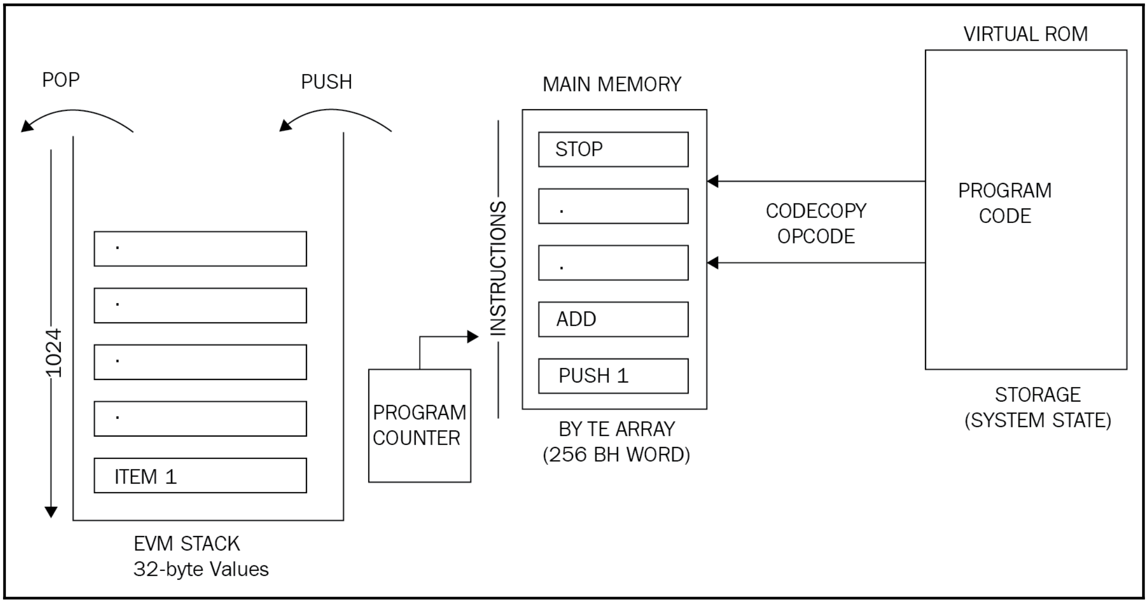
TRANSACTION

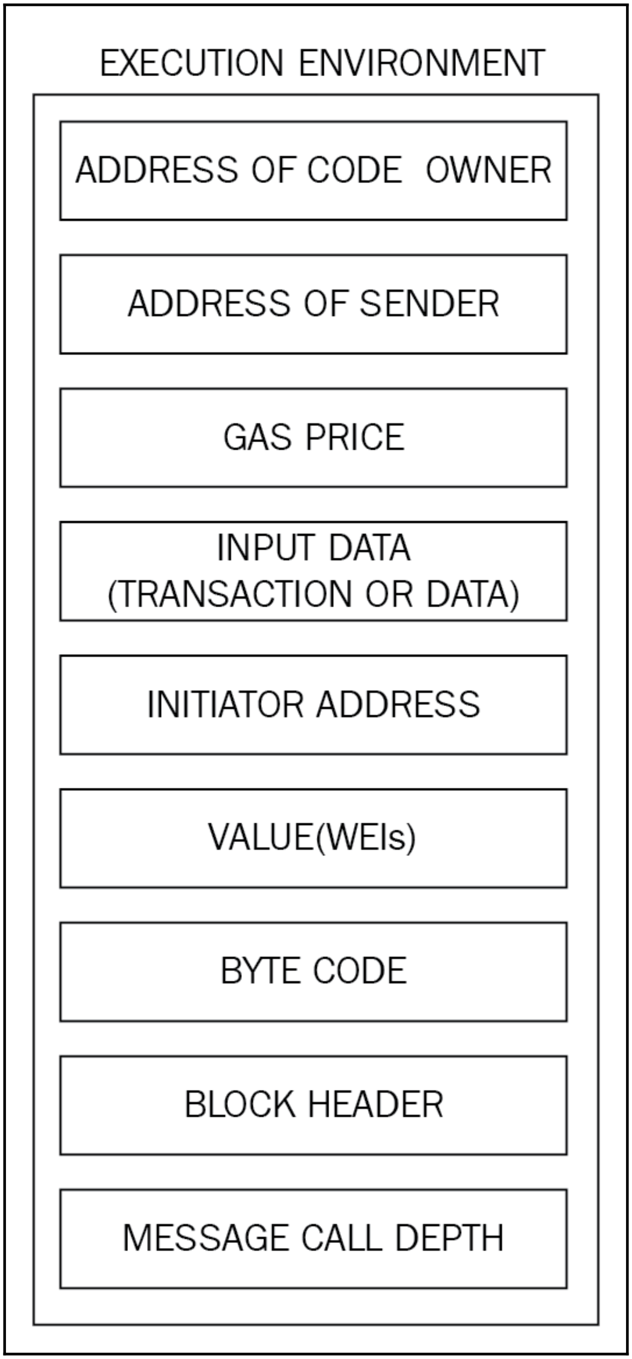
CONTRACT CREATION

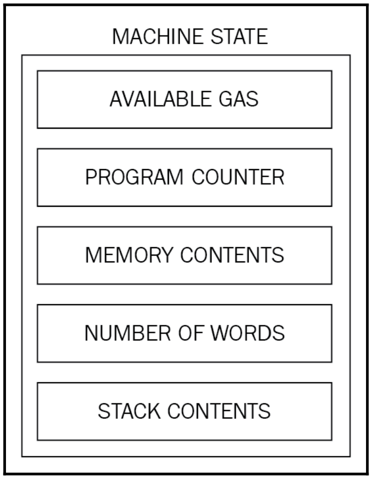
SENDER	TRANSACTOR
GAS	GAS PRICE
ENDOWMENT	BY TE ARRAY
EVM CODE	STACK DEPTH

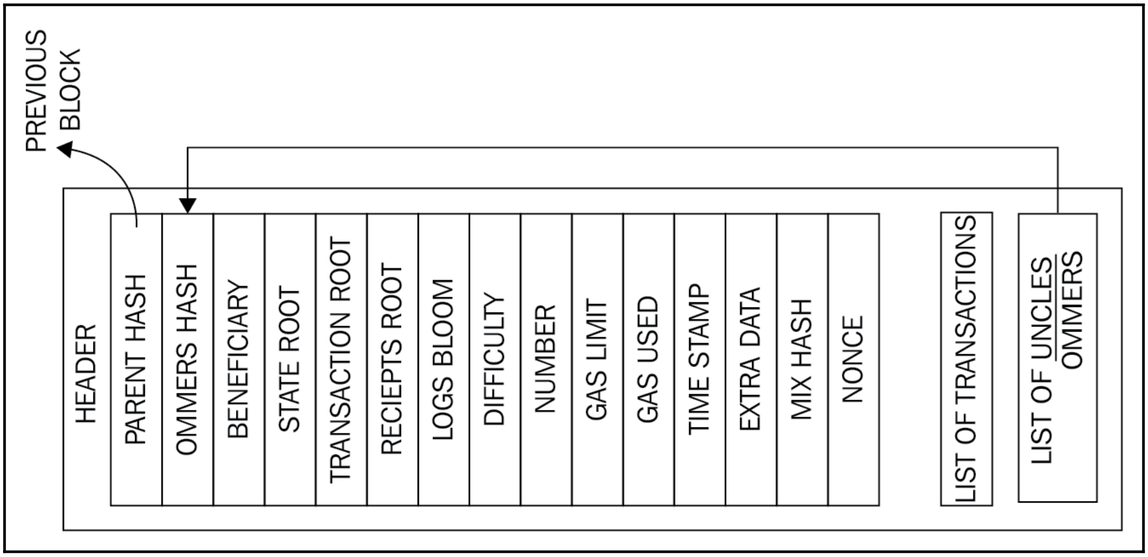
MASSAGE CALL

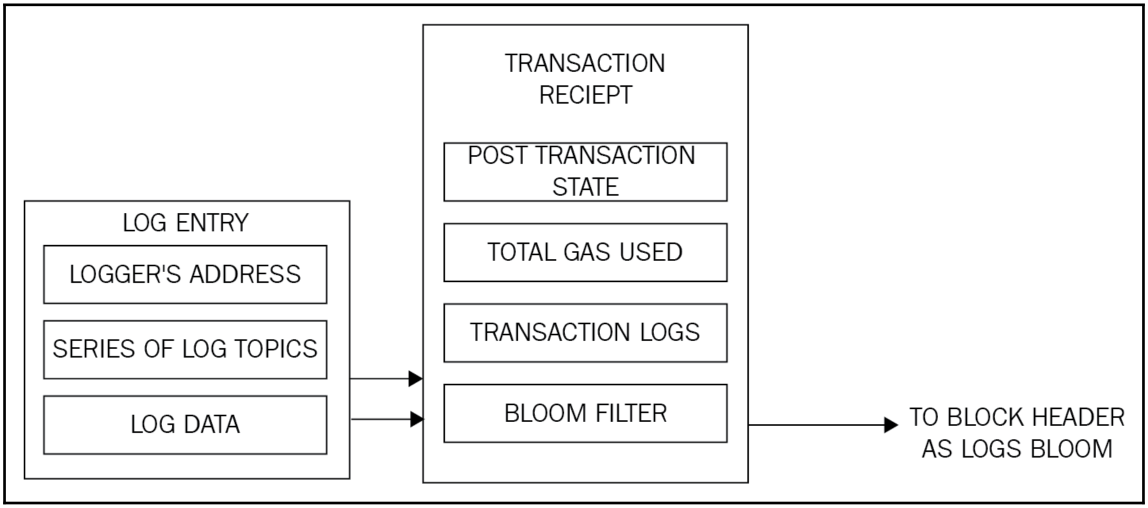
SENDER	ORIGINATOR
RECIPIENT	ACCOUNT
GAS	VALUE
GAS PRICE	BY TE ARRAY
CALL DATA	STACK DEPTH

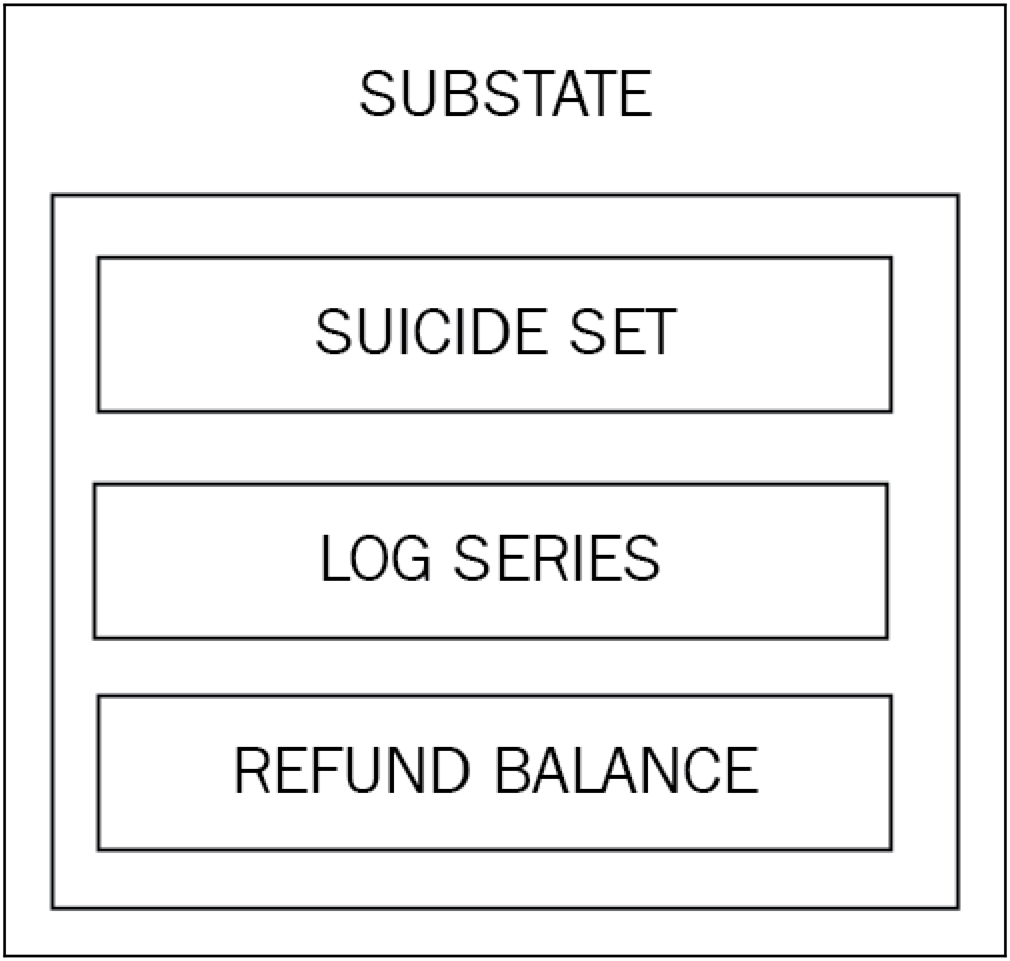

POP
PUSH
1024
.
.
.
.
ITEM 1
EVM STACK
32-byte Values
PROGRAM
COUNTER
INSTRUCTIONS
MAIN MEMORY
STOP
.
.
ADD
PUSH 1
BY TE ARRAY
(256 BH WORD)
CODECOPY
OPCODE
VIRTUAL ROM
PROGRAM
CODE
STORAGE
(SYSTEM STATE)

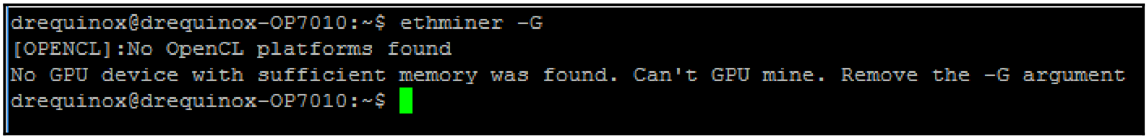

EXECUTION ENVIRONMENT
ADDRESS OF CODE OWNER
ADDRESS OF SENDER
GAS PRICE
INPUT DATA
(TRANSACTION OR DATA)
INITIATOR ADDRESS
VALUE(WEIs)
BYTE CODE
BLOCK HEADER
MESSAGE CALL DEPTH


MACHINE STATE
AVAILABLE GAS
PROGRAM COUNTER
MEMORY CONTENTS
NUMBER OF WORDS
STACK CONTENTS

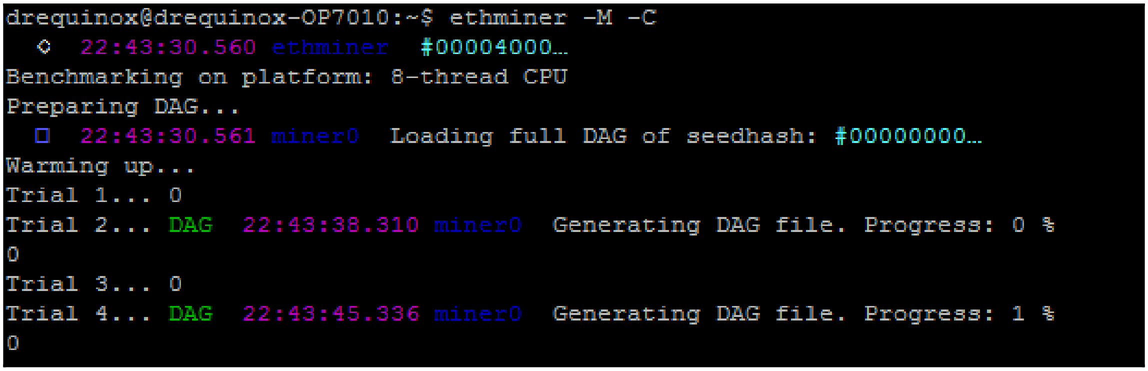

PREVIOUS BLOCK
HEADER
PARENT HASH
OMMERS HASH
BENEFICIARY
STATE ROOT
TRANSACTION ROOT
RECIEPTS ROOT
LOGS BLOOM
DIFFICULTY
NUMBER
GAS LIMIT
GAS USED
TIME STAMP
EXTRA DATA
MIX HASH
NONCE
LIST OF TRANSACTIONS
LIST OF UNCLES
OMMERS


LOG ENTRY
LOGGER'S ADDRESS
SERIES OF LOG TOPICS
LOG DATA
TRANSACTION RECIEPT
POST TRANSACTION STATE
TOTAL GAS USED
TRANSACTION LOGS
BLOOM FILTER
TO BLOCK HEADER AS LOGS BLOOM

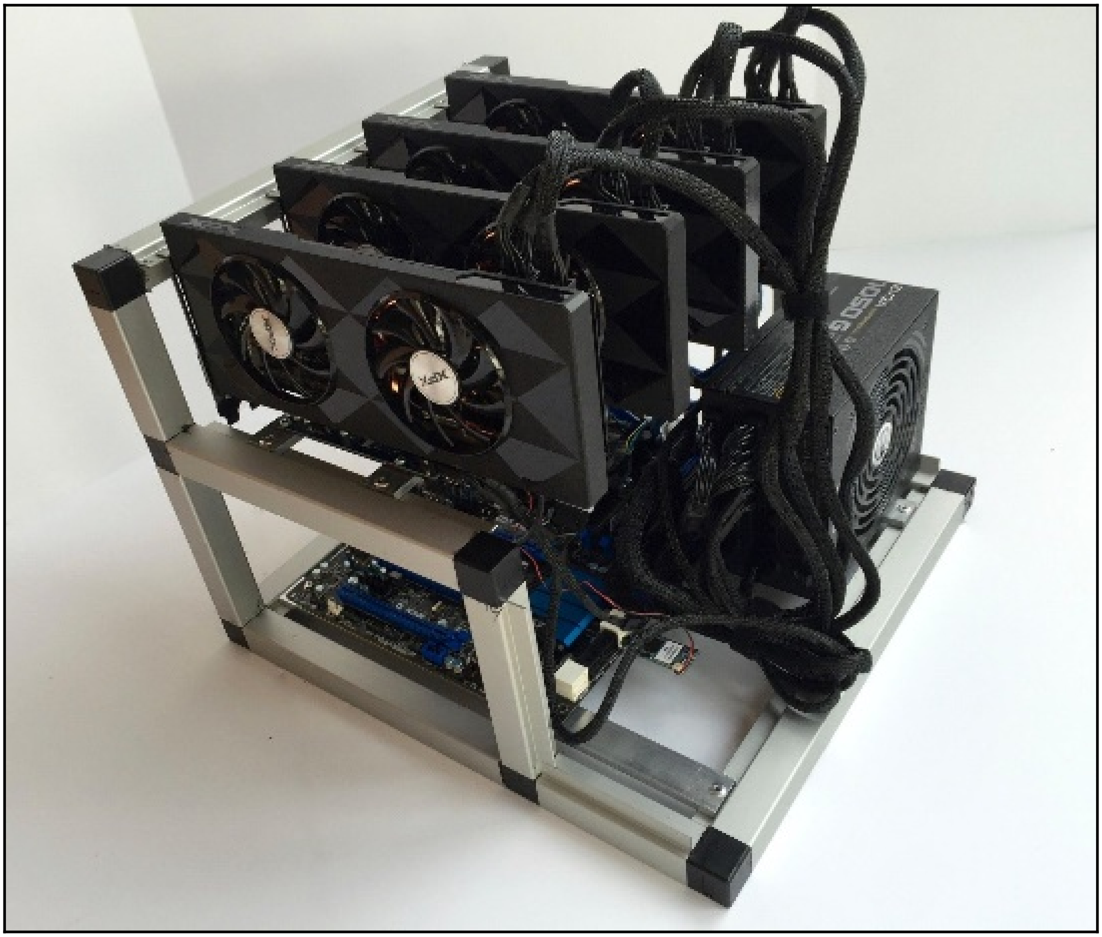


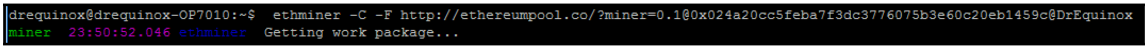


```
drequinox@drequinox-OP7010:~$ ethminer -G
[OPENCL]:No OpenCL platforms found
No GPU device with sufficient memory was found. Can't GPU mine. Remove the -G argument
drequinox@drequinox-OP7010:~$
```

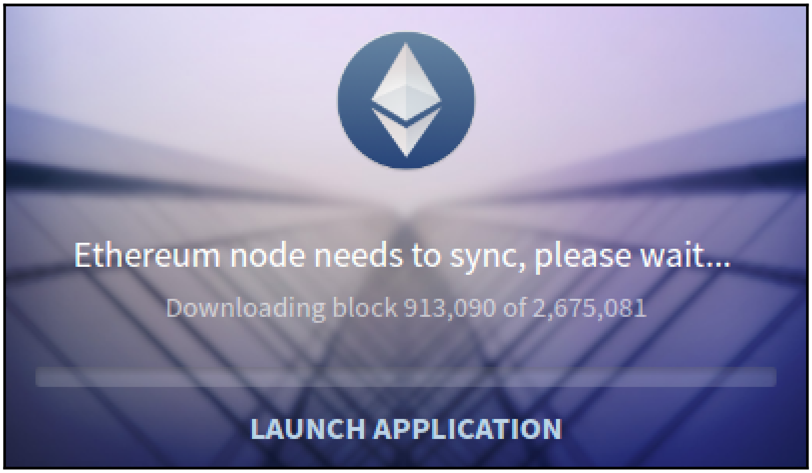


```
drequinox@drequinox-OP7010:~$ ethminer -M -C
  ◇  22:43:30.560 ethminer  #00004000…
Benchmarking on platform: 8-thread CPU
Preparing DAG...
  □  22:43:30.561 miner0  Loading full DAG of seedhash: #00000000…
Warming up...
Trial 1... 0
Trial 2... DAG  22:43:38.310 miner0  Generating DAG file. Progress: 0 %
0
Trial 3... 0
Trial 4... DAG  22:43:45.336 miner0  Generating DAG file. Progress: 1 %
0
```



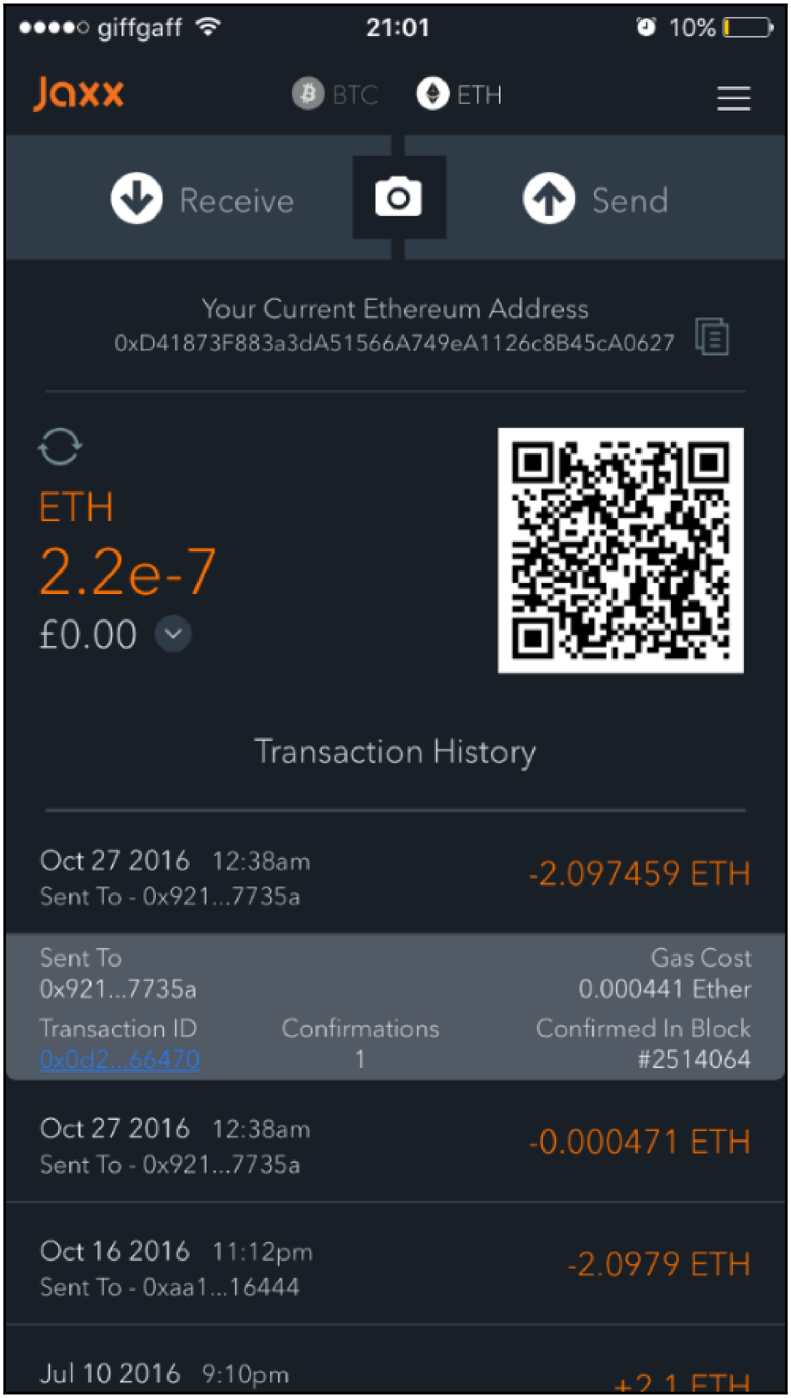


```
drequinox@drequinox-OP7010:~$  ethminer -C -F http://ethereumpool.co/?miner=0.1@0x024a20cc5feba7f3dc3776075b3e60c20eb1459c@DrEquinox
miner  23:50:52.046 ethminer  Getting work package...
```



Ethereum node needs to sync, please wait...

Downloading block 913,090 of 2,675,081



●●●●○ giffgaff 21:01 10%

Jaxx BTC ETH

Receive Send

Your Current Ethereum Address
0xD41873F883a3dA51566A749eA1126c8B45cA0627

ETH
2.2e-7
£0.00

Transaction History

Oct 27 2016 12:38am
Sent To - 0x921...7735a
-2.097459 ETH

Sent To
0x921...7735a

Gas Cost
0.000441 Ether

Transaction ID
0x0d2...66470

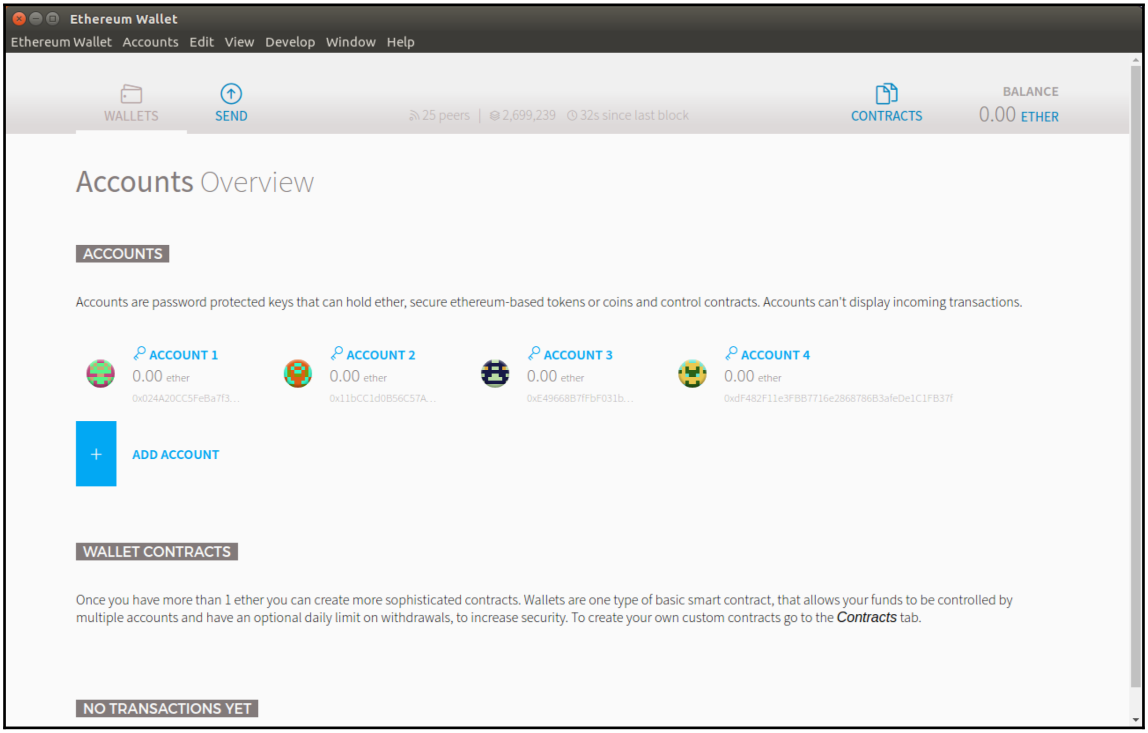
Confirmations
1

Confirmed In Block
#2514064

Oct 27 2016 12:38am
Sent To - 0x921...7735a
-0.000471 ETH

Oct 16 2016 11:12pm
Sent To - 0xaa1...16444
-2.0979 ETH

Jul 10 2016 9:10pm
+2.1 ETH


Ethereum Wallet
Ethereum Wallet Accounts Edit View Develop Window Help
WALLETS
SEND
25 peers | 2,699,239 32s since last block
CONTRACTS
BALANCE
0.00 ETHER

Accounts Overview

ACCOUNTS

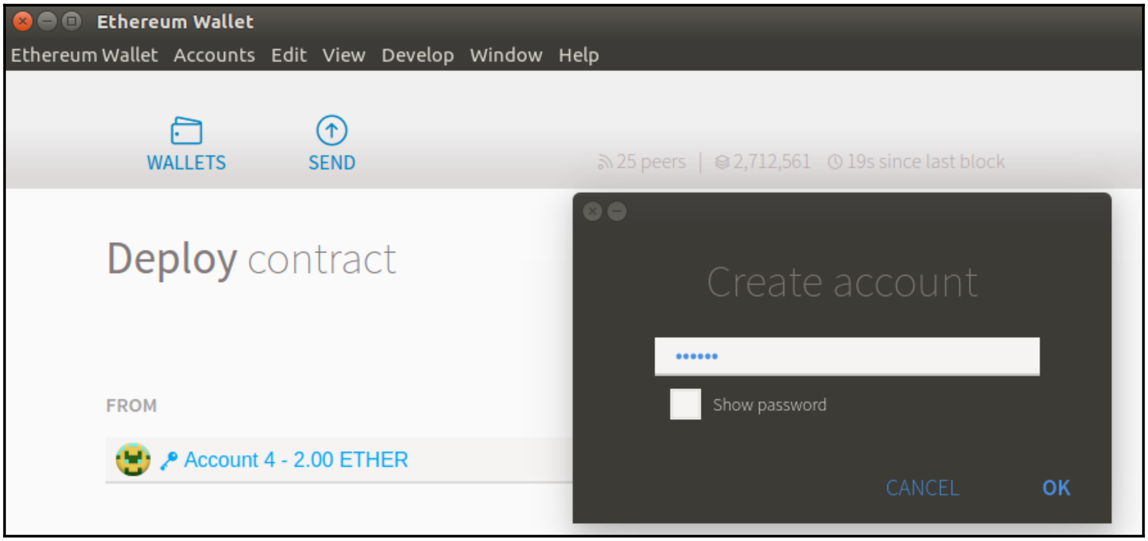
Accounts are password protected keys that can hold ether, secure ethereum-based tokens or coins and control contracts. Accounts can't display incoming transactions.

ACCOUNT 1	ACCOUNT 2	ACCOUNT 3	ACCOUNT 4
0.00 ether	0.00 ether	0.00 ether	0.00 ether
0x024A20CC5FeBa7f3...	0x11bCC1d0B56C57A...	0xE49668B7fFbF031b...	0xdF482F11e3FBB7716e2868786B3afeDe1C1FB37f

WALLET CONTRACTS

Once you have more than 1 ether you can create more sophisticated contracts. Wallets are one type of basic smart contract, that allows your funds to be controlled by multiple accounts and have an optional daily limit on withdrawals, to increase security. To create your own custom contracts go to the *Contracts* tab.

