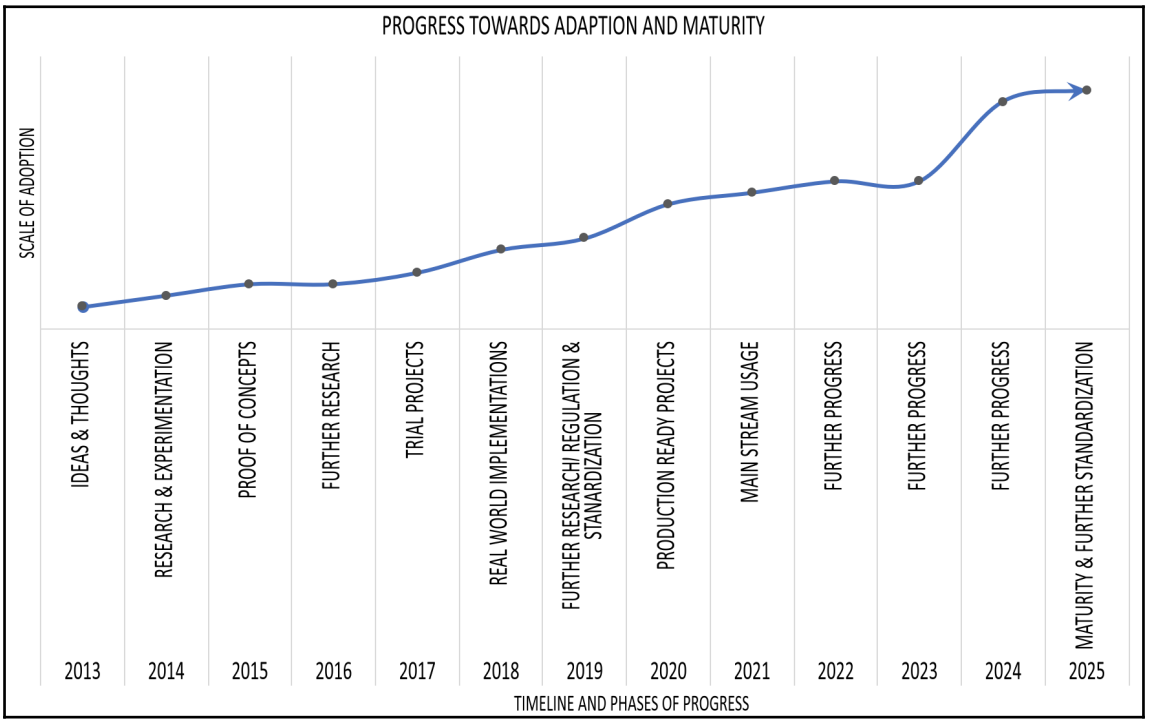
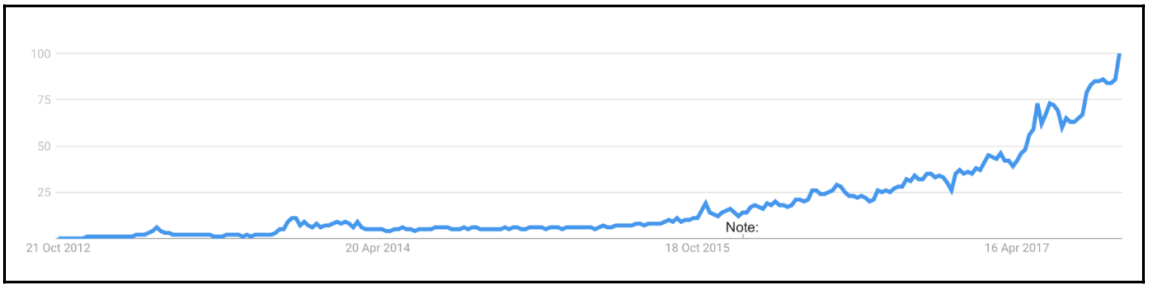
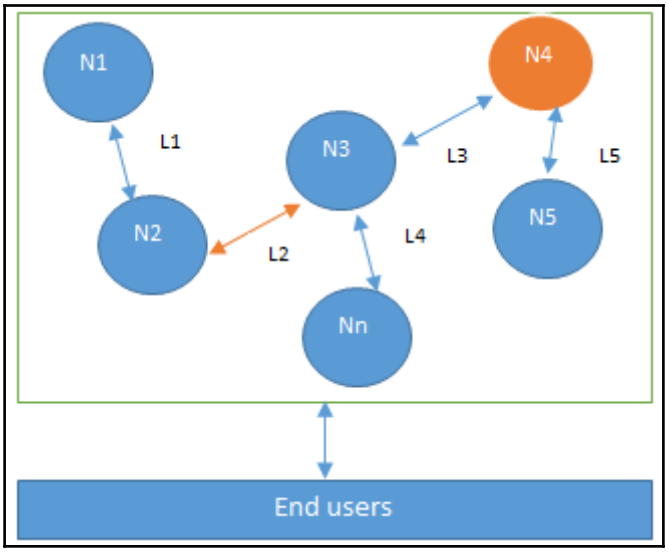
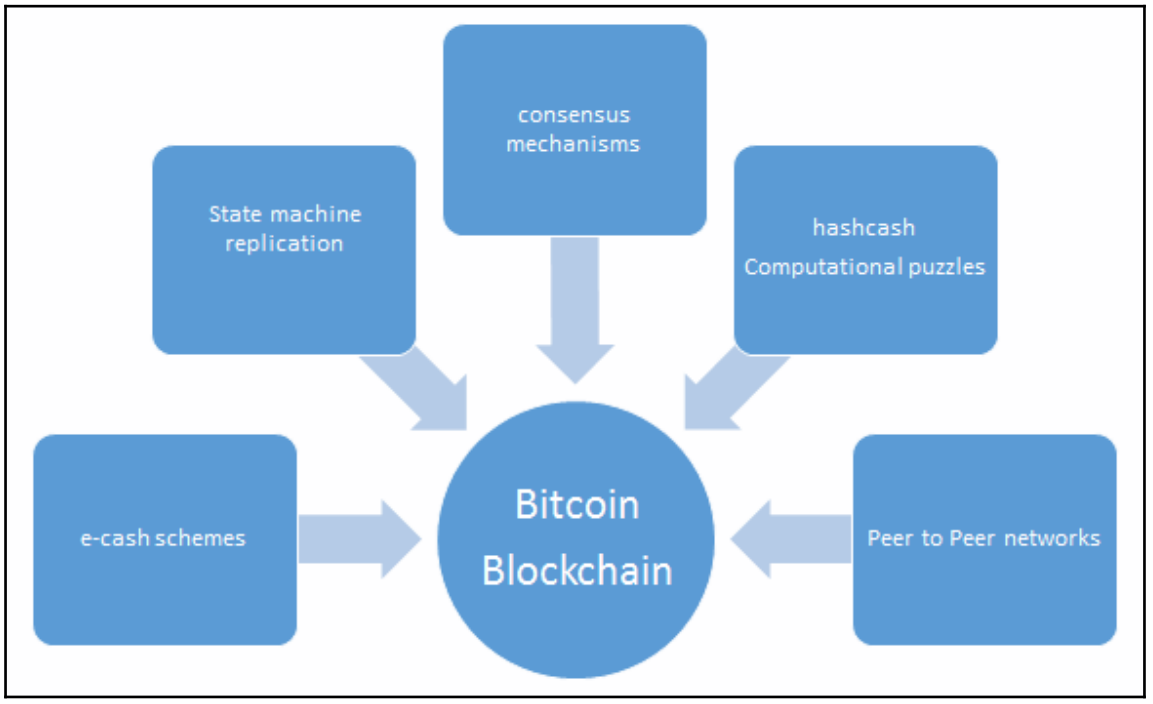
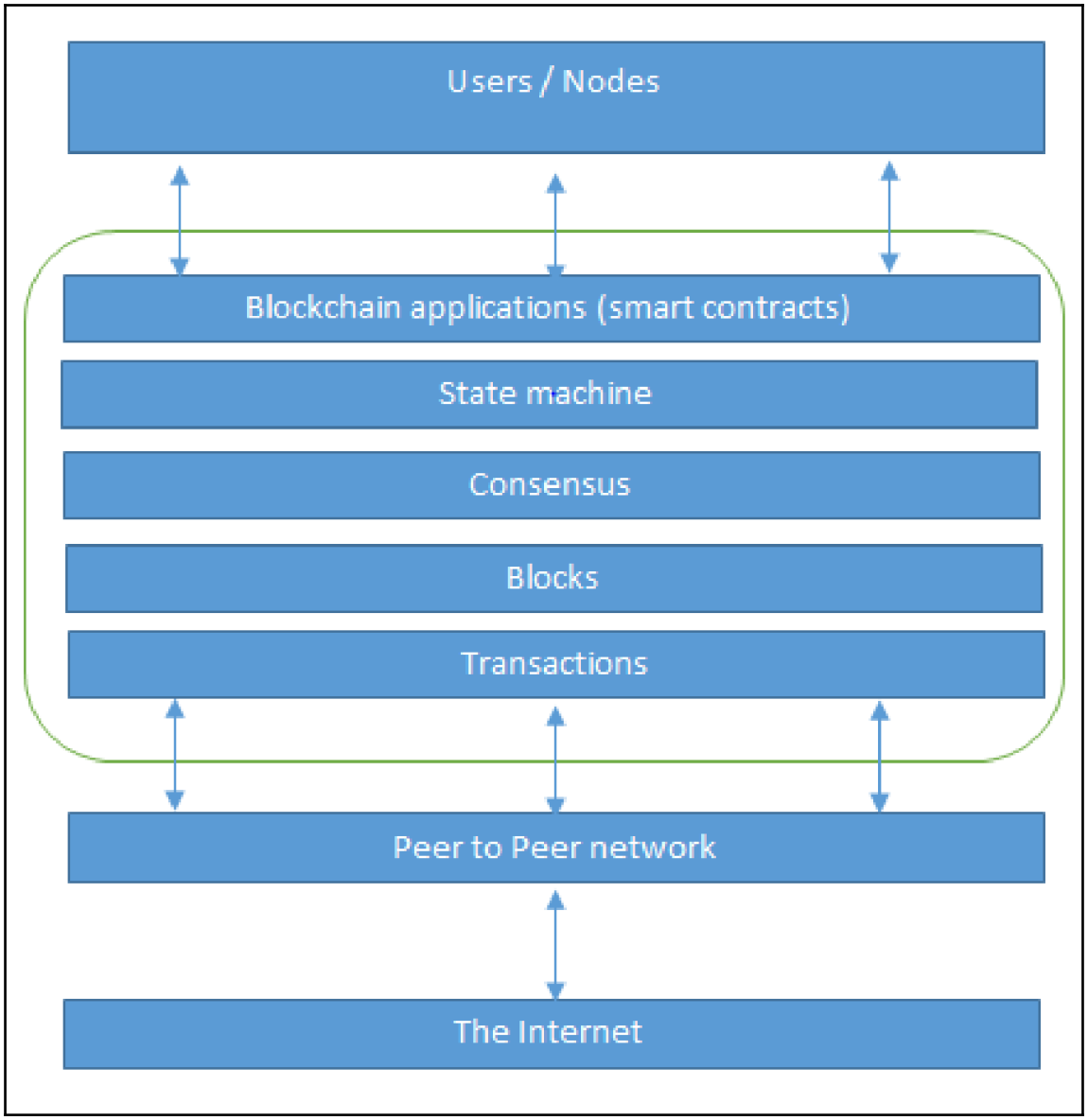
Chapter 1: Blockchain 101

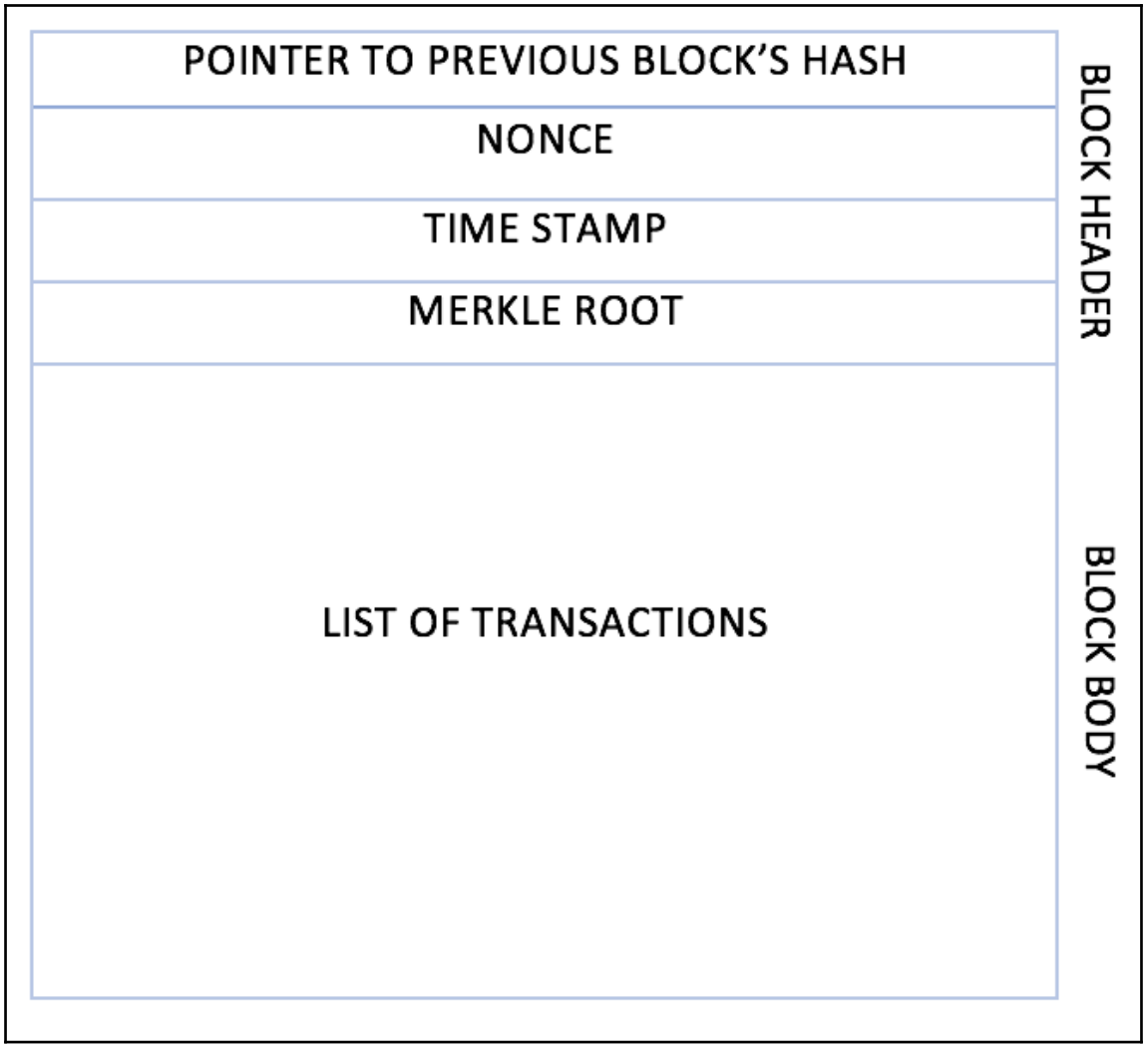


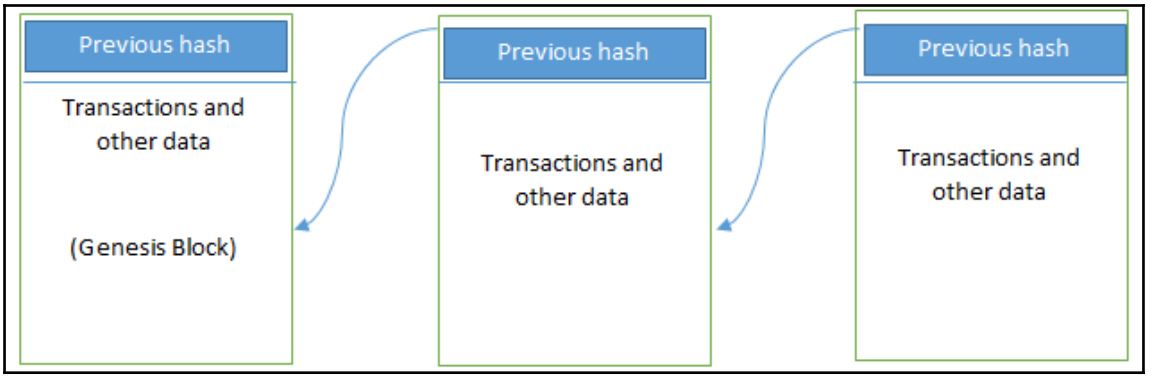



N1
N2
N3
N4
N5
Nn
L1
L2
L3
L4
L5
End users

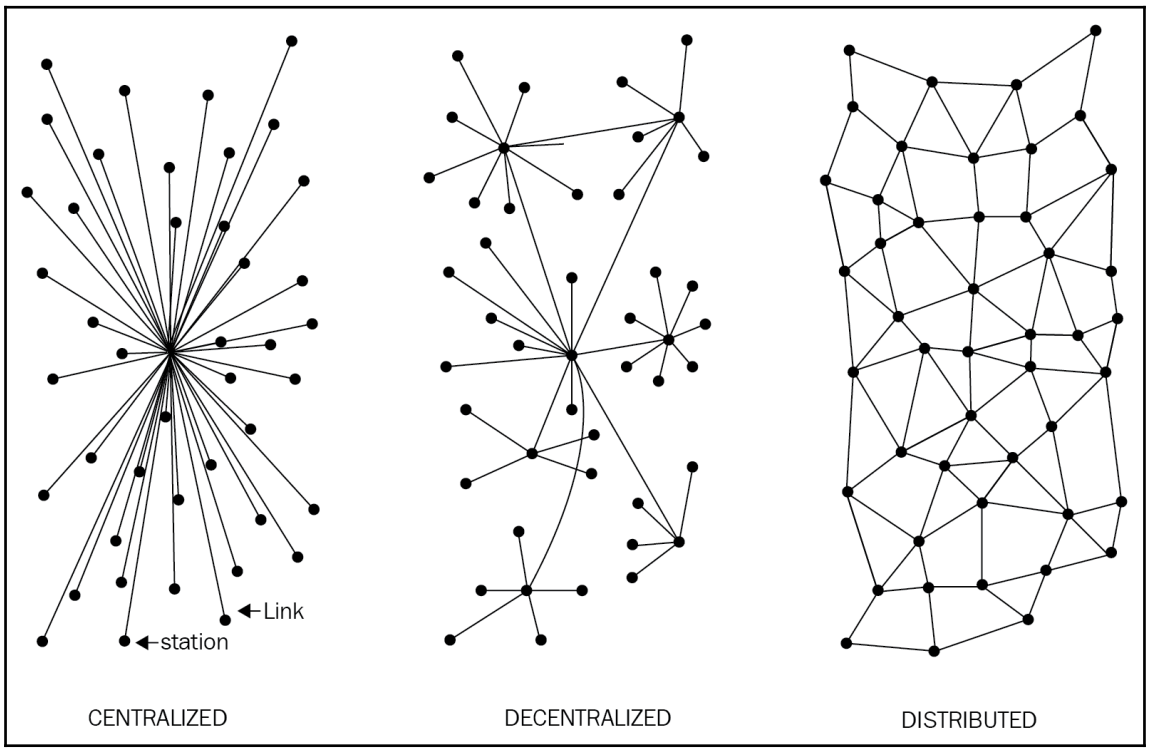

consensus mechanisms
State machine replication
hashcash Computational puzzles
e-cash schemes
Bitcoin Blockchain
Peer to Peer networks