NO TRANSACTIONS YET


Ethereum Wallet
Ethereum Wallet Accounts Edit View Develop Window Help
WALLETS
SEND
25 peers | 2,712,561 19s since last block

Deploy contract

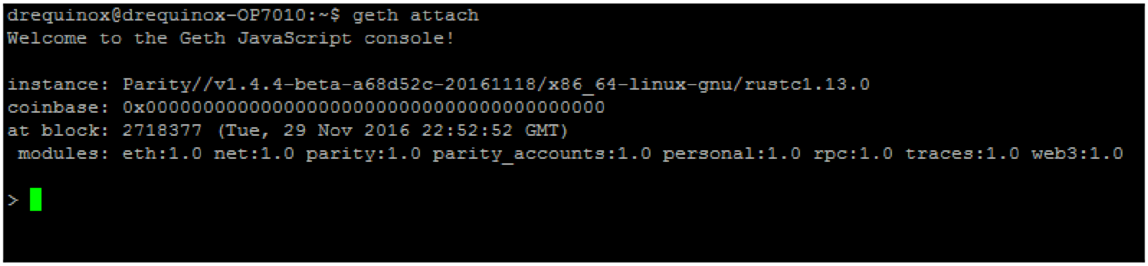
FROM

Account 4 - 2.00 ETHER

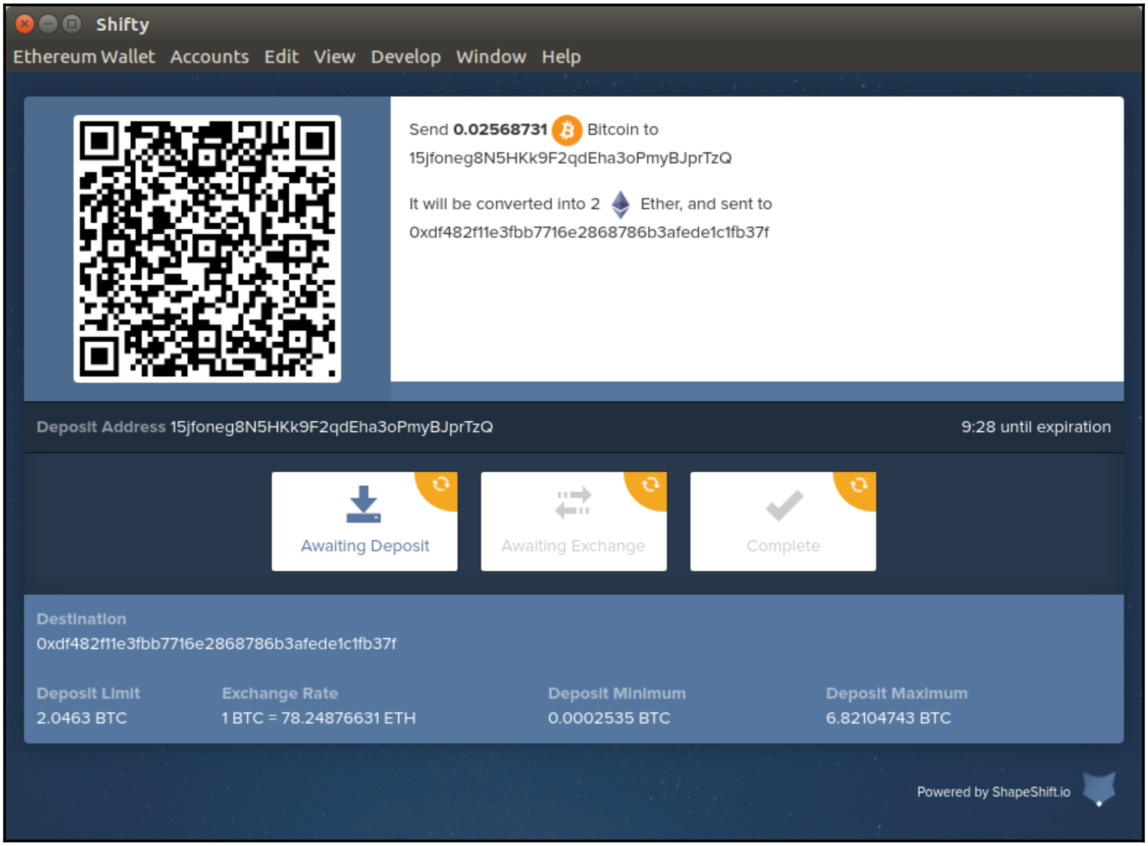
Create account

••••••

□ Show password



```
drequinox@drequinox-OP7010:~$ geth attach
Welcome to the Geth JavaScript console!

instance: Parity//v1.4.4-beta-a68d52c-20161118/x86_64-linux-gnu/rustc1.13.0
coinbase: 0x0000000000000000000000000000000000000000
at block: 2718377 (Tue, 29 Nov 2016 22:52:52 GMT)
 modules: eth:1.0 net:1.0 parity:1.0 parity_accounts:1.0 personal:1.0 rpc:1.0 traces:1.0 web3:1.0

>
```



Send **0.02568731** Bitcoin to
15jfoneg8N5HKk9F2qdEha3oPmyBJprTzQ

It will be converted into 2 Ether, and sent to
0xdf482f11e3fbb7716e2868786b3afede1c1fb37f

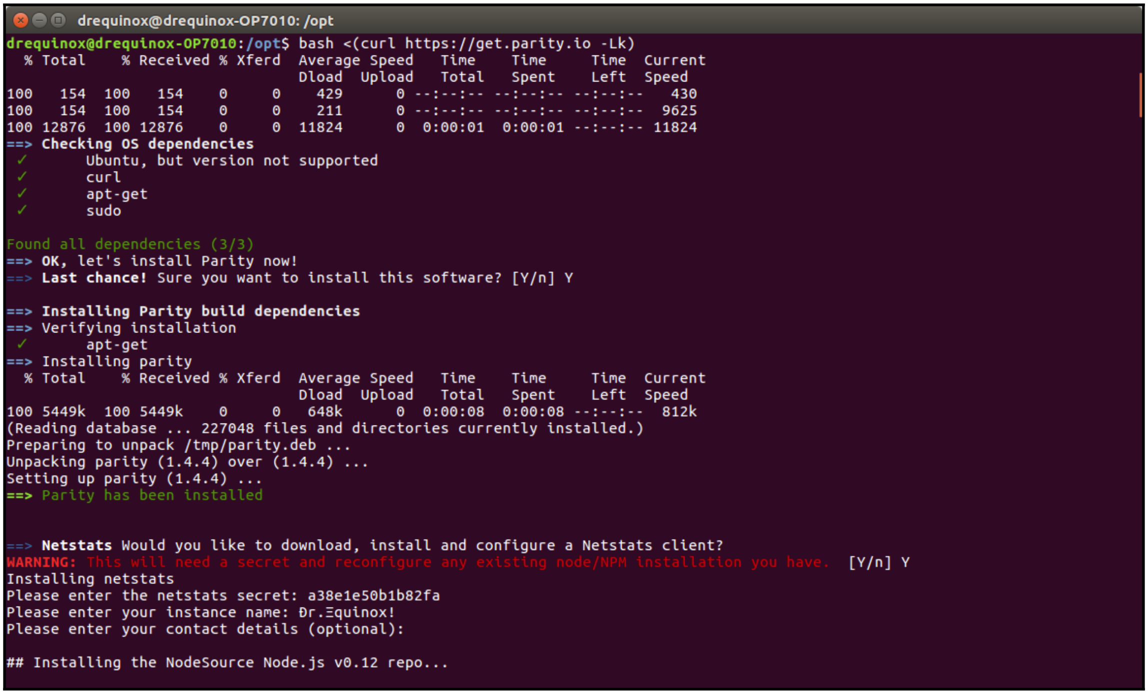
Deposit Address 15jfoneg8N5HKk9F2qdEha3oPmyBJprTzQ

9:28 until expiration

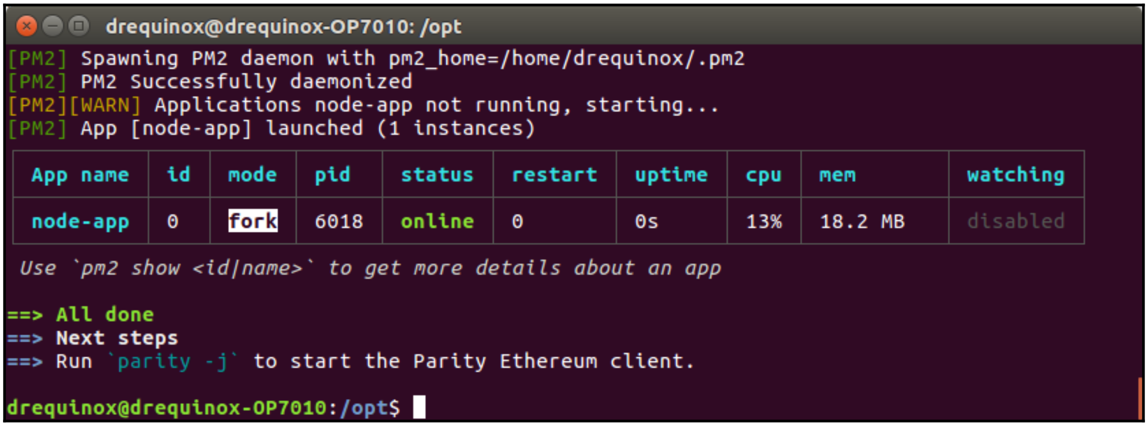
Destination
0xdf482f11e3fbb7716e2868786b3afede1c1fb37f

Deposit Limit	Exchange Rate	Deposit Minimum	Deposit Maximum
2.0463 BTC	1 BTC = 78.24876631 ETH	0.0002535 BTC	6.82104743 BTC

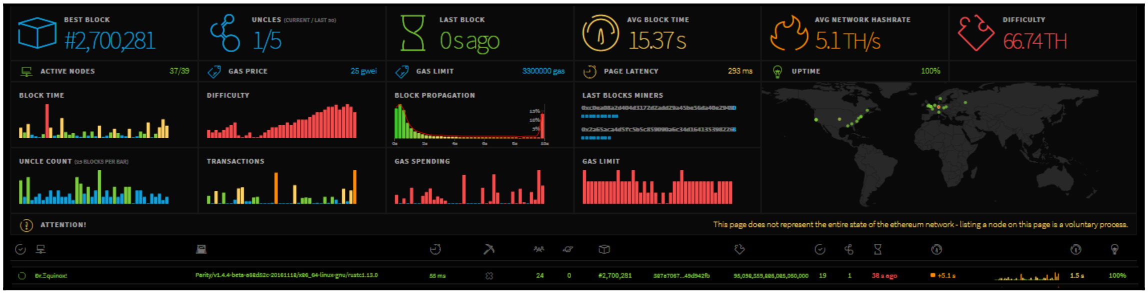
Powered by ShapeShift.io



```
drequinox@drequinox-OP7010:/opt$ bash <(curl https://get.parity.io -Lk)
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   154  100   154    0     0    429      0 --:--:-- --:--:-- --:--:--   430
100   154  100   154    0     0    211      0 --:--:-- --:--:-- --:--:--  9625
100 12876  100 12876    0     0  11824      0  0:00:01  0:00:01 --:--:-- 11824
==> Checking OS dependencies
 ✓      Ubuntu, but version not supported
 ✓      curl
 ✓      apt-get
 ✓      sudo

Found all dependencies (3/3)
==> OK, let's install Parity now!
==> Last chance! Sure you want to install this software? [Y/n] Y

==> Installing Parity build dependencies
==> Verifying installation
 ✓      apt-get
==> Installing parity
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 5449k  100 5449k    0     0   648k      0  0:00:08  0:00:08 --:--:--  812k
(Reading database ... 227048 files and directories currently installed.)
Preparing to unpack /tmp/parity.deb ...
Unpacking parity (1.4.4) over (1.4.4) ...
Setting up parity (1.4.4) ...
==> Parity has been installed


==> Netstats Would you like to download, install and configure a Netstats client?
WARNING: This will need a secret and reconfigure any existing node/NPM installation you have.  [Y/n] Y
Installing netstats
Please enter the netstats secret: a38e1e50b1b82fa
Please enter your instance name: Đr.Ξquinox!
Please enter your contact details (optional):

## Installing the NodeSource Node.js v0.12 repo...
```

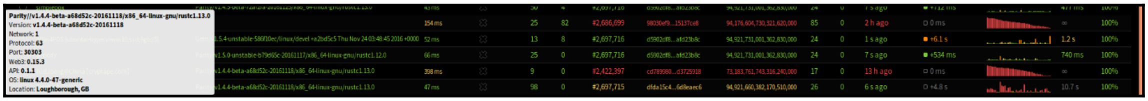


```
[PM2] Spawning PM2 daemon with pm2_home=/home/drequinox/.pm2
[PM2] PM2 Successfully daemonized
[PM2][WARN] Applications node-app not running, starting...
[PM2] App [node-app] launched (1 instances)
│ App name │ id │ mode │ pid  │ status │ restart │ uptime │ cpu │ mem     │ watching │
│ node-app │ 0  │ fork │ 6018 │ online │ 0       │ 0s     │ 13% │ 18.2 MB │ disabled │
 Use `pm2 show <id|name>` to get more details about an app

==> All done
==> Next steps
==> Run `parity -j` to start the Parity Ethereum client.

drequinox@drequinox-OP7010:/opt$ █
```



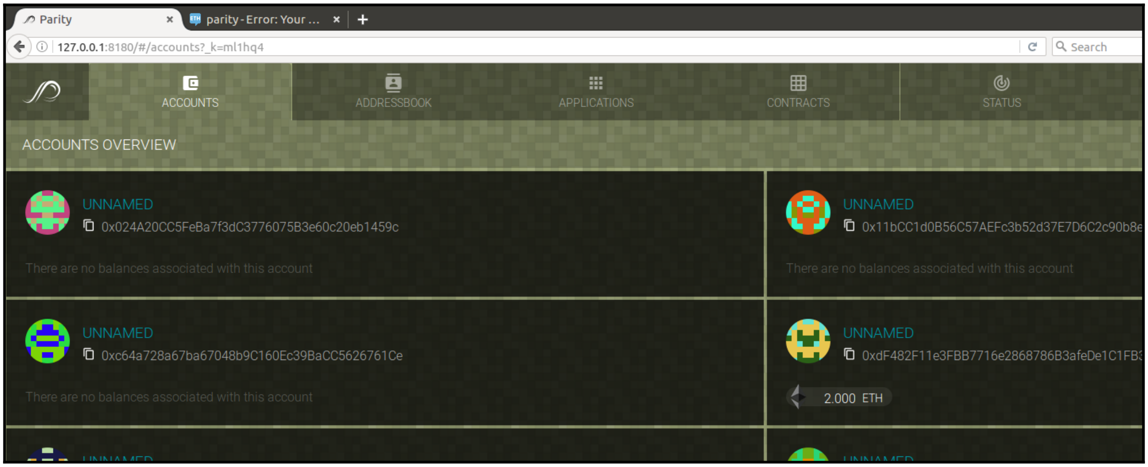
This page does not represent the entire state of the ethereum network - listing a node on this page is a voluntary process.

○	Br.Ξquinox!	Parity/v1.4.4-beta-a68d52c-20161118/x86_64-linux-gnu/rustc1.13.0	55 ms		24	0	#2,700,281	387a7067...49d942fb	95,098,359,886,085,060,000	19	1	38 s ago	+5.1 s		1.5 s	100%



Parity//v1.4.4-beta-a68d52c-20161118/x86_64-linux-gnu/rustc1.13.0
Version: **v1.4.4-beta-a68d52c-20161118**
Network: **1**
Protocol: **63**
Port: **30303**
Web3: **0.15.3**
API: **0.1.1**
OS: **linux 4.4.0-47-generic**
Location: **Loughborough, GB**

	43 ms		30	4	#2,697,716	d5902df8...afd23b8c	94,921,731,001,362,830,000	24	0	7 s ago	+712 ms	477 ms	100%
	154 ms		25	82	#2,686,699	98030ef9...15137ce8	94,176,604,730,321,620,000	85	0	2 h ago	0 ms	∞	100%
Geth/v1.5.4-unstable-586f10ec/linux/devel +a2bd5c5 Thu Nov 24 03:48:45 2016 +0000	52 ms		13	8	#2,697,716	d5902df8...afd23b8c	94,921,731,001,362,830,000	24	0	1 s ago	+6.1 s	1.2 s	100%
Parity/v1.5.0-unstable-b79d65c-20161117/x86_64-linux-gnu/rustc1.12.0	66 ms		25	0	#2,697,716	d5902df8...afd23b8c	94,921,731,001,362,830,000	24	0	7 s ago	+534 ms	740 ms	100%
Parity/v1.4.4-beta-a68d52c-20161118/x86_64-linux-gnu/rustc1.13.0	398 ms		9	0	#2,422,397	cd789980...d3725918	73,183,761,743,316,240,000	17	0	13 h ago	0 ms	∞	100%
Parity/v1.4.4-beta-a68d52c-20161118/x86_64-linux-gnu/rustc1.13.0	47 ms		98	0	#2,697,715	dfda15c4...6d8eaec6	94,921,660,382,170,510,000	26	0	6 s ago	+4.8 s	10.7 s	100%



ACCOUNTS OVERVIEW

UNNAMED
0x024A20CC5FeBa7f3dC3776075B3e60c20eb1459c
There are no balances associated with this account

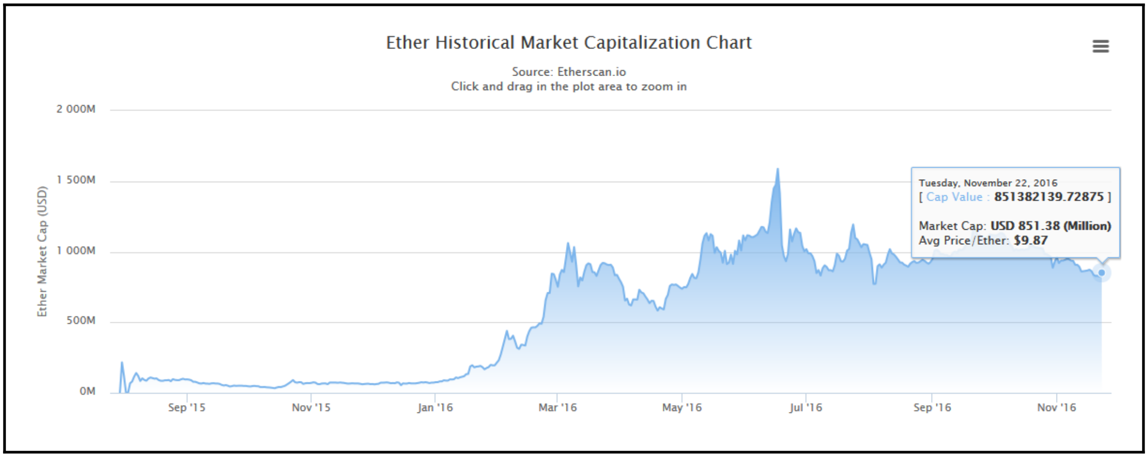
UNNAMED
0x11bCC1d0B56C57AEFc3b52d37E7D6C2c90b8e

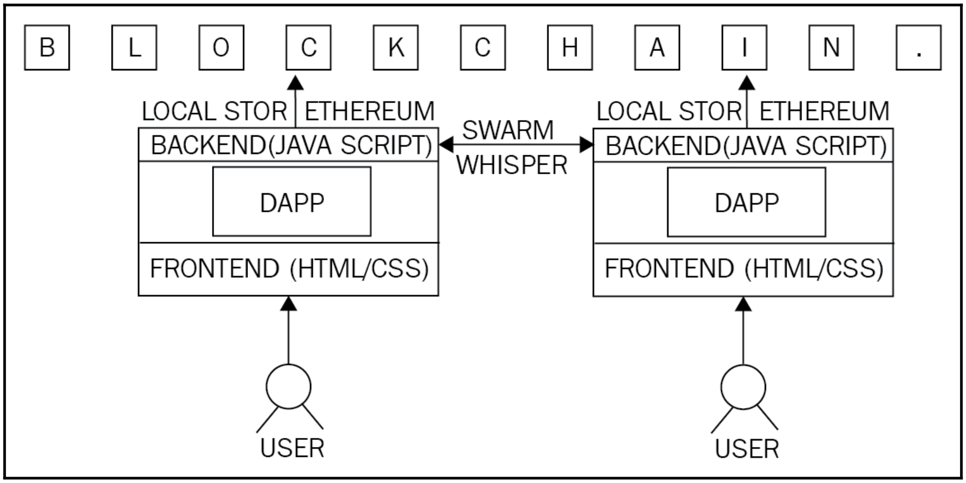
There are no balances associated with this account

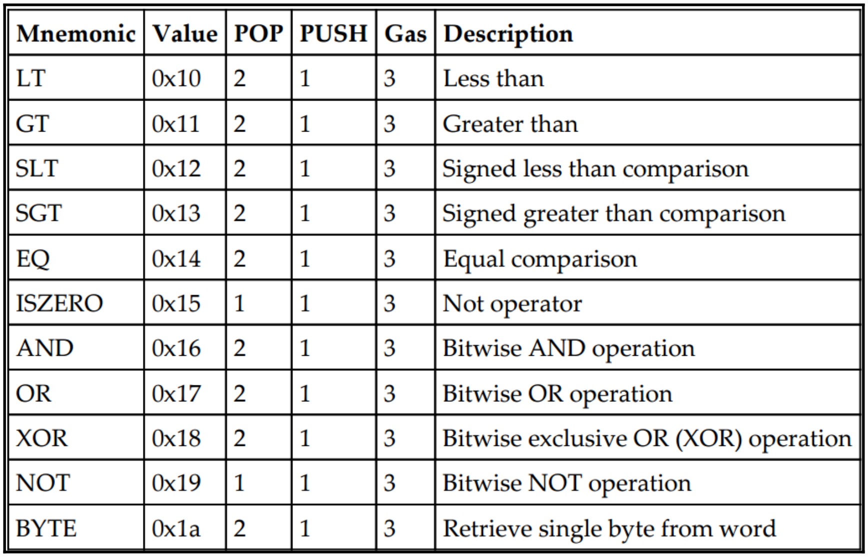
UNNAMED
0xc64a728a67ba67048b9C160Ec39BaCC5626761Ce
There are no balances associated with this account

UNNAMED
0xdF482F11e3FBB7716e2868786B3afeDe1C1FB3

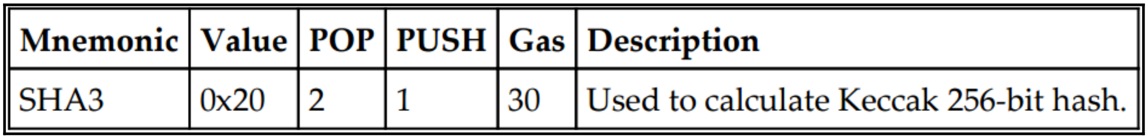
2.000 ETH


Ether Historical Market Capitalization Chart
Source: Etherscan.io
Click and drag in the plot area to zoom in
Ether Market Cap (USD)
2 000M
1 500M
1 000M
500M
0M
Sep '15
Nov '15
Jan '16
Mar '16
May '16
Jul '16
Sep '16
Nov '16
Tuesday, November 22, 2016
[Cap Value : 851382139.72875]
Market Cap: USD 851.38 (Million)
Avg Price/Ether: $9.87

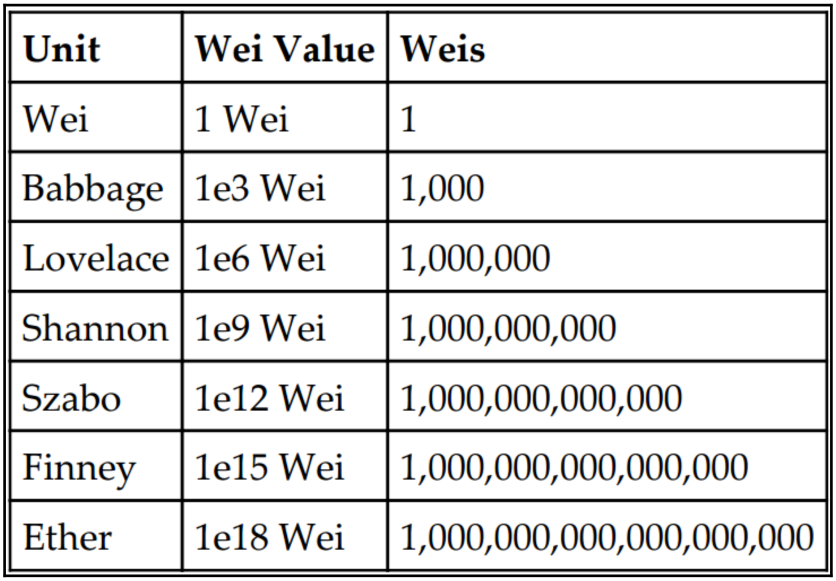

B L O C K C H A I N .
LOCAL STOR
ETHEREUM
BACKEND(JAVA SCRIPT)
DAPP
FRONTEND (HTML/CSS)
USER
SWARM
WHISPER
LOCAL STOR
ETHEREUM
BACKEND(JAVA SCRIPT)
DAPP
FRONTEND (HTML/CSS)
USER



Mnemonic	Value	POP	PUSH	Gas	Description
LT	0x10	2	1	3	Less than
GT	0x11	2	1	3	Greater than
SLT	0x12	2	1	3	Signed less than comparison
SGT	0x13	2	1	3	Signed greater than comparison
EQ	0x14	2	1	3	Equal comparison
ISZERO	0x15	1	1	3	Not operator
AND	0x16	2	1	3	Bitwise AND operation
OR	0x17	2	1	3	Bitwise OR operation
XOR	0x18	2	1	3	Bitwise exclusive OR (XOR) operation
NOT	0x19	1	1	3	Bitwise NOT operation
BYTE	0x1a	2	1	3	Retrieve single byte from word



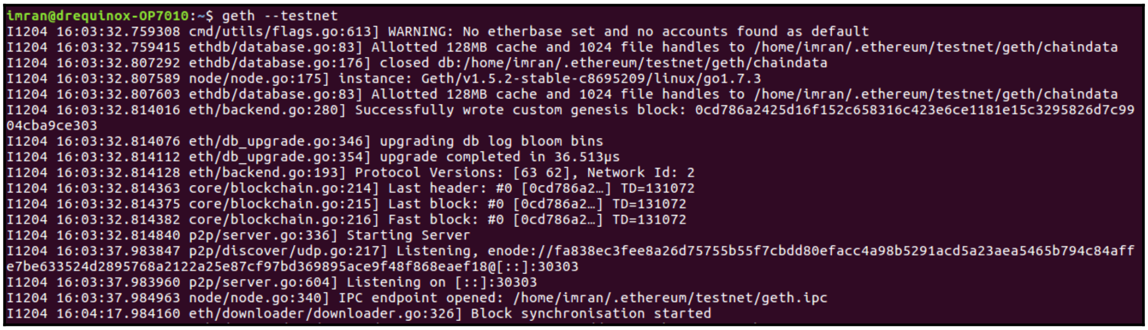
Mnemonic	Value	POP	PUSH	Gas	Description
SHA3	0x20	2	1	30	Used to calculate Keccak 256-bit hash.



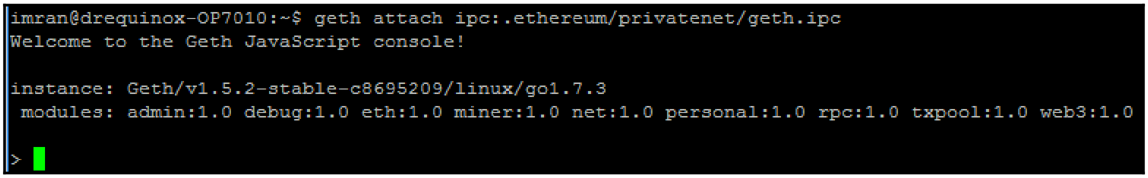
Unit	Wei Value	Weis
Wei	1 Wei	1
Babbage	1e3 Wei	1,000
Lovelace	1e6 Wei	1,000,000
Shannon	1e9 Wei	1,000,000,000
Szabo	1e12 Wei	1,000,000,000,000
Finney	1e15 Wei	1,000,000,000,000,000
Ether	1e18 Wei	1,000,000,000,000,000,000

Operation Name	**Gas Cost**
step	1
stop	0
suicide	0
sha3	30
sload	20
txdata	5
transaction	500
contract creation	53000

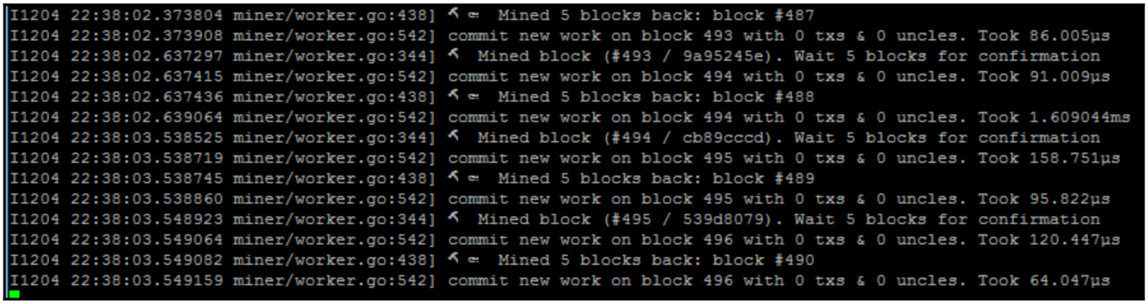
Chapter 8: Ethereum development



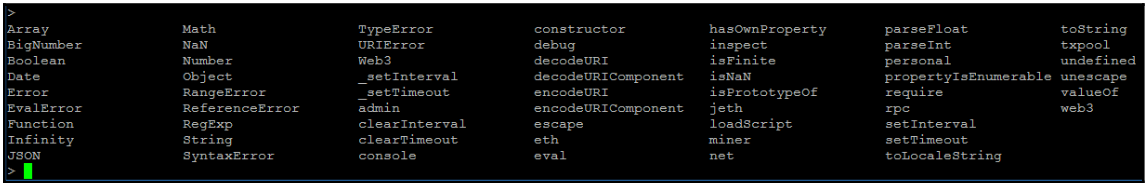
```
imran@drequinox-OP7010:~$ geth --testnet
I1204 16:03:32.759308 cmd/utils/flags.go:613] WARNING: No etherbase set and no accounts found as default
I1204 16:03:32.759415 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to /home/imran/.ethereum/testnet/geth/chaindata
I1204 16:03:32.807292 ethdb/database.go:176] closed db:/home/imran/.ethereum/testnet/geth/chaindata
I1204 16:03:32.807589 node/node.go:175] instance: Geth/v1.5.2-stable-c8695209/linux/go1.7.3
I1204 16:03:32.807603 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to /home/imran/.ethereum/testnet/geth/chaindata
I1204 16:03:32.814016 eth/backend.go:280] Successfully wrote custom genesis block: 0cd786a2425d16f152c658316c423e6ce1181e15c3295826d7c99
04cba9ce303
I1204 16:03:32.814076 eth/db_upgrade.go:346] upgrading db log bloom bins
I1204 16:03:32.814112 eth/db_upgrade.go:354] upgrade completed in 36.513µs
I1204 16:03:32.814128 eth/backend.go:193] Protocol Versions: [63 62], Network Id: 2
I1204 16:03:32.814363 core/blockchain.go:214] Last header: #0 [0cd786a2…] TD=131072
I1204 16:03:32.814375 core/blockchain.go:215] Last block: #0 [0cd786a2…] TD=131072
I1204 16:03:32.814382 core/blockchain.go:216] Fast block: #0 [0cd786a2…] TD=131072
I1204 16:03:32.814840 p2p/server.go:336] Starting Server
I1204 16:03:37.983847 p2p/discover/udp.go:217] Listening, enode://fa838ec3fee8a26d75755b55f7cbdd80efacc4a98b5291acd5a23aea5465b794c84aff
e7be633524d2895768a2122a25e87cf97bd369895ace9f48f868eaef18@[::]:30303
I1204 16:03:37.983960 p2p/server.go:604] Listening on [::]:30303
I1204 16:03:37.984963 node/node.go:340] IPC endpoint opened: /home/imran/.ethereum/testnet/geth.ipc
I1204 16:04:17.984160 eth/downloader/downloader.go:326] Block synchronisation started
```



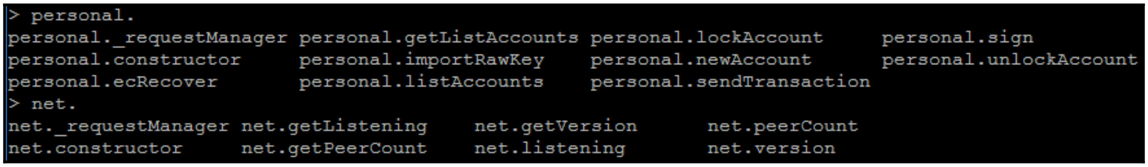
```
imran@drequinox-OP7010:~$ geth attach ipc:.ethereum/privatenet/geth.ipc
Welcome to the Geth JavaScript console!

instance: Geth/v1.5.2-stable-c8695209/linux/go1.7.3
 modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txpool:1.0 web3:1.0

>
```



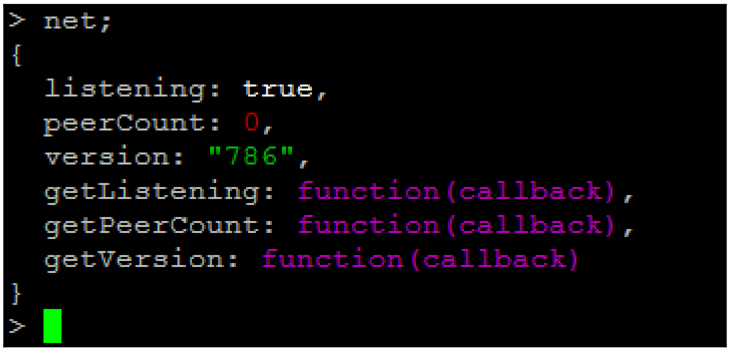
```
I1204 22:38:02.373804 miner/worker.go:438] 🔨 🔗  Mined 5 blocks back: block #487
I1204 22:38:02.373908 miner/worker.go:542] commit new work on block 493 with 0 txs & 0 uncles. Took 86.005µs
I1204 22:38:02.637297 miner/worker.go:344] 🔨  Mined block (#493 / 9a95245e). Wait 5 blocks for confirmation
I1204 22:38:02.637415 miner/worker.go:542] commit new work on block 494 with 0 txs & 0 uncles. Took 91.009µs
I1204 22:38:02.637436 miner/worker.go:438] 🔨 🔗  Mined 5 blocks back: block #488
I1204 22:38:02.639064 miner/worker.go:542] commit new work on block 494 with 0 txs & 0 uncles. Took 1.609044ms
I1204 22:38:03.538525 miner/worker.go:344] 🔨  Mined block (#494 / cb89cccd). Wait 5 blocks for confirmation
I1204 22:38:03.538719 miner/worker.go:542] commit new work on block 495 with 0 txs & 0 uncles. Took 158.751µs
I1204 22:38:03.538745 miner/worker.go:438] 🔨 🔗  Mined 5 blocks back: block #489
I1204 22:38:03.538860 miner/worker.go:542] commit new work on block 495 with 0 txs & 0 uncles. Took 95.822µs
I1204 22:38:03.548923 miner/worker.go:344] 🔨  Mined block (#495 / 539d8079). Wait 5 blocks for confirmation
I1204 22:38:03.549064 miner/worker.go:542] commit new work on block 496 with 0 txs & 0 uncles. Took 120.447µs
I1204 22:38:03.549082 miner/worker.go:438] 🔨 🔗  Mined 5 blocks back: block #490
I1204 22:38:03.549159 miner/worker.go:542] commit new work on block 496 with 0 txs & 0 uncles. Took 64.047µs
```



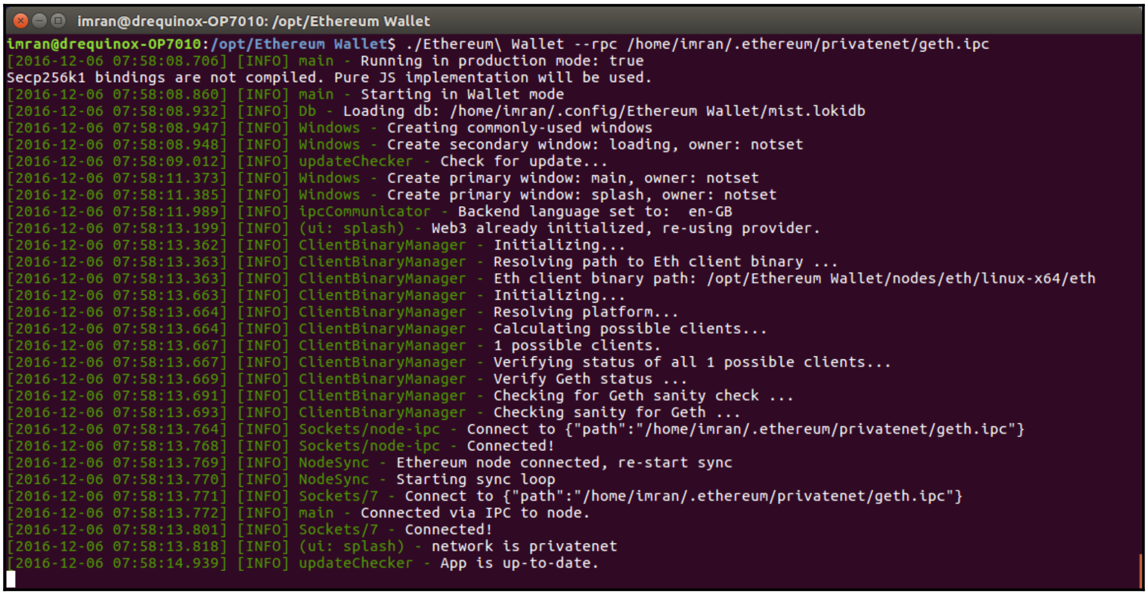
```
>
Array                Math                 TypeError            constructor          hasOwnProperty       parseFloat           toString
BigNumber            NaN                  URIError             debug                inspect              parseInt             txpool
Boolean              Number               Web3                 decodeURI            isFinite             personal             undefined
Date                 Object               _setInterval         decodeURIComponent   isNaN                propertyIsEnumerable unescape
Error                RangeError           _setTimeout          encodeURI            isPrototypeOf        require              valueOf
EvalError            ReferenceError       admin                encodeURIComponent   jeth                 rpc                  web3
Function             RegExp               clearInterval        escape               loadScript           setInterval
Infinity             String               clearTimeout         eth                  miner                setTimeout
JSON                 SyntaxError          console              eval                 net                  toLocaleString
>
```



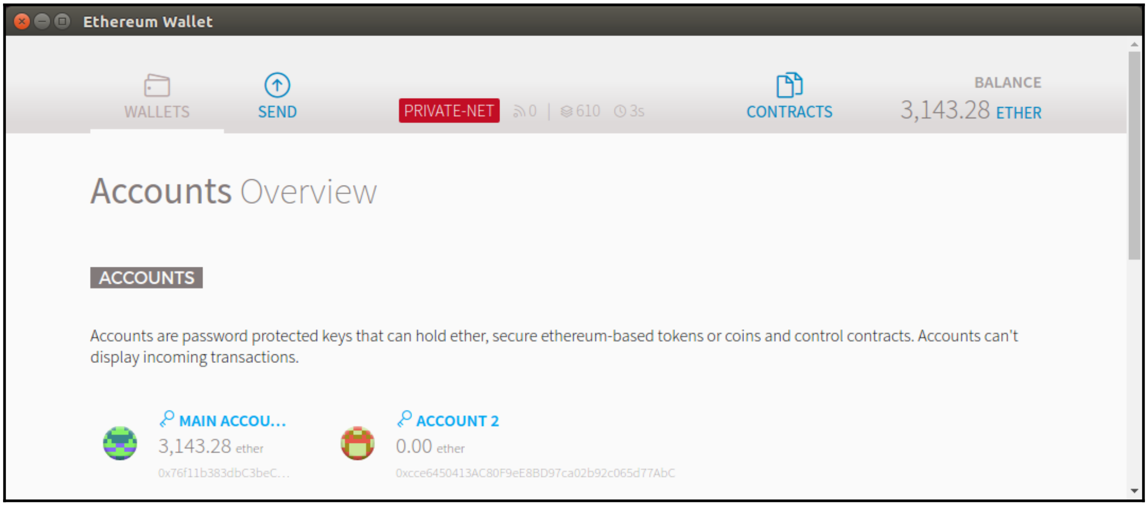
```
> personal.
personal._requestManager personal.getListAccounts personal.lockAccount     personal.sign
personal.constructor     personal.importRawKey    personal.newAccount      personal.unlockAccount
personal.ecRecover       personal.listAccounts    personal.sendTransaction
> net.
net._requestManager net.getListening    net.getVersion      net.peerCount
net.constructor     net.getPeerCount    net.listening       net.version
```



```
> net;
{
  listening: true,
  peerCount: 0,
  version: "786",
  getListening: function(callback),
  getPeerCount: function(callback),
  getVersion: function(callback)
}
> 
```



```
imran@drequinox-OP7010:/opt/Ethereum Wallet$ ./Ethereum\ Wallet --rpc /home/imran/.ethereum/privatenet/geth.ipc
[2016-12-06 07:58:08.706] [INFO] main - Running in production mode: true
Secp256k1 bindings are not compiled. Pure JS implementation will be used.
[2016-12-06 07:58:08.860] [INFO] main - Starting in Wallet mode
[2016-12-06 07:58:08.932] [INFO] Db - Loading db: /home/imran/.config/Ethereum Wallet/mist.lokidb
[2016-12-06 07:58:08.947] [INFO] Windows - Creating commonly-used windows
[2016-12-06 07:58:08.948] [INFO] Windows - Create secondary window: loading, owner: notset
[2016-12-06 07:58:09.012] [INFO] updateChecker - Check for update...
[2016-12-06 07:58:11.373] [INFO] Windows - Create primary window: main, owner: notset
[2016-12-06 07:58:11.385] [INFO] Windows - Create primary window: splash, owner: notset
[2016-12-06 07:58:11.989] [INFO] ipcCommunicator - Backend language set to:  en-GB
[2016-12-06 07:58:13.199] [INFO] (ui: splash) - Web3 already initialized, re-using provider.
[2016-12-06 07:58:13.362] [INFO] ClientBinaryManager - Initializing...
[2016-12-06 07:58:13.363] [INFO] ClientBinaryManager - Resolving path to Eth client binary ...
[2016-12-06 07:58:13.363] [INFO] ClientBinaryManager - Eth client binary path: /opt/Ethereum Wallet/nodes/eth/linux-x64/eth
[2016-12-06 07:58:13.663] [INFO] ClientBinaryManager - Initializing...
[2016-12-06 07:58:13.664] [INFO] ClientBinaryManager - Resolving platform...
[2016-12-06 07:58:13.664] [INFO] ClientBinaryManager - Calculating possible clients...
[2016-12-06 07:58:13.667] [INFO] ClientBinaryManager - 1 possible clients.
[2016-12-06 07:58:13.667] [INFO] ClientBinaryManager - Verifying status of all 1 possible clients...
[2016-12-06 07:58:13.669] [INFO] ClientBinaryManager - Verify Geth status ...
[2016-12-06 07:58:13.691] [INFO] ClientBinaryManager - Checking for Geth sanity check ...
[2016-12-06 07:58:13.693] [INFO] ClientBinaryManager - Checking sanity for Geth ...
[2016-12-06 07:58:13.764] [INFO] Sockets/node-ipc - Connect to {"path":"/home/imran/.ethereum/privatenet/geth.ipc"}
[2016-12-06 07:58:13.768] [INFO] Sockets/node-ipc - Connected!
[2016-12-06 07:58:13.769] [INFO] NodeSync - Ethereum node connected, re-start sync
[2016-12-06 07:58:13.770] [INFO] NodeSync - Starting sync loop
[2016-12-06 07:58:13.771] [INFO] Sockets/7 - Connect to {"path":"/home/imran/.ethereum/privatenet/geth.ipc"}
[2016-12-06 07:58:13.772] [INFO] main - Connected via IPC to node.
[2016-12-06 07:58:13.801] [INFO] Sockets/7 - Connected!
[2016-12-06 07:58:13.818] [INFO] (ui: splash) - network is privatenet
[2016-12-06 07:58:14.939] [INFO] updateChecker - App is up-to-date.
```



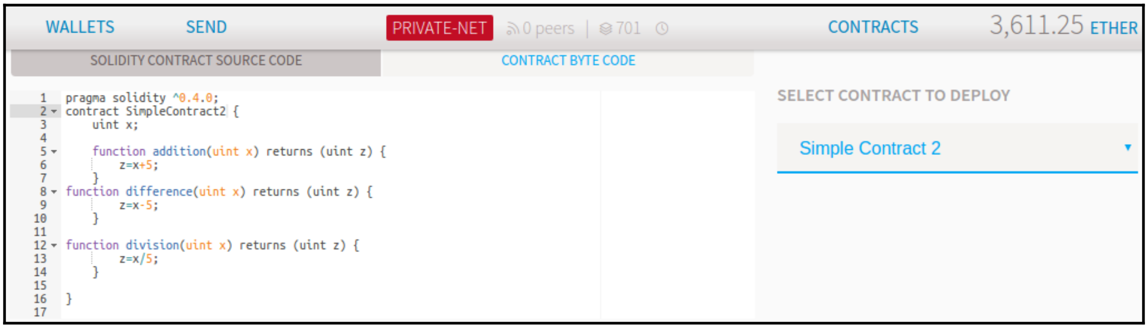
Accounts Overview

ACCOUNTS

Accounts are password protected keys that can hold ether, secure ethereum-based tokens or coins and control contracts. Accounts can't display incoming transactions.

MAIN ACCOU...
3,143.28 ether
0x76f11b383dbC3beC...

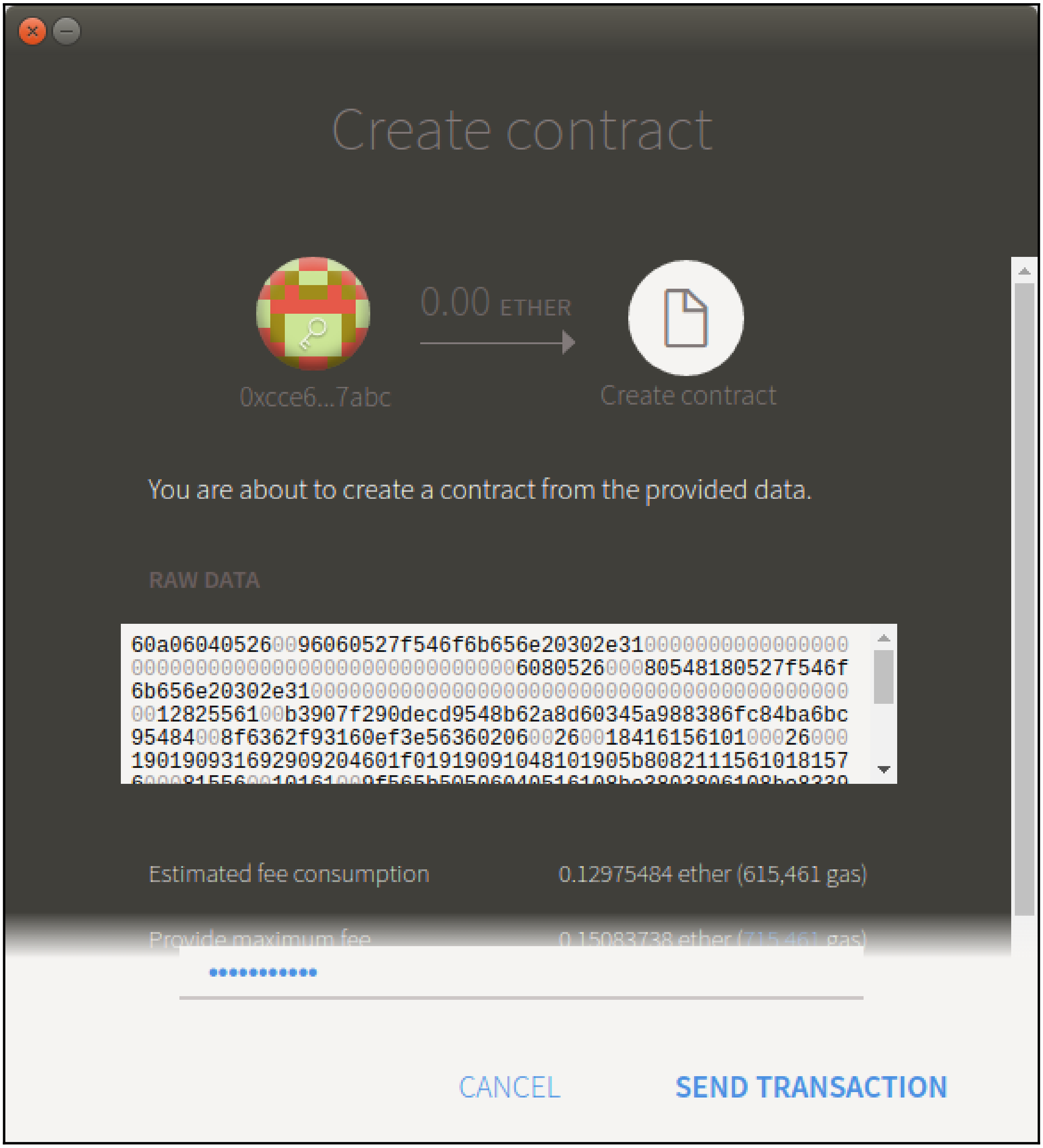
ACCOUNT 2
0.00 ether
0xcce6450413AC80F9eE8BD97ca02b92c065d77AbC



```
pragma solidity ^0.4.0;
contract SimpleContract2 {
    uint x;

    function addition(uint x) returns (uint z) {
        z=x+5;
    }
function difference(uint x) returns (uint z) {
        z=x-5;
    }

function division(uint x) returns (uint z) {
        z=x/5;
    }

}

```

SELECT CONTRACT TO DEPLOY

Simple Contract 2



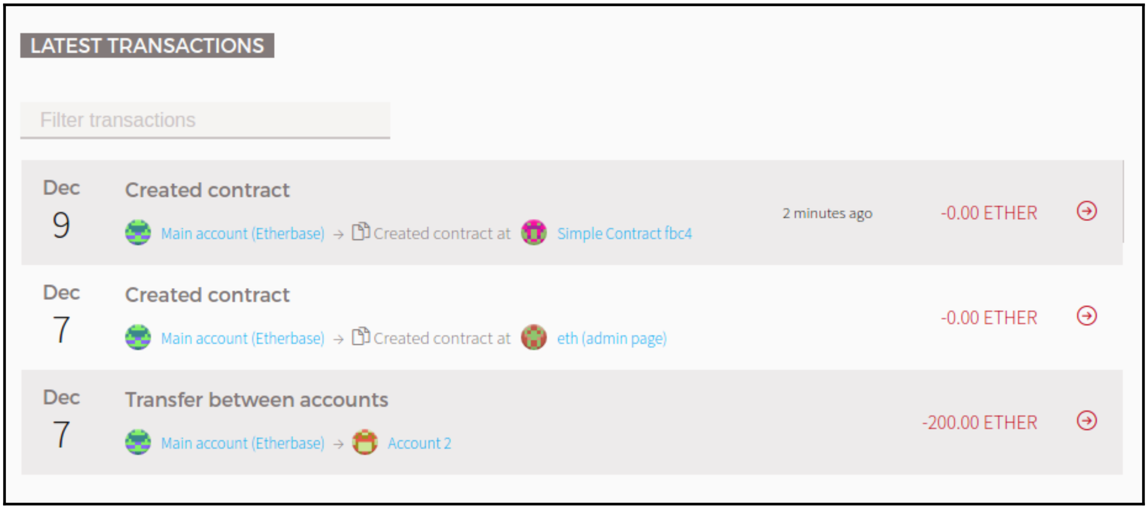
You are about to create a contract from the provided data.

RAW DATA

```
60a0604052600960605277f546f6b656e20302e310000000000000000
000000000000000000000000000000608052600080548180527f546f
6b656e20302e31000000000000000000000000000000000000000000
00128255610 0b3907f290decd9548b62a8d60345a988386fc84ba6bc
95484008f6362f93160ef3e5636020600260018416156101000260000
19019093169290920460 1f01919091048101905b8082111561018157
6000815560010161000f565b50506040516108be3803806108be8339
```

Estimated fee consumption 0.12975484 ether (615,461 gas)

Provide maximum fee 0.15083738 ether (715,461 gas)

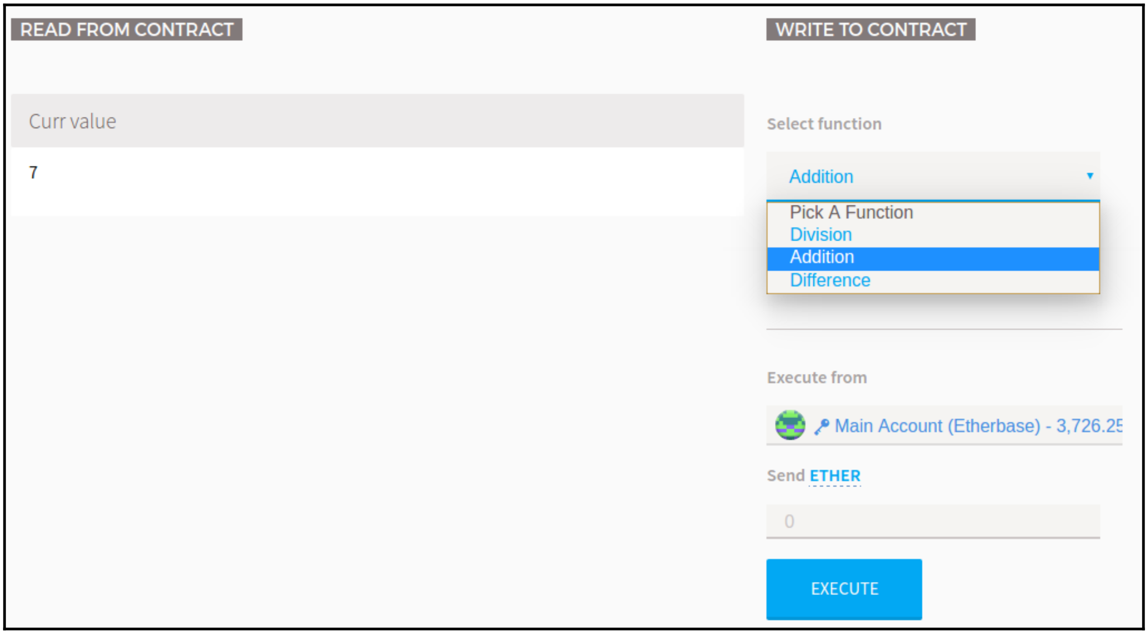


LATEST TRANSACTIONS

Dec 9 — Created contract — Main account (Etherbase) → Created contract at Simple Contract fbc4 — 2 minutes ago — -0.00 ETHER

Dec 7 — Created contract — Main account (Etherbase) → Created contract at eth (admin page) — -0.00 ETHER

Dec 7 — Transfer between accounts — Main account (Etherbase) → Account 2 — -200.00 ETHER



READ FROM CONTRACT

Curr value

7

WRITE TO CONTRACT

Select function

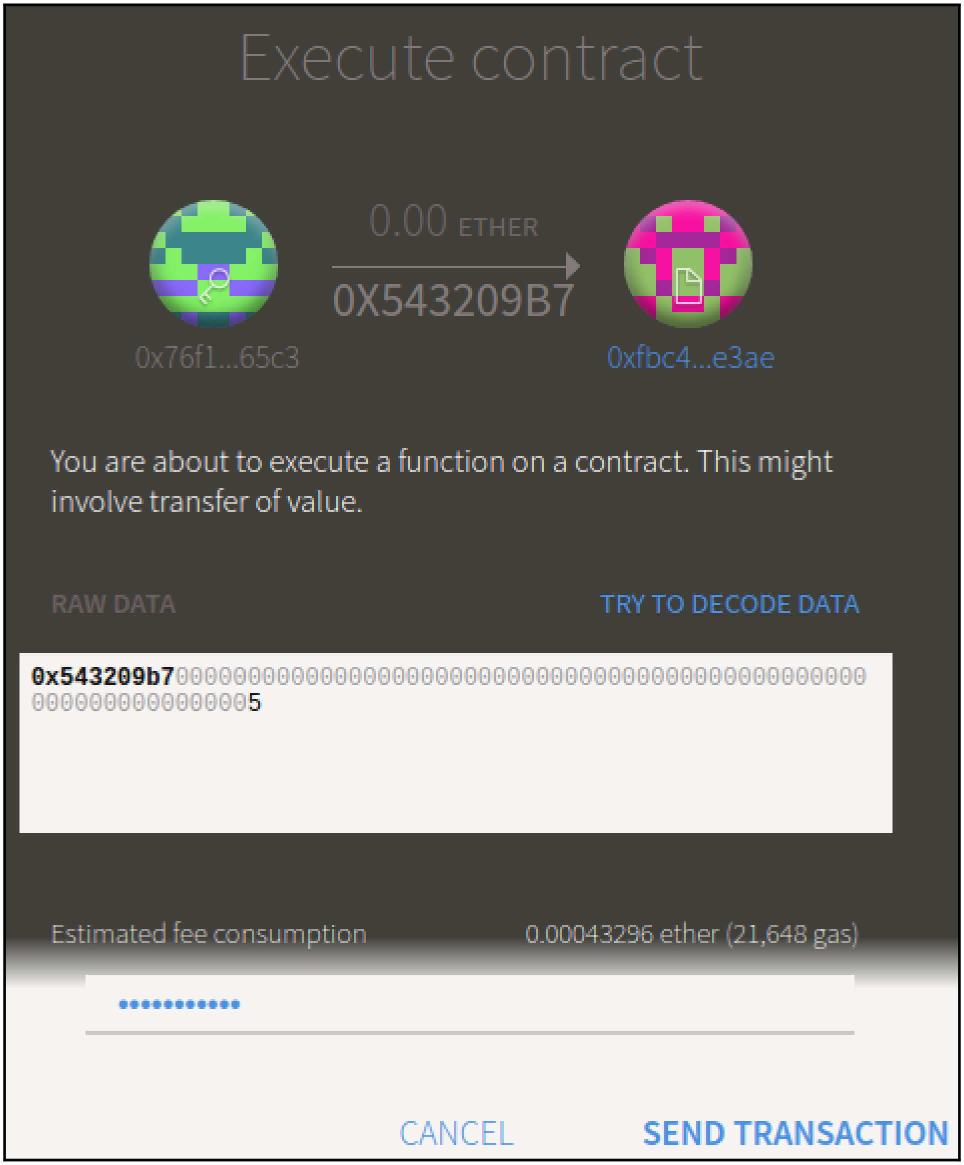
Addition

Execute from

Main Account (Etherbase) - 3,726.25

Send ETHER

0



Execute contract

0.00 ETHER

0X543209B7

0x76f1...65c3

0xfbc4...e3ae

You are about to execute a function on a contract. This might involve transfer of value.

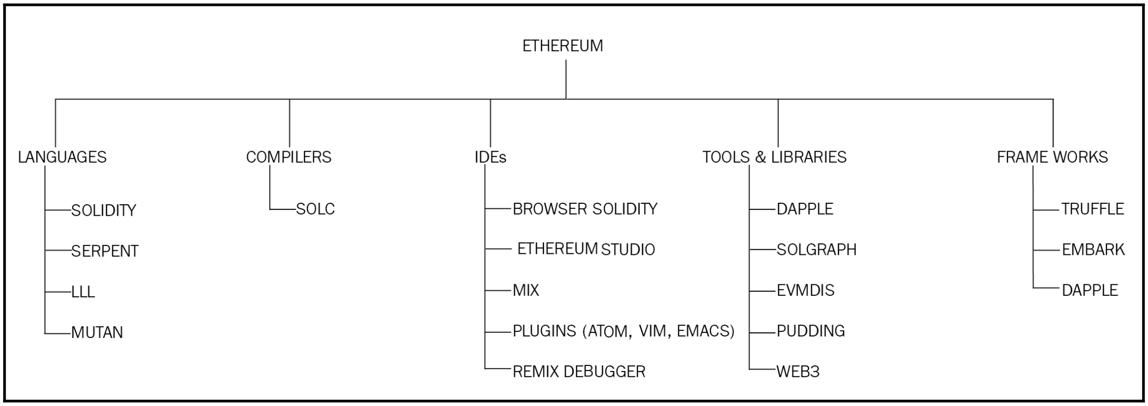
RAW DATA TRY TO DECODE DATA

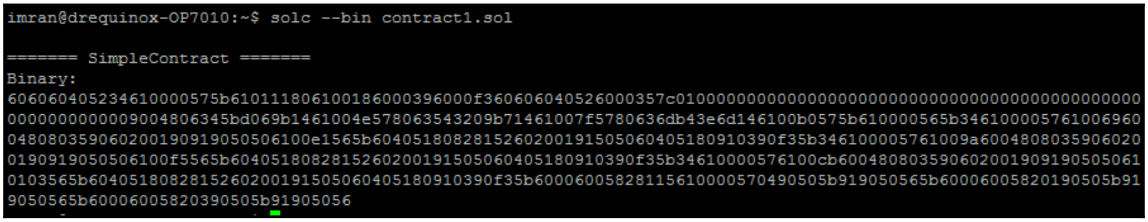
```
0x543209b7000000000000000000000000000000000000000000000000
0000000000000005
```

Estimated fee consumption 0.00043296 ether (21,648 gas)

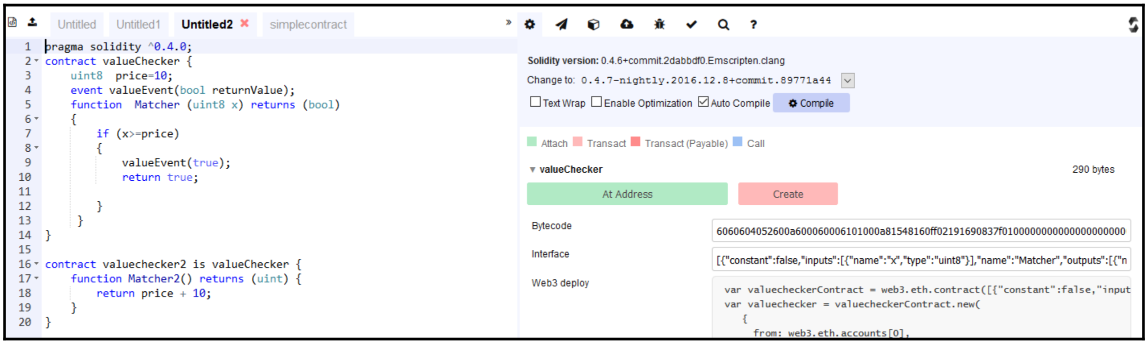
••••••••••••

CANCEL SEND TRANSACTION





```
imran@drequinox-OP7010:~$ solc --bin contract1.sol

======= SimpleContract =======
Binary:
6060604052346100005753b61011180610018600039600 0f360606040526000357c010000000000000000000000000000000000000000000000
00000000000009004806345bd069b1461004e578063543209b71461007f5780636db43e6d146100b0575b610000565b3461000057610069 60
04808035906020019091905050506100e1565b604051808281526020019150506040518091039 0f35b34610000576100 9a6004808035906020
019091905050506100f5565b60405180828152602001915050604051809103 90f35b34610000576100cb600480803590602001909190505061
0103565b6040518082815260200191505060405180910390f35b600060058281156100005704905 05b919050565b6000600582019050 5b91
9050565b6000600582039050 5b91905056
```



Untitled | Untitled1 | **Untitled2** ✖ | simplecontract

```
pragma solidity ^0.4.0;
contract valueChecker {
    uint8  price=10;
    event valueEvent(bool returnValue);
    function  Matcher (uint8 x) returns (bool)
    {
        if (x>=price)
        {
            valueEvent(true);
            return true;

        }
     }
}

contract valuechecker2 is valueChecker {
    function Matcher2() returns (uint) {
        return price + 10;
    }
}
```

Solidity version: 0.4.6+commit.2dabbdf0.Emscripten.clang

Change to: 0.4.7-nightly.2016.12.8+commit.89771a44

□ Text Wrap □ Enable Optimization ☑ Auto Compile

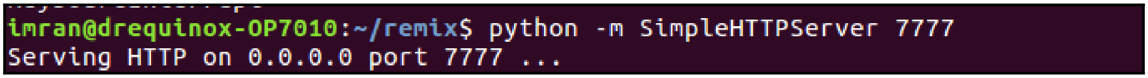
▼ **valueChecker** 290 bytes

Bytecode: 6060604052600a600060006101000a81548160ff02191690837f010000000000000000000

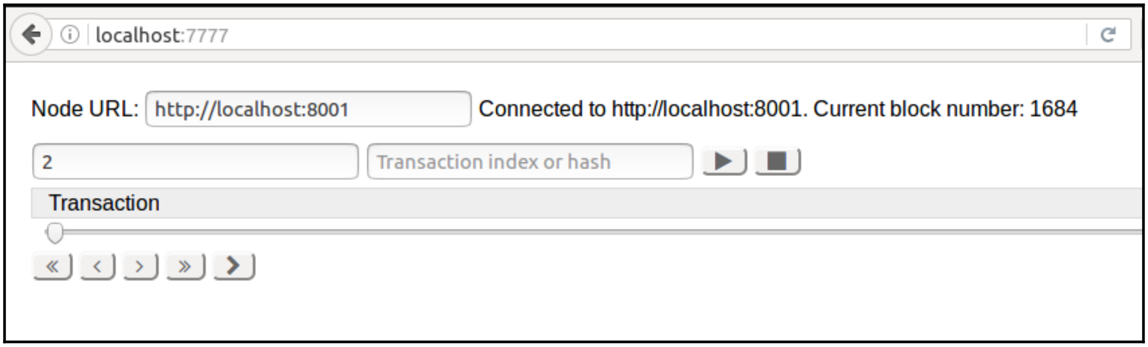
Interface: [{"constant":false,"inputs":[{"name":"x","type":"uint8"}],"name":"Matcher","outputs":[{"n

Web3 deploy:

```
var valuecheckerContract = web3.eth.contract([{"constant":false,"input
var valuechecker = valuecheckerContract.new(
   {
     from: web3.eth.accounts[0],
```



```
imran@drequinox-OP7010:~/remix$ python -m SimpleHTTPServer 7777
Serving HTTP on 0.0.0.0 port 7777 ...
```

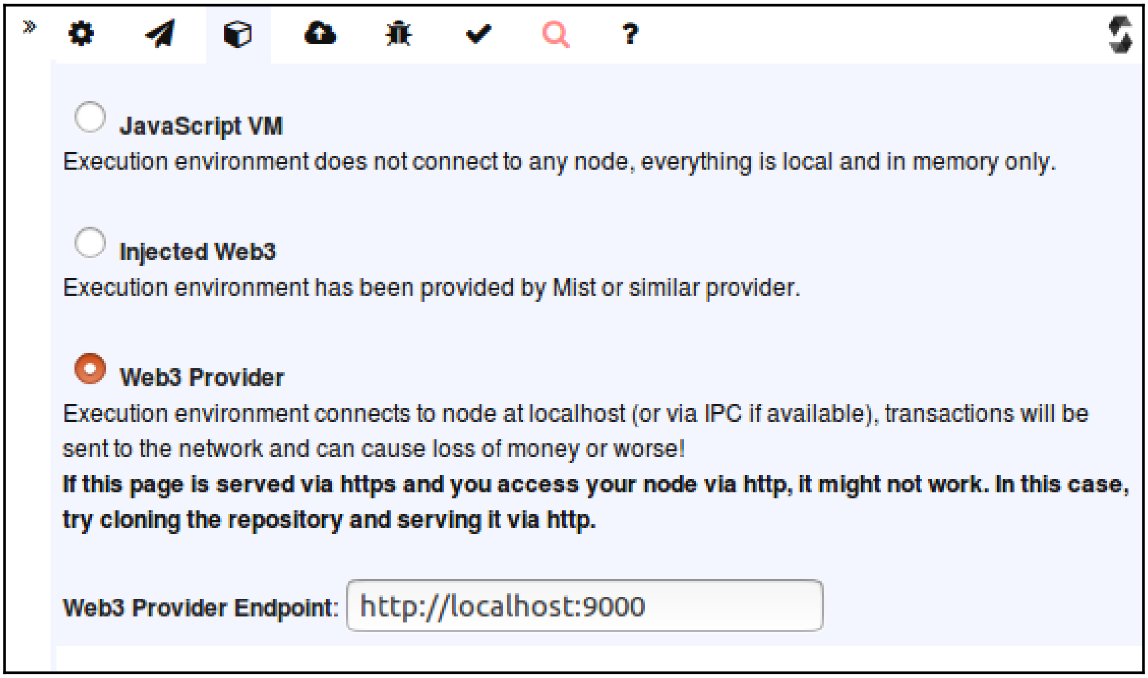


Node URL: http://localhost:8001 Connected to http://localhost:8001. Current block number: 1684

2

Transaction index or hash

Transaction



○ **JavaScript VM**

Execution environment does not connect to any node, everything is local and in memory only.

○ **Injected Web3**

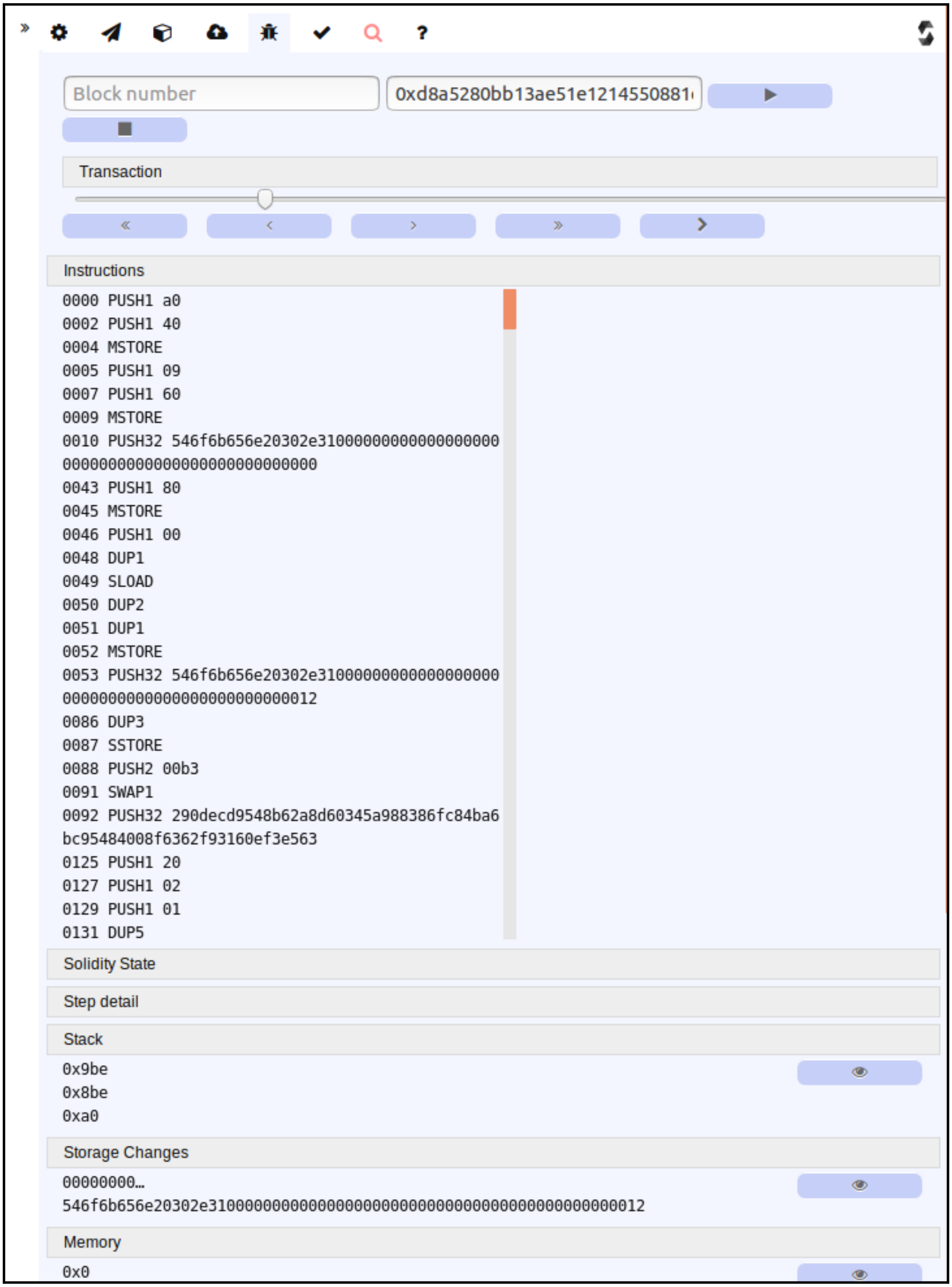
Execution environment has been provided by Mist or similar provider.

● **Web3 Provider**

Execution environment connects to node at localhost (or via IPC if available), transactions will be sent to the network and can cause loss of money or worse!

If this page is served via https and you access your node via http, it might not work. In this case, try cloning the repository and serving it via http.