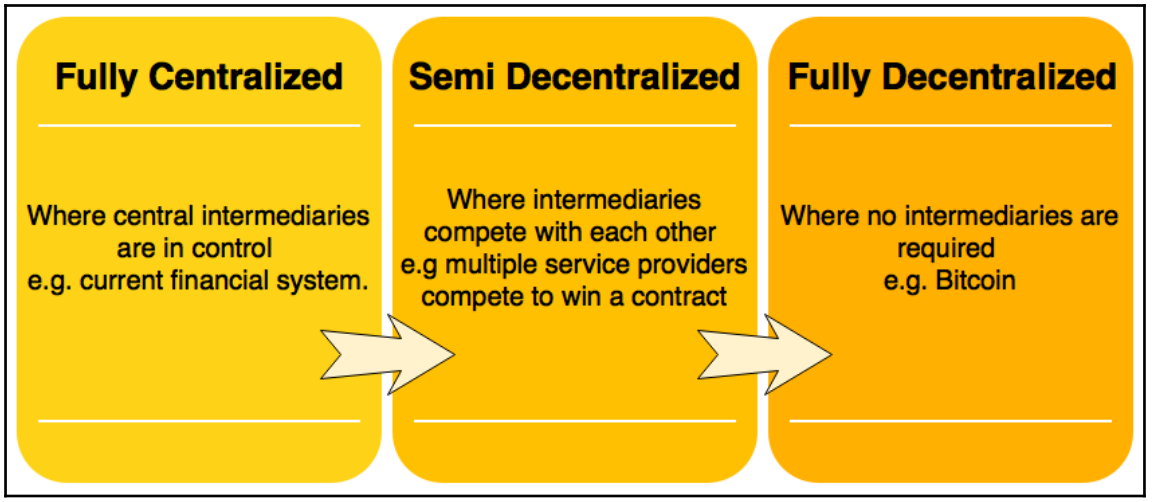

Users / Nodes
Blockchain applications (smart contracts)
State machine
Consensus
Blocks
Transactions
Peer to Peer network
The Internet

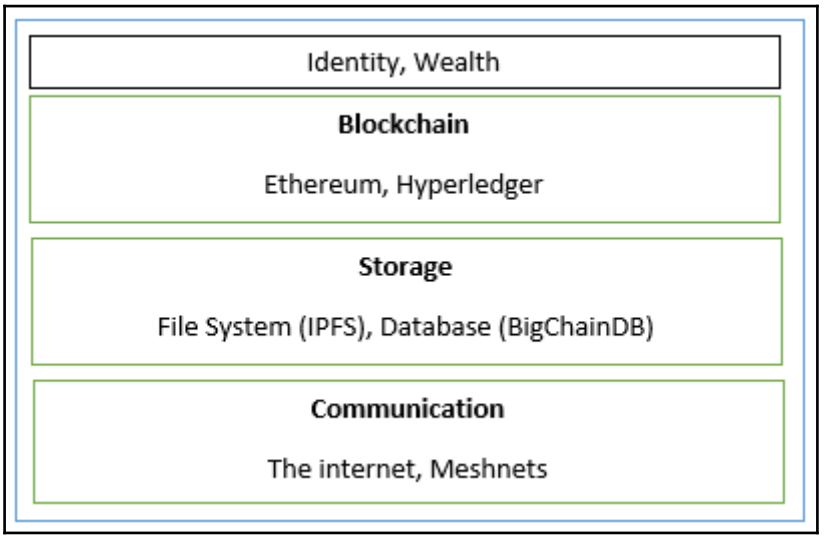

POINTER TO PREVIOUS BLOCK'S HASH
NONCE
TIME STAMP
MERKLE ROOT
LIST OF TRANSACTIONS
BLOCK HEADER
BLOCK BODY


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

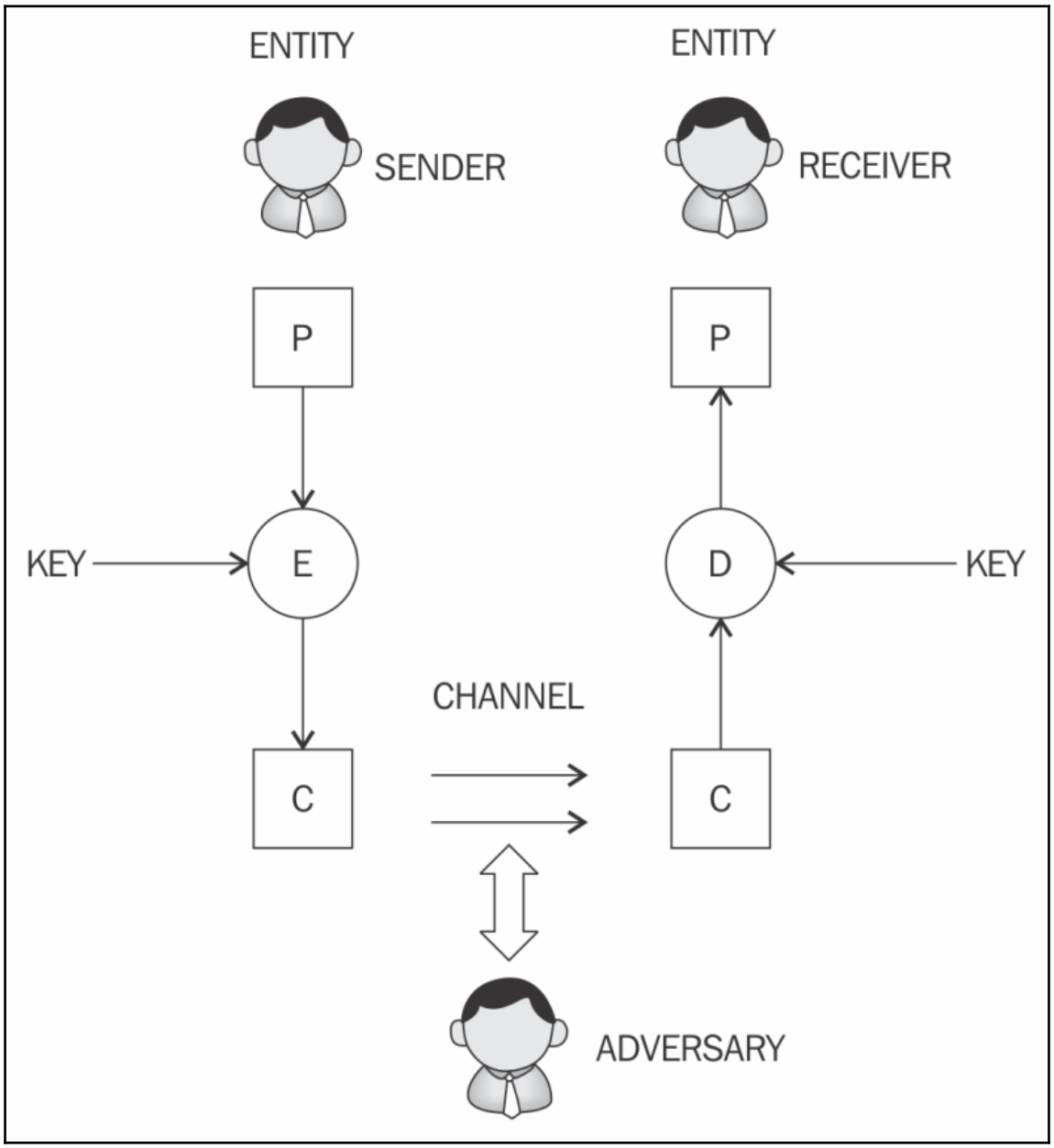
Chapter 2: Decentralization

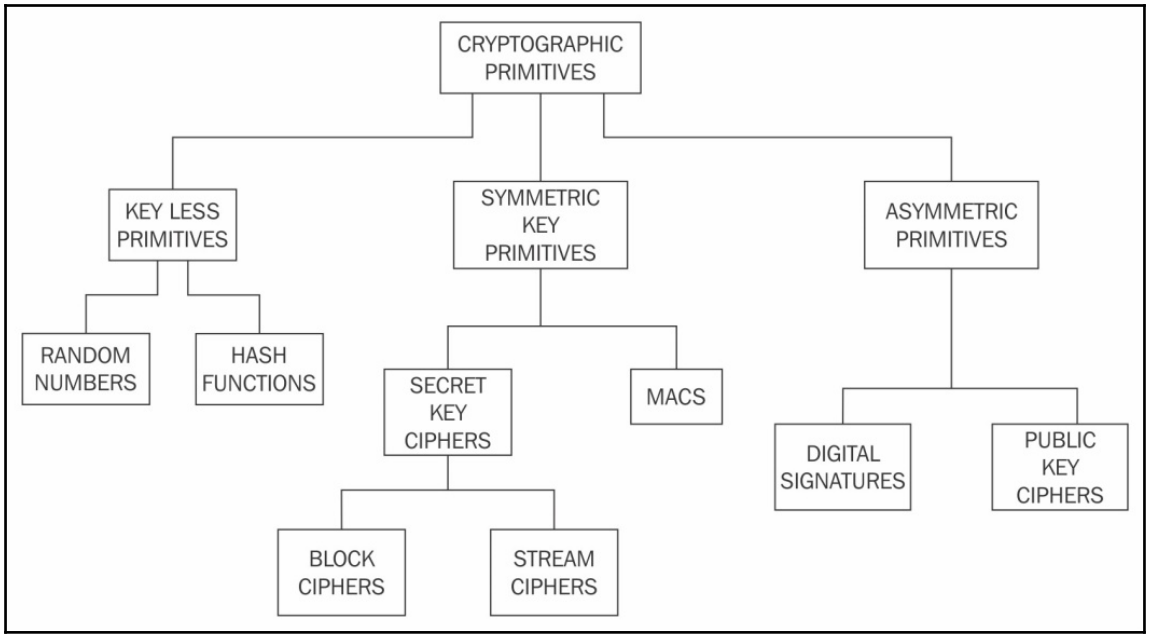


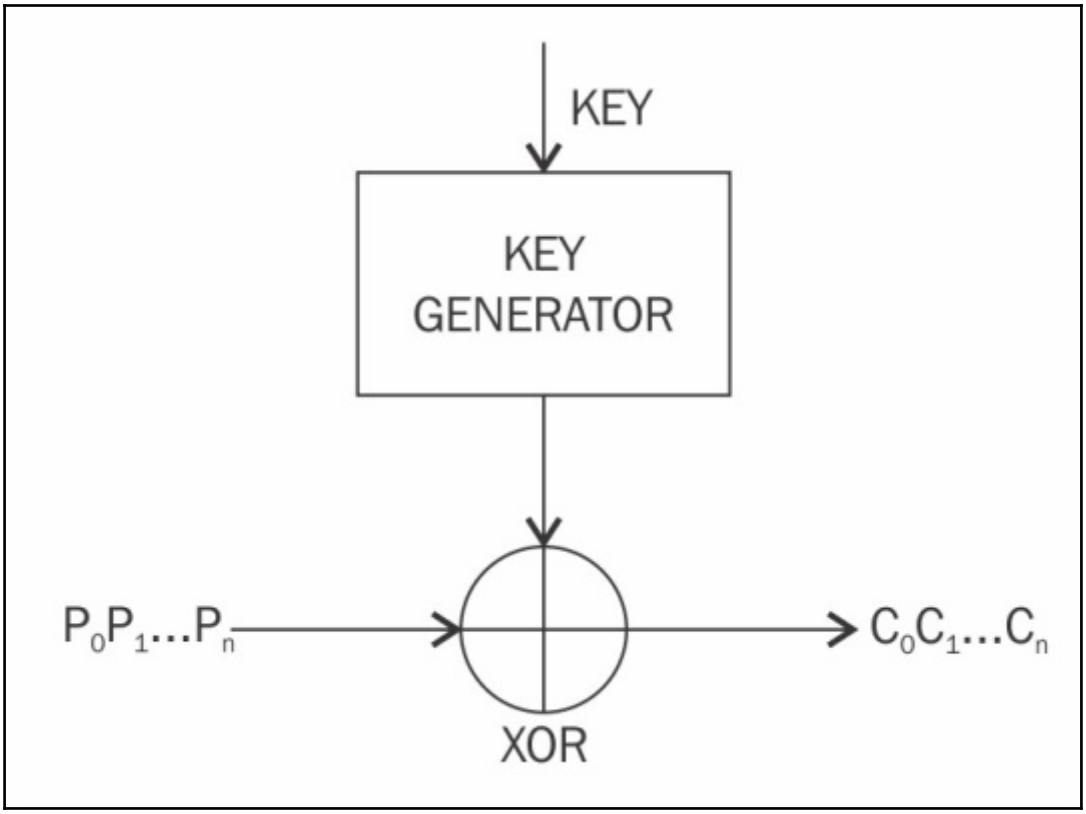

Fully Centralized
Where central intermediaries are in control
e.g. current financial system.
Semi Decentralized
Where intermediaries compete with each other
e.g multiple service providers compete to win a contract
Fully Decentralized
Where no intermediaries are required
e.g. Bitcoin

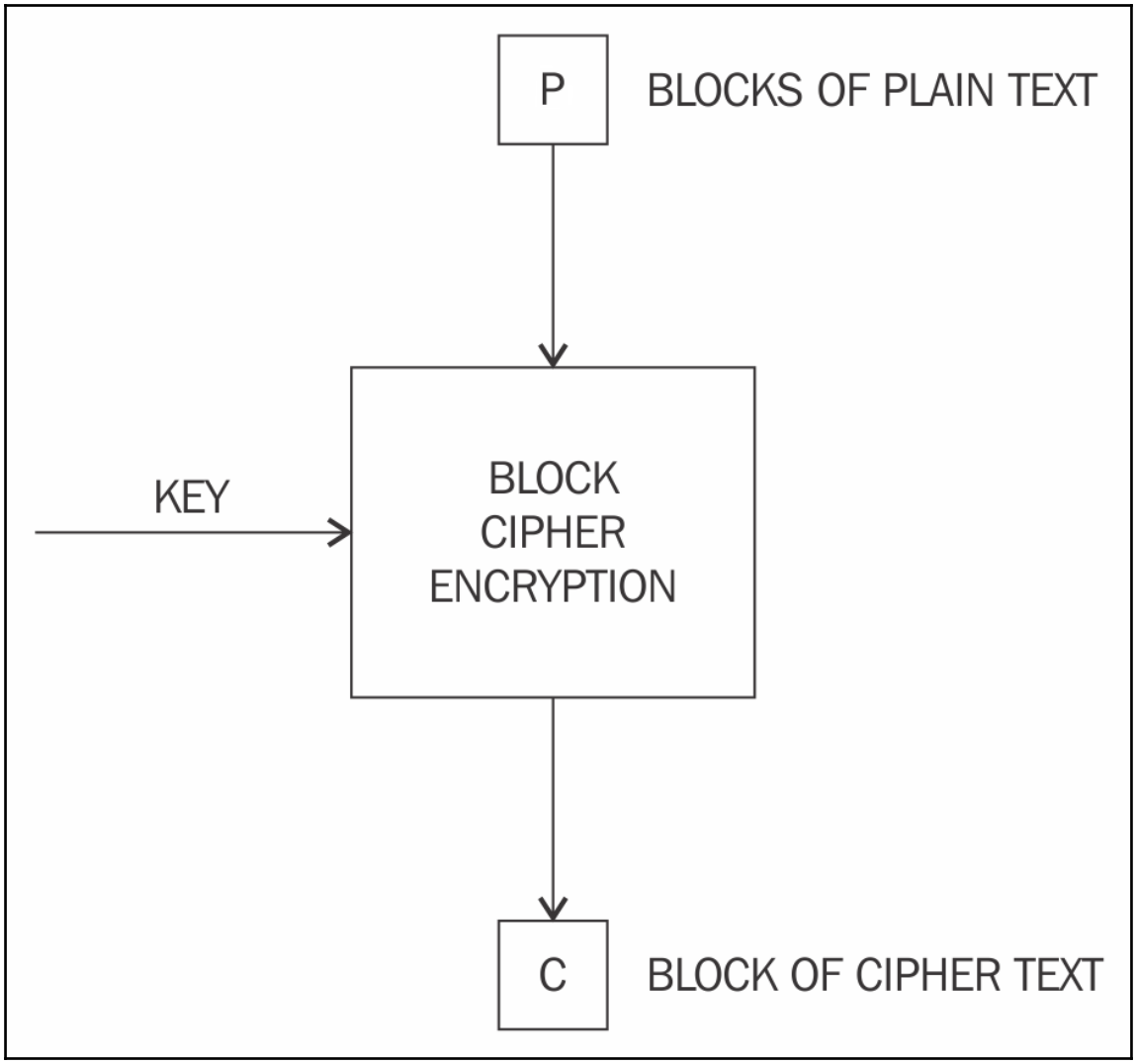

Identity, Wealth
Blockchain
Ethereum, Hyperledger
Storage
File System (IPFS), Database (BigChainDB)
Communication
The internet, Meshnets

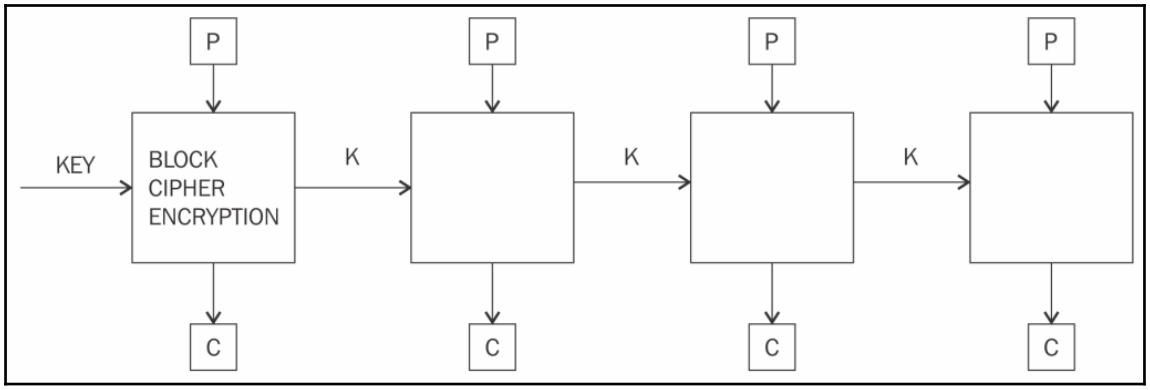
Chapter 3: Symmetric Cryptography

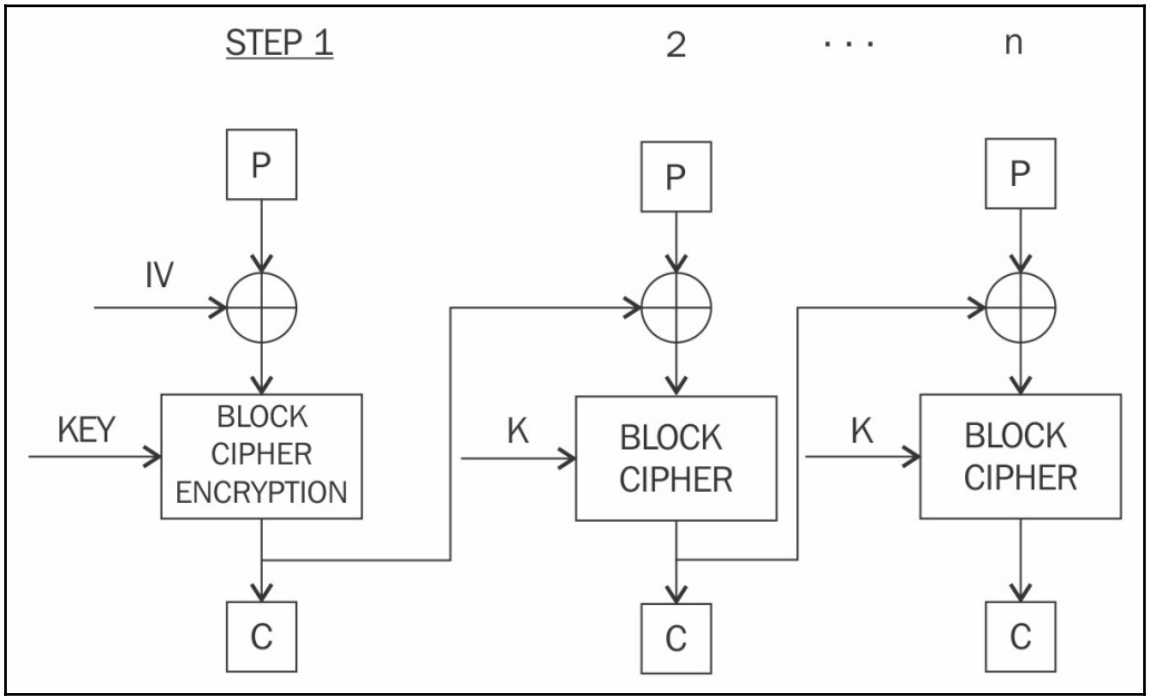


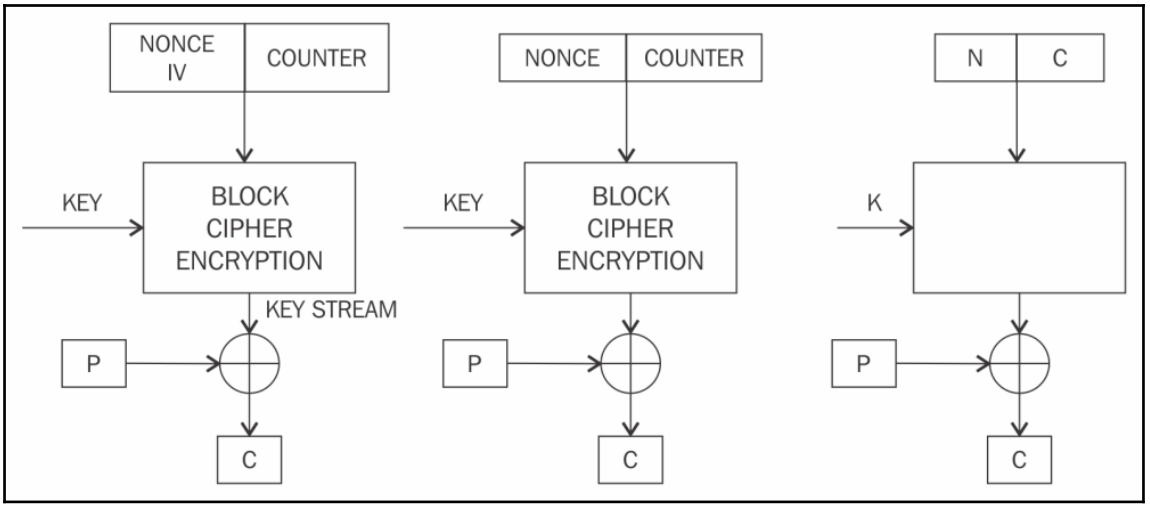

CRYPTOGRAPHIC PRIMITIVES
KEY LESS PRIMITIVES
SYMMETRIC KEY PRIMITIVES
ASYMMETRIC PRIMITIVES
RANDOM NUMBERS
HASH FUNCTIONS
SECRET KEY CIPHERS
MACS
DIGITAL SIGNATURES
PUBLIC KEY CIPHERS
BLOCK CIPHERS
STREAM CIPHERS

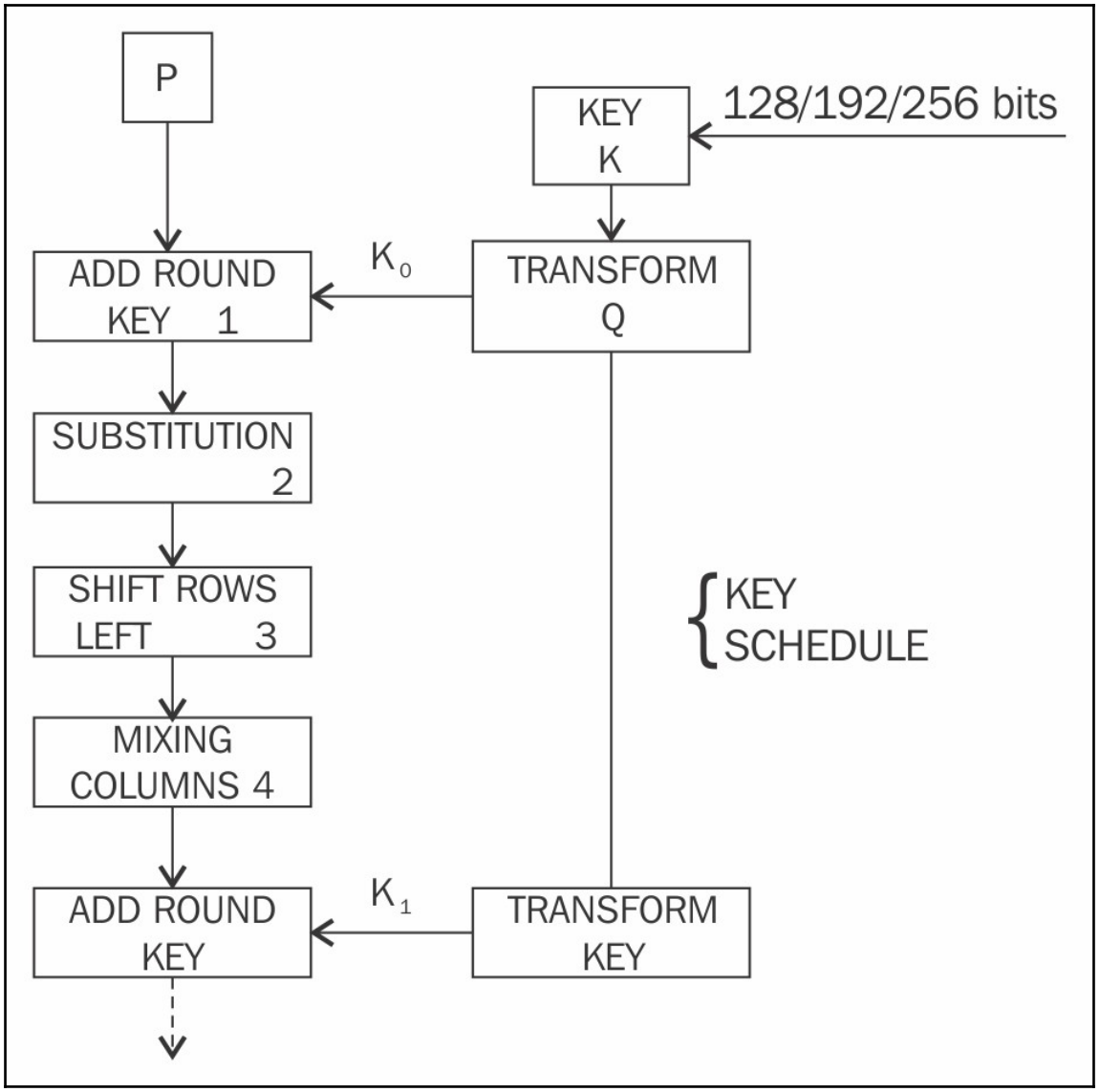

KEY
KEY GENERATOR
$P_0P_1...P_n$
$C_0C_1...C_n$
XOR


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

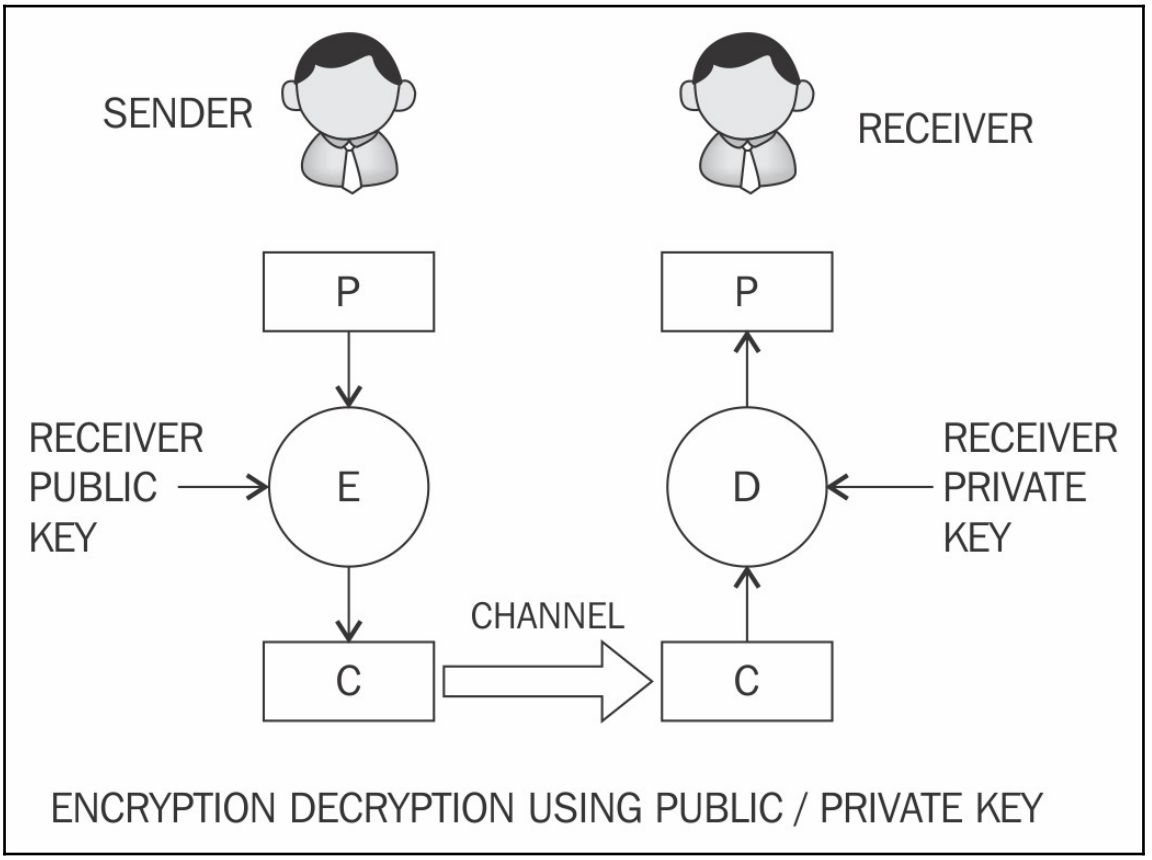


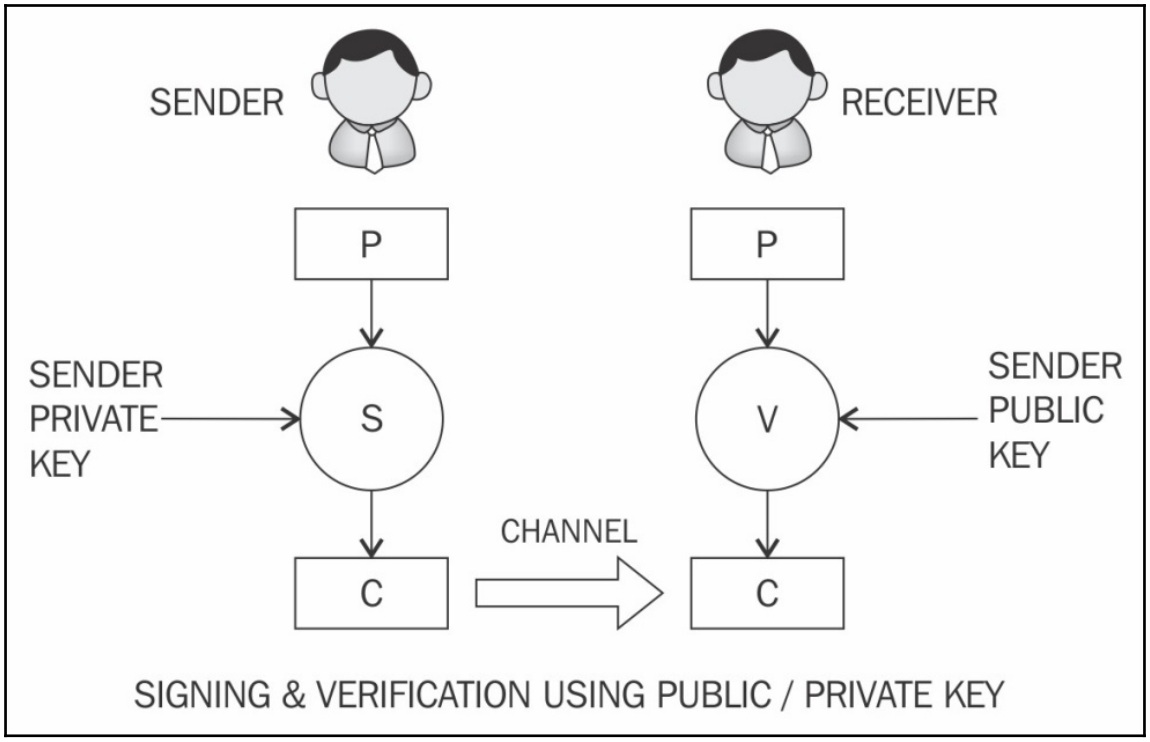

```
Salted__w  s_ÿ  þ~?                    :~/Crypt$
:~/Crypt$
```

```
:~/Crypt$ cat message.ptx
Salted__w░░░s_ÿ░h~?░░░░░░░░:~/Crypt$
```