Web3 Provider Endpoint: http://localhost:9000



```
0000 PUSH1 a0
0002 PUSH1 40
0004 MSTORE
0005 PUSH1 09
0007 PUSH1 60
0009 MSTORE
0010 PUSH32 546f6b656e20302e31000000000000000000
0000000000000000000000000000
0043 PUSH1 80
0045 MSTORE
0046 PUSH1 00
0048 DUP1
0049 SLOAD
0050 DUP2
0051 DUP1
0052 MSTORE
0053 PUSH32 546f6b656e20302e31000000000000000000
0000000000000000000000000012
0086 DUP3
0087 SSTORE
0088 PUSH2 00b3
0091 SWAP1
0092 PUSH32 290decd9548b62a8d60345a988386fc84ba6
bc95484008f6362f93160ef3e563
0125 PUSH1 20
0127 PUSH1 02
0129 PUSH1 01
0131 DUP5
```

Stack

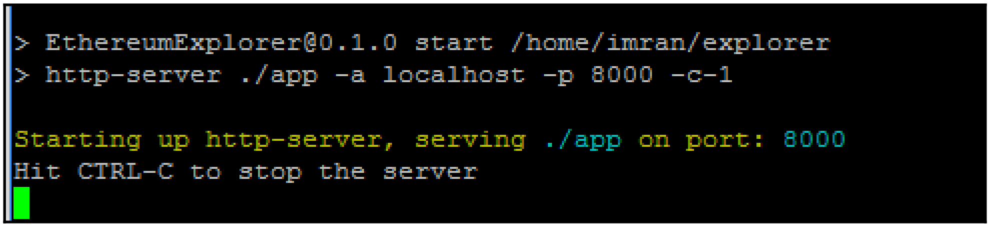
```
0x9be
0x8be
0xa0
```

Storage Changes

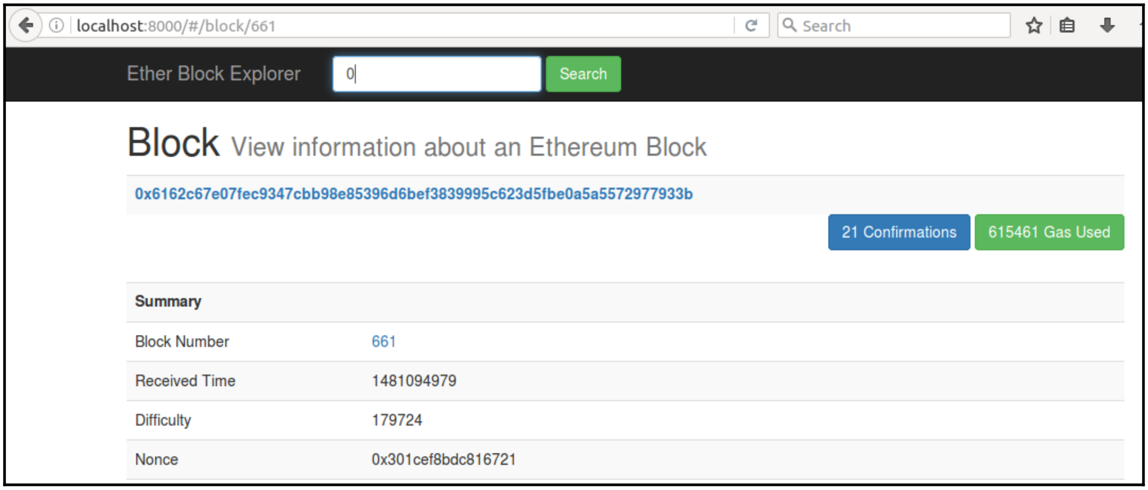
```
00000000…
546f6b656e20302e310000000000000000000000000000000000000000000012
```

Memory

```
0x0
```



```
> EthereumExplorer@0.1.0 start /home/imran/explorer
> http-server ./app -a localhost -p 8000 -c-1

Starting up http-server, serving ./app on port: 8000
Hit CTRL-C to stop the server
```

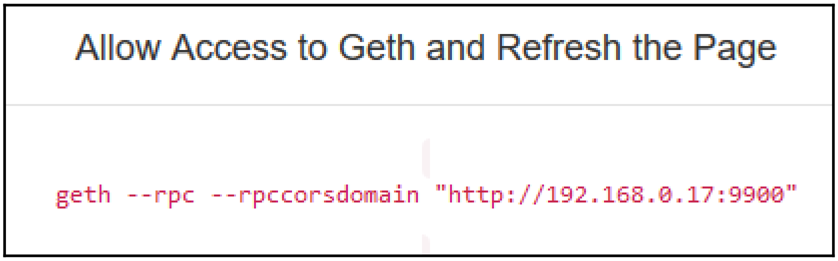


Block View information about an Ethereum Block

0x6162c67e07fec9347cbb98e85396d6bef3839995c623d5fbe0a5a5572977933b

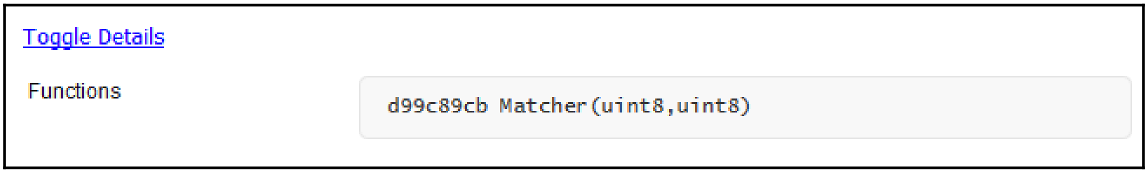
21 Confirmations 615461 Gas Used

Summary	
Block Number	661
Received Time	1481094979
Difficulty	179724
Nonce	0x301cef8bdc816721



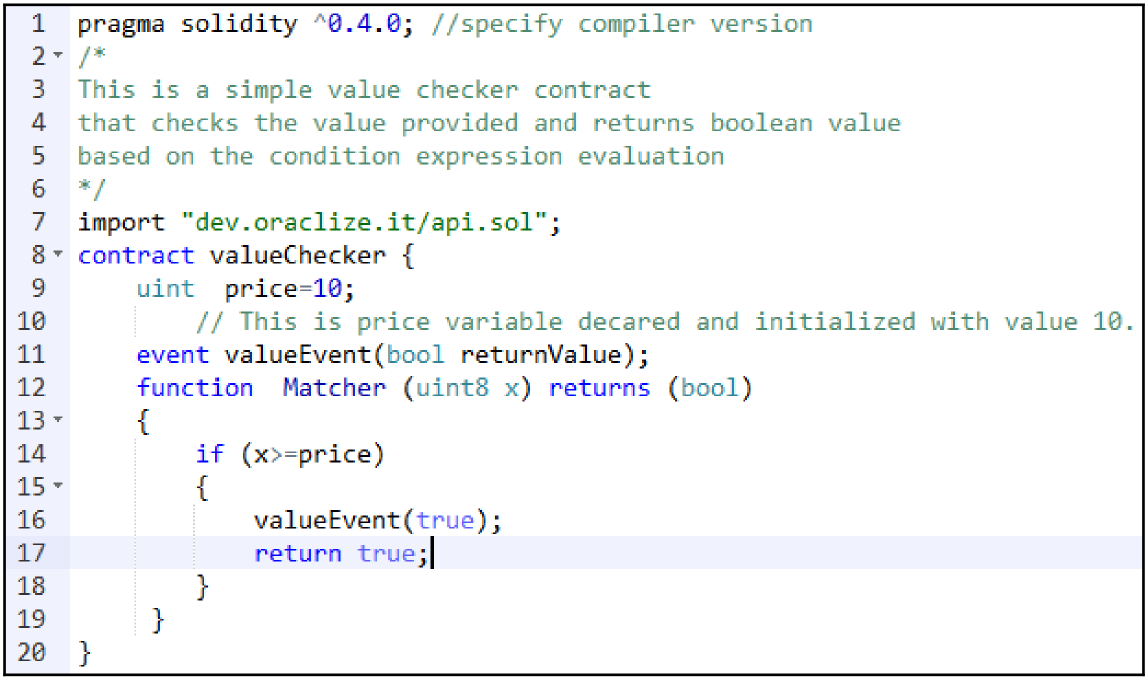
Allow Access to Geth and Refresh the Page

```
geth --rpc --rpccorsdomain "http://192.168.0.17:9900"
```

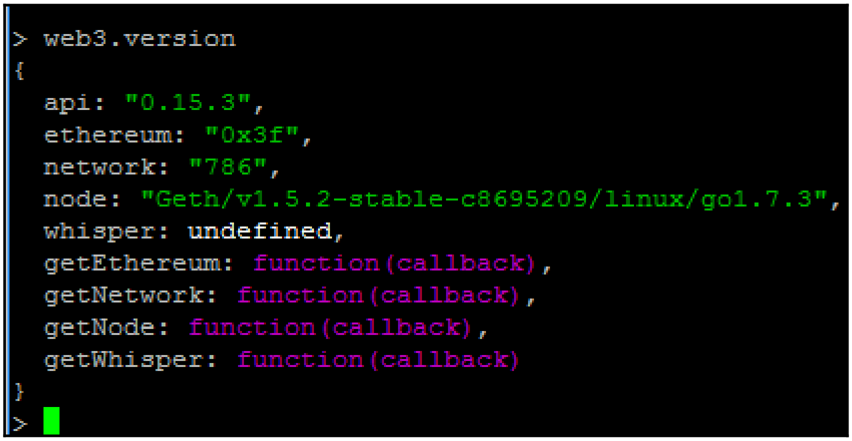


Functions

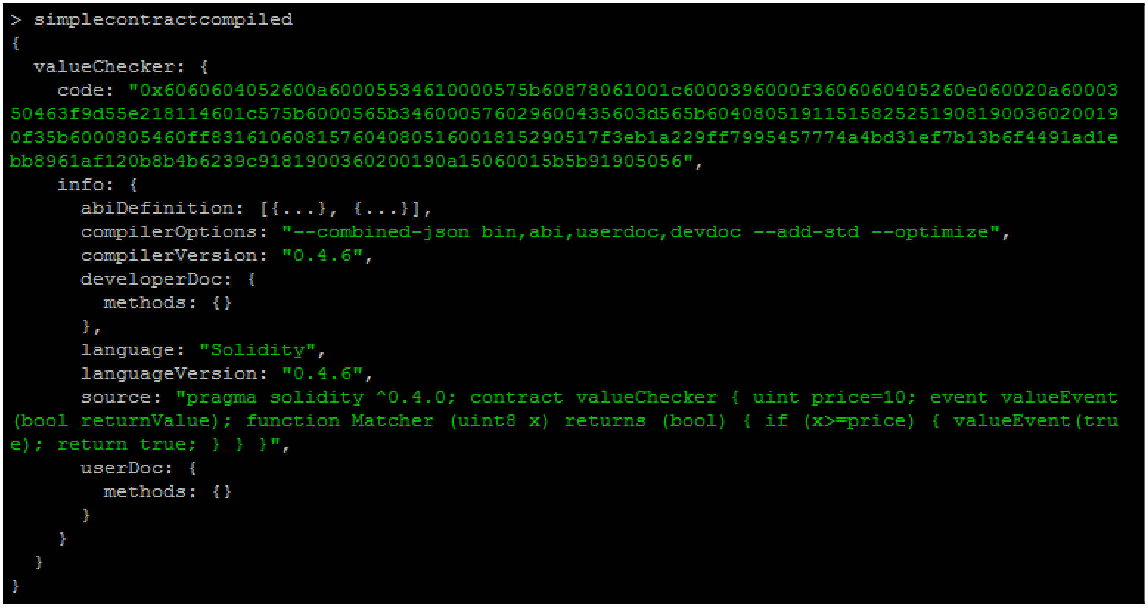
```
d99c89cb Matcher(uint8,uint8)
```



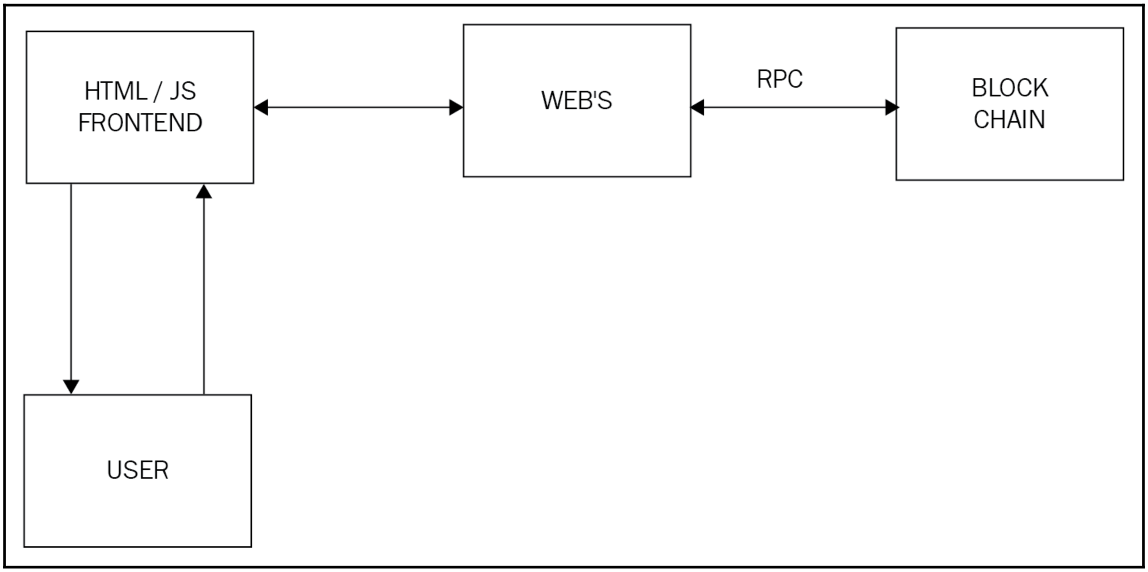
```
pragma solidity ^0.4.0; //specify compiler version
/*
This is a simple value checker contract
that checks the value provided and returns boolean value
based on the condition expression evaluation
*/
import "dev.oraclize.it/api.sol";
contract valueChecker {
    uint  price=10;
        // This is price variable decared and initialized with value 10.
    event valueEvent(bool returnValue);
    function  Matcher (uint8 x) returns (bool)
    {
        if (x>=price)
        {
            valueEvent(true);
            return true;
        }
     }
}
```

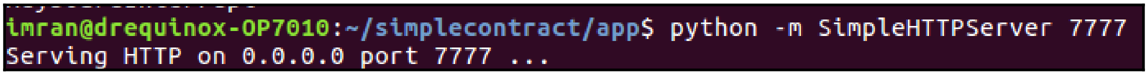


```
> web3.version
{
  api: "0.15.3",
  ethereum: "0x3f",
  network: "786",
  node: "Geth/v1.5.2-stable-c8695209/linux/go1.7.3",
  whisper: undefined,
  getEthereum: function(callback),
  getNetwork: function(callback),
  getNode: function(callback),
  getWhisper: function(callback)
}
>
```

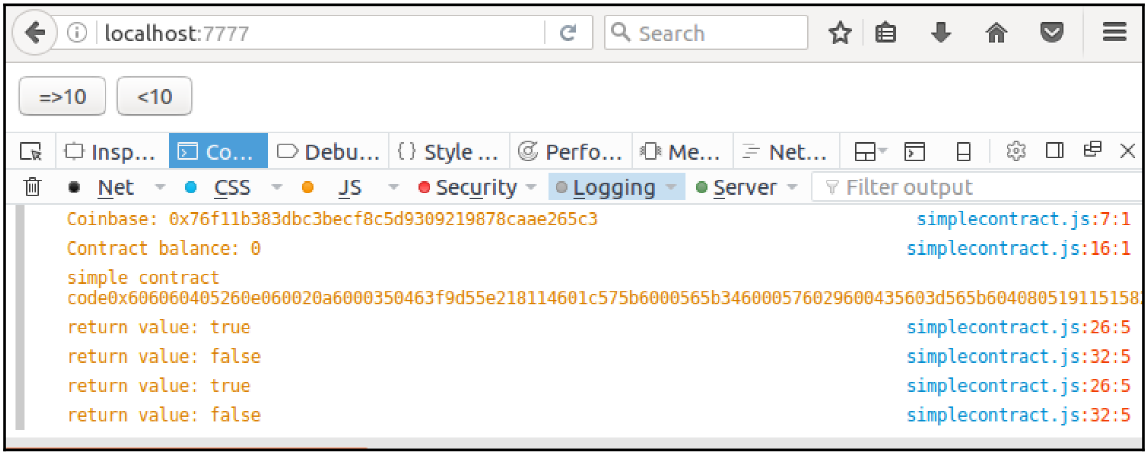


```
> simplecontractcompiled
{
  valueChecker: {
    code: "0x6060604052600a60005534610000575b60878061001c6000396000f3606060405260e060020a60003
50463f9d55e218114601c575b6000565b346000576029600435603d565b60408051911515825251908190036020019
0f35b6000805460ff831610608157604080516001815290517f3eb1a229ff7995457774a4bd31ef7b13b6f4491ad1e
bb8961af120b8b4b6239c9181900360200190a15060015b5b91905056",
    info: {
      abiDefinition: [{...}, {...}],
      compilerOptions: "--combined-json bin,abi,userdoc,devdoc --add-std --optimize",
      compilerVersion: "0.4.6",
      developerDoc: {
        methods: {}
      },
      language: "Solidity",
      languageVersion: "0.4.6",
      source: "pragma solidity ^0.4.0; contract valueChecker { uint price=10; event valueEvent
(bool returnValue); function Matcher (uint8 x) returns (bool) { if (x>=price) { valueEvent(tru
e); return true; } } }",
      userDoc: {
        methods: {}
      }
    }
  }
}
```

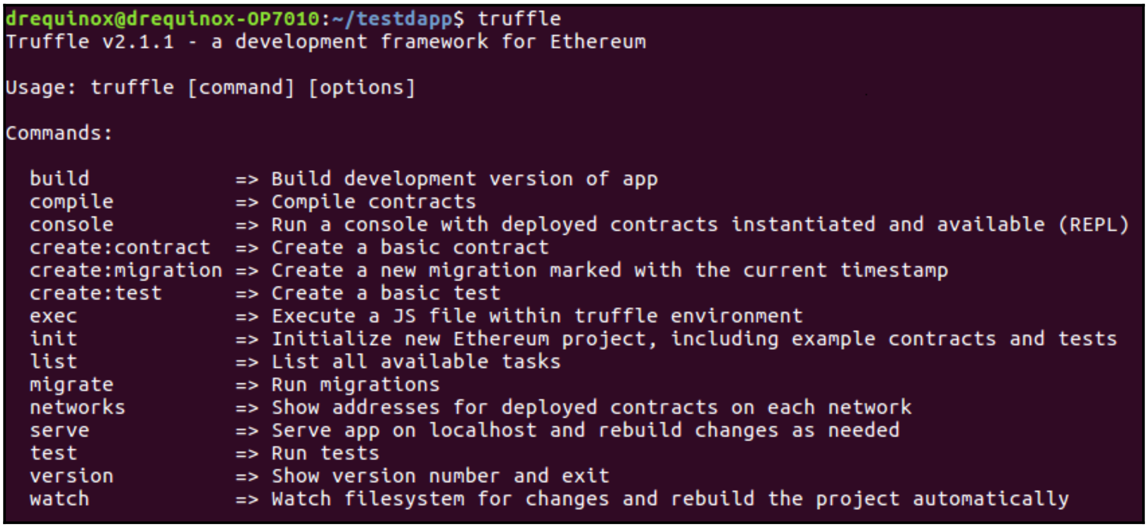




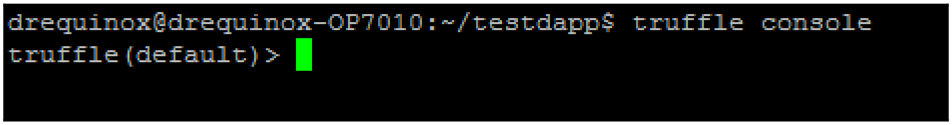
```
imran@drequinox-OP7010:~/simplecontract/app$ python -m SimpleHTTPServer 7777
Serving HTTP on 0.0.0.0 port 7777 ...
```



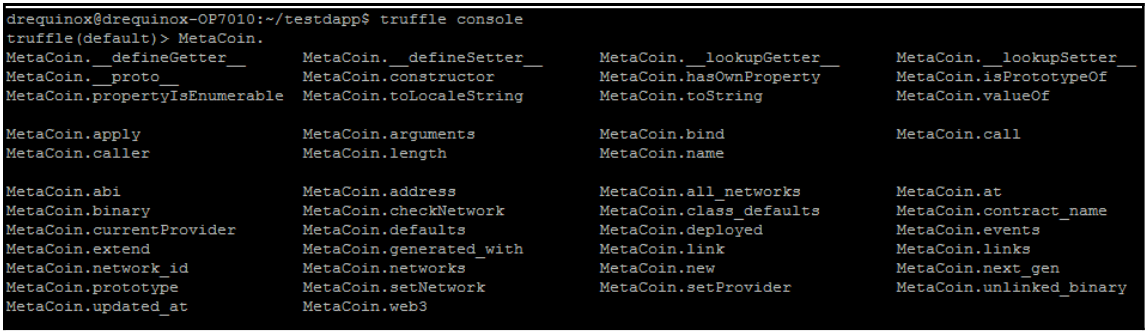
```
Coinbase: 0x76f11b383dbc3becf8c5d9309219878caae265c3          simplecontract.js:7:1
Contract balance: 0                                           simplecontract.js:16:1
simple contract
code0x606060405260e060020a6000350463f9d55e218114601c575b6000565b346000576029600435603d565b604080519115158
return value: true                                            simplecontract.js:26:5
return value: false                                           simplecontract.js:32:5
return value: true                                            simplecontract.js:26:5
return value: false                                           simplecontract.js:32:5
```



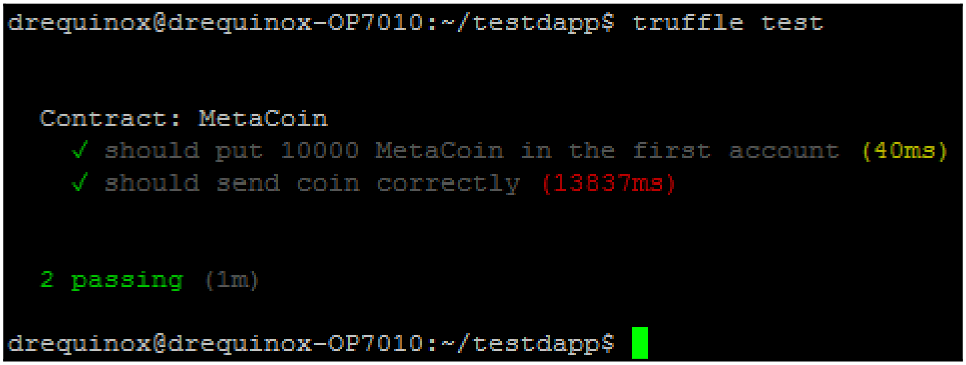
```
drequinox@drequinox-OP7010:~/testdapp$ truffle
Truffle v2.1.1 - a development framework for Ethereum

Usage: truffle [command] [options]

Commands:

  build            => Build development version of app
  compile          => Compile contracts
  console          => Run a console with deployed contracts instantiated and available (REPL)
  create:contract  => Create a basic contract
  create:migration => Create a new migration marked with the current timestamp
  create:test      => Create a basic test
  exec             => Execute a JS file within truffle environment
  init             => Initialize new Ethereum project, including example contracts and tests
  list             => List all available tasks
  migrate          => Run migrations
  networks         => Show addresses for deployed contracts on each network
  serve            => Serve app on localhost and rebuild changes as needed
  test             => Run tests
  version          => Show version number and exit
  watch            => Watch filesystem for changes and rebuild the project automatically
```



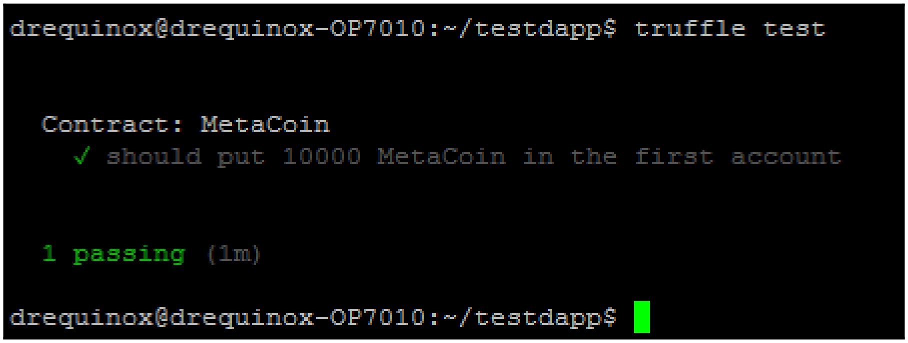
```
drequinox@drequinox-OP7010:~/testdapp$ truffle console
truffle(default)>
```



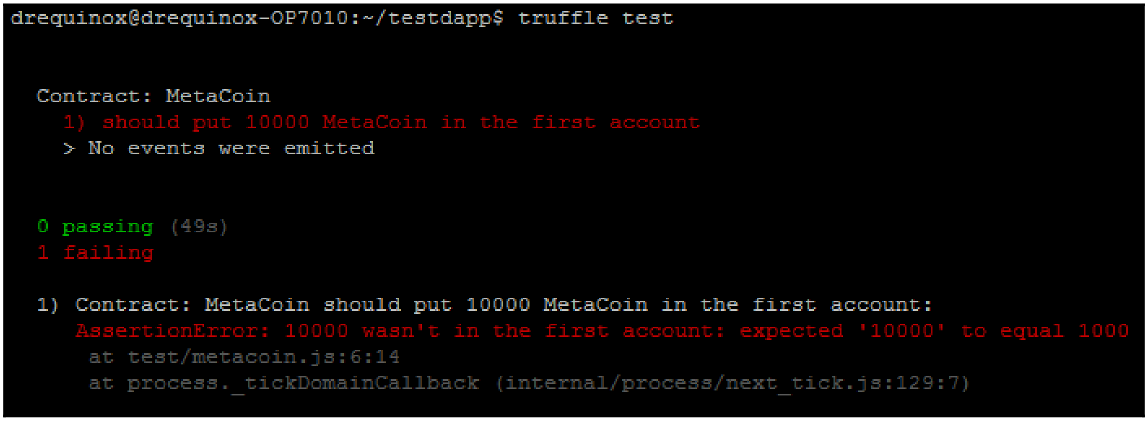
```
drequinox@drequinox-OP7010:~/testdapp$ truffle console
truffle(default)> MetaCoin.
MetaCoin.__defineGetter__      MetaCoin.__defineSetter__      MetaCoin.__lookupGetter__      MetaCoin.__lookupSetter__
MetaCoin.__proto__             MetaCoin.constructor           MetaCoin.hasOwnProperty        MetaCoin.isPrototypeOf
MetaCoin.propertyIsEnumerable  MetaCoin.toLocaleString        MetaCoin.toString              MetaCoin.valueOf

MetaCoin.apply                 MetaCoin.arguments             MetaCoin.bind                  MetaCoin.call
MetaCoin.caller                MetaCoin.length                MetaCoin.name

MetaCoin.abi                   MetaCoin.address               MetaCoin.all_networks          MetaCoin.at
MetaCoin.binary                MetaCoin.checkNetwork          MetaCoin.class_defaults        MetaCoin.contract_name
MetaCoin.currentProvider       MetaCoin.defaults              MetaCoin.deployed              MetaCoin.events
MetaCoin.extend                MetaCoin.generated_with        MetaCoin.link                  MetaCoin.links
MetaCoin.network_id            MetaCoin.networks              MetaCoin.new                   MetaCoin.next_gen
MetaCoin.prototype             MetaCoin.setNetwork            MetaCoin.setProvider           MetaCoin.unlinked_binary
MetaCoin.updated_at            MetaCoin.web3
```



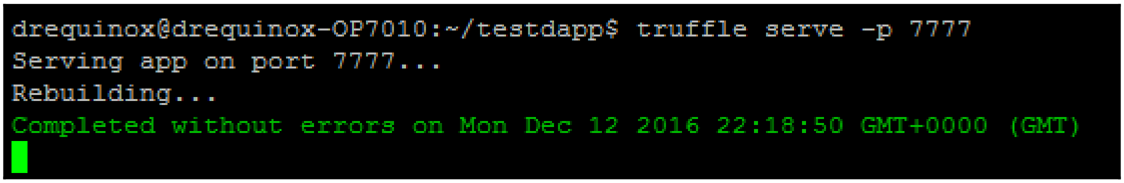
```
drequinox@drequinox-OP7010:~/testdapp$ truffle test


  Contract: MetaCoin
    ✓ should put 10000 MetaCoin in the first account (40ms)
    ✓ should send coin correctly (13837ms)


  2 passing (1m)

drequinox@drequinox-OP7010:~/testdapp$ █
```



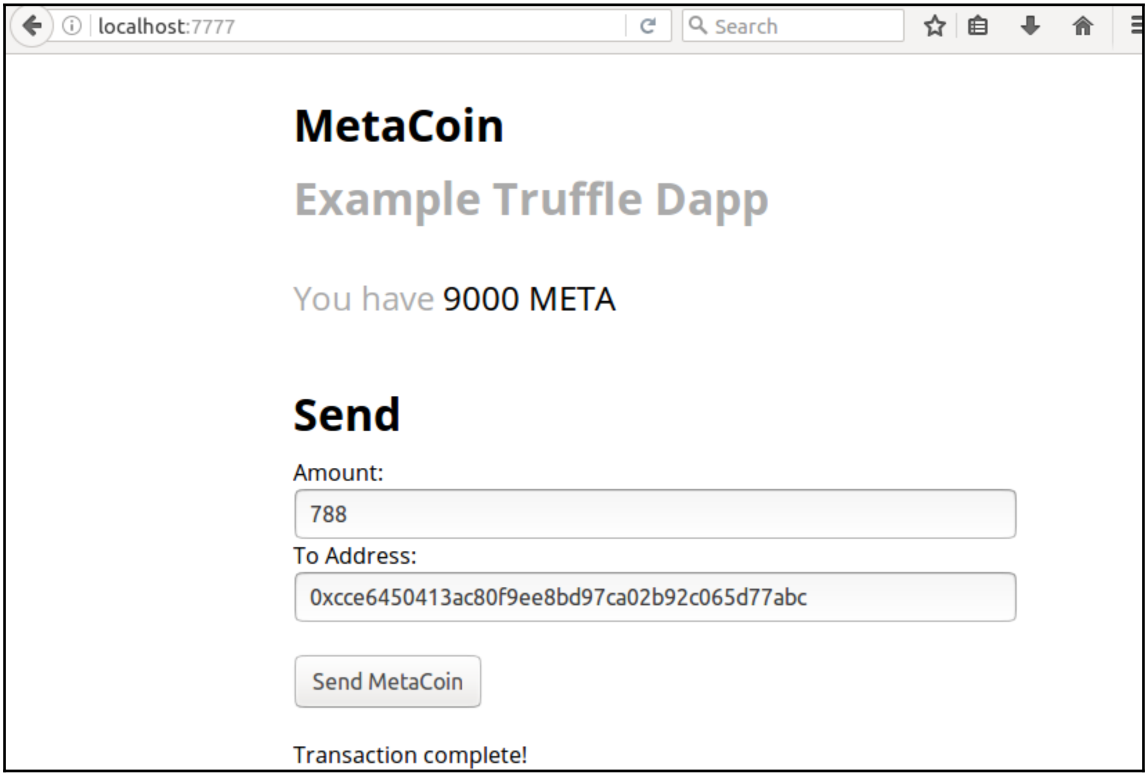
```
drequinox@drequinox-OP7010:~/testdapp$ truffle test


  Contract: MetaCoin
    ✓ should put 10000 MetaCoin in the first account


  1 passing (1m)

drequinox@drequinox-OP7010:~/testdapp$ █
```



```
drequinox@drequinox-OP7010:~/testdapp$ truffle test


  Contract: MetaCoin
    1) should put 10000 MetaCoin in the first account
    > No events were emitted


  0 passing (49s)
  1 failing

  1) Contract: MetaCoin should put 10000 MetaCoin in the first account:
     AssertionError: 10000 wasn't in the first account: expected '10000' to equal 1000
      at test/metacoin.js:6:14
      at process._tickDomainCallback (internal/process/next_tick.js:129:7)
```



```
drequinox@drequinox-OP7010:~/testdapp$ truffle serve -p 7777
Serving app on port 7777...
Rebuilding...
Completed without errors on Mon Dec 12 2016 22:18:50 GMT+0000 (GMT)
```



MetaCoin

Example Truffle Dapp

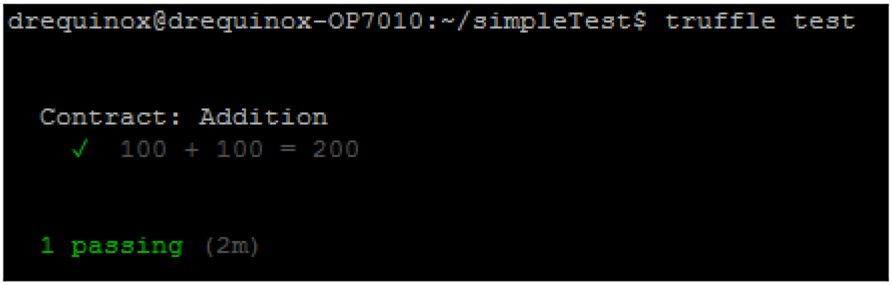
You have 9000 META

Send

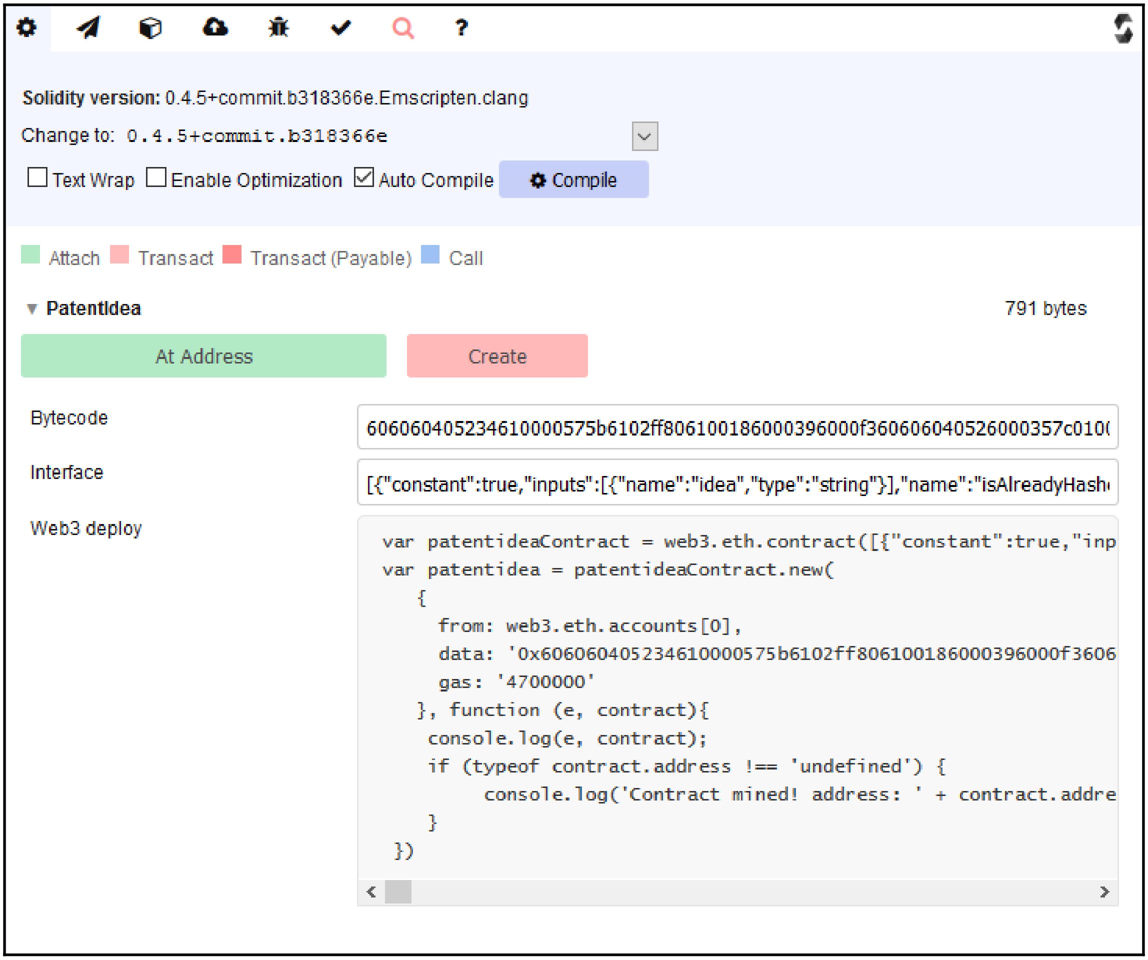
Amount: 788

To Address: 0xcce6450413ac80f9ee8bd97ca02b92c065d77abc

Transaction complete!



```
drequinox@drequinox-OP7010:~/simpleTest$ truffle test


  Contract: Addition
    ✓  100 + 100 = 200


  1 passing (2m)
```