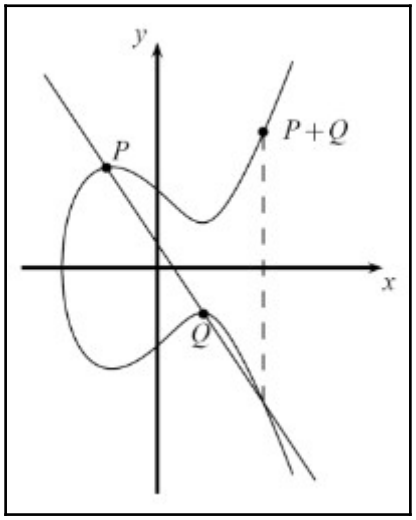
```
Cipher Types
-aes-128-cbc               -aes-128-ccm               -aes-128-cfb
-aes-128-cfb1              -aes-128-cfb8              -aes-128-ctr
-aes-128-ecb               -aes-128-ofb               -aes-192-cbc
-aes-192-ccm               -aes-192-cfb               -aes-192-cfb1
-aes-192-cfb8              -aes-192-ctr               -aes-192-ecb
-aes-192-ofb               -aes-256-cbc               -aes-256-ccm
-aes-256-cfb               -aes-256-cfb1              -aes-256-cfb8
-aes-256-ctr               -aes-256-ecb               -aes-256-ofb
-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-wrap            -id-aes192-CCM             -id-aes192-wrap
-id-aes256-CCM             -id-aes256-wrap            -id-smime-alg-CMS3DESwrap
-idea                      -idea-cbc                  -idea-cfb
-idea-ecb                  -idea-ofb                  -rc2
-rc2-40-cbc                -rc2-64-cbc                -rc2-cbc
-rc2-cfb                   -rc2-ecb                   -rc2-ofb
-rc4                       -rc4-40                    -seed
-seed-cbc                  -seed-cfb                  -seed-ecb
-seed-ofb
```

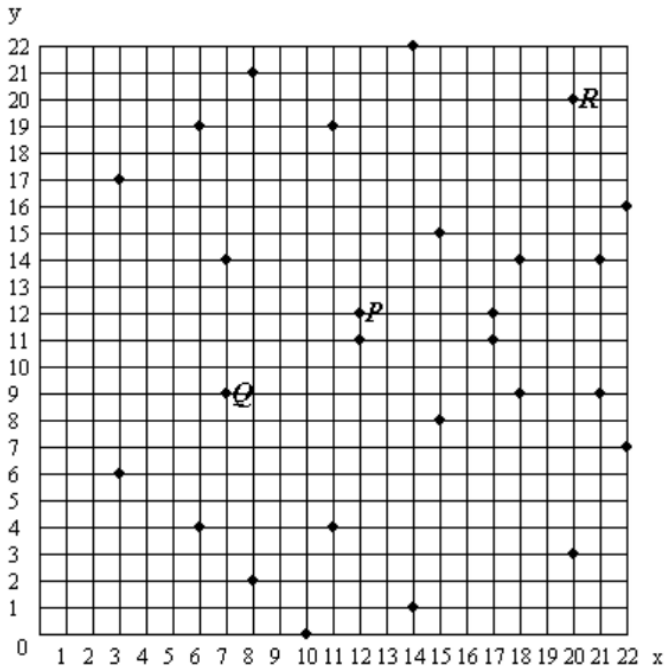
Chapter 4: Public Key Cryptography





SIGNING & VERIFICATION USING PUBLIC / PRIVATE KEY





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

27 solutions

P (12, 12)

Q (7, 9)

R (20, 20)

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

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

$= 3 * 14 \bmod 23$

$= 19$

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

$= 361 - 12 - 7 \bmod 23$

$= 20$

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

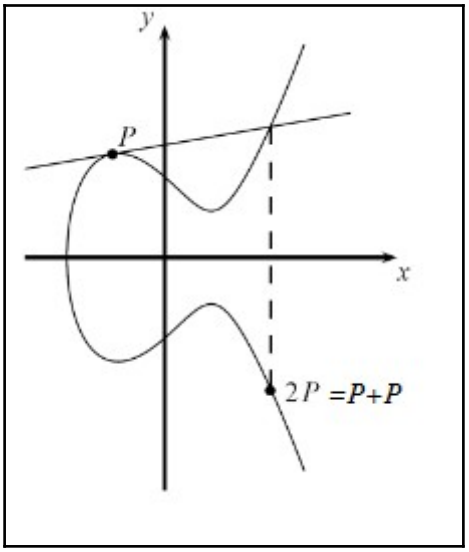
$= -12 + 19 * (12 - 20) \bmod 23$

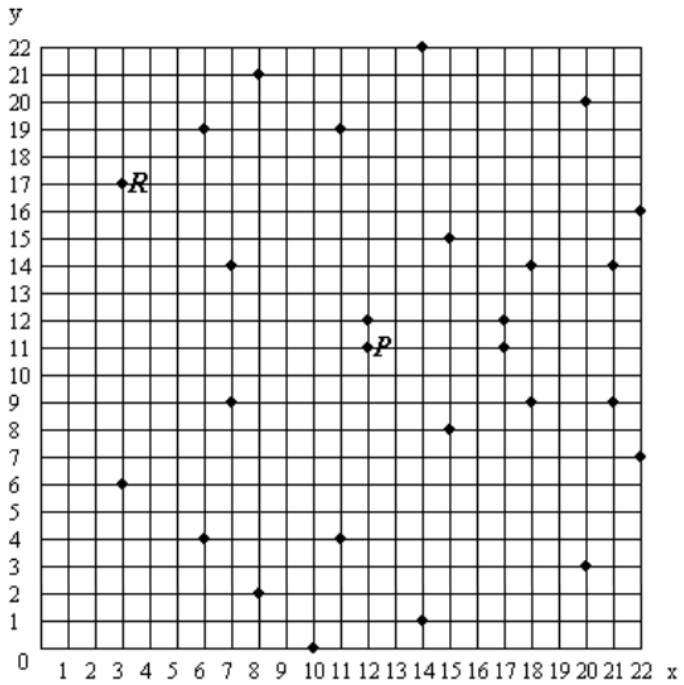
$= 11 + 19 * 15 \bmod 23$

$= 11 + 9 \bmod 23$

$= 20$

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


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

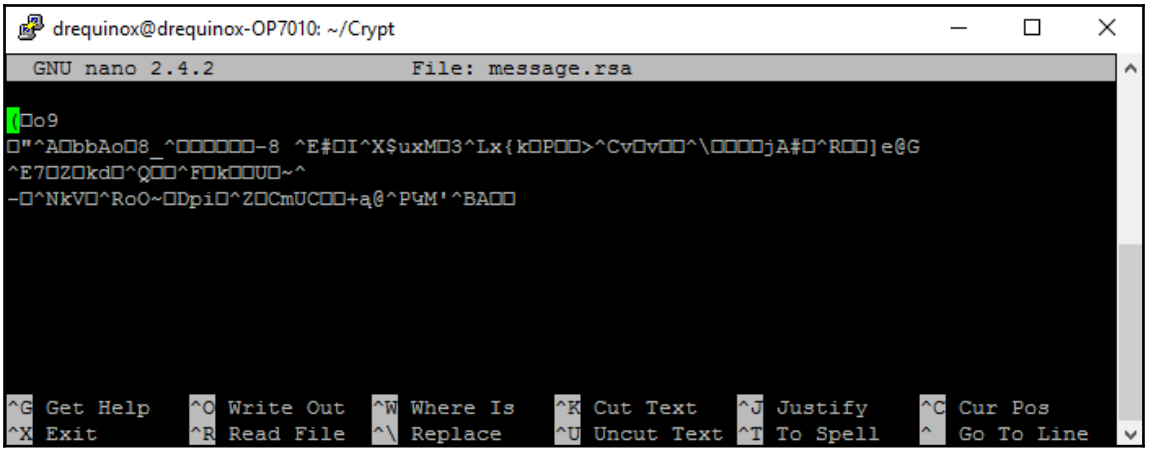
and in uncompressed form is:

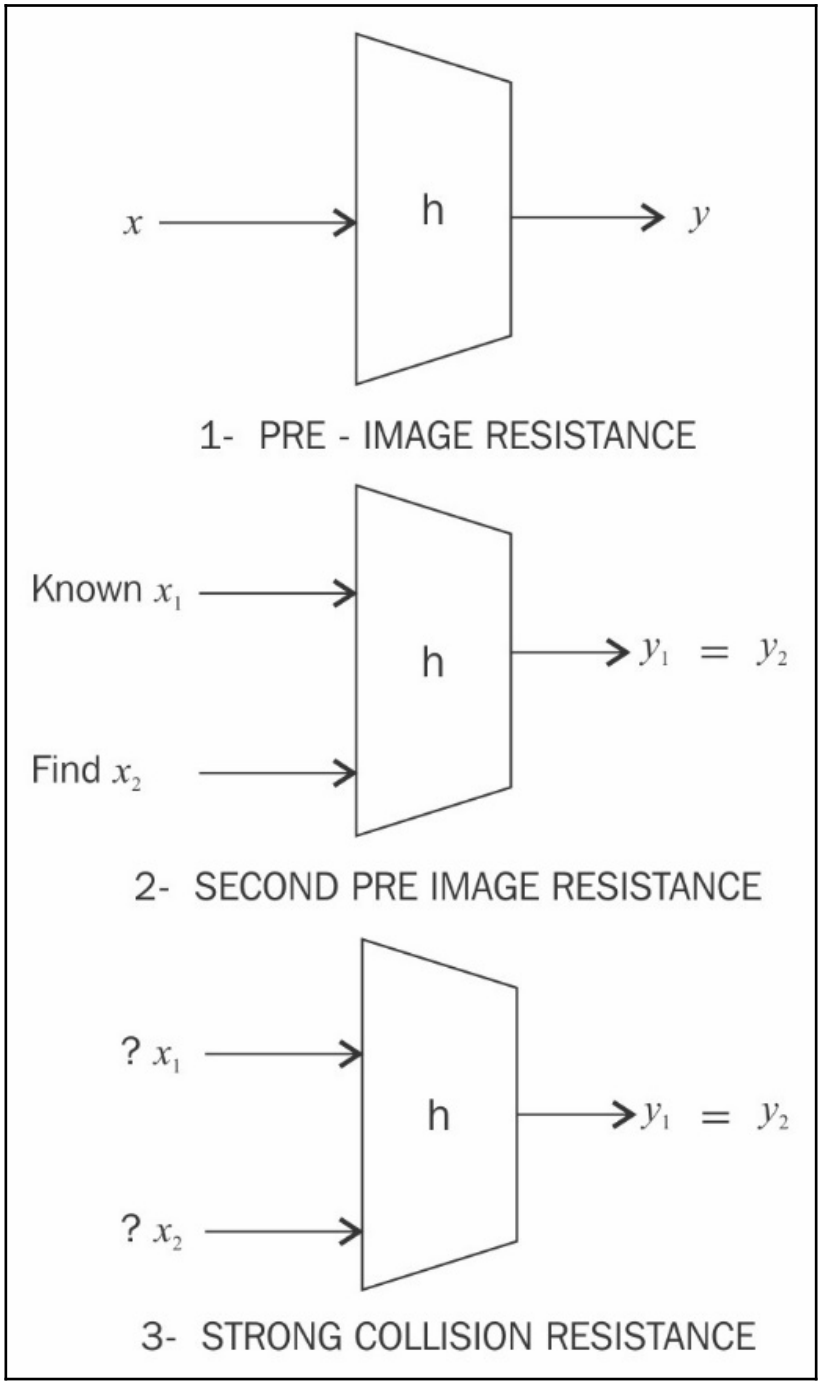
G = 04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8

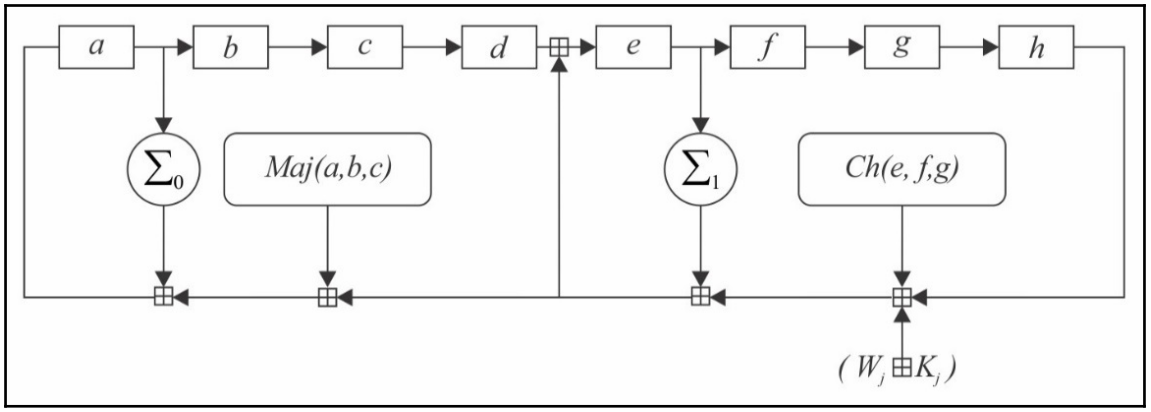
Finally the order n of G and the cofactor are:

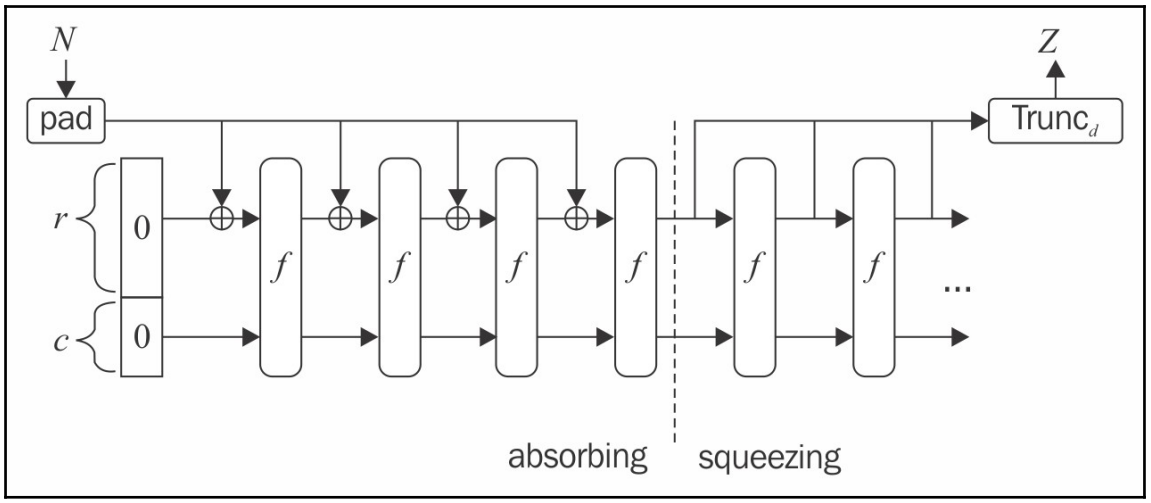
n = FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141