Solidity version: 0.4.5+commit.b318366e.Emscripten.clang

Change to: `0.4.5+commit.b318366e`

☐ Text Wrap ☐ Enable Optimization ☑ Auto Compile

🟩 Attach 🟥 Transact 🟥 Transact (Payable) 🟦 Call

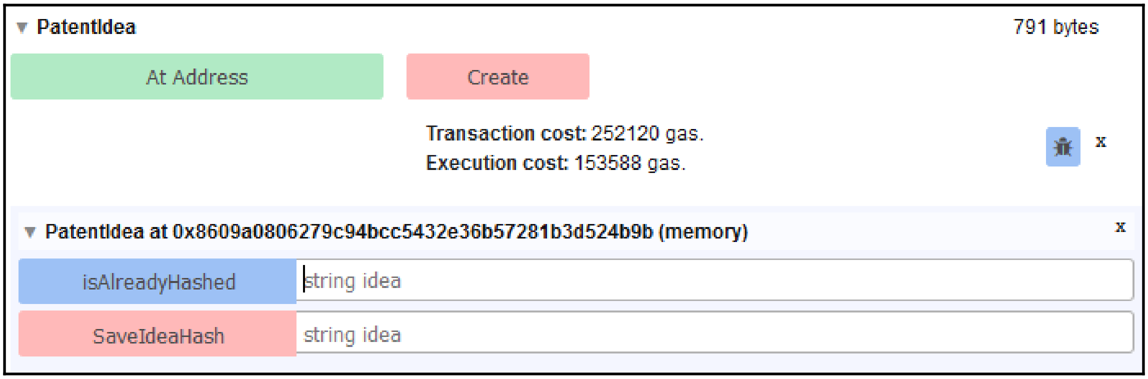
▼ **PatentIdea** 791 bytes

Bytecode: 6060604052346100005 75b6102ff80610018600039 6000f3606060405260003 57c010(

Interface: [{"constant":true,"inputs":[{"name":"idea","type":"string"}],"name":"isAlreadyHash(

Web3 deploy

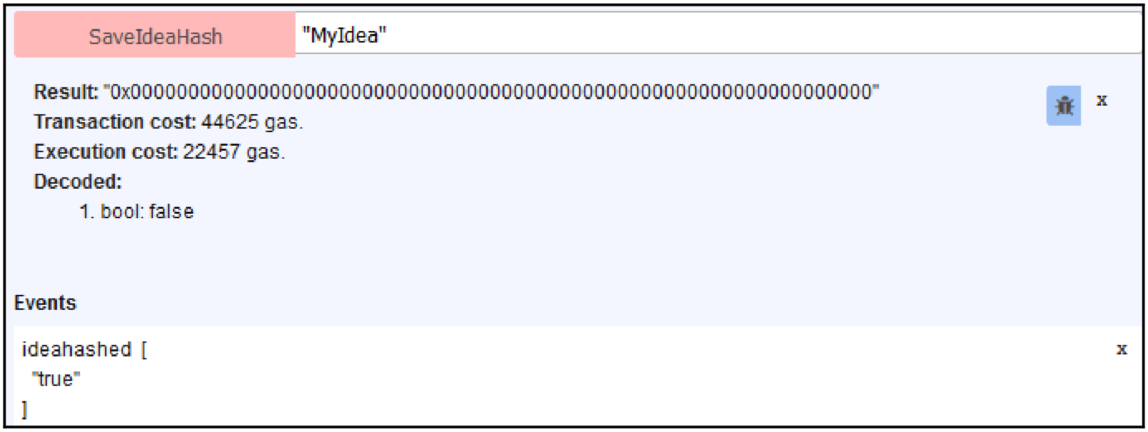
```
var patentideaContract = web3.eth.contract([{"constant":true,"inp
var patentidea = patentideaContract.new(
   {
     from: web3.eth.accounts[0],
     data: '0x6060604052346100005 75b6102ff80610018600039 6000f3606
     gas: '4700000'
   }, function (e, contract){
    console.log(e, contract);
    if (typeof contract.address !== 'undefined') {
         console.log('Contract mined! address: ' + contract.addre
    }
 })
```



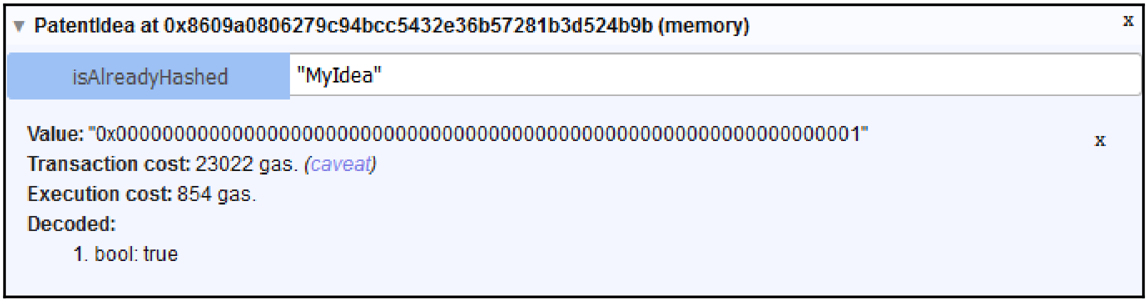
▼ **PatentIdea** 791 bytes

Transaction cost: 252120 gas.
Execution cost: 153588 gas.

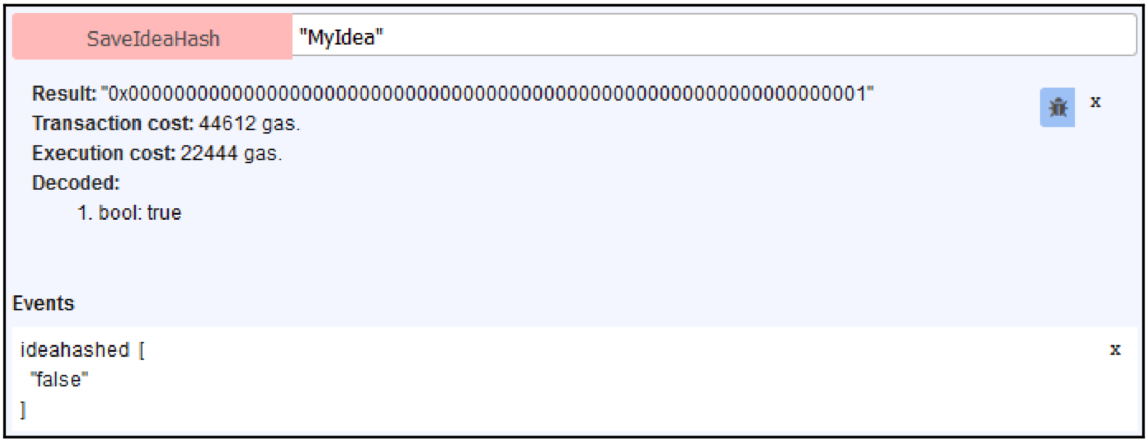
▼ **PatentIdea at 0x8609a0806279c94bcc5432e36b57281b3d524b9b (memory)**



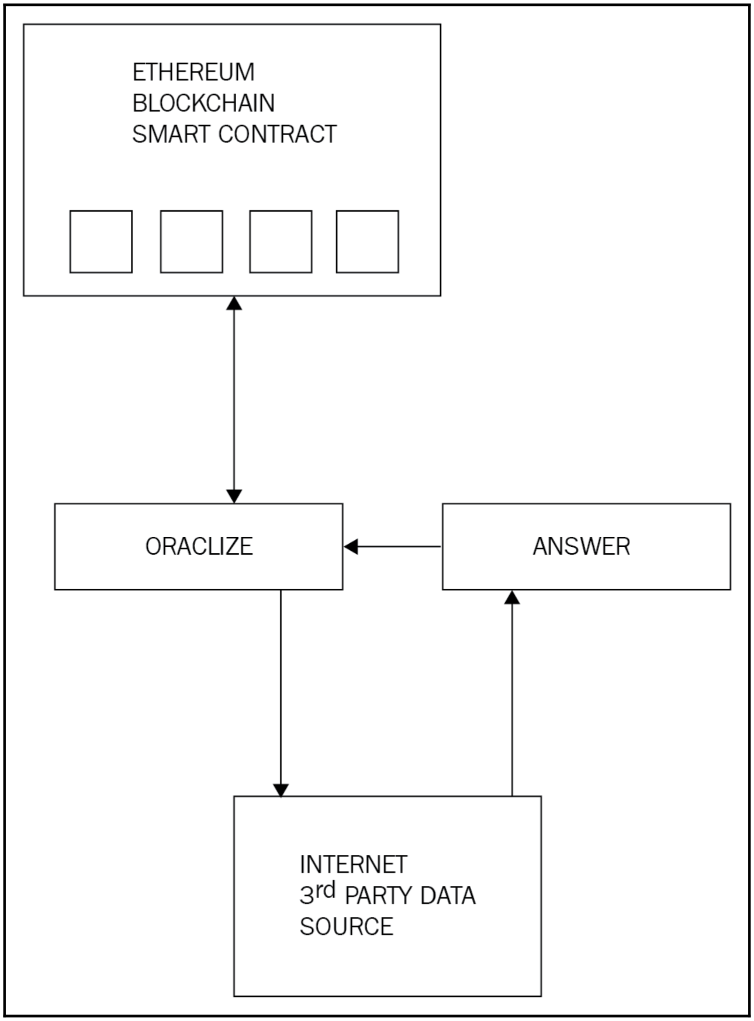
```
"MyIdea"

Result: "0x0000000000000000000000000000000000000000000000000000000000000000"
Transaction cost: 44625 gas.
Execution cost: 22457 gas.
Decoded:
        1. bool: false

Events
ideahashed [
  "true"
]
```

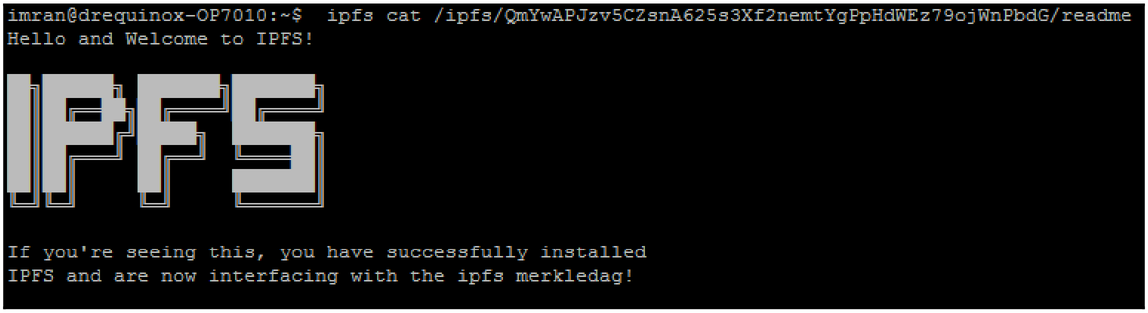


```
▼ PatentIdea at 0x8609a0806279c94bcc5432e36b57281b3d524b9b (memory)
"MyIdea"

Value: "0x0000000000000000000000000000000000000000000000000000000000000001"
Transaction cost: 23022 gas. (caveat)
Execution cost: 854 gas.
Decoded:
        1. bool: true
```

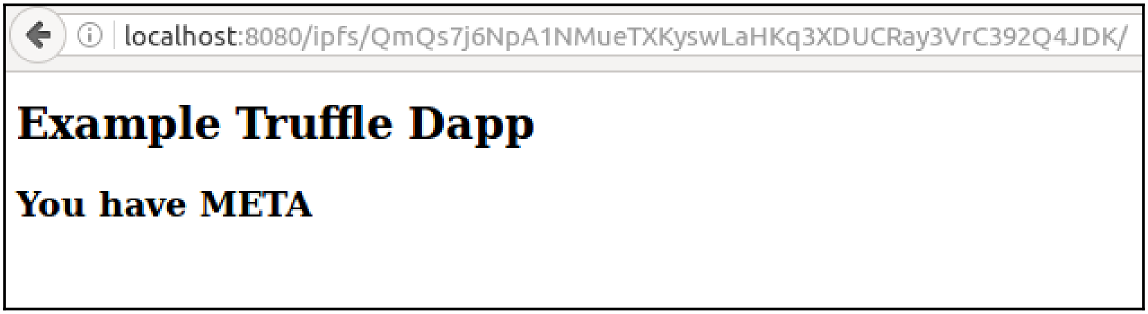


```
"MyIdea"

Result: "0x0000000000000000000000000000000000000000000000000000000000000001"
Transaction cost: 44612 gas.
Execution cost: 22444 gas.
Decoded:
        1. bool: true

Events
ideahashed [
  "false"
]
```





```
imran@drequinox-OP7010:~$  ipfs cat /ipfs/QmYwAPJzv5CZsnA625s3Xf2nemtYgPpHdWEz79ojWnPbdG/readme
Hello and Welcome to IPFS!

If you're seeing this, you have successfully installed
IPFS and are now interfacing with the ipfs merkledag!
```

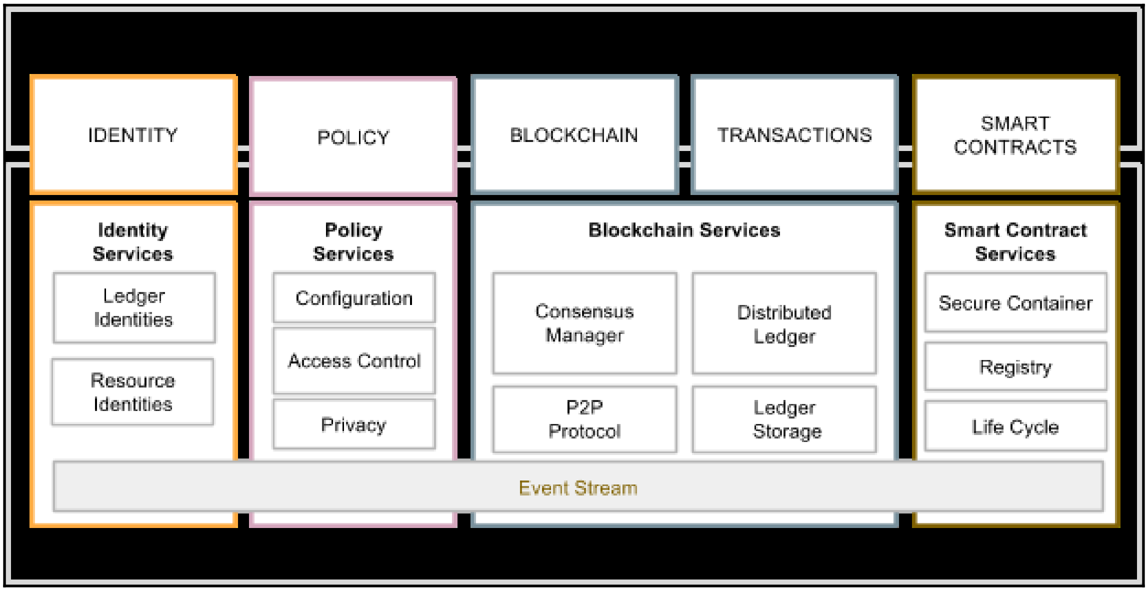


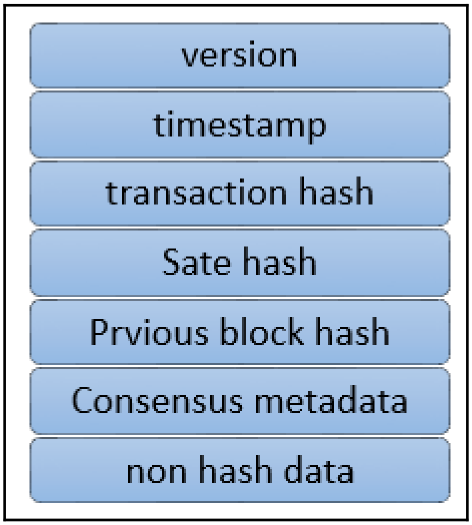
localhost:8080/ipfs/QmQs7j6NpA1NMueTXKyswLaHKq3XDUCRay3VrC392Q4JDK/

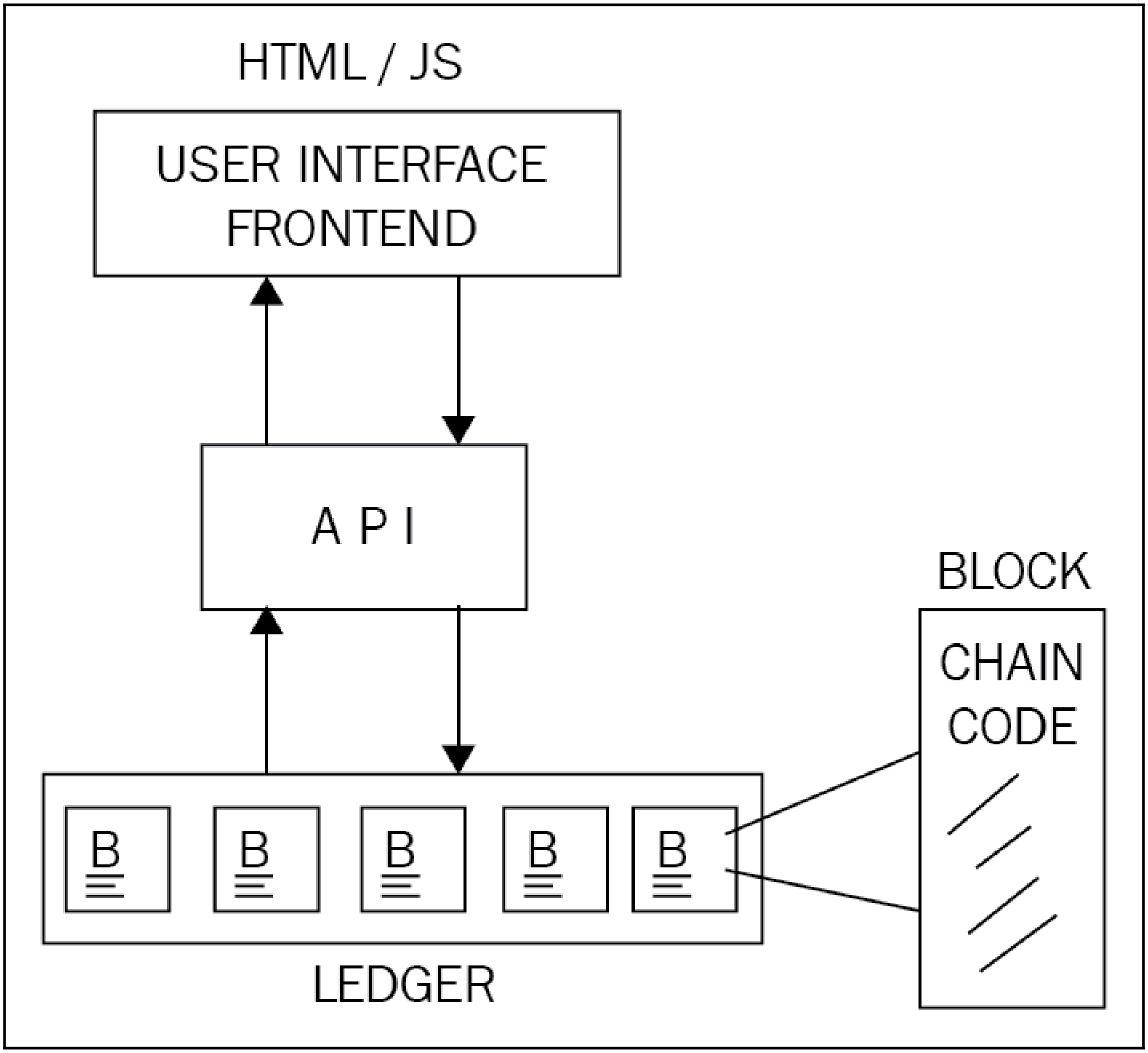
Example Truffle Dapp

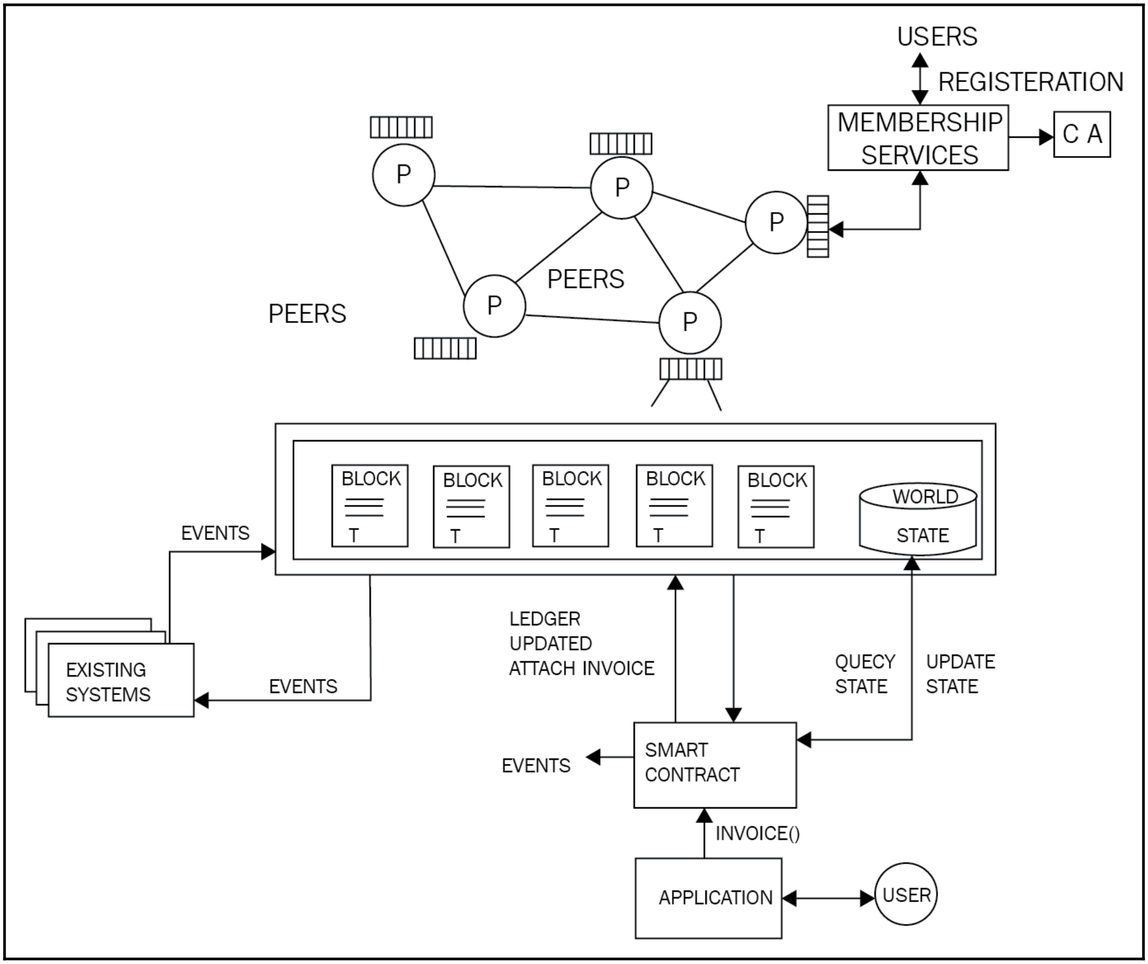
You have META

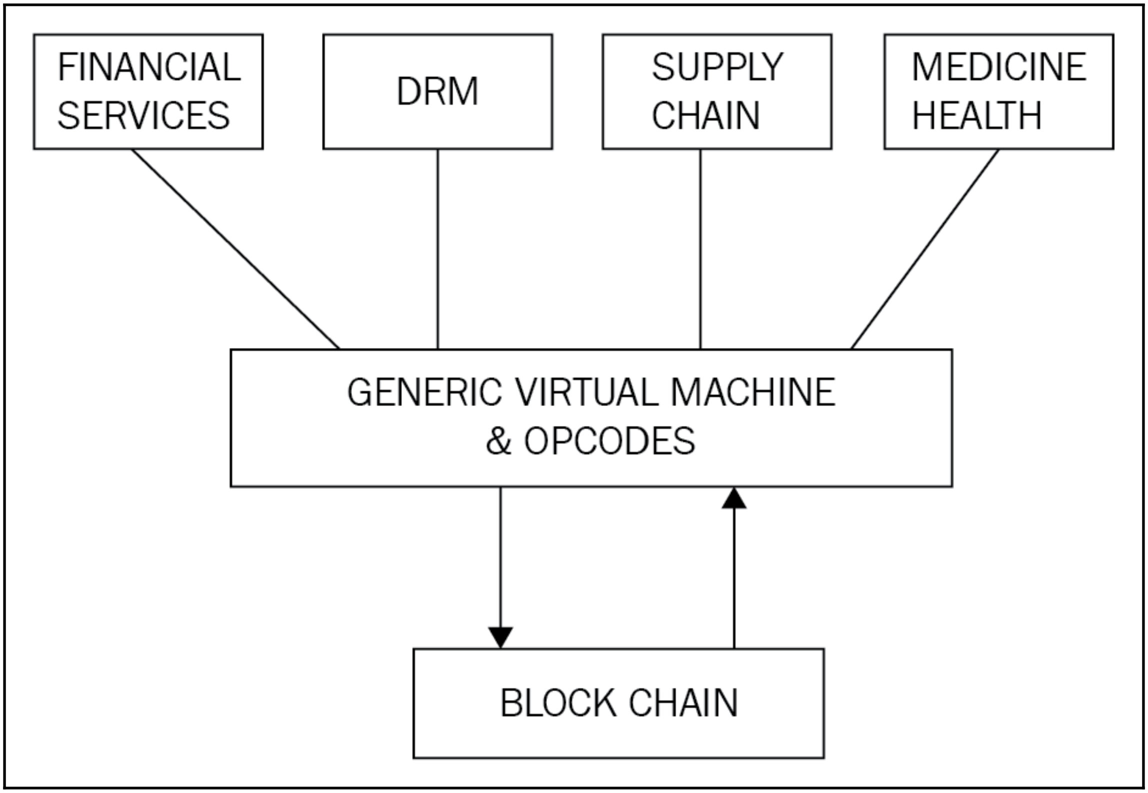
Chapter 9: Hyperledger

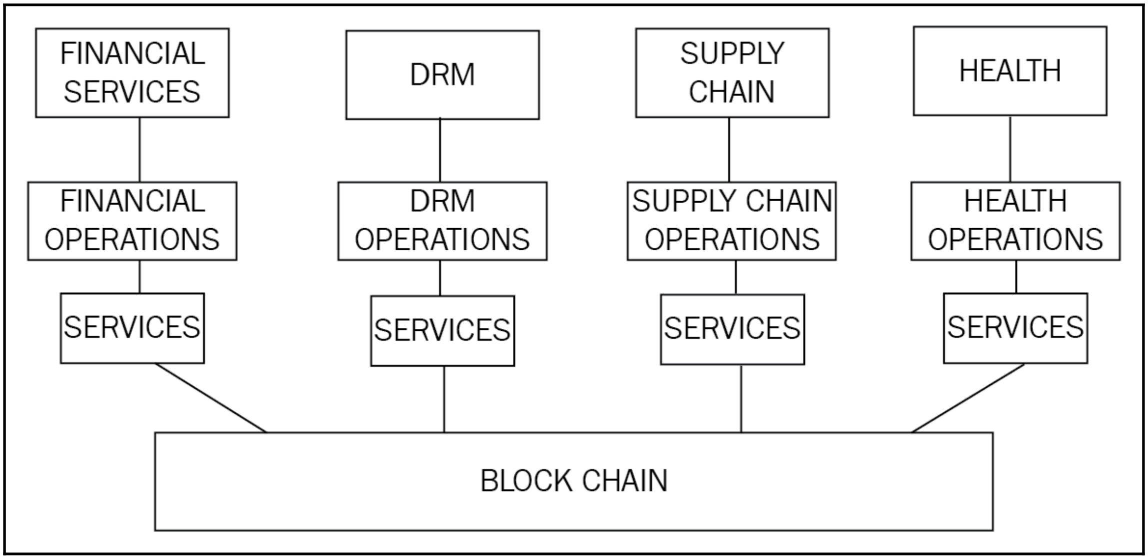


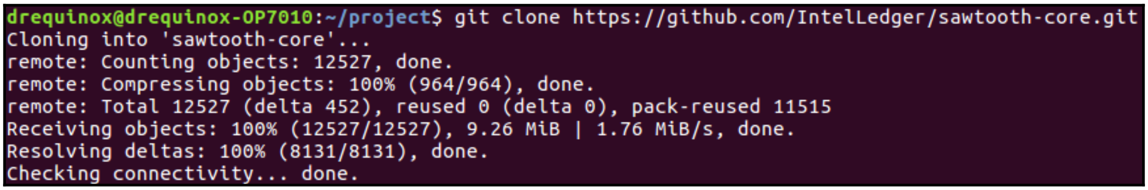



HTML / JS
USER INTERFACE
FRONTEND
A P I
BLOCK
CHAIN
CODE
B
B
B
B
B
LEDGER

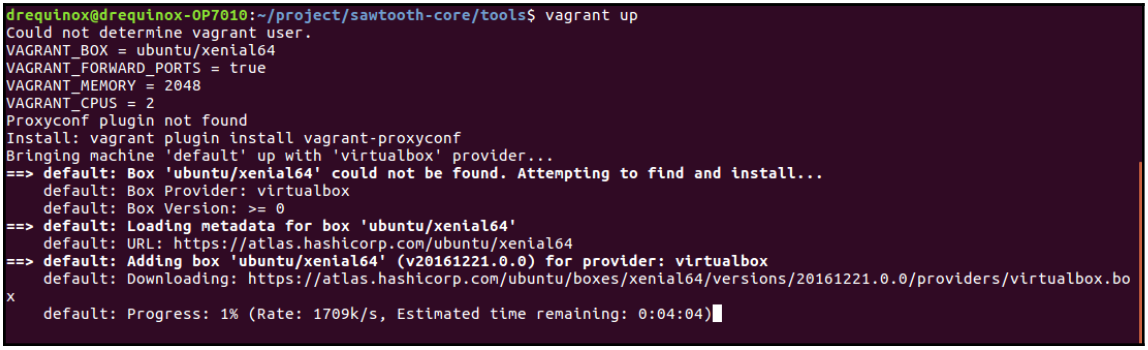

USERS
REGISTERATION
MEMBERSHIP SERVICES
C A
P
P
P
P
P
PEERS
PEERS
BLOCK
T
BLOCK
T
BLOCK
T
BLOCK
T
BLOCK
T
WORLD STATE
EVENTS
EXISTING SYSTEMS
EVENTS
LEDGER UPDATED ATTACH INVOICE
QUECY STATE
UPDATE STATE
SMART CONTRACT
EVENTS
INVOICE()
APPLICATION
USER


FINANCIAL SERVICES
DRM
SUPPLY CHAIN
MEDICINE HEALTH
GENERIC VIRTUAL MACHINE & OPCODES
BLOCK CHAIN

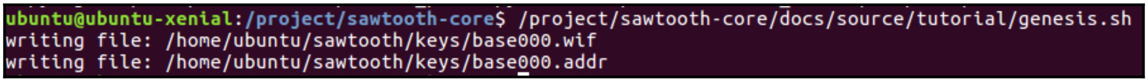




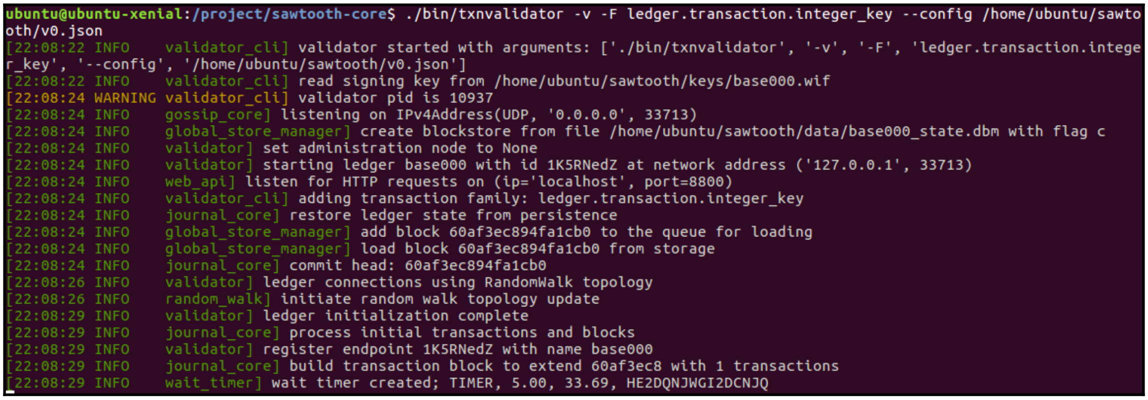
```
drequinox@drequinox-OP7010:~/project$ git clone https://github.com/IntelLedger/sawtooth-core.git
Cloning into 'sawtooth-core'...
remote: Counting objects: 12527, done.
remote: Compressing objects: 100% (964/964), done.
remote: Total 12527 (delta 452), reused 0 (delta 0), pack-reused 11515
Receiving objects: 100% (12527/12527), 9.26 MiB | 1.76 MiB/s, done.
Resolving deltas: 100% (8131/8131), done.
Checking connectivity... done.
```



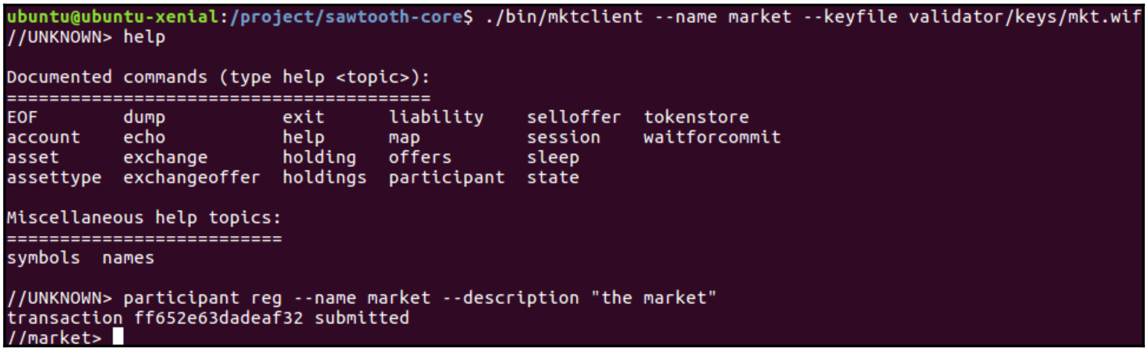
```
drequinox@drequinox-OP7010:~/project/sawtooth-core/tools$ vagrant up
Could not determine vagrant user.
VAGRANT_BOX = ubuntu/xenial64
VAGRANT_FORWARD_PORTS = true
VAGRANT_MEMORY = 2048
VAGRANT_CPUS = 2
Proxyconf plugin not found
Install: vagrant plugin install vagrant-proxyconf
Bringing machine 'default' up with 'virtualbox' provider...
==> default: Box 'ubuntu/xenial64' could not be found. Attempting to find and install...
    default: Box Provider: virtualbox
    default: Box Version: >= 0
==> default: Loading metadata for box 'ubuntu/xenial64'
    default: URL: https://atlas.hashicorp.com/ubuntu/xenial64
==> default: Adding box 'ubuntu/xenial64' (v20161221.0.0) for provider: virtualbox
    default: Downloading: https://atlas.hashicorp.com/ubuntu/boxes/xenial64/versions/20161221.0.0/providers/virtualbox.bo
x
    default: Progress: 1% (Rate: 1709k/s, Estimated time remaining: 0:04:04)
```



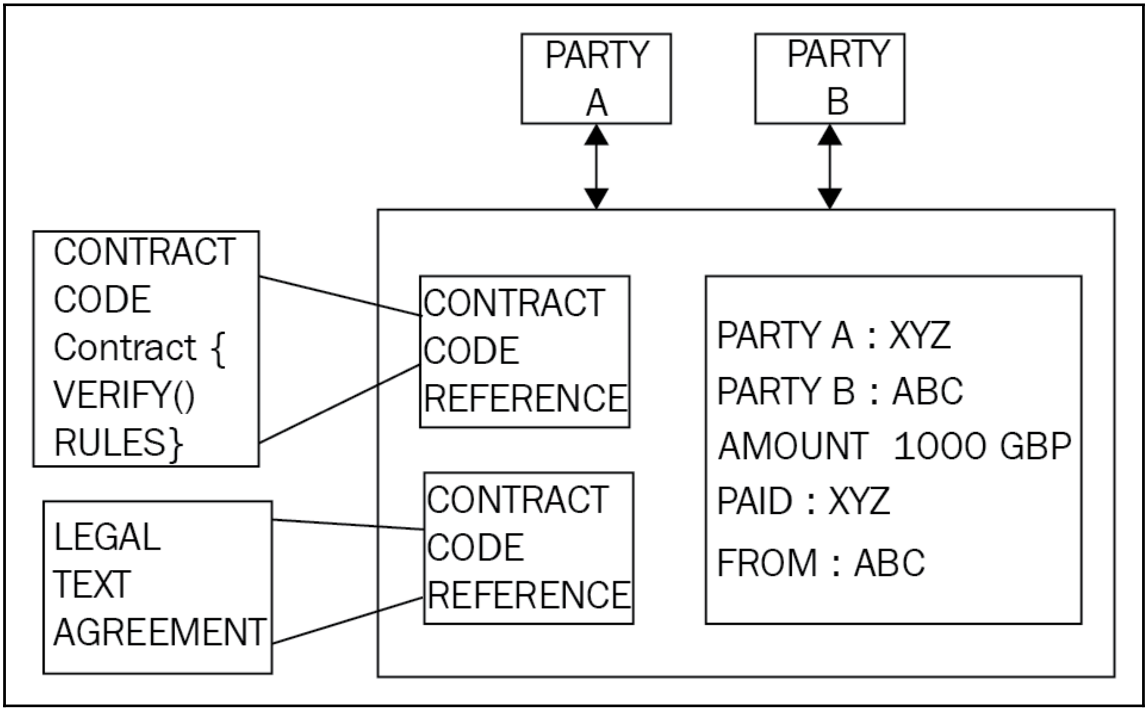
```
ubuntu@ubuntu-xenial:/project/sawtooth-core$ /project/sawtooth-core/docs/source/tutorial/genesis.sh
writing file: /home/ubuntu/sawtooth/keys/base000.wif
writing file: /home/ubuntu/sawtooth/keys/base000.addr
```

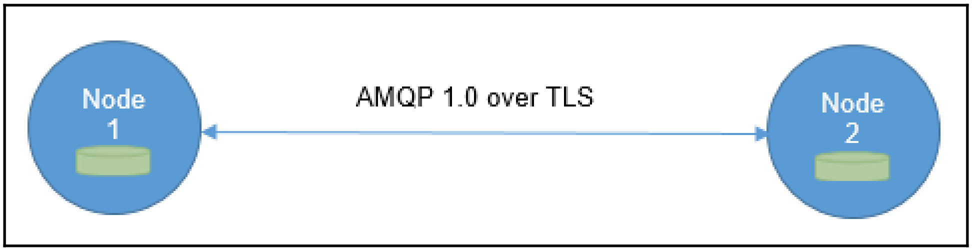


```
ubuntu@ubuntu-xenial:/project/sawtooth-core$ ./bin/txnvalidator -v -F ledger.transaction.integer_key --config /home/ubuntu/sawto
oth/v0.json
[22:08:22 INFO    validator_cli] validator started with arguments: ['./bin/txnvalidator', '-v', '-F', 'ledger.transaction.intege
r_key', '--config', '/home/ubuntu/sawtooth/v0.json']
[22:08:22 INFO    validator_cli] read signing key from /home/ubuntu/sawtooth/keys/base000.wif
[22:08:24 WARNING validator_cli] validator pid is 10937
[22:08:24 INFO    gossip_core] listening on IPv4Address(UDP, '0.0.0.0', 33713)
[22:08:24 INFO    global_store_manager] create blockstore from file /home/ubuntu/sawtooth/data/base000_state.dbm with flag c
[22:08:24 INFO    validator] set administration node to None
[22:08:24 INFO    validator] starting ledger base000 with id 1K5RNedZ at network address ('127.0.0.1', 33713)
[22:08:24 INFO    web_api] listen for HTTP requests on (ip='localhost', port=8800)
[22:08:24 INFO    validator_cli] adding transaction family: ledger.transaction.integer_key
[22:08:24 INFO    journal_core] restore ledger state from persistence
[22:08:24 INFO    global_store_manager] add block 60af3ec894fa1cb0 to the queue for loading
[22:08:24 INFO    global_store_manager] load block 60af3ec894fa1cb0 from storage
[22:08:24 INFO    journal_core] commit head: 60af3ec894fa1cb0
[22:08:26 INFO    validator] ledger connections using RandomWalk topology
[22:08:26 INFO    random_walk] initiate random walk topology update
[22:08:29 INFO    validator] ledger initialization complete
[22:08:29 INFO    journal_core] process initial transactions and blocks
[22:08:29 INFO    validator] register endpoint 1K5RNedZ with name base000
[22:08:29 INFO    journal_core] build transaction block to extend 60af3ec8 with 1 transactions
[22:08:29 INFO    wait_timer] wait timer created; TIMER, 5.00, 33.69, HE2DQNJWGI2DCNJQ
```

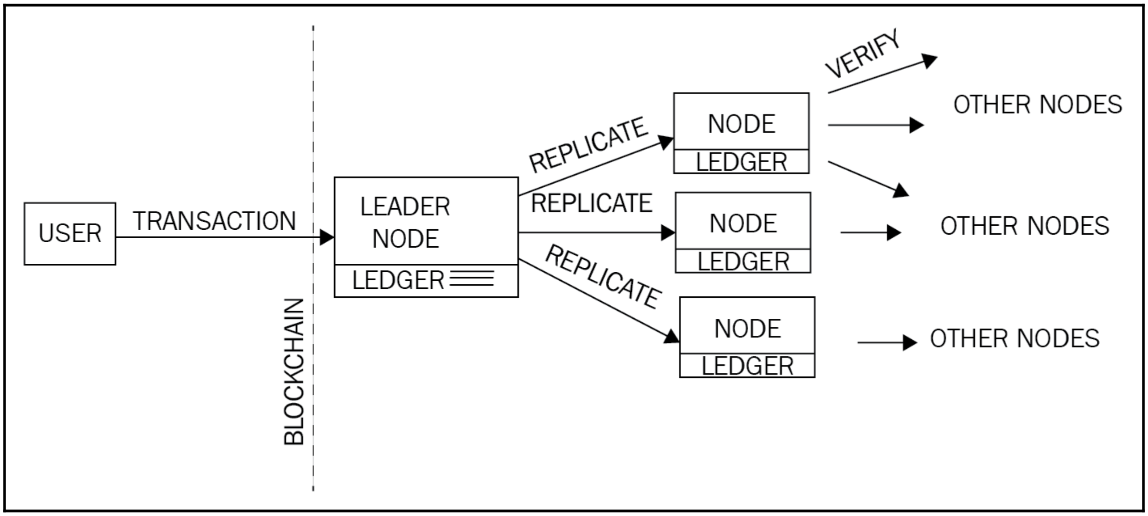


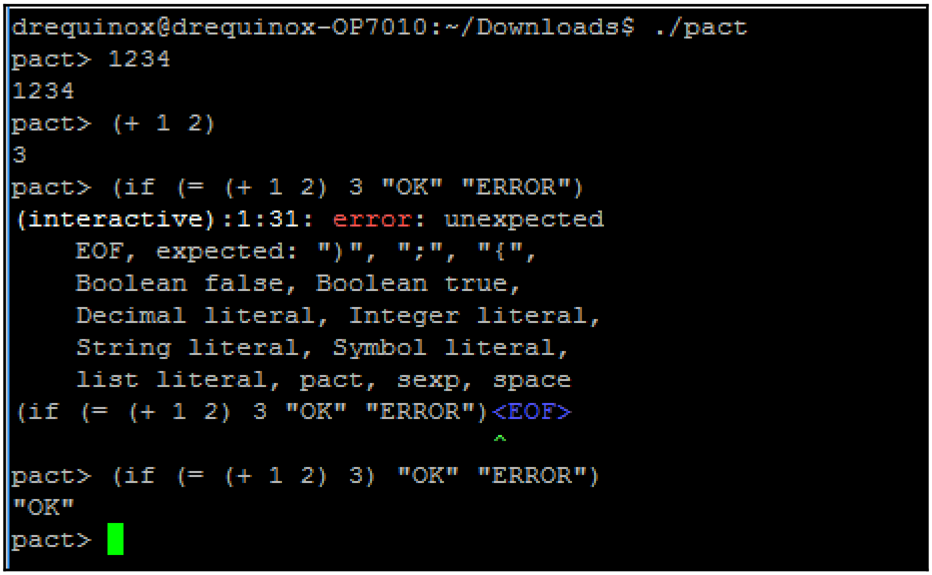
```
ubuntu@ubuntu-xenial:/project/sawtooth-core$ ./bin/mktclient --name market --keyfile validator/keys/mkt.wif
//UNKNOWN> help

Documented commands (type help <topic>):
========================================
EOF        dump           exit      liability    selloffer  tokenstore
account    echo           help      map          session    waitforcommit
asset      exchange       holding   offers       sleep
assettype  exchangeoffer  holdings  participant  state

Miscellaneous help topics:
==========================
symbols  names

//UNKNOWN> participant reg --name market --description "the market"
transaction ff652e63dadeaf32 submitted
//market>
```


PARTY A
PARTY B
CONTRACT CODE Contract { VERIFY() RULES}
CONTRACT CODE REFERENCE
PARTY A : XYZ
PARTY B : ABC
AMOUNT 1000 GBP
PAID : XYZ
FROM : ABC
LEGAL TEXT AGREEMENT
CONTRACT CODE REFERENCE

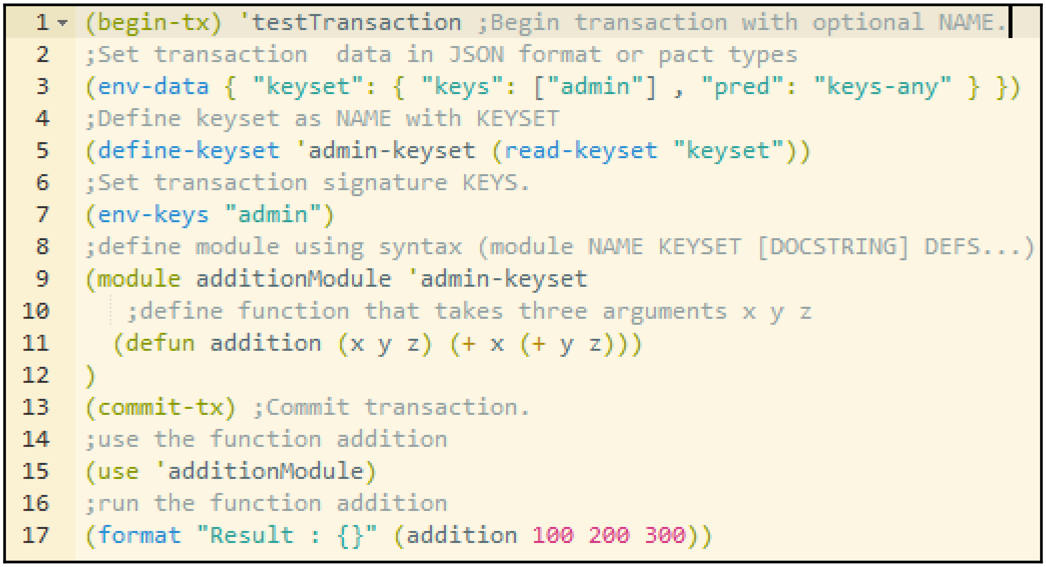

Node 1
AMQP 1.0 over TLS
Node 2

Chapter 10: Alternative Blockchains

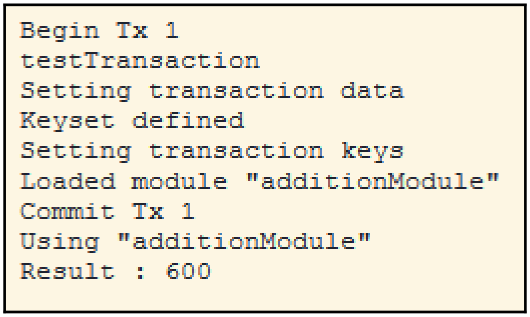




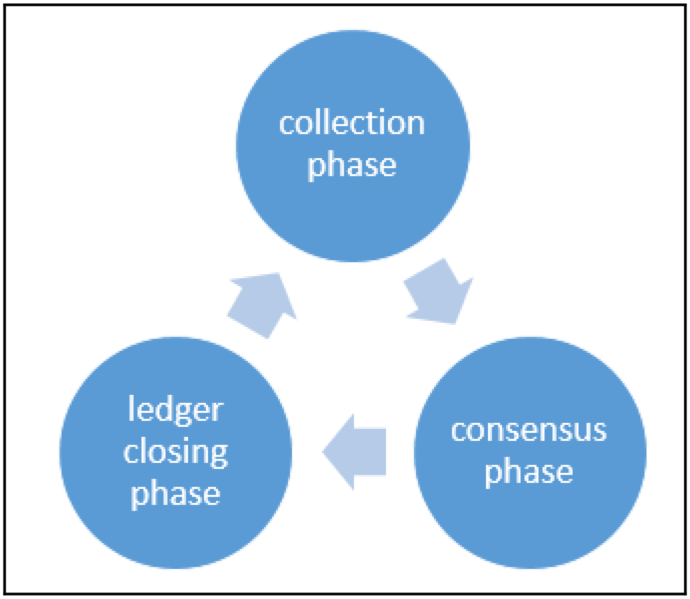
```
drequinox@drequinox-OP7010:~/Downloads$ ./pact
pact> 1234
1234
pact> (+ 1 2)
3
pact> (if (= (+ 1 2) 3 "OK" "ERROR")
(interactive):1:31: error: unexpected
    EOF, expected: ")", ";", "{",
    Boolean false, Boolean true,
    Decimal literal, Integer literal,
    String literal, Symbol literal,
    list literal, pact, sexp, space
(if (= (+ 1 2) 3 "OK" "ERROR")<EOF>
                              ^

pact> (if (= (+ 1 2) 3) "OK" "ERROR")
"OK"
pact>
```

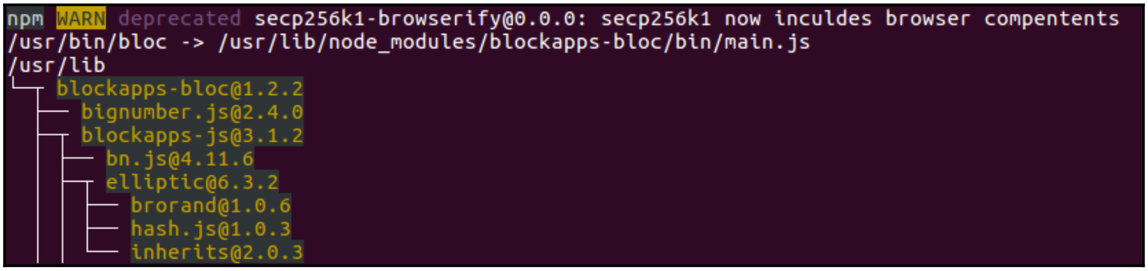


```
(begin-tx) 'testTransaction ;Begin transaction with optional NAME.
;Set transaction  data in JSON format or pact types
(env-data { "keyset": { "keys": ["admin"] , "pred": "keys-any" } })
;Define keyset as NAME with KEYSET
(define-keyset 'admin-keyset (read-keyset "keyset"))
;Set transaction signature KEYS.
(env-keys "admin")
;define module using syntax (module NAME KEYSET [DOCSTRING] DEFS...)
(module additionModule 'admin-keyset
   ;define function that takes three arguments x y z
  (defun addition (x y z) (+ x (+ y z)))
)
(commit-tx) ;Commit transaction.
;use the function addition
(use 'additionModule)
;run the function addition
(format "Result : {}" (addition 100 200 300))
```

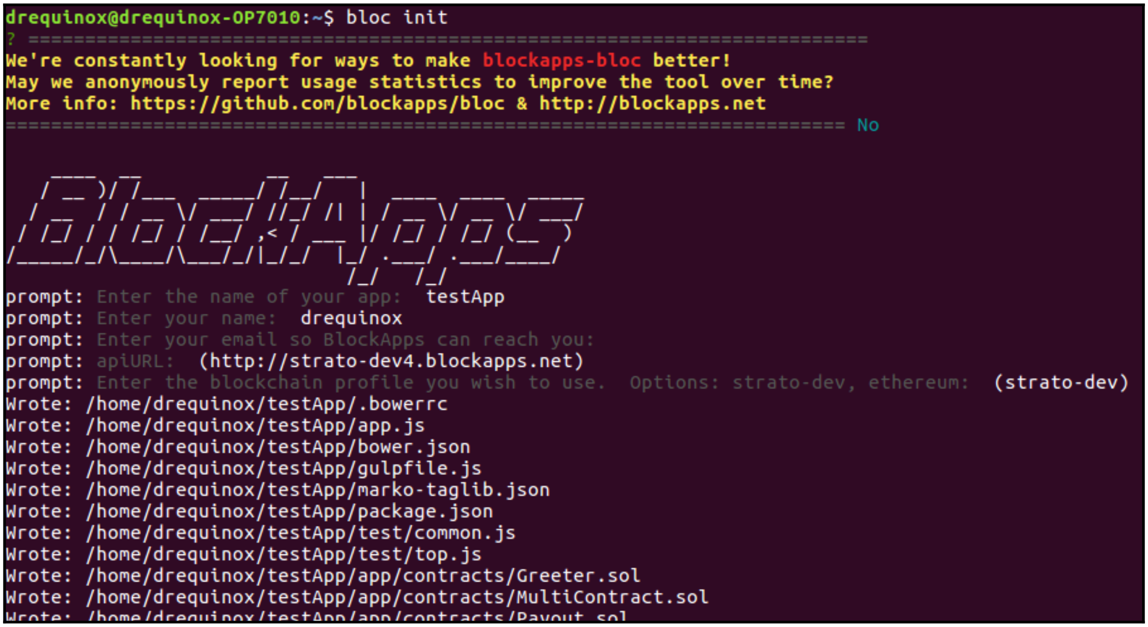


```
Begin Tx 1
testTransaction
Setting transaction data
Keyset defined
Setting transaction keys
Loaded module "additionModule"
Commit Tx 1
Using "additionModule"
Result : 600
```

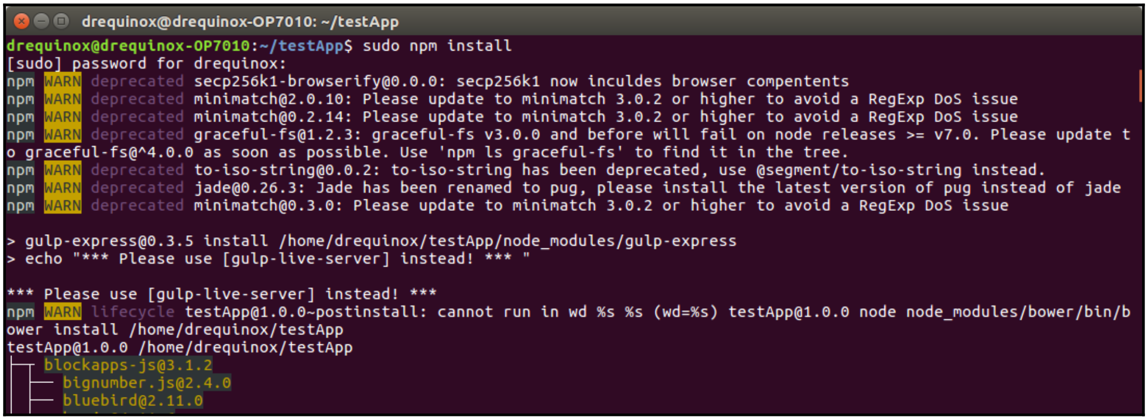




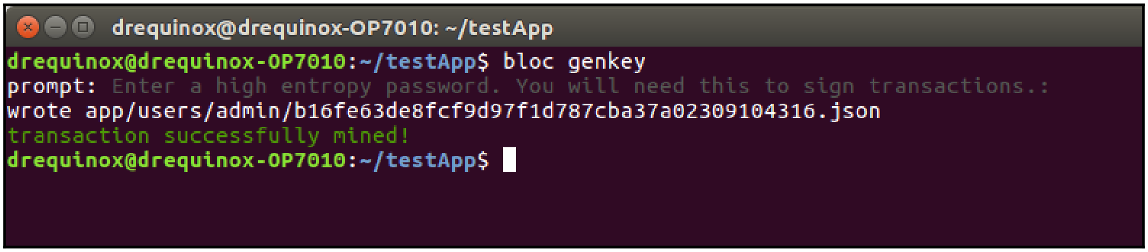
```
npm WARN deprecated secp256k1-browserify@0.0.0: secp256k1 now inculdes browser compentents
/usr/bin/bloc -> /usr/lib/node_modules/blockapps-bloc/bin/main.js
/usr/lib
└─┬ blockapps-bloc@1.2.2
  ├── bignumber.js@2.4.0
  ├─┬ blockapps-js@3.1.2
  │ ├── bn.js@4.11.6
  │ ├─┬ elliptic@6.3.2
  │ │ ├── brorand@1.0.6
  │ │ ├── hash.js@1.0.3
  │ │ └── inherits@2.0.3
```



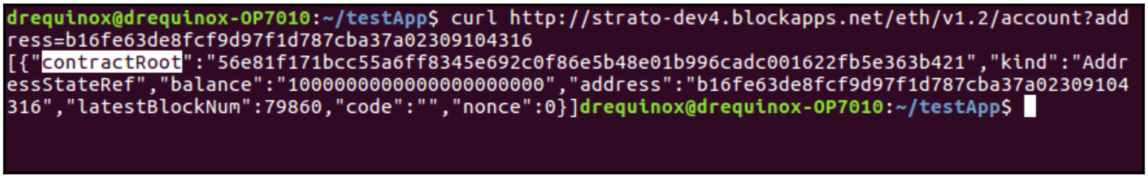
```
drequinox@drequinox-OP7010:~$ bloc init
? ==========================================================================
We're constantly looking for ways to make blockapps-bloc better!
May we anonymously report usage statistics to improve the tool over time?
More info: https://github.com/blockapps/bloc & http://blockapps.net
========================================================================== No


    ____  __           __   ___
   / __ )/ /___  _____/ /__/   |  ____  ____  _____
  / __  / / __ \/ ___/ //_/ /| | / __ \/ __ \/ ___/
 / /_/ / / /_/ / /__/ ,< / ___ |/ /_/ / /_/ (__  )
/_____/_/\____/\___/_/|_/_/  |_/ .___/ .___/____/
                              /_/   /_/
prompt: Enter the name of your app:  testApp
prompt: Enter your name:  drequinox
prompt: Enter your email so BlockApps can reach you:
prompt: apiURL:  (http://strato-dev4.blockapps.net)
prompt: Enter the blockchain profile you wish to use.  Options: strato-dev, ethereum:  (strato-dev)
Wrote: /home/drequinox/testApp/.bowerrc
Wrote: /home/drequinox/testApp/app.js
Wrote: /home/drequinox/testApp/bower.json
Wrote: /home/drequinox/testApp/gulpfile.js
Wrote: /home/drequinox/testApp/marko-taglib.json
Wrote: /home/drequinox/testApp/package.json
Wrote: /home/drequinox/testApp/test/common.js
Wrote: /home/drequinox/testApp/test/top.js
Wrote: /home/drequinox/testApp/app/contracts/Greeter.sol
Wrote: /home/drequinox/testApp/app/contracts/MultiContract.sol
Wrote: /home/drequinox/testApp/app/contracts/Payout.sol
```



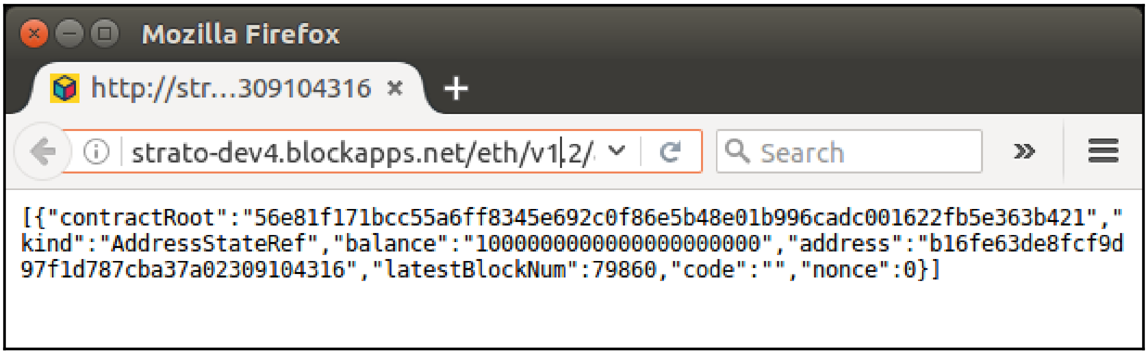
```
drequinox@drequinox-OP7010:~/testApp$ sudo npm install
[sudo] password for drequinox:
npm WARN deprecated secp256k1-browserify@0.0.0: secp256k1 now inculdes browser compentents
npm WARN deprecated minimatch@2.0.10: Please update to minimatch 3.0.2 or higher to avoid a RegExp DoS issue
npm WARN deprecated minimatch@0.2.14: Please update to minimatch 3.0.2 or higher to avoid a RegExp DoS issue
npm WARN deprecated graceful-fs@1.2.3: graceful-fs v3.0.0 and before will fail on node releases >= v7.0. Please update t
o graceful-fs@^4.0.0 as soon as possible. Use 'npm ls graceful-fs' to find it in the tree.
npm WARN deprecated to-iso-string@0.0.2: to-iso-string has been deprecated, use @segment/to-iso-string instead.
npm WARN deprecated jade@0.26.3: Jade has been renamed to pug, please install the latest version of pug instead of jade
npm WARN deprecated minimatch@0.3.0: Please update to minimatch 3.0.2 or higher to avoid a RegExp DoS issue

> gulp-express@0.3.5 install /home/drequinox/testApp/node_modules/gulp-express
> echo "*** Please use [gulp-live-server] instead! *** "

*** Please use [gulp-live-server] instead! ***
npm WARN lifecycle testApp@1.0.0~postinstall: cannot run in wd %s %s (wd=%s) testApp@1.0.0 node node_modules/bower/bin/b
ower install /home/drequinox/testApp
testApp@1.0.0 /home/drequinox/testApp
├─┬ blockapps-js@3.1.2
│ ├── bignumber.js@2.4.0
│ ├── bluebird@2.11.0
```



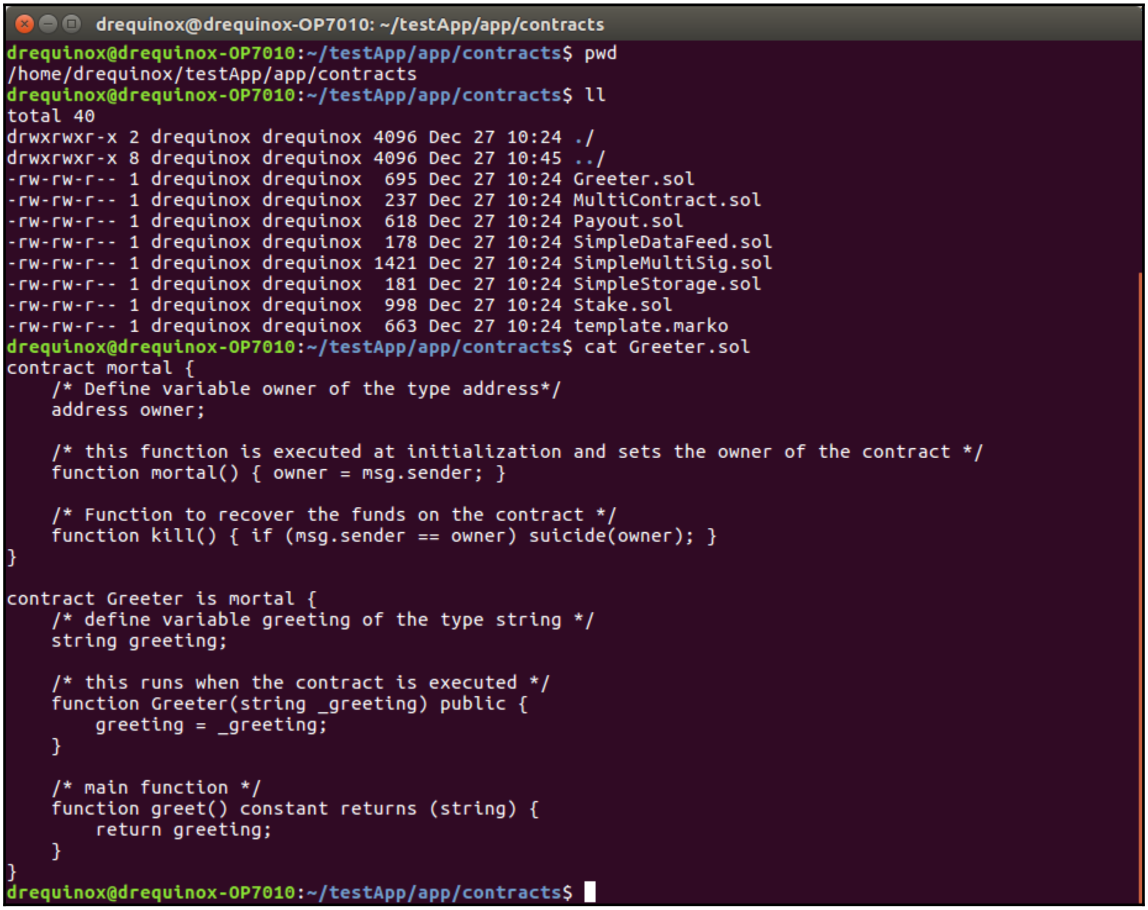
```
drequinox@drequinox-OP7010:~/testApp$ bloc genkey
prompt: Enter a high entropy password. You will need this to sign transactions.:
wrote app/users/admin/b16fe63de8fcf9d97f1d787cba37a02309104316.json
transaction successfully mined!
drequinox@drequinox-OP7010:~/testApp$ 
```



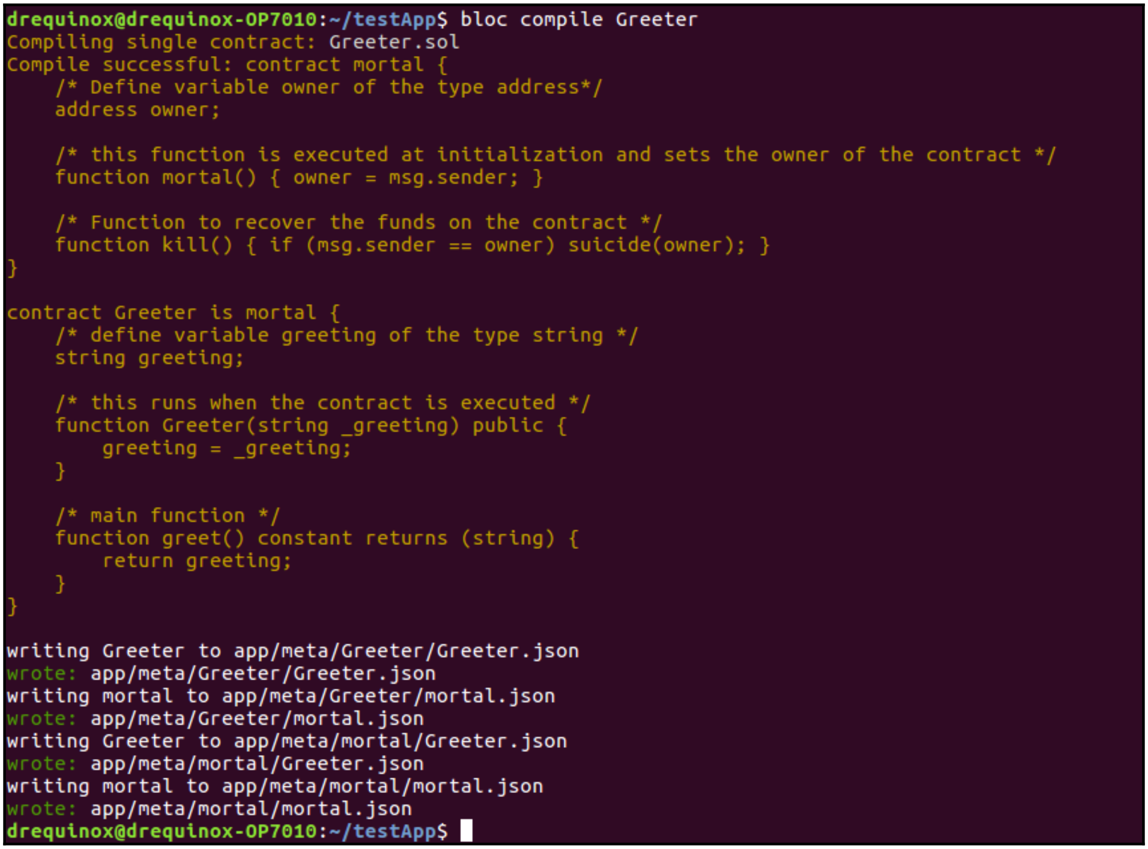
```
drequinox@drequinox-OP7010:~/testApp$ curl http://strato-dev4.blockapps.net/eth/v1.2/account?add
ress=b16fe63de8fcf9d97f1d787cba37a02309104316
[{"contractRoot":"56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421","kind":"Addr
essStateRef","balance":"1000000000000000000000","address":"b16fe63de8fcf9d97f1d787cba37a02309104
316","latestBlockNum":79860,"code":"","nonce":0}]drequinox@drequinox-OP7010:~/testApp$ 
```



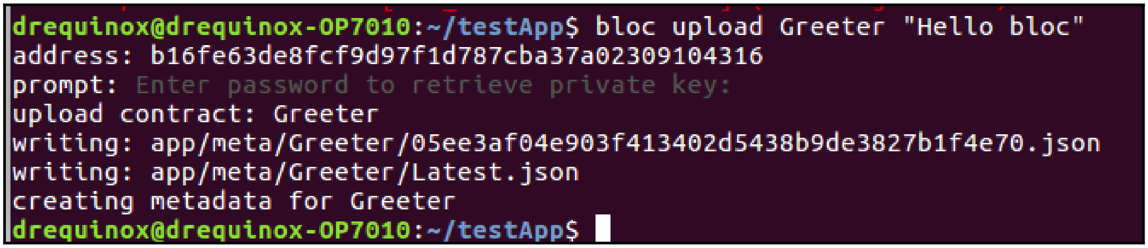
```
[{"contractRoot":"56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421","
kind":"AddressStateRef","balance":"1000000000000000000000","address":"b16fe63de8fcf9d
97f1d787cba37a02309104316","latestBlockNum":79860,"code":"","nonce":0}]
```