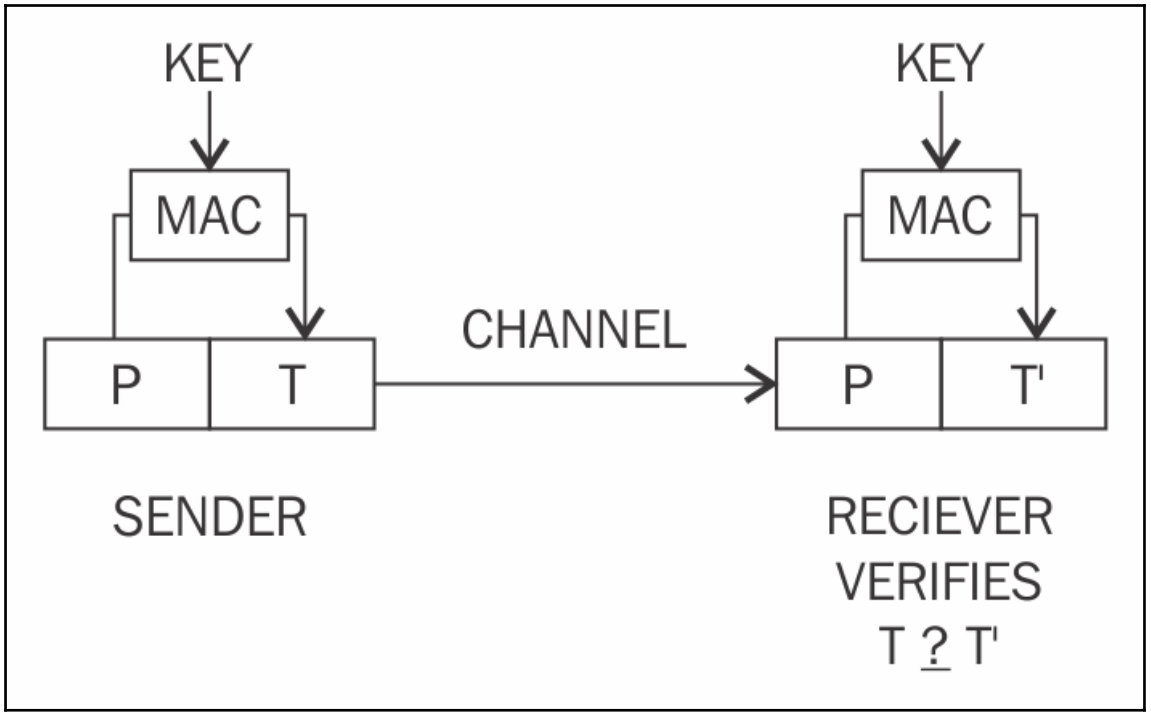
h = 01

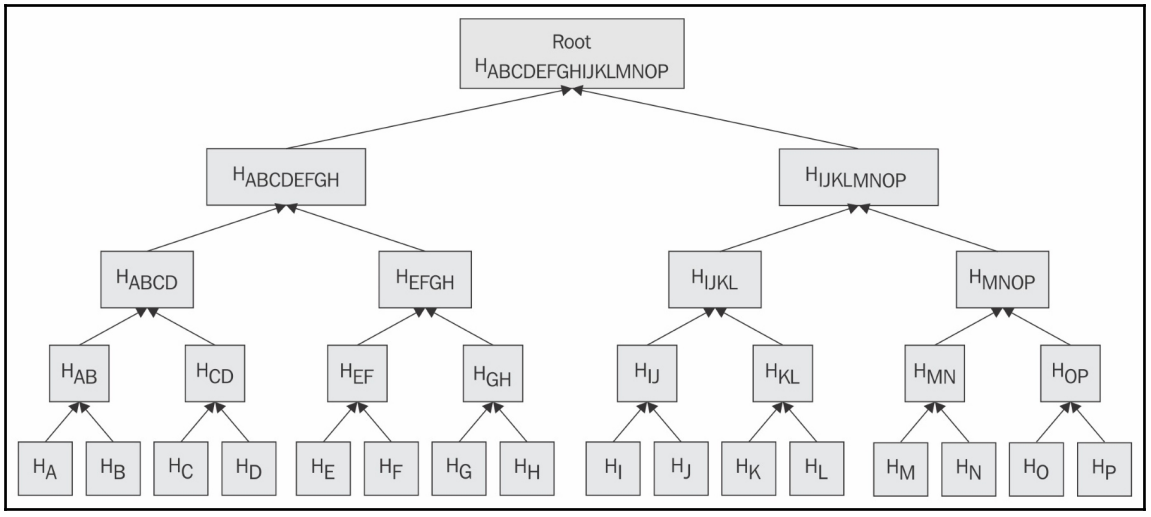

drequinox@drequinox-OP7010: ~/Crypt
GNU nano 2.4.2 File: message.rsa
(□o9
□"^A□bbAo□8_^□□□□□□-8 ^E#□I^X$uxM□3^Lx{k□P□□>^Cv□v□□^\□□□□jA#□^R□□]e@G
^E7□Z□kd□^Q□□^F□k□□U□~^
-□^NkV□^RoO~□Dpi□^Z□CmUC□□+ą@^P%M'^BA□□
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^ Go To Line

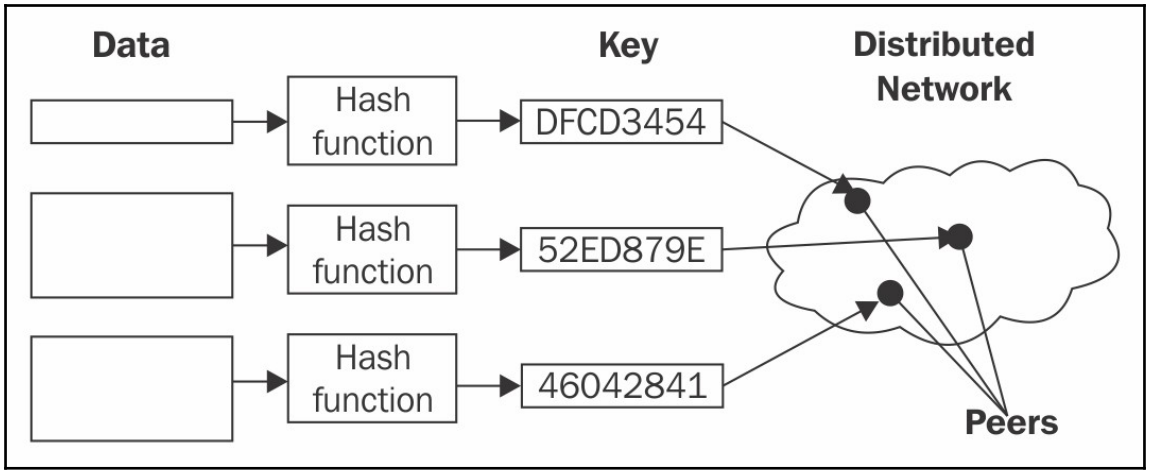

x
h
y
1- PRE - IMAGE RESISTANCE
Known x_1
Find x_2
h
$y_1 = y_2$
2- SECOND PRE IMAGE RESISTANCE
? x_1
? x_2
h
$y_1 = y_2$
3- STRONG COLLISION RESISTANCE

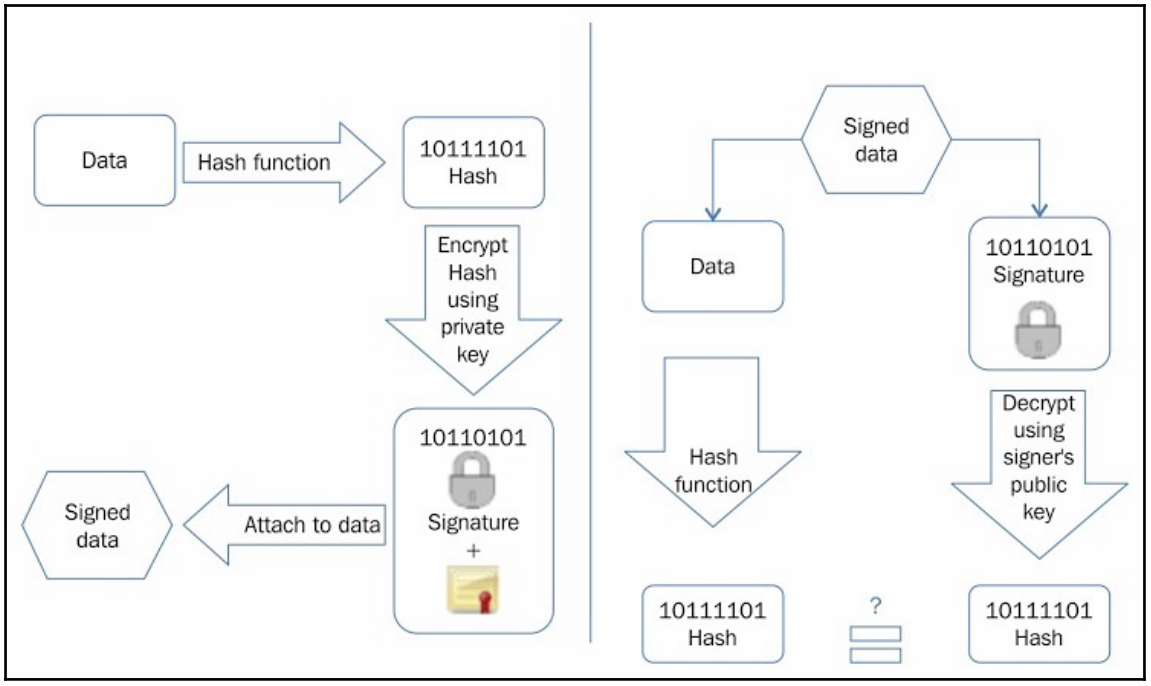

a
b
c
d
e
f
g
h
$\sum_0$
Maj(a,b,c)
$\sum_1$
Ch(e, f,g)
$(W_j \boxplus K_j)$


N
pad
Z
Trunc$_d$
r
c
0
0
f
f
f
f
f
f
...
absorbing
squeezing


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

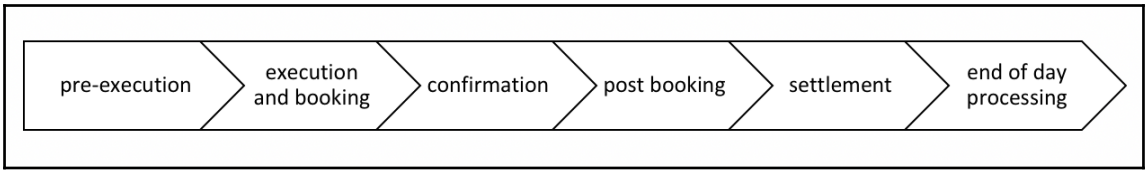

Root
HABCDEFGHIJKLMNOP
HABCDEFGH
HIJKLMNOP
HABCD
HEFGH
HIJKL
HMNOP
HAB
HCD
HEF
HGH
HIJ
HKL
HMN
HOP
HA
HB
HC
HD
HE
HF
HG
HH
HI
HJ
HK
HL
HM
HN
HO
HP



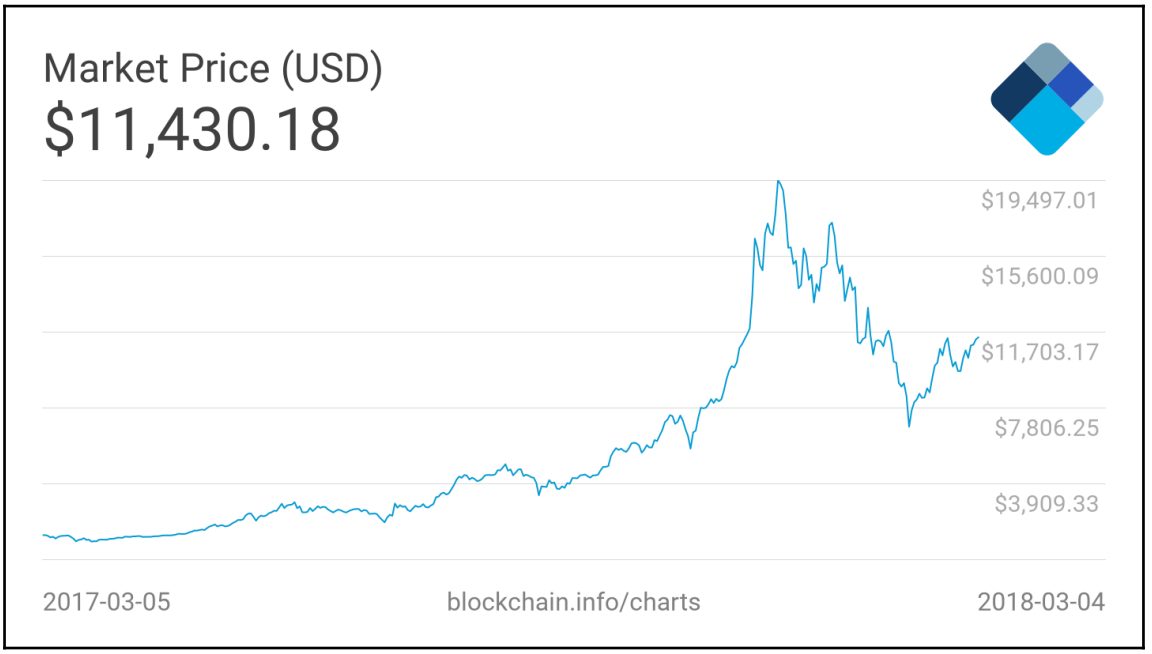


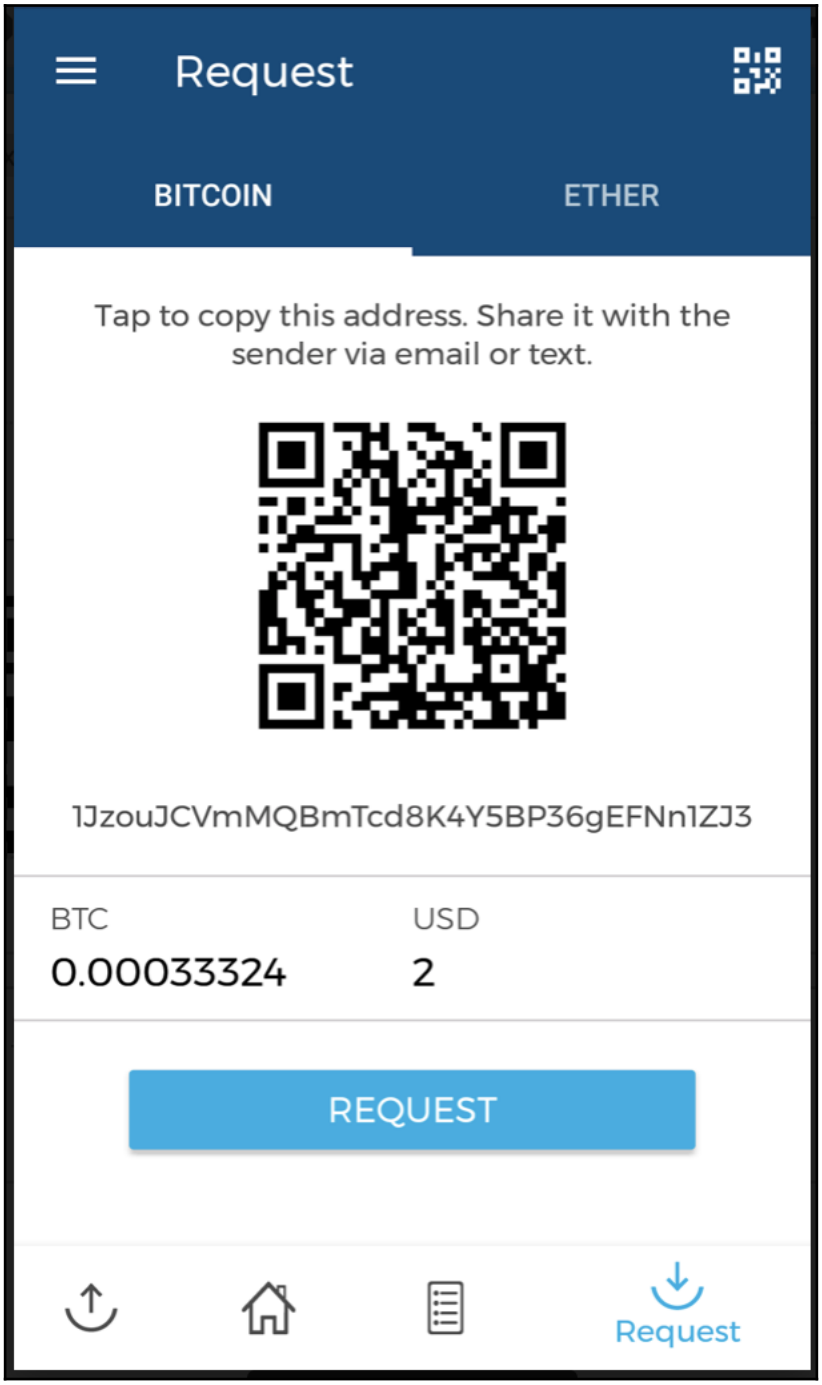

```
V  _[  h] h t    + T~Ol  s {  Cq"# A Q U, uf   p* □ *7    T'  u eAy
$ x <$ a  `  :L qWh  uG     = $  :~/Crypt$
```

```
drequinox@drequinox-OP7010: ~/Crypt
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$
```