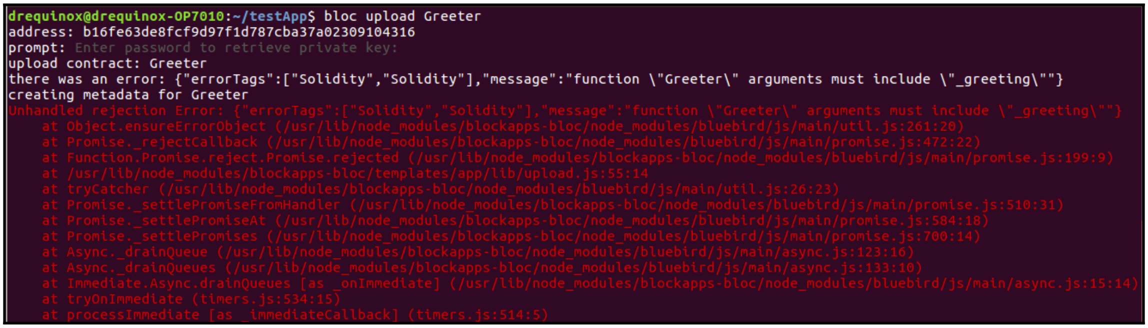
```
drequinox@drequinox-OP7010:~/testApp/app/contracts$ pwd
/home/drequinox/testApp/app/contracts
drequinox@drequinox-OP7010:~/testApp/app/contracts$ ll
total 40
drwxrwxr-x 2 drequinox drequinox 4096 Dec 27 10:24 ./
drwxrwxr-x 8 drequinox drequinox 4096 Dec 27 10:45 ../
-rw-rw-r-- 1 drequinox drequinox  695 Dec 27 10:24 Greeter.sol
-rw-rw-r-- 1 drequinox drequinox  237 Dec 27 10:24 MultiContract.sol
-rw-rw-r-- 1 drequinox drequinox  618 Dec 27 10:24 Payout.sol
-rw-rw-r-- 1 drequinox drequinox  178 Dec 27 10:24 SimpleDataFeed.sol
-rw-rw-r-- 1 drequinox drequinox 1421 Dec 27 10:24 SimpleMultiSig.sol
-rw-rw-r-- 1 drequinox drequinox  181 Dec 27 10:24 SimpleStorage.sol
-rw-rw-r-- 1 drequinox drequinox  998 Dec 27 10:24 Stake.sol
-rw-rw-r-- 1 drequinox drequinox  663 Dec 27 10:24 template.marko
drequinox@drequinox-OP7010:~/testApp/app/contracts$ cat Greeter.sol
contract mortal {
    /* Define variable owner of the type address*/
    address owner;

    /* this function is executed at initialization and sets the owner of the contract */
    function mortal() { owner = msg.sender; }

    /* Function to recover the funds on the contract */
    function kill() { if (msg.sender == owner) suicide(owner); }
}

contract Greeter is mortal {
    /* define variable greeting of the type string */
    string greeting;

    /* this runs when the contract is executed */
    function Greeter(string _greeting) public {
        greeting = _greeting;
    }

    /* main function */
    function greet() constant returns (string) {
        return greeting;
    }
}
drequinox@drequinox-OP7010:~/testApp/app/contracts$ 
```



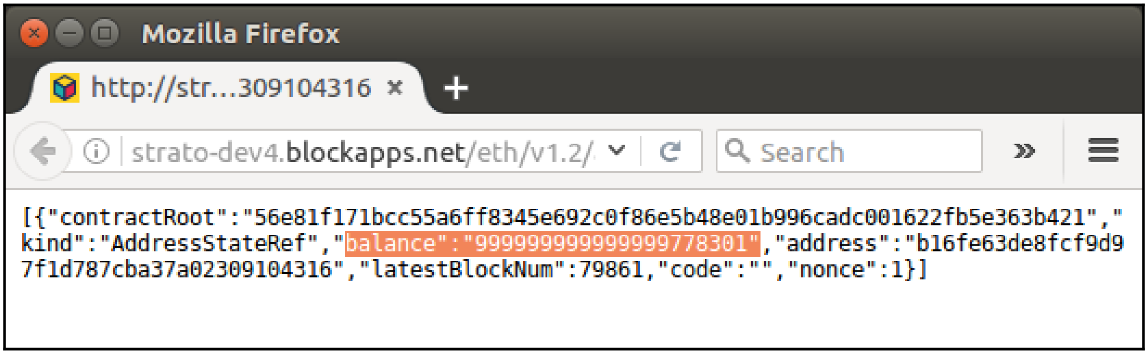
```
drequinox@drequinox-OP7010:~/testApp$ bloc compile Greeter
Compiling single contract: Greeter.sol
Compile successful: contract mortal {
    /* Define variable owner of the type address*/
    address owner;

    /* this function is executed at initialization and sets the owner of the contract */
    function mortal() { owner = msg.sender; }

    /* Function to recover the funds on the contract */
    function kill() { if (msg.sender == owner) suicide(owner); }
}

contract Greeter is mortal {
    /* define variable greeting of the type string */
    string greeting;

    /* this runs when the contract is executed */
    function Greeter(string _greeting) public {
        greeting = _greeting;
    }

    /* main function */
    function greet() constant returns (string) {
        return greeting;
    }
}

writing Greeter to app/meta/Greeter/Greeter.json
wrote: app/meta/Greeter/Greeter.json
writing mortal to app/meta/Greeter/mortal.json
wrote: app/meta/Greeter/mortal.json
writing Greeter to app/meta/mortal/Greeter.json
wrote: app/meta/mortal/Greeter.json
writing mortal to app/meta/mortal/mortal.json
wrote: app/meta/mortal/mortal.json
drequinox@drequinox-OP7010:~/testApp$
```



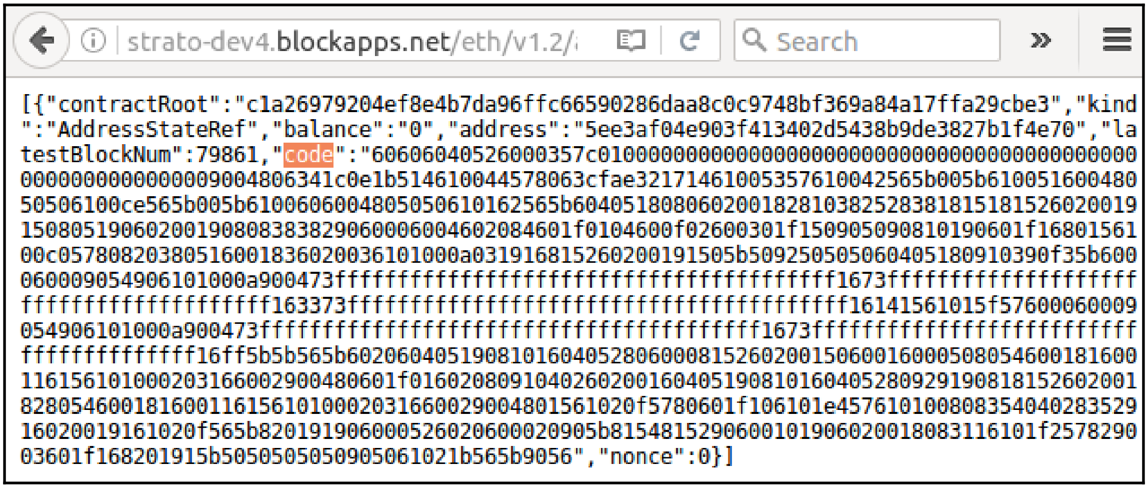
```
drequinox@drequinox-OP7010:~/testApp$ bloc upload Greeter "Hello bloc"
address: b16fe63de8fcf9d97f1d787cba37a02309104316
prompt: Enter password to retrieve private key:
upload contract: Greeter
writing: app/meta/Greeter/05ee3af04e903f413402d5438b9de3827b1f4e70.json
writing: app/meta/Greeter/Latest.json
creating metadata for Greeter
drequinox@drequinox-OP7010:~/testApp$
```



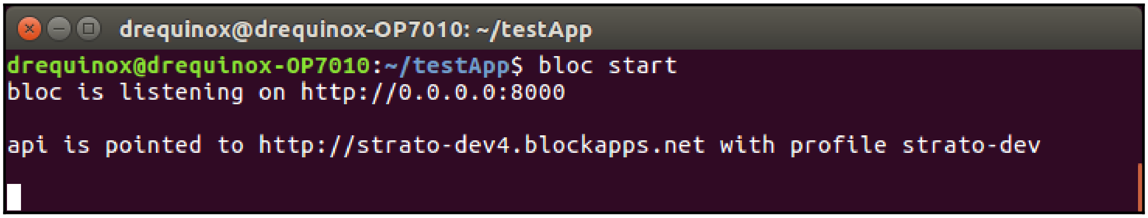
```
drequinox@drequinox-OP7010:~/testApp$ bloc upload Greeter
address: b16fe63de8fcf9d97f1d787cba37a02309104316
prompt: Enter password to retrieve private key:
upload contract: Greeter
there was an error: {"errorTags":["Solidity","Solidity"],"message":"function \"Greeter\" arguments must include \"_greeting\""}
creating metadata for Greeter
Unhandled rejection Error: {"errorTags":["Solidity","Solidity"],"message":"function \"Greeter\" arguments must include \"_greeting\""}
    at Object.ensureErrorObject (/usr/lib/node_modules/blockapps-bloc/node_modules/bluebird/js/main/util.js:261:20)
    at Promise._rejectCallback (/usr/lib/node_modules/blockapps-bloc/node_modules/bluebird/js/main/promise.js:472:22)
    at Function.Promise.reject.Promise.rejected (/usr/lib/node_modules/blockapps-bloc/node_modules/bluebird/js/main/promise.js:199:9)
    at /usr/lib/node_modules/blockapps-bloc/templates/app/lib/upload.js:55:14
    at tryCatcher (/usr/lib/node_modules/blockapps-bloc/node_modules/bluebird/js/main/util.js:26:23)
    at Promise._settlePromiseFromHandler (/usr/lib/node_modules/blockapps-bloc/node_modules/bluebird/js/main/promise.js:510:31)
    at Promise._settlePromiseAt (/usr/lib/node_modules/blockapps-bloc/node_modules/bluebird/js/main/promise.js:584:18)
    at Promise._settlePromises (/usr/lib/node_modules/blockapps-bloc/node_modules/bluebird/js/main/promise.js:700:14)
    at Async._drainQueue (/usr/lib/node_modules/blockapps-bloc/node_modules/bluebird/js/main/async.js:123:16)
    at Async._drainQueues (/usr/lib/node_modules/blockapps-bloc/node_modules/bluebird/js/main/async.js:133:10)
    at Immediate.Async.drainQueues [as _onImmediate] (/usr/lib/node_modules/blockapps-bloc/node_modules/bluebird/js/main/async.js:15:14)
    at tryOnImmediate (timers.js:534:15)
    at processImmediate [as _immediateCallback] (timers.js:514:5)
```



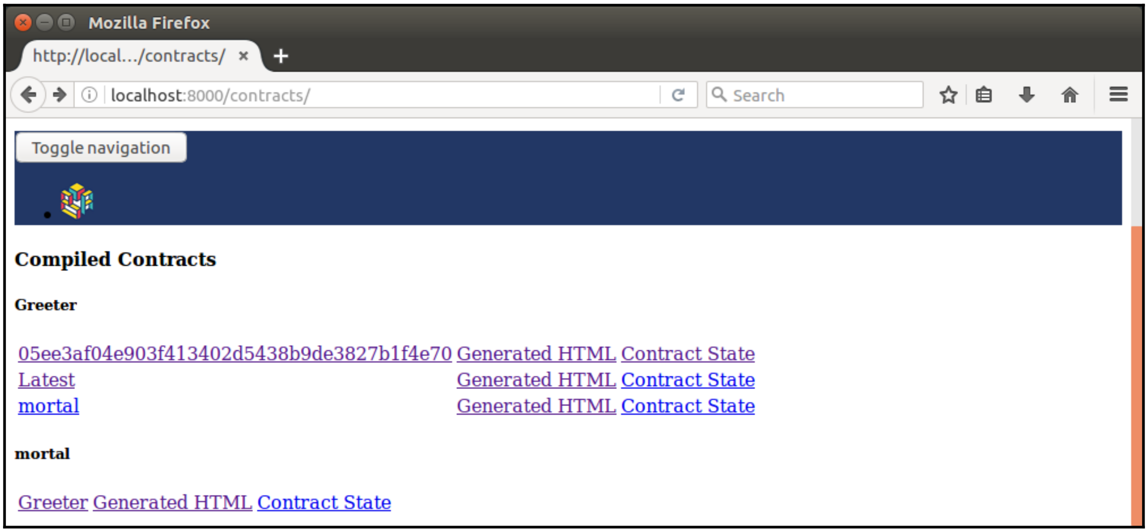
```
[{"contractRoot":"56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421","
kind":"AddressStateRef","balance":"9999999999999999778301","address":"b16fe63de8fcf9d9
7f1d787cba37a02309104316","latestBlockNum":79861,"code":"","nonce":1}]
```



```
[{"contractRoot":"c1a26979204ef8e4b7da96ffc66590286daa8c0c9748bf369a84a17ffa29cbe3","kind
":"AddressStateRef","balance":"0","address":"5ee3af04e903f413402d5438b9de3827b1f4e70","la
testBlockNum":79861,"code":"60606040526000357c010000000000000000000000000000000000000000
00000000000000009004806341c0e1b514610044578063cfae32171461005357610042565b005b610051600480
50506100ce565b005b610060600480505061016256 5b604051808060200182810382528381815181526020019
15080519060200190808383829060006004602084601f0104600f02600301f150905090810190601f16801561
00c05780820380516001836020036101000a031916815260200191505b509250505060405180910390f35b600
060009054906101000a900473ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffff
fffffffffffffffffffff163373ffffffffffffffffffffffffffffffffffffffff16141561015f57600060009
054906101000a900473ffffffffffffffffffffffffffffffffffffffff1673fffffffffffffffffffffffff
fffffffffffffff16ff5b5b565b6020604051908101604052806000815260200150600160005080546001816 00
116156101000203166002900480601f0160208091040260200160405190810160405280929190818152602001
8280546001816001161561010002031660029004801561020f5780601f106101e457610100808354040283529
16020019161020f565b820191906000526020600020905b815481529060010190602001808311610 1f2578290
03601f168201915b505050505090506 1021b565b9056","nonce":0}]
```



```
drequinox@drequinox-OP7010:~/testApp$ bloc start
bloc is listening on http://0.0.0.0:8000

api is pointed to http://strato-dev4.blockapps.net with profile strato-dev
```



Compiled Contracts

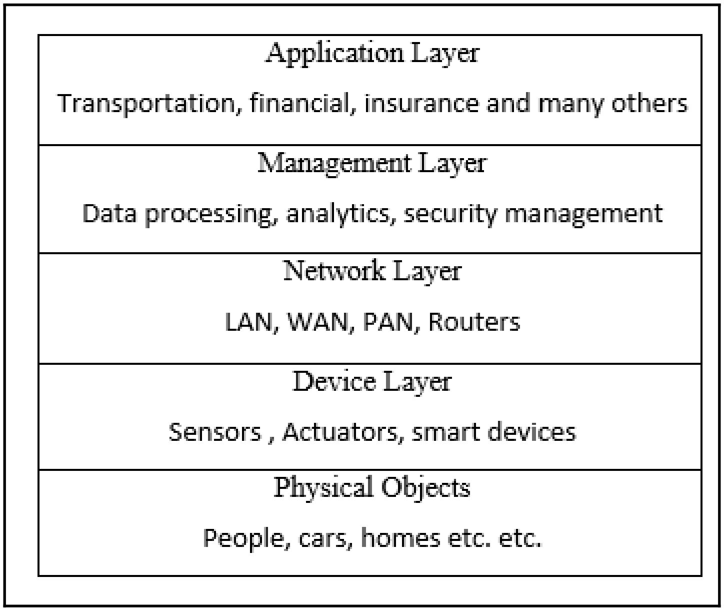
Greeter

05ee3af04e903f413402d5438b9de3827b1f4e70 Generated HTML Contract State
Latest Generated HTML Contract State
mortal Generated HTML Contract State

mortal

Greeter Generated HTML Contract State

Chapter 11: Blockchain-Outside of Currencies



Application Layer

Transportation, financial, insurance and many others

Management Layer

Data processing, analytics, security management

Network Layer

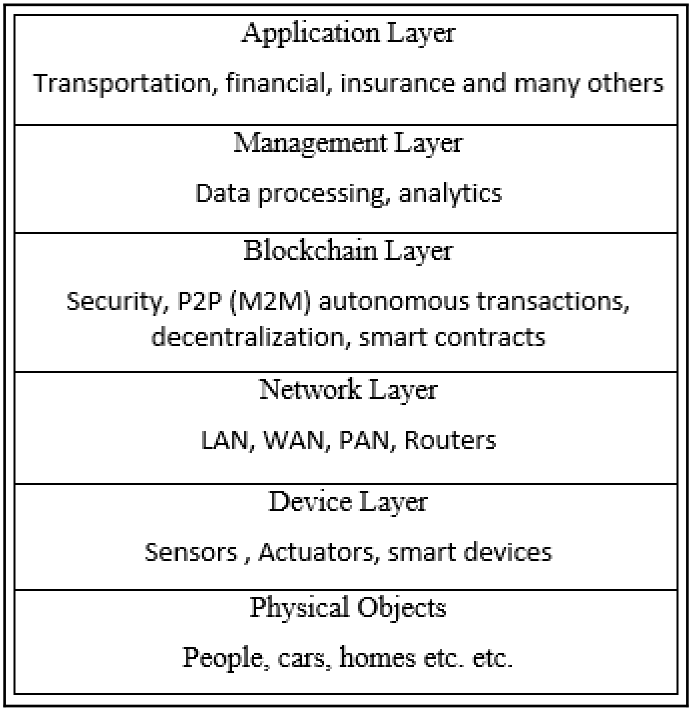
LAN, WAN, PAN, Routers

Device Layer

Sensors , Actuators, smart devices

Physical Objects

People, cars, homes etc. etc.



Application Layer

Transportation, financial, insurance and many others

Management Layer

Data processing, analytics

Blockchain Layer

Security, P2P (M2M) autonomous transactions, decentralization, smart contracts

Network Layer

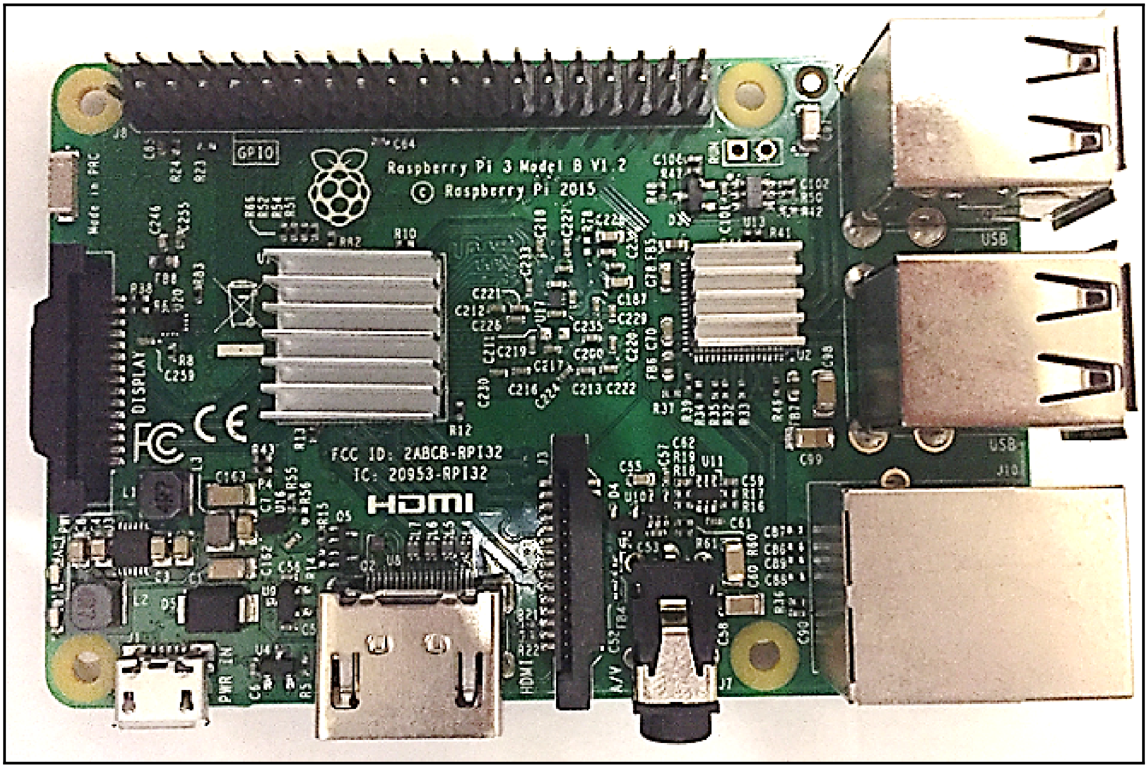
LAN, WAN, PAN, Routers

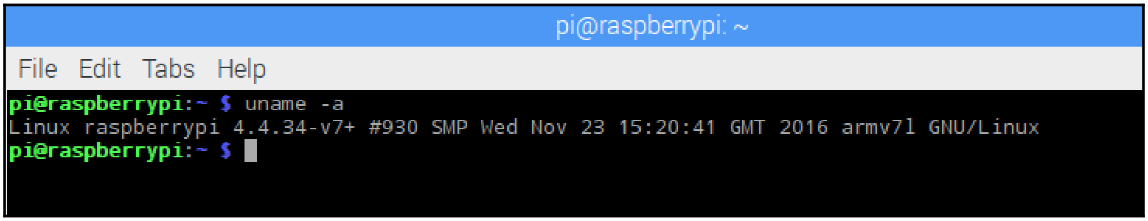
Device Layer

Sensors , Actuators, smart devices

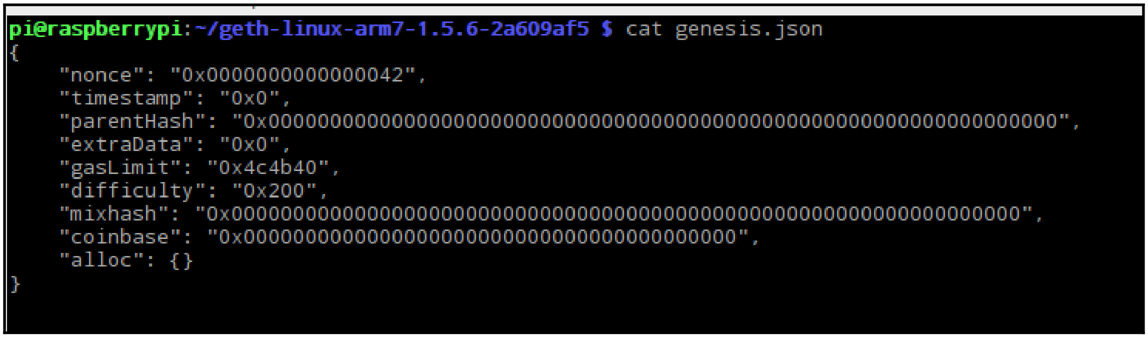
Physical Objects

People, cars, homes etc. etc.

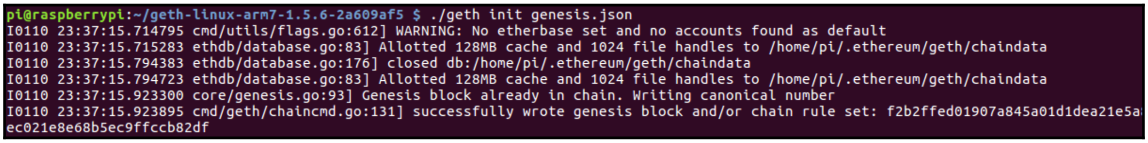




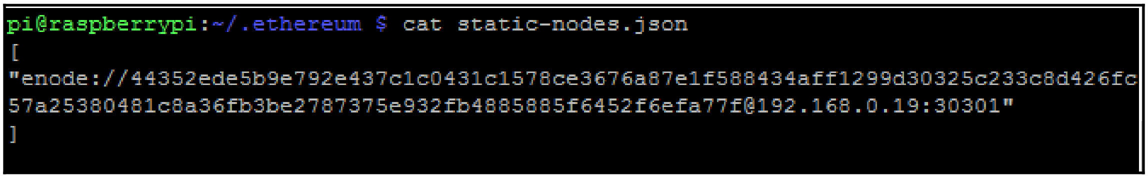
```
pi@raspberrypi:~ $ uname -a
Linux raspberrypi 4.4.34-v7+ #930 SMP Wed Nov 23 15:20:41 GMT 2016 armv7l GNU/Linux
pi@raspberrypi:~ $
```



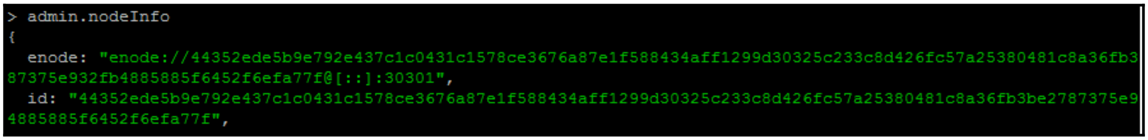
```
pi@raspberrypi:~/geth-linux-arm7-1.5.6-2a609af5 $ cat genesis.json
{
    "nonce": "0x0000000000000042",
    "timestamp": "0x0",
    "parentHash": "0x0000000000000000000000000000000000000000000000000000000000000000",
    "extraData": "0x0",
    "gasLimit": "0x4c4b40",
    "difficulty": "0x200",
    "mixhash": "0x0000000000000000000000000000000000000000000000000000000000000000",
    "coinbase": "0x0000000000000000000000000000000000000000",
    "alloc": {}
}
```



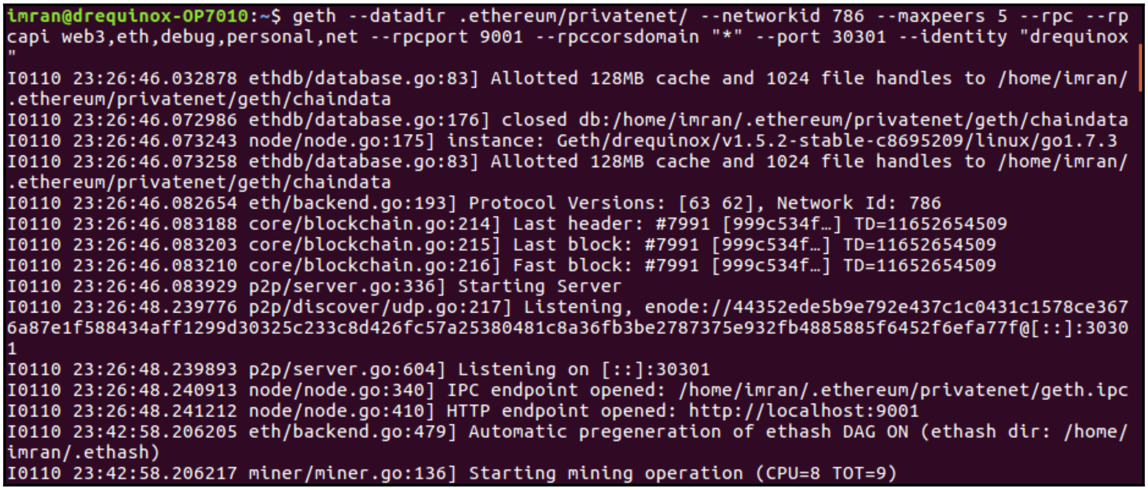
```
pi@raspberrypi:~/geth-linux-arm7-1.5.6-2a609af5 $ ./geth init genesis.json
I0110 23:37:15.714795 cmd/utils/flags.go:612] WARNING: No etherbase set and no accounts found as default
I0110 23:37:15.715283 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to /home/pi/.ethereum/geth/chaindata
I0110 23:37:15.794383 ethdb/database.go:176] closed db:/home/pi/.ethereum/geth/chaindata
I0110 23:37:15.794723 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to /home/pi/.ethereum/geth/chaindata
I0110 23:37:15.923300 core/genesis.go:93] Genesis block already in chain. Writing canonical number
I0110 23:37:15.923895 cmd/geth/chaincmd.go:131] successfully wrote genesis block and/or chain rule set: f2b2ffed01907a845a01d1dea21e5a
ec021e8e68b5ec9ffccb82df
```



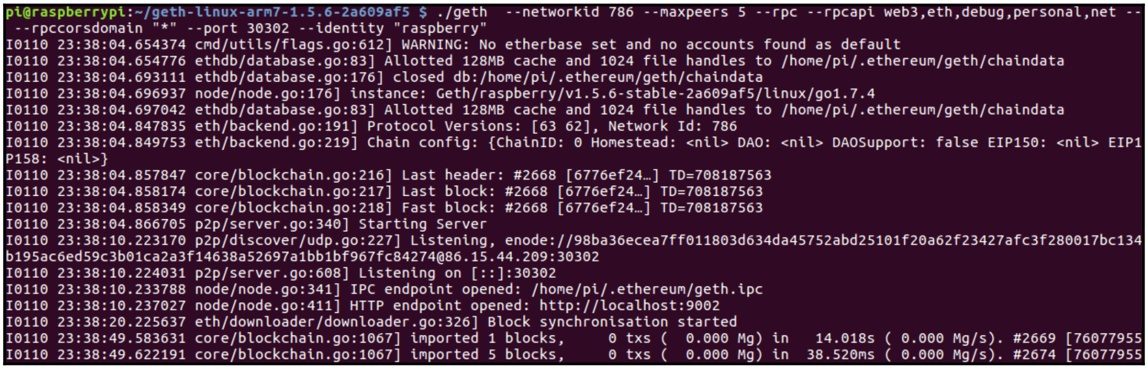
```
pi@raspberrypi:~/.ethereum $ cat static-nodes.json
[
"enode://44352ede5b9e792e437c1c0431c1578ce3676a87e1f588434aff1299d30325c233c8d426fc
57a25380481c8a36fb3be2787375e932fb4885885f6452f6efa77f@192.168.0.19:30301"
]
```



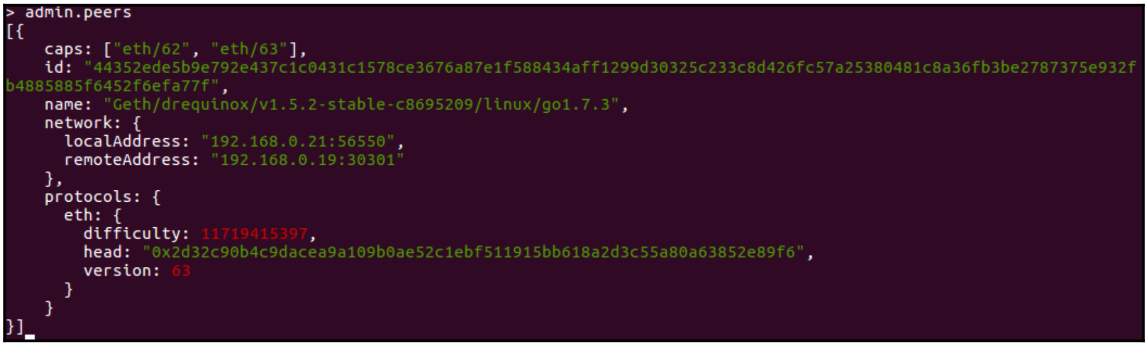
```
> admin.nodeInfo
{
  enode: "enode://44352ede5b9e792e437c1c0431c1578ce3676a87e1f588434aff1299d30325c233c8d426fc57a25380481c8a36fb3
87375e932fb4885885f6452f6efa77f@[::]:30301",
  id: "44352ede5b9e792e437c1c0431c1578ce3676a87e1f588434aff1299d30325c233c8d426fc57a25380481c8a36fb3be2787375e9
4885885f6452f6efa77f",
```



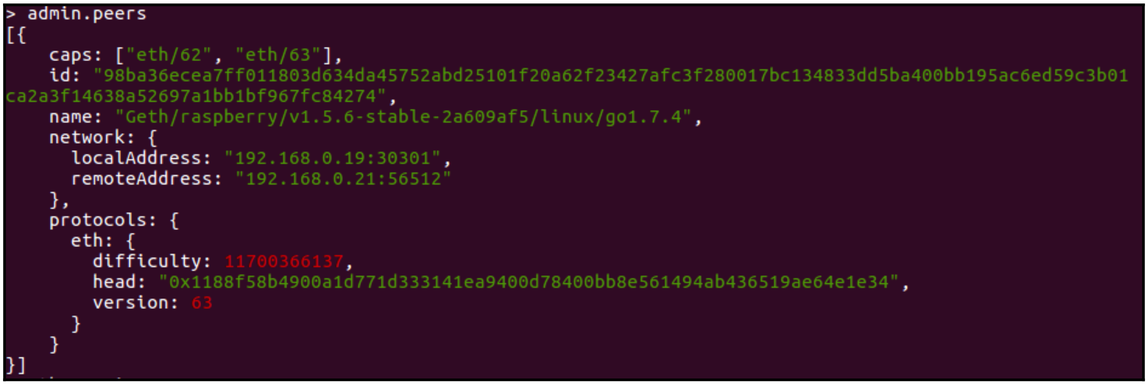
```
imran@drequinox-OP7010:~$ geth --datadir .ethereum/privatenet/ --networkid 786 --maxpeers 5 --rpc --rp
capi web3,eth,debug,personal,net --rpcport 9001 --rpccorsdomain "*" --port 30301 --identity "drequinox
"
I0110 23:26:46.032878 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to /home/imran/
.ethereum/privatenet/geth/chaindata
I0110 23:26:46.072986 ethdb/database.go:176] closed db:/home/imran/.ethereum/privatenet/geth/chaindata
I0110 23:26:46.073243 node/node.go:175] instance: Geth/drequinox/v1.5.2-stable-c8695209/linux/go1.7.3
I0110 23:26:46.073258 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to /home/imran/
.ethereum/privatenet/geth/chaindata
I0110 23:26:46.082654 eth/backend.go:193] Protocol Versions: [63 62], Network Id: 786
I0110 23:26:46.083188 core/blockchain.go:214] Last header: #7991 [999c534f…] TD=11652654509
I0110 23:26:46.083203 core/blockchain.go:215] Last block: #7991 [999c534f…] TD=11652654509
I0110 23:26:46.083210 core/blockchain.go:216] Fast block: #7991 [999c534f…] TD=11652654509
I0110 23:26:46.083929 p2p/server.go:336] Starting Server
I0110 23:26:48.239776 p2p/discover/udp.go:217] Listening, enode://44352ede5b9e792e437c1c0431c1578ce367
6a87e1f588434aff1299d30325c233c8d426fc57a25380481c8a36fb3be2787375e932fb4885885f6452f6efa77f@[::]:3030
1
I0110 23:26:48.239893 p2p/server.go:604] Listening on [::]:30301
I0110 23:26:48.240913 node/node.go:340] IPC endpoint opened: /home/imran/.ethereum/privatenet/geth.ipc
I0110 23:26:48.241212 node/node.go:410] HTTP endpoint opened: http://localhost:9001
I0110 23:42:58.206205 eth/backend.go:479] Automatic pregeneration of ethash DAG ON (ethash dir: /home/
imran/.ethash)
I0110 23:42:58.206217 miner/miner.go:136] Starting mining operation (CPU=8 TOT=9)
```