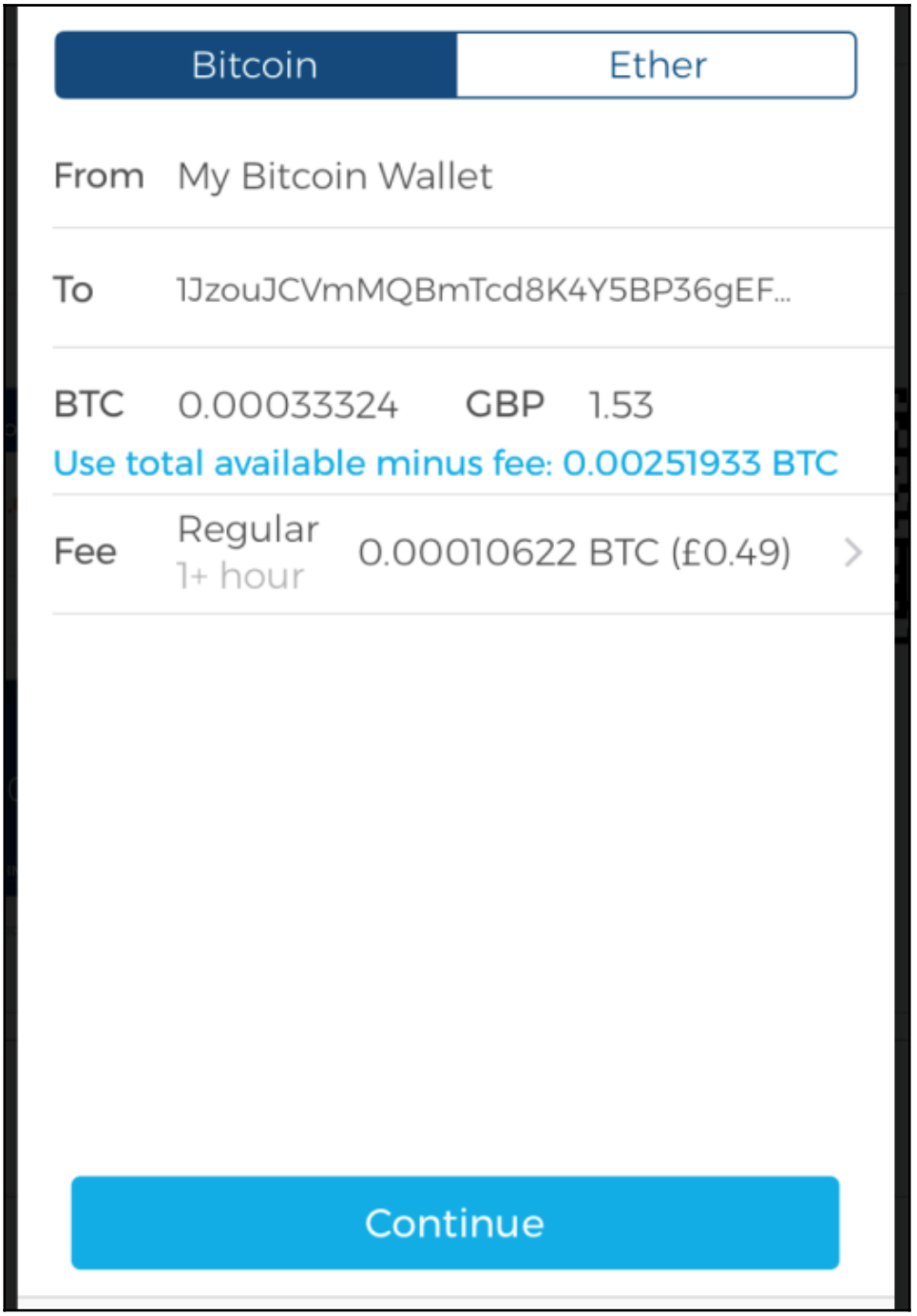
Chapter 5: Introducing Bitcoin

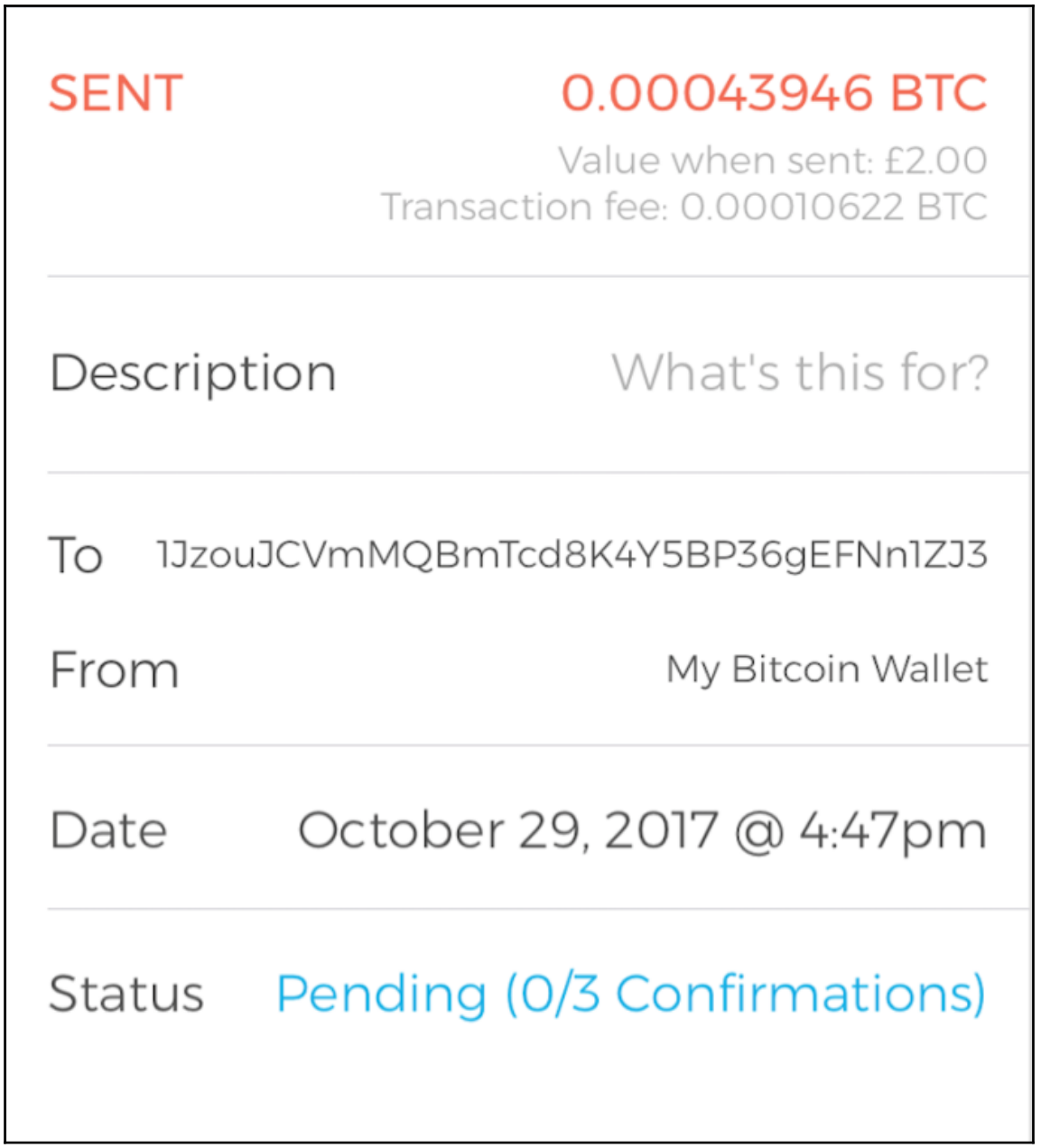


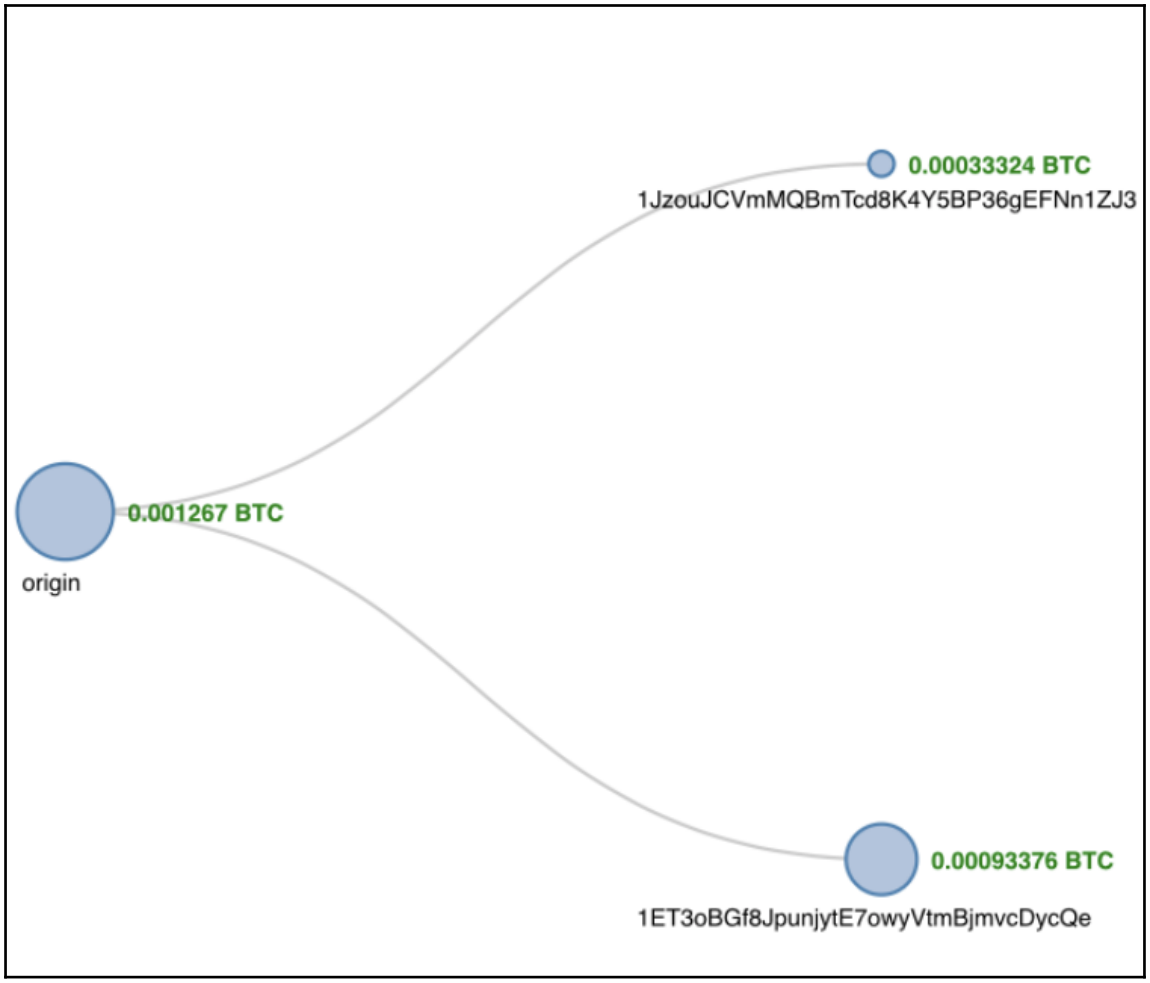

Request
BITCOIN
ETHER
Tap to copy this address. Share it with the sender via email or text.
1JzouJCVmMQBmTcd8K4Y5BP36gEFNn1ZJ3
BTC
0.00033324
USD
2
REQUEST
Request

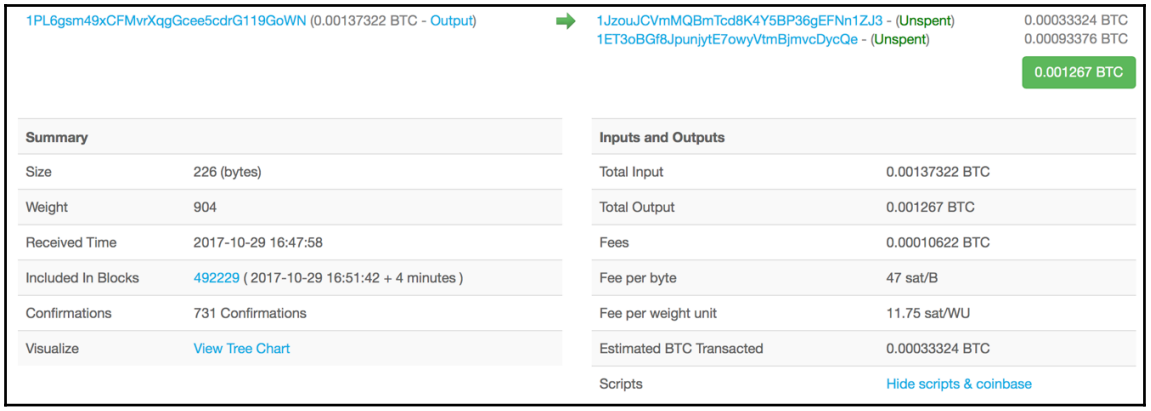
Please send 0.00033324 BTC to the Bitcoin address 1JzouJCVmMQBmTcd8K4Y5BP36gEFNn1ZJ3.

bitcoin://1JzouJCVmMQBmTcd8K4Y5BP36gEFNn1ZJ3?amount=0.00033324


Bitcoin
Ether
From My Bitcoin Wallet
To 1JzouJCVmMQBmTcd8K4Y5BP36gEF...
BTC 0.00033324 GBP 1.53
Use total available minus fee: 0.00251933 BTC
Fee Regular 1+ hour 0.00010622 BTC (£0.49)
Continue


SENT
0.00043946 BTC
Value when sent: £2.00
Transaction fee: 0.00010622 BTC
Description
What's this for?
To
1JzouJCVmMQBmTcd8K4Y5BP36gEFNn1ZJ3
From
My Bitcoin Wallet
Date
October 29, 2017 @ 4:47pm
Status
Pending (0/3 Confirmations)


0.00033324 BTC
1JzouJCVmMQBmTcd8K4Y5BP36gEFNn1ZJ3
0.001267 BTC
origin
0.00093376 BTC
1ET3oBGf8JpunjytE7owyVtmBjmvcDycQe



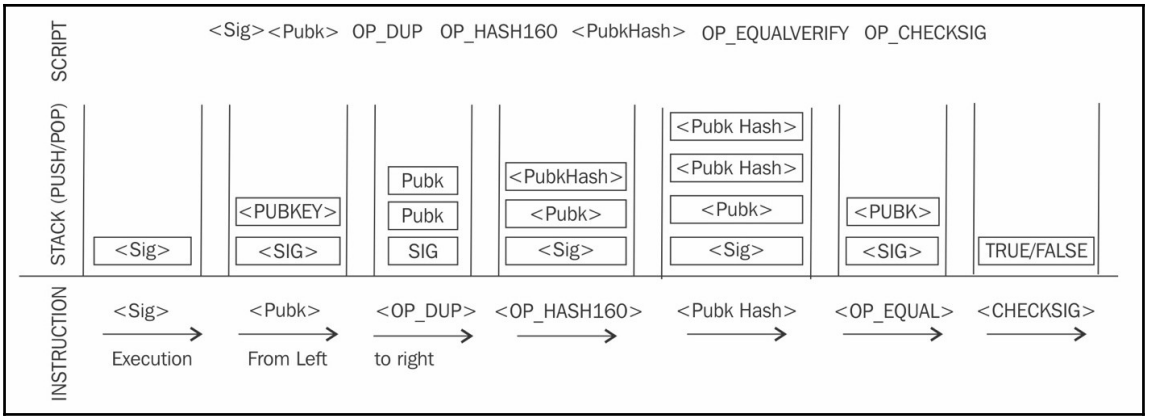
DENOMINATION	ABBREVIATION	FAMILIAR NAME	VALUE IN BTC
Satoshi	SAT	Satoshi	0.00000001 BTC
Microbit	µBTC (uBTC)	Microbitcoin or Bit	0.000001 BTC
Millibit	mBTC	Millibitcoin	0.001 BTC
Centibit	cBTC	Centibitcoin	0.01 BTC
Decibit	dBTC	Decibitcoin	0.1 BTC
Bitcoin	BTC	Bitcoin	1 BTC
DecaBit	daBTC	Decabitcoin	10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

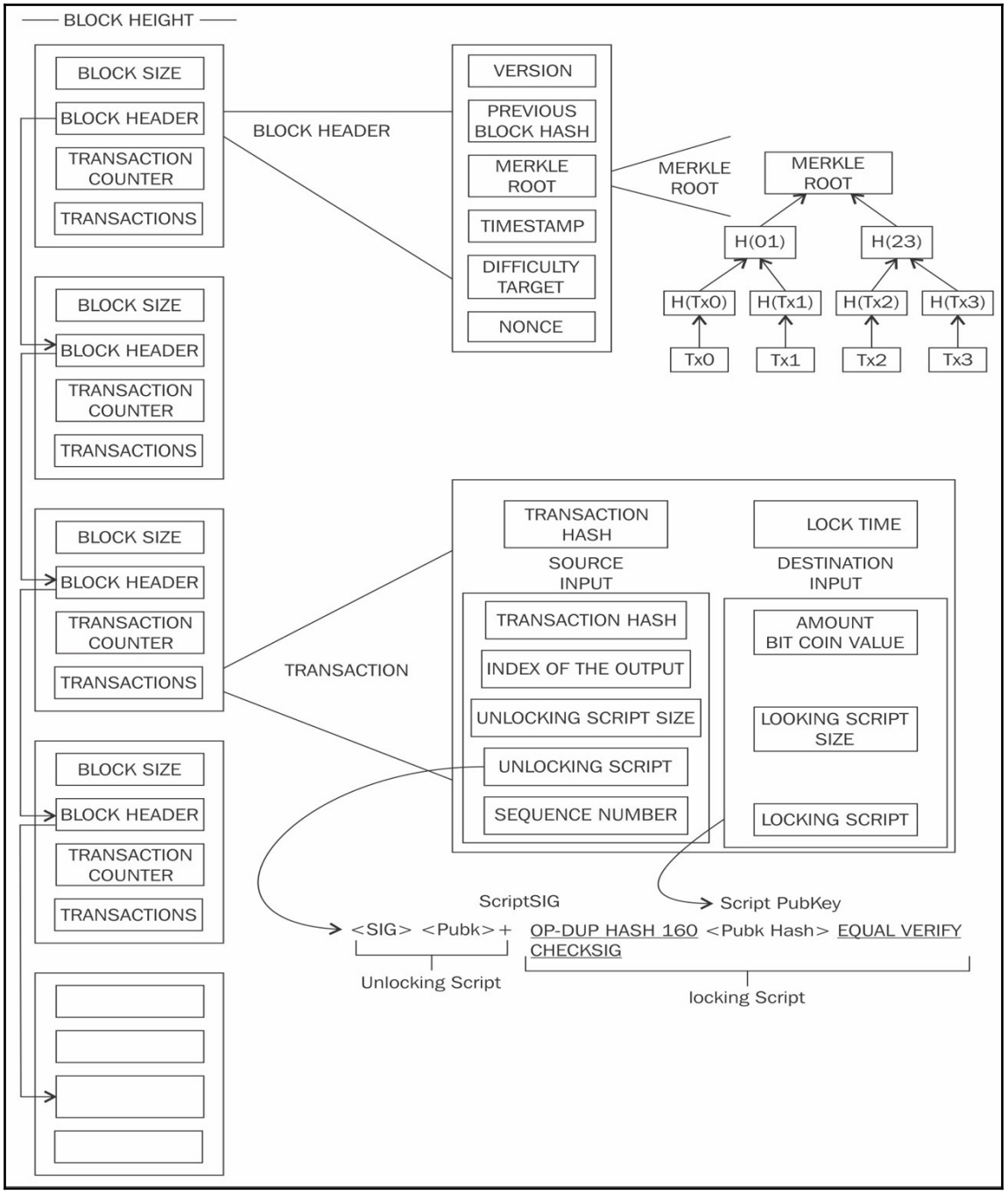

SK79LntVwAcpMCQUJ9sYkJaWDX34GN.
L2306.