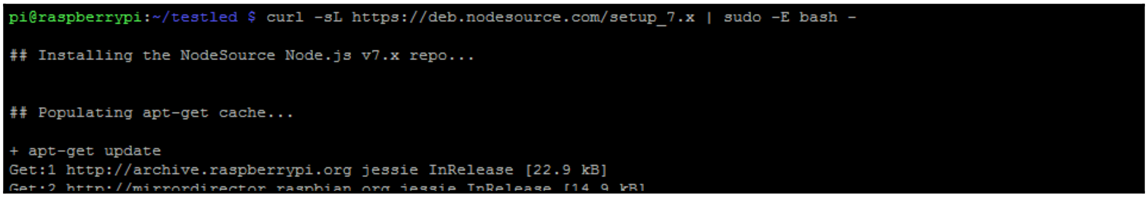
```
pi@raspberrypi:~/geth-linux-arm7-1.5.6-2a609af5 $ ./geth  --networkid 786 --maxpeers 5 --rpc --rpcapi web3,eth,debug,personal,net --
 --rpccorsdomain "*" --port 30302 --identity "raspberry"
I0110 23:38:04.654374 cmd/utils/flags.go:612] WARNING: No etherbase set and no accounts found as default
I0110 23:38:04.654776 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to /home/pi/.ethereum/geth/chaindata
I0110 23:38:04.693111 ethdb/database.go:176] closed db:/home/pi/.ethereum/geth/chaindata
I0110 23:38:04.696937 node/node.go:176] instance: Geth/raspberry/v1.5.6-stable-2a609af5/linux/go1.7.4
I0110 23:38:04.697042 ethdb/database.go:83] Allotted 128MB cache and 1024 file handles to /home/pi/.ethereum/geth/chaindata
I0110 23:38:04.847835 eth/backend.go:191] Protocol Versions: [63 62], Network Id: 786
I0110 23:38:04.849753 eth/backend.go:219] Chain config: {ChainID: 0 Homestead: <nil> DAO: <nil> DAOSupport: false EIP150: <nil> EIP1
P158: <nil>}
I0110 23:38:04.857847 core/blockchain.go:216] Last header: #2668 [6776ef24…] TD=708187563
I0110 23:38:04.858174 core/blockchain.go:217] Last block: #2668 [6776ef24…] TD=708187563
I0110 23:38:04.858349 core/blockchain.go:218] Fast block: #2668 [6776ef24…] TD=708187563
I0110 23:38:04.866705 p2p/server.go:340] Starting Server
I0110 23:38:10.223170 p2p/discover/udp.go:227] Listening, enode://98ba36ecea7ff011803d634da45752abd25101f20a62f23427afc3f280017bc134
b195ac6ed59c3b01ca2a3f14638a52697a1bb1bf967fc84274@86.15.44.209:30302
I0110 23:38:10.224031 p2p/server.go:608] Listening on [::]:30302
I0110 23:38:10.233788 node/node.go:341] IPC endpoint opened: /home/pi/.ethereum/geth.ipc
I0110 23:38:10.237027 node/node.go:411] HTTP endpoint opened: http://localhost:9002
I0110 23:38:20.225637 eth/downloader/downloader.go:326] Block synchronisation started
I0110 23:38:49.583631 core/blockchain.go:1067] imported 1 blocks,     0 txs (  0.000 Mg) in   14.018s ( 0.000 Mg/s). #2669 [76077955
I0110 23:38:49.622191 core/blockchain.go:1067] imported 5 blocks,     0 txs (  0.000 Mg) in  38.520ms ( 0.000 Mg/s). #2674 [76077955
```



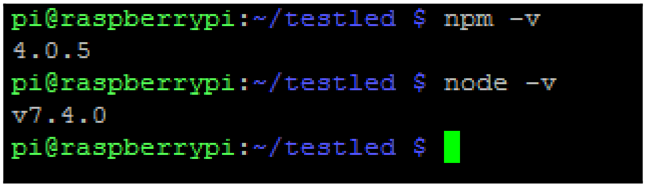
```
> admin.peers
[{
    caps: ["eth/62", "eth/63"],
    id: "44352ede5b9e792e437c1c0431c1578ce3676a87e1f588434aff1299d30325c233c8d426fc57a25380481c8a36fb3be2787375e932f
b4885885f6452f6efa77f",
    name: "Geth/drequinox/v1.5.2-stable-c8695209/linux/go1.7.3",
    network: {
      localAddress: "192.168.0.21:56550",
      remoteAddress: "192.168.0.19:30301"
    },
    protocols: {
      eth: {
        difficulty: 11719415397,
        head: "0x2d32c90b4c9dacea9a109b0ae52c1ebf511915bb618a2d3c55a80a63852e89f6",
        version: 63
      }
    }
}]
```



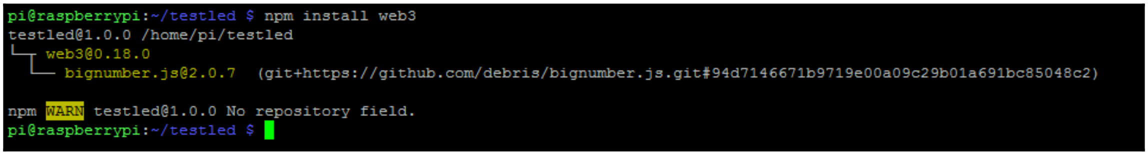
```
> admin.peers
[{
    caps: ["eth/62", "eth/63"],
    id: "98ba36ecea7ff011803d634da45752abd25101f20a62f23427afc3f280017bc134833dd5ba400bb195ac6ed59c3b01
ca2a3f14638a52697a1bb1bf967fc84274",
    name: "Geth/raspberry/v1.5.6-stable-2a609af5/linux/go1.7.4",
    network: {
      localAddress: "192.168.0.19:30301",
      remoteAddress: "192.168.0.21:56512"
    },
    protocols: {
      eth: {
        difficulty: 11700366137,
        head: "0x1188f58b4900a1d771d333141ea9400d78400bb8e561494ab436519ae64e1e34",
        version: 63
      }
    }
}]
```



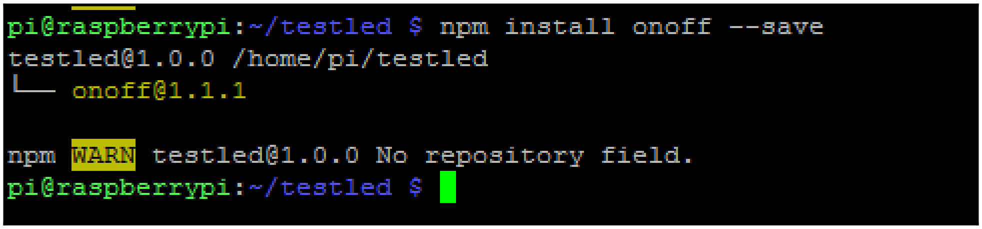
```
pi@raspberrypi:~/testled $ curl -sL https://deb.nodesource.com/setup_7.x | sudo -E bash -

## Installing the NodeSource Node.js v7.x repo...


## Populating apt-get cache...

+ apt-get update
Get:1 http://archive.raspberrypi.org jessie InRelease [22.9 kB]
Get:2 http://mirrordirector.raspbian.org jessie InRelease [14.9 kB]
```



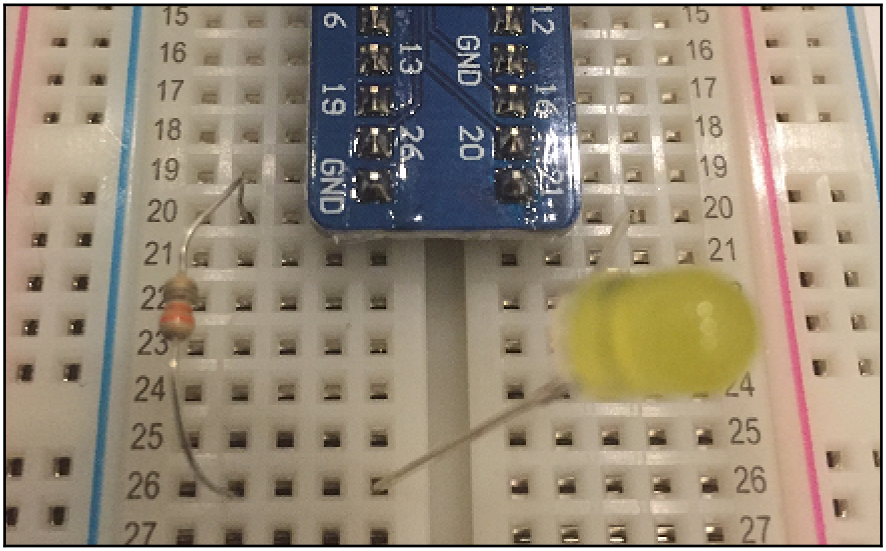
```
pi@raspberrypi:~/testled $ npm -v
4.0.5
pi@raspberrypi:~/testled $ node -v
v7.4.0
pi@raspberrypi:~/testled $ █
```

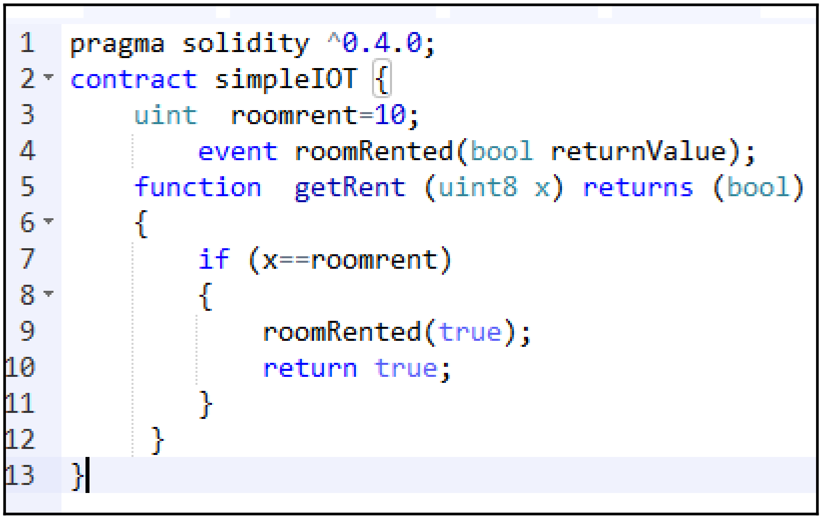


```
pi@raspberrypi:~/testled $ npm install web3
testled@1.0.0 /home/pi/testled
└─┬ web3@0.18.0
  └── bignumber.js@2.0.7  (git+https://github.com/debris/bignumber.js.git#94d7146671b9719e00a09c29b01a691bc85048c2)

npm WARN testled@1.0.0 No repository field.
pi@raspberrypi:~/testled $ █
```

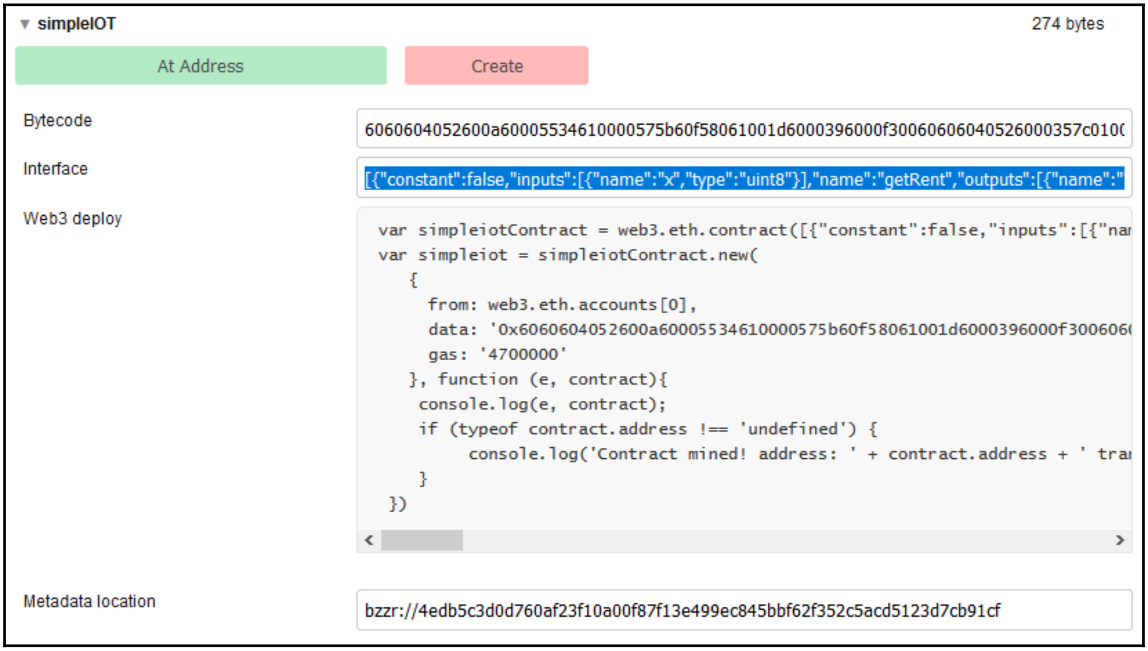


```
pi@raspberrypi:~/testled $ npm install onoff --save
testled@1.0.0 /home/pi/testled
└── onoff@1.1.1

npm WARN testled@1.0.0 No repository field.
pi@raspberrypi:~/testled $ █
```





```
pragma solidity ^0.4.0;
contract simpleIOT {
    uint  roomrent=10;
        event roomRented(bool returnValue);
    function  getRent (uint8 x) returns (bool)
    {
        if (x==roomrent)
        {
            roomRented(true);
            return true;
        }
     }
}
```



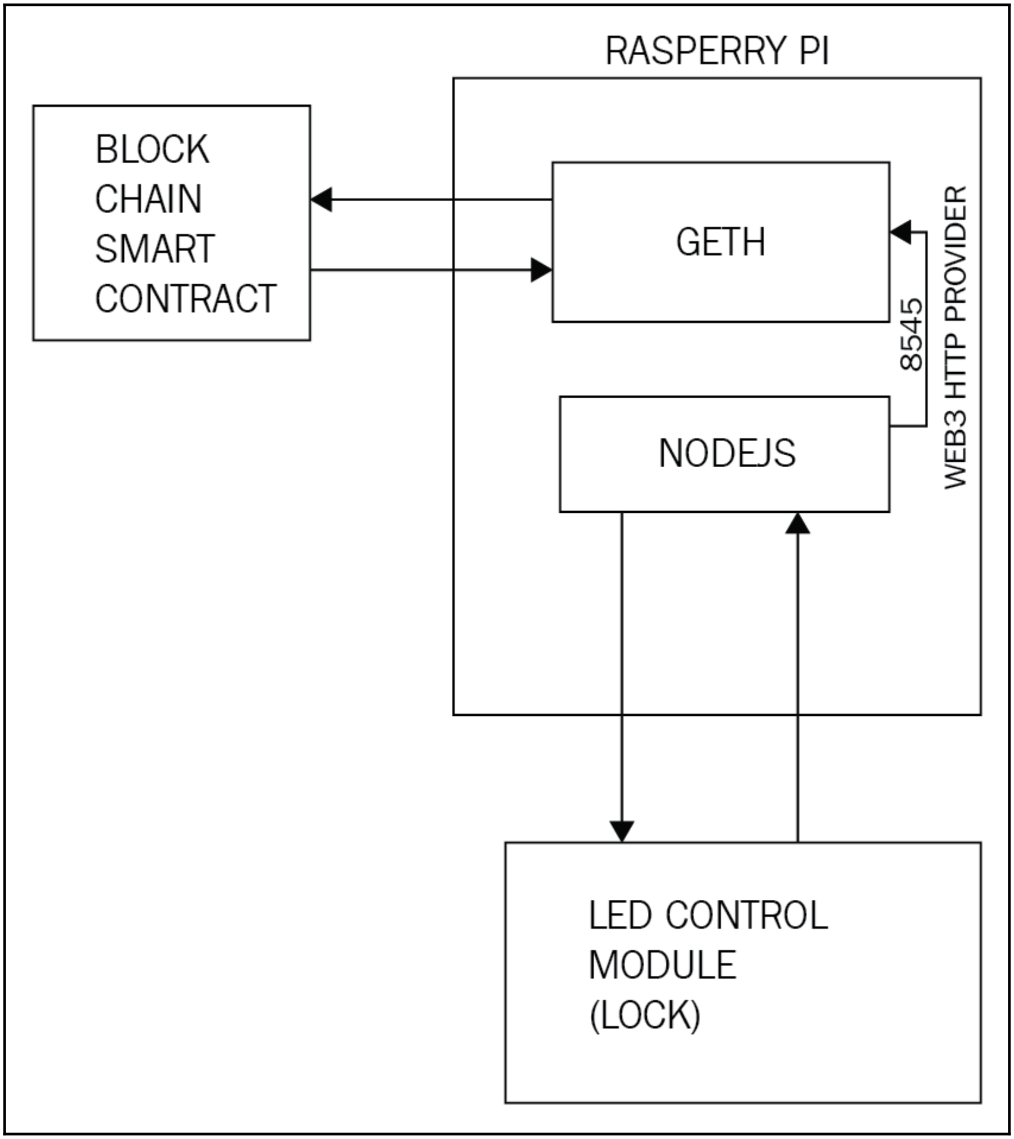
Bytecode
6060604052600a600055346100005755b60f58061001d6000396000f30060606040526000357c010

Interface
[{"constant":false,"inputs":[{"name":"x","type":"uint8"}],"name":"getRent","outputs":[{"name":"

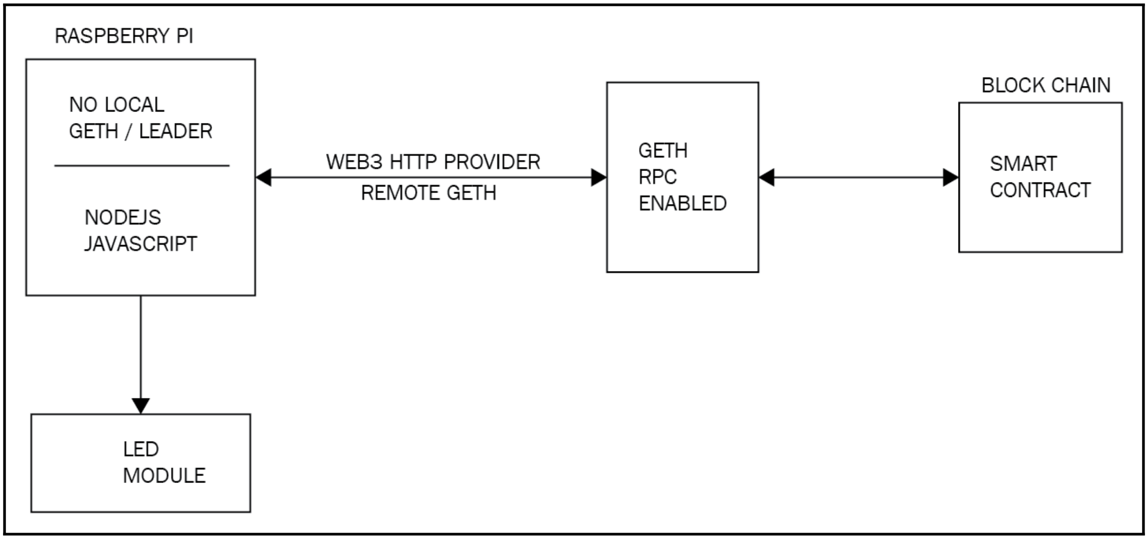
Web3 deploy

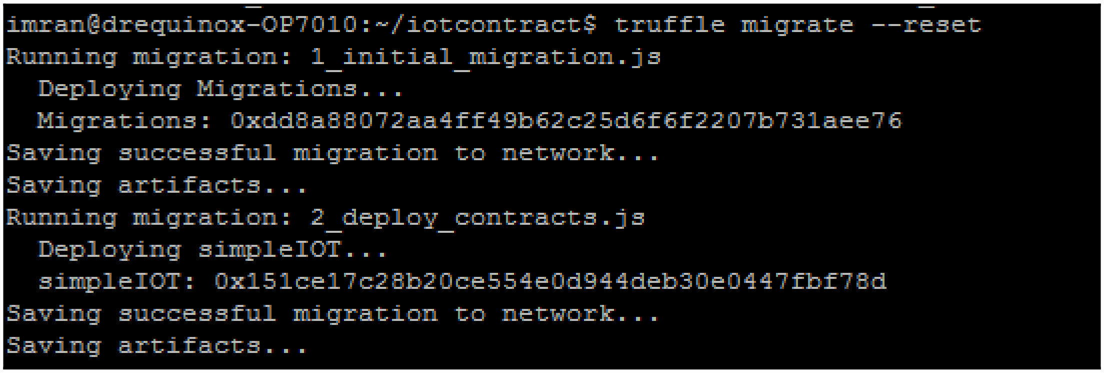
```
var simpleiotContract = web3.eth.contract([{"constant":false,"inputs":[{"na
var simpleiot = simpleiotContract.new(
   {
     from: web3.eth.accounts[0],
     data: '0x6060604052600a600055346100005755b60f58061001d6000396000f300606
     gas: '4700000'
   }, function (e, contract){
    console.log(e, contract);
    if (typeof contract.address !== 'undefined') {
         console.log('Contract mined! address: ' + contract.address + ' tra
    }
 })
```

Metadata location
bzzr://4edb5c3d0d760af23f10a00f87f13e499ec845bbf62f352c5acd5123d7cb91cf

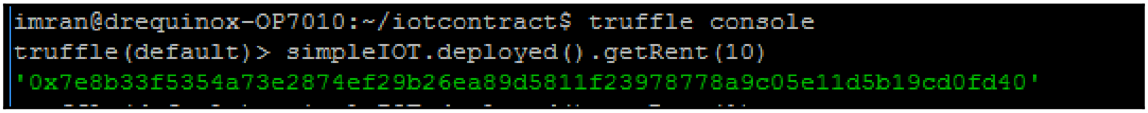


RASPERRY PI
BLOCK
CHAIN
SMART
CONTRACT
GETH
8545
WEB3 HTTP PROVIDER
NODEJS
LED CONTROL
MODULE
(LOCK)

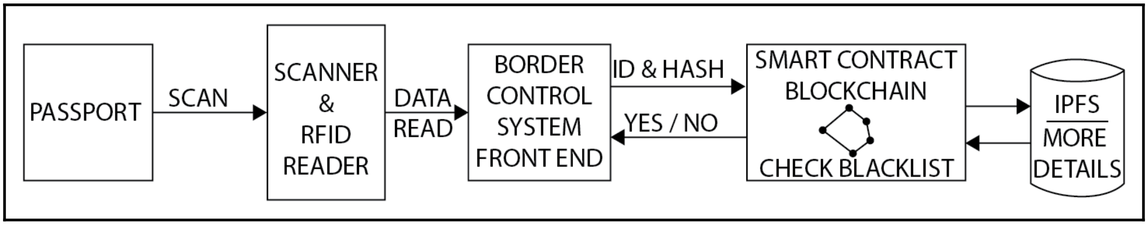




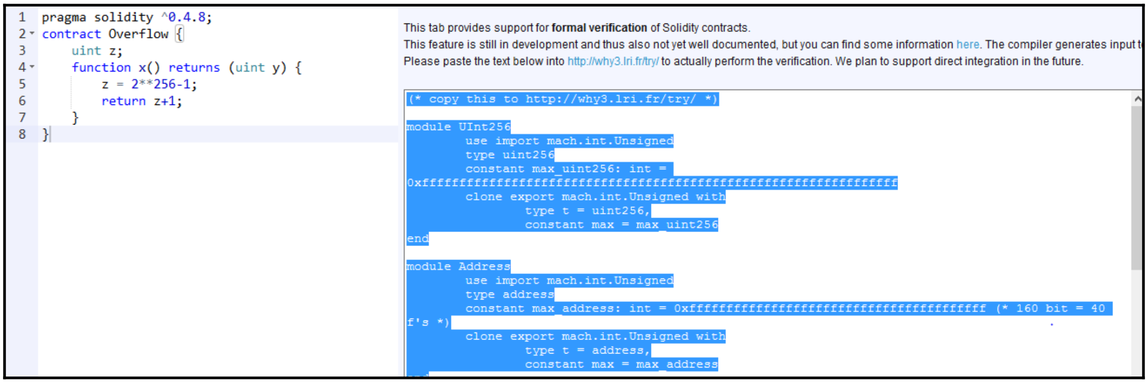
```
imran@drequinox-OP7010:~/iotcontract$ truffle migrate --reset
Running migration: 1_initial_migration.js
  Deploying Migrations...
  Migrations: 0xdd8a88072aa4ff49b62c25d6f6f2207b731aee76
Saving successful migration to network...
Saving artifacts...
Running migration: 2_deploy_contracts.js
  Deploying simpleIOT...
  simpleIOT: 0x151ce17c28b20ce554e0d944deb30e0447fbf78d
Saving successful migration to network...
Saving artifacts...
```



```
imran@drequinox-OP7010:~/iotcontract$ truffle console
truffle(default)> simpleIOT.deployed().getRent(10)
'0x7e8b33f5354a73e2874ef29b26ea89d5811f23978778a9c05e11d5b19cd0fd40'
```


PASSPORT
SCAN
SCANNER & RFID READER
DATA READ
BORDER CONTROL SYSTEM FRONT END
ID & HASH
YES / NO
SMART CONTRACT BLOCKCHAIN
CHECK BLACKLIST
IPFS
MORE DETAILS

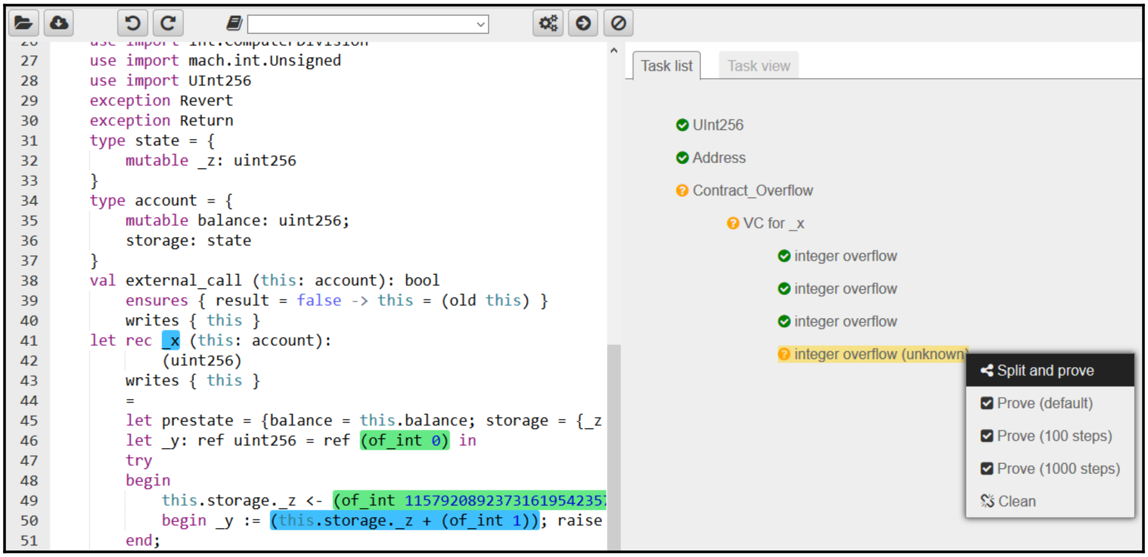
Chapter 12: Scalability and Other Challenges



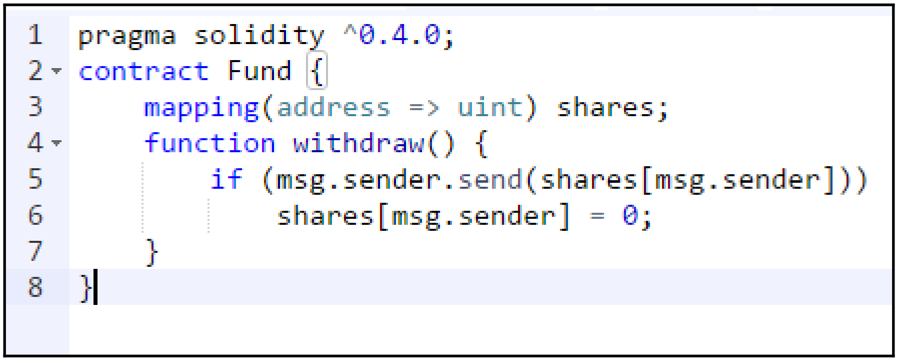
```
pragma solidity ^0.4.8;
contract Overflow {
    uint z;
    function x() returns (uint y) {
        z = 2**256-1;
        return z+1;
    }
}
```

This tab provides support for **formal verification** of Solidity contracts.
This feature is still in development and thus also not yet well documented, but you can find some information here. The compiler generates input t
Please paste the text below into http://why3.lri.fr/try/ to actually perform the verification. We plan to support direct integration in the future.

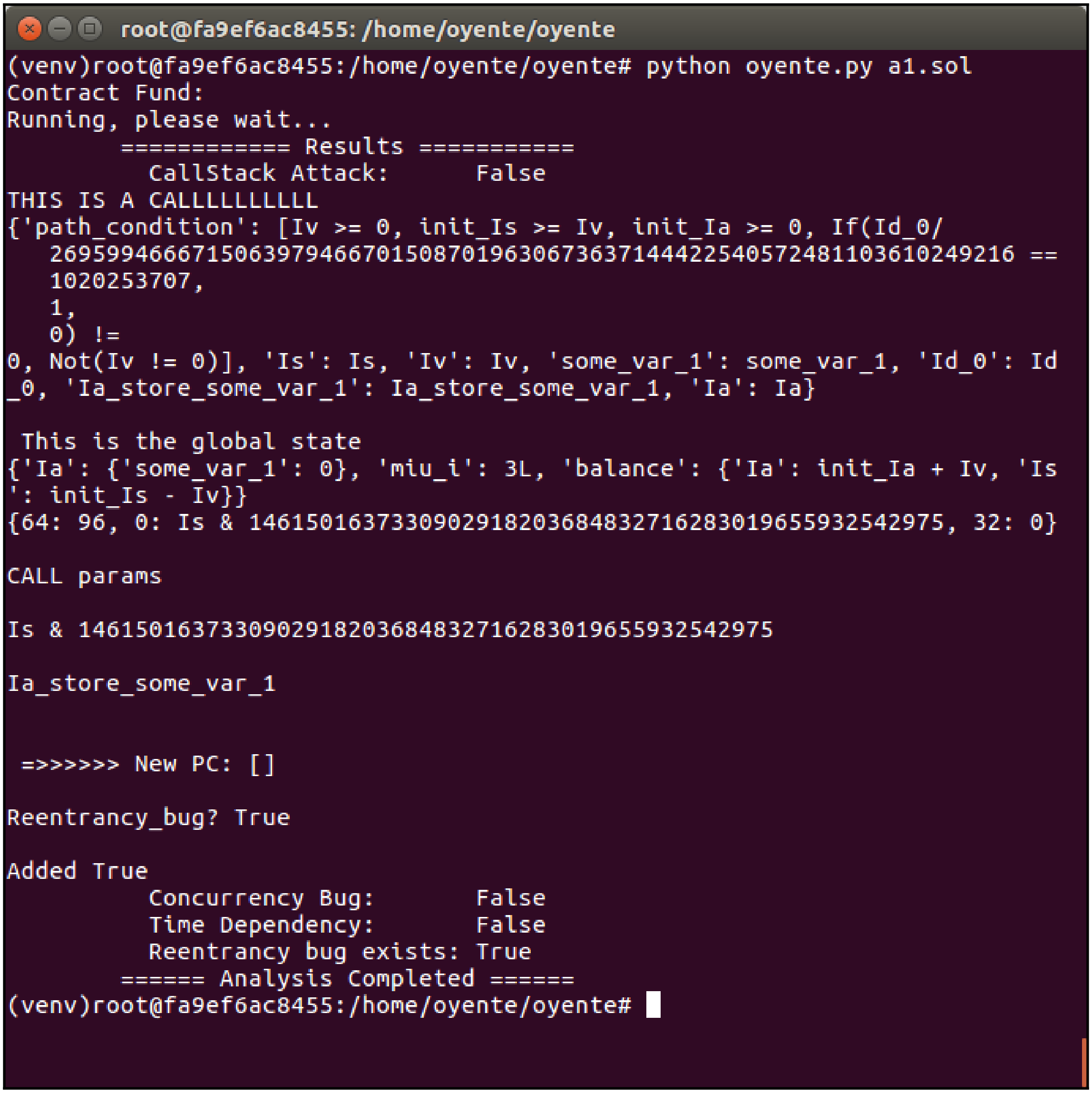
```
(* copy this to http://why3.lri.fr/try/ *)

module UInt256
        use import mach.int.Unsigned
        type uint256
        constant max_uint256: int =
0xffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
        clone export mach.int.Unsigned with
                type t = uint256,
                constant max = max_uint256
end

module Address
        use import mach.int.Unsigned
        type address
        constant max_address: int = 0xffffffffffffffffffffffffffffffffffffffff (* 160 bit = 40
f's *)
        clone export mach.int.Unsigned with
                type t = address,
                constant max = max_address
```



```
    use import int.ComputerDivision
    use import mach.int.Unsigned
    use import UInt256
    exception Revert
    exception Return
    type state = {
        mutable _z: uint256
    }
    type account = {
        mutable balance: uint256;
        storage: state
    }
    val external_call (this: account): bool
        ensures { result = false -> this = (old this) }
        writes { this }
    let rec _x (this: account):
            (uint256)
        writes { this }
        =
        let prestate = {balance = this.balance; storage = {_z
        let _y: ref uint256 = ref (of_int 0) in
        try
        begin
            this.storage._z <- (of_int 115792089237316195423
            begin _y := (this.storage._z + (of_int 1)); raise
        end;
```



```
pragma solidity ^0.4.0;
contract Fund {
    mapping(address => uint) shares;
    function withdraw() {
        if (msg.sender.send(shares[msg.sender]))
            shares[msg.sender] = 0;
    }
}
```



```
(venv)root@fa9ef6ac8455:/home/oyente/oyente# python oyente.py a1.sol
Contract Fund:
Running, please wait...
        ============ Results ===========
          CallStack Attack:      False
THIS IS A CALLLLLLLLLL
{'path_condition': [Iv >= 0, init_Is >= Iv, init_Ia >= 0, If(Id_0/
   26959946667150639794667015087019630673637144422540572481103610249216 ==
   1020253707,
   1,
   0) !=
0, Not(Iv != 0)], 'Is': Is, 'Iv': Iv, 'some_var_1': some_var_1, 'Id_0': Id
_0, 'Ia_store_some_var_1': Ia_store_some_var_1, 'Ia': Ia}

 This is the global state
{'Ia': {'some_var_1': 0}, 'miu_i': 3L, 'balance': {'Ia': init_Ia + Iv, 'Is
': init_Is - Iv}}
{64: 96, 0: Is & 1461501637330902918203684832716283019655932542975, 32: 0}

CALL params

Is & 1461501637330902918203684832716283019655932542975

Ia_store_some_var_1


 =>>>>>> New PC: []

Reentrancy_bug? True

Added True
          Concurrency Bug:       False
          Time Dependency:       False
          Reentrancy bug exists: True
        ====== Analysis Completed ======
(venv)root@fa9ef6ac8455:/home/oyente/oyente# 
```