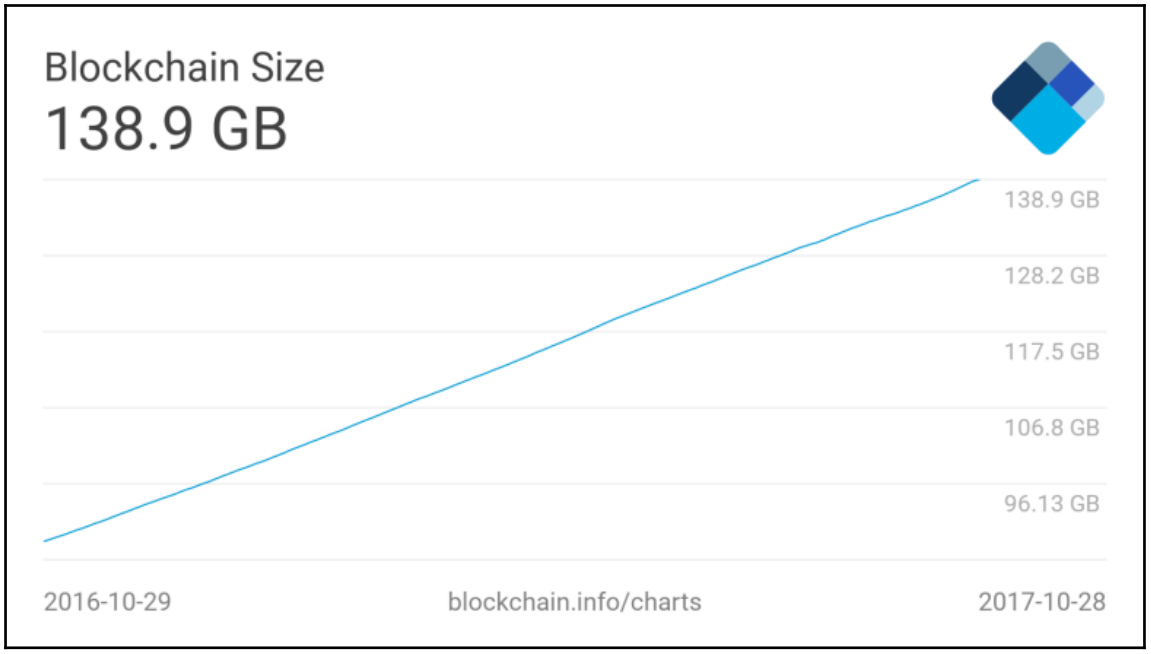

Load & Verify
Bitcoin Address
1BM3NdAUcue
bitcoin
Amount:
Private Key
Spend

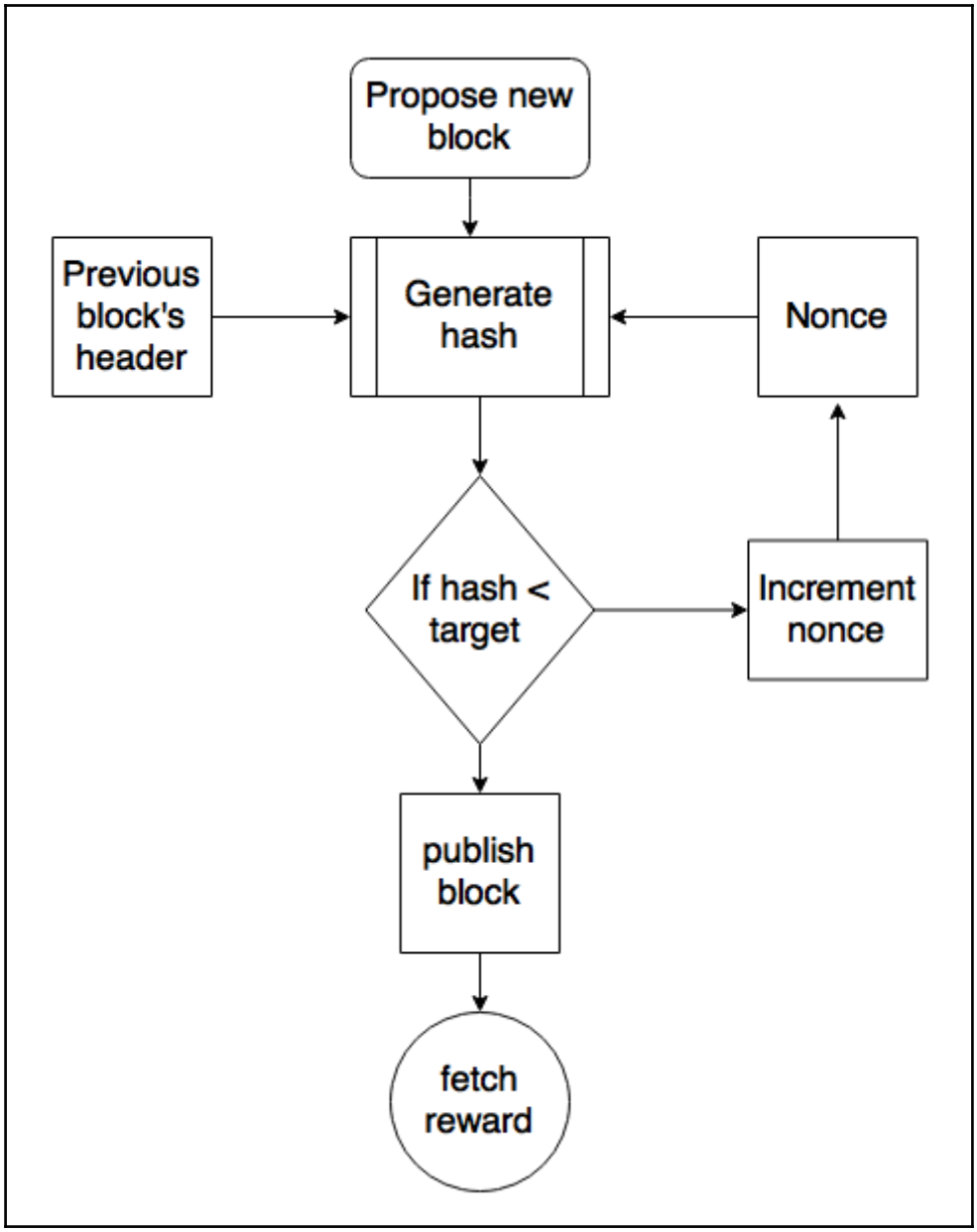

1BasHiry2VoCQCdX6X
64oxvKRuf7fW6qGr

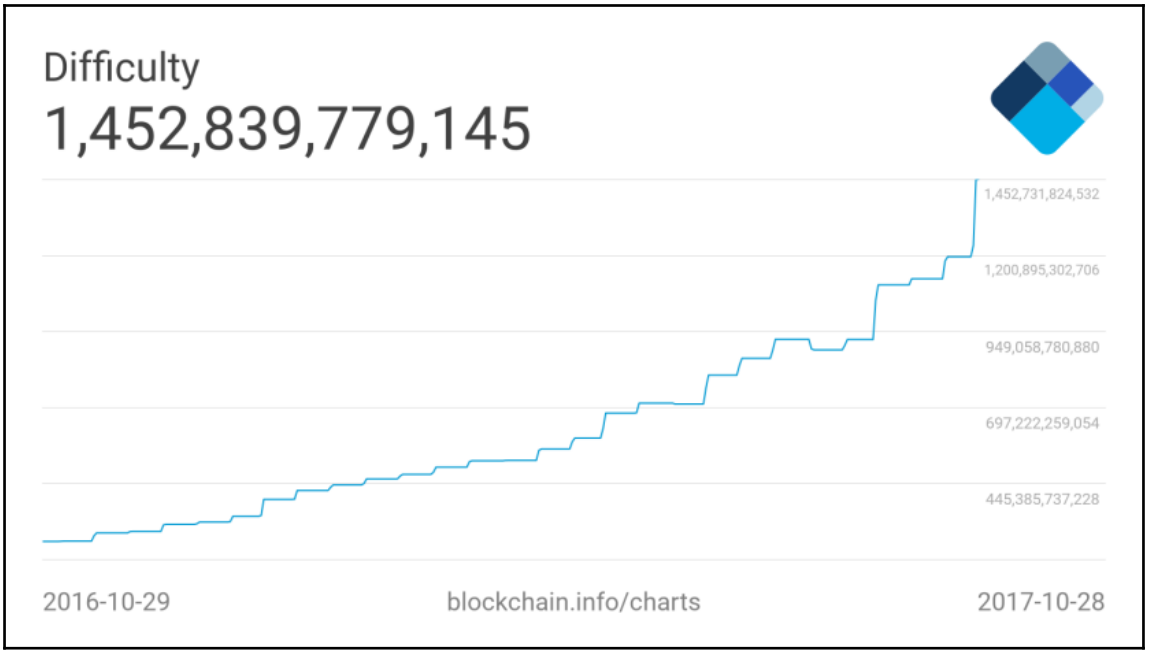

Private
Public
To deposit funds to this paper wallet, send cryptocurrency to its public address, anytime.
Verify your balance by searching for the public address using a blockain explorer such as blockchain.info.
DO NOT REVEAL THE PRIVATE KEY until you are ready to import the balance on this wallet to a cryptocurrency client, exchange or online wallet.
Amount : _____ Date : _____
Notes : _____
Public key
1BasHiry2VoCQCdX6X64oxvKRuf7fW6qGr
Private key
5KQvbs4SYGoPi3q8FVpT1VYekGwhzHHT44Z7wNNymbJdEYzc2UY

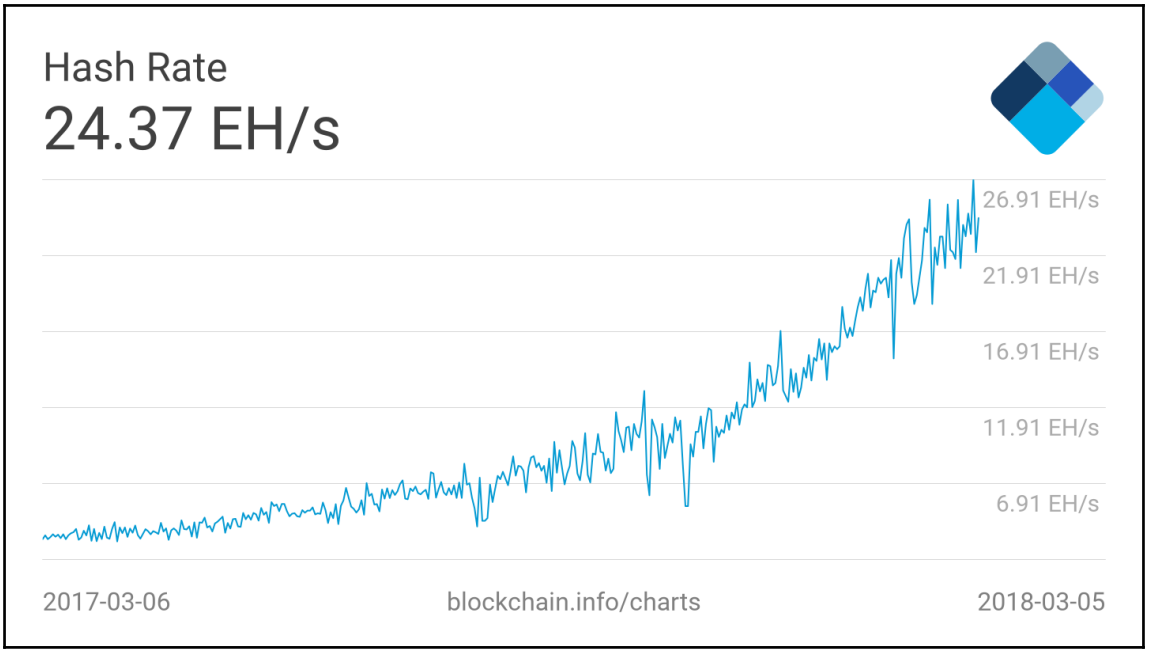

SCRIPT
<Sig><Pubk> OP_DUP OP_HASH160 <PubkHash> OP_EQUALVERIFY OP_CHECKSIG
STACK (PUSH/POP)
<Sig>
<PUBKEY>
<SIG>
Pubk
Pubk
SIG
<PubkHash>
<Pubk>
<Sig>
<Pubk Hash>
<Pubk Hash>
<Pubk>
<Sig>
<PUBK>
<SIG>
TRUE/FALSE
INSTRUCTION
<Sig>
Execution
<Pubk>
From Left
<OP_DUP>
to right
<OP_HASH160>
<Pubk Hash>
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

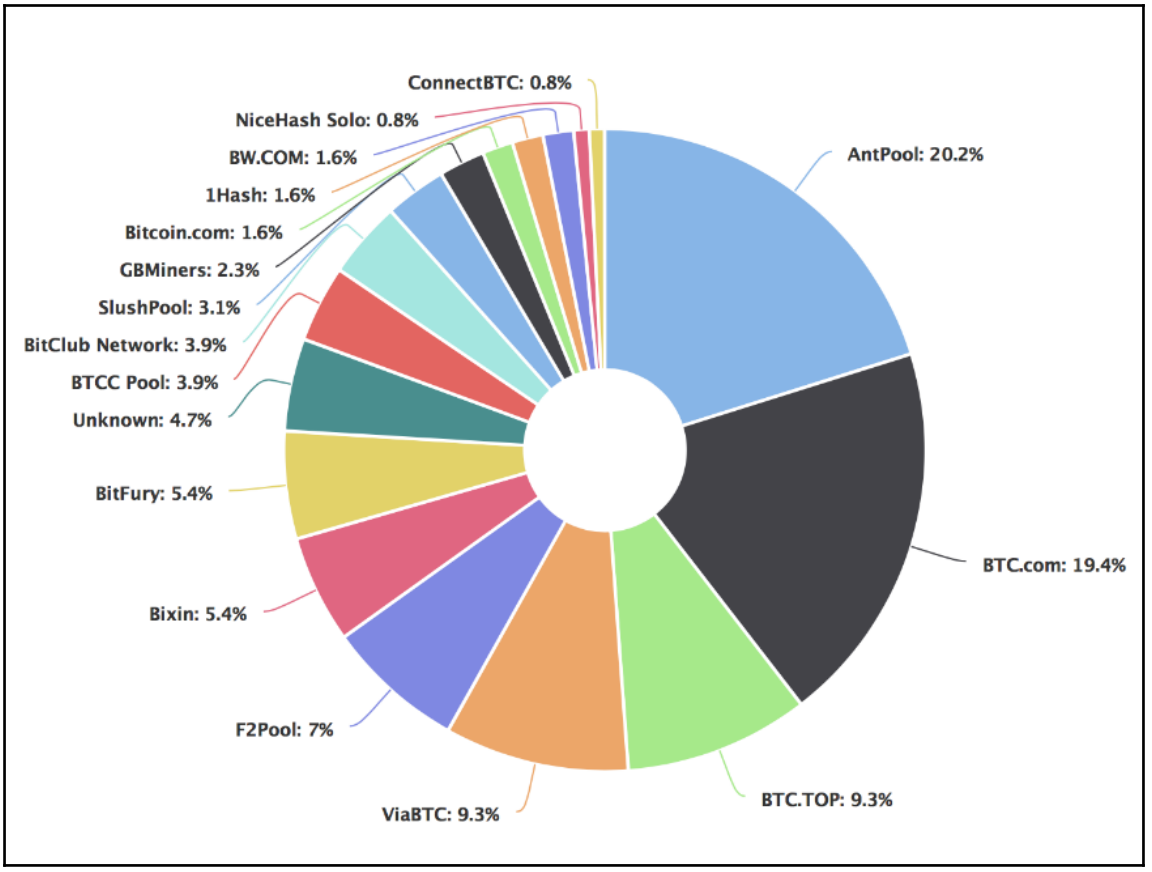

BLOCK HEIGHT
BLOCK SIZE
BLOCK HEADER
TRANSACTION COUNTER
TRANSACTIONS
BLOCK HEADER
VERSION
PREVIOUS BLOCK HASH
MERKLE ROOT
TIMESTAMP
DIFFICULTY TARGET
NONCE
MERKLE ROOT
MERKLE ROOT
H(01)
H(23)
H(Tx0)
H(Tx1)
H(Tx2)
H(Tx3)
Tx0
Tx1
Tx2
Tx3
TRANSACTION
TRANSACTION HASH
LOCK TIME
SOURCE INPUT
DESTINATION 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
138.9 GB
138.9 GB
128.2 GB
117.5 GB
106.8 GB
96.13 GB
2016-10-29
blockchain.info/charts
2017-10-28

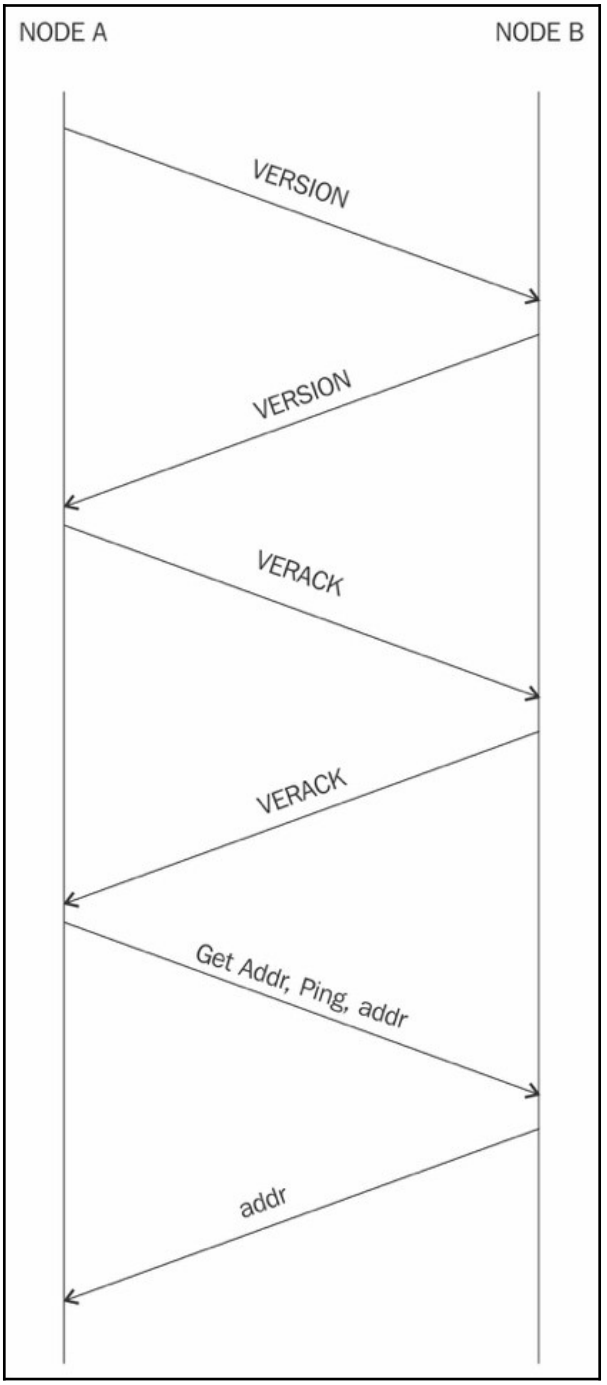

Propose new block
Previous block's header
Generate hash
Nonce
If hash < target
Increment nonce
publish block
fetch reward

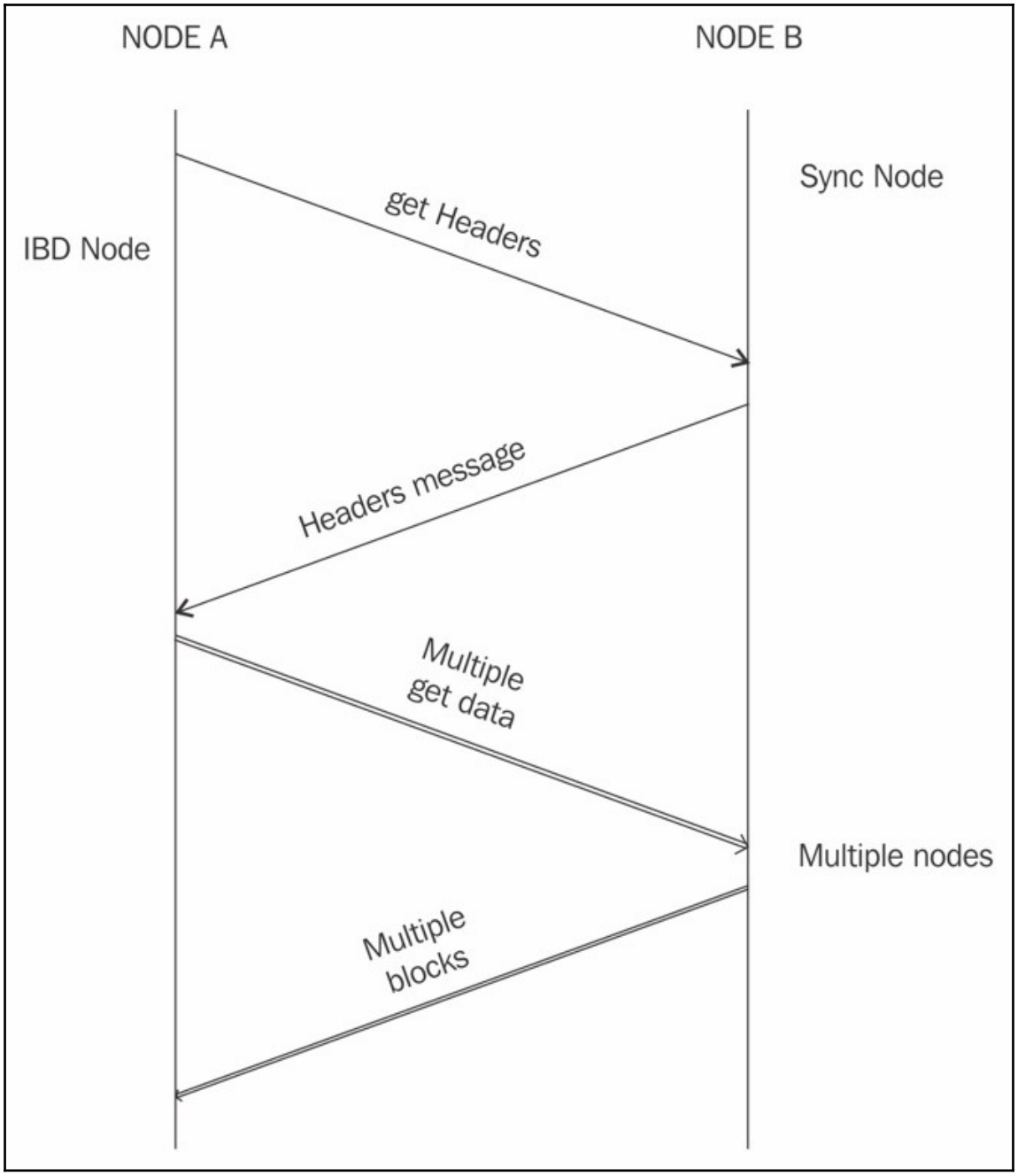

Difficulty
1,452,839,779,145
1,452,731,824,532
1,200,895,302,706
949,058,780,880
697,222,259,054
445,385,737,228
2016-10-29
blockchain.info/charts
2017-10-28

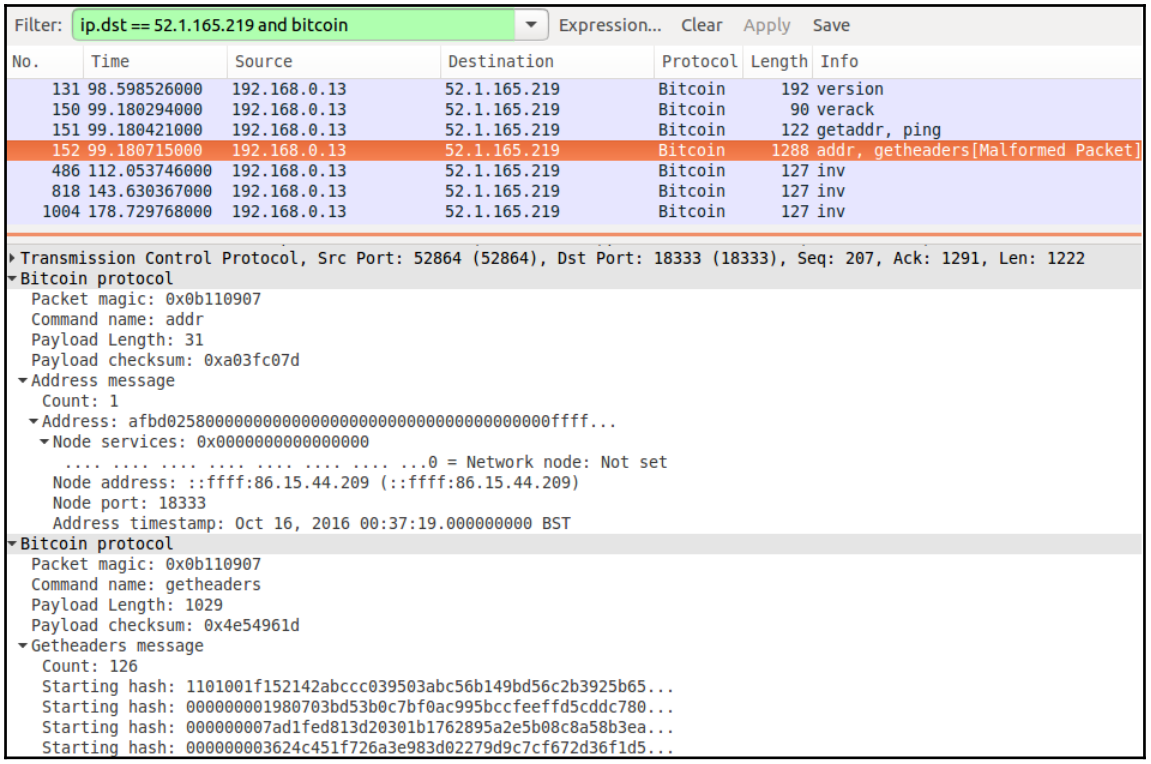

Hash Rate
24.37 EH/s
26.91 EH/s
21.91 EH/s
16.91 EH/s
11.91 EH/s
6.91 EH/s
2017-03-06
blockchain.info/charts
2018-03-05


ConnectBTC: 0.8%
NiceHash Solo: 0.8%
BW.COM: 1.6%
1Hash: 1.6%
Bitcoin.com: 1.6%
GBMiners: 2.3%
SlushPool: 3.1%
BitClub Network: 3.9%
BTCC Pool: 3.9%
Unknown: 4.7%
BitFury: 5.4%
Bixin: 5.4%
F2Pool: 7%
ViaBTC: 9.3%
BTC.TOP: 9.3%
BTC.com: 19.4%
AntPool: 20.2%

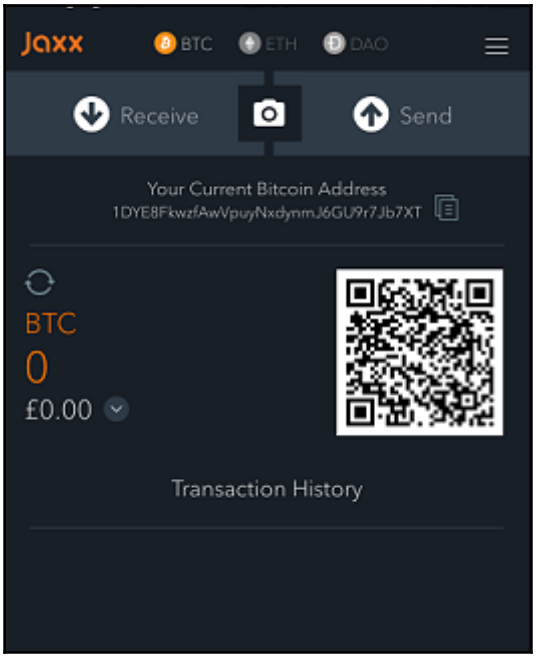
Network	Magic value	Hex
main	0xD9B4BEF9	F9 BE B4 D9
testnet3	0x0709110B	0B 11 09 07


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

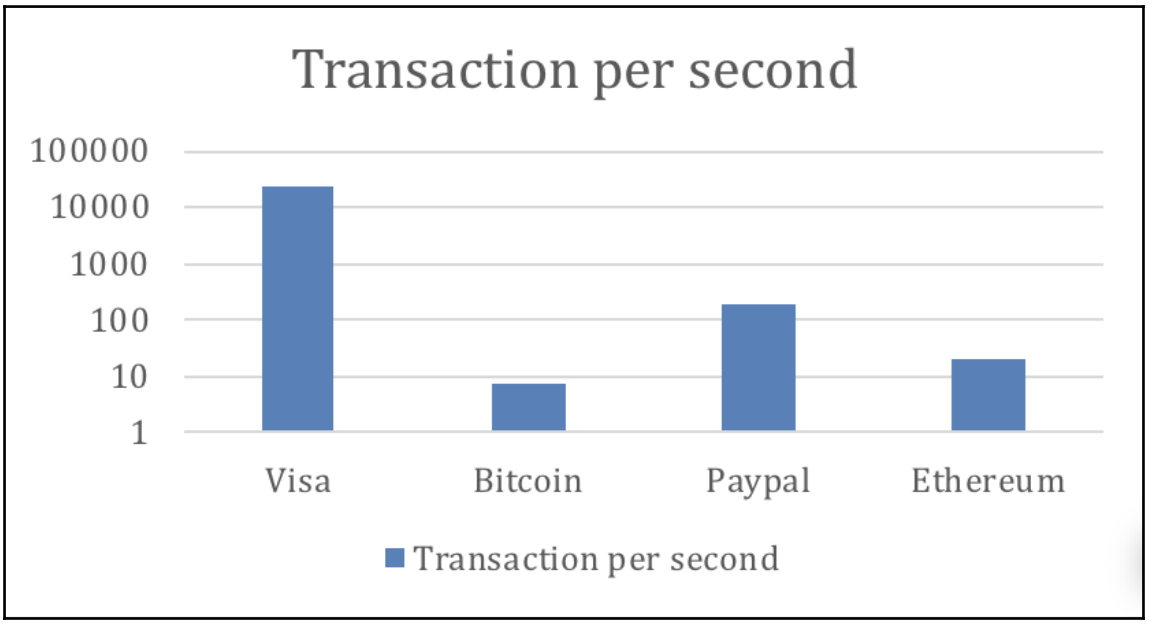

NODE A
NODE B
IBD Node
Sync Node
get Headers
Headers message
Multiple
get data
Multiple nodes
Multiple
blocks

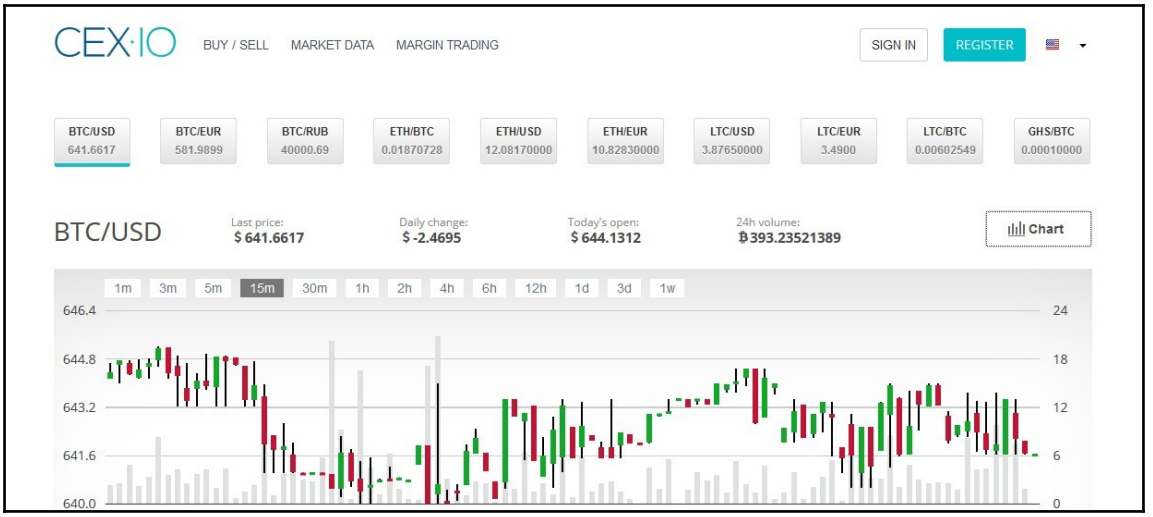

Filter: ip.dst == 52.1.165.219 and bitcoin
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
131 98.598526000 192.168.0.13 52.1.165.219 Bitcoin 192 version
150 99.180294000 192.168.0.13 52.1.165.219 Bitcoin 90 verack
151 99.180421000 192.168.0.13 52.1.165.219 Bitcoin 122 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: afbd025800000000000000000000000000000000000000000ffff...
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


Jaxx
BTC
ETH
DAO
Receive
Send
Your Current Bitcoin Address
1DYE8FkwzfAwVpuyNxdynmJ6GU9r7Jb7XT
BTC
0
£0.00
Transaction History


bitcoin
ACCEPTED HERE


Transaction per second
100000
10000
1000
100
10
1
Visa
Bitcoin
Paypal
Ethereum
Transaction per second



Sell Orders

Total BTC available: 656.41831367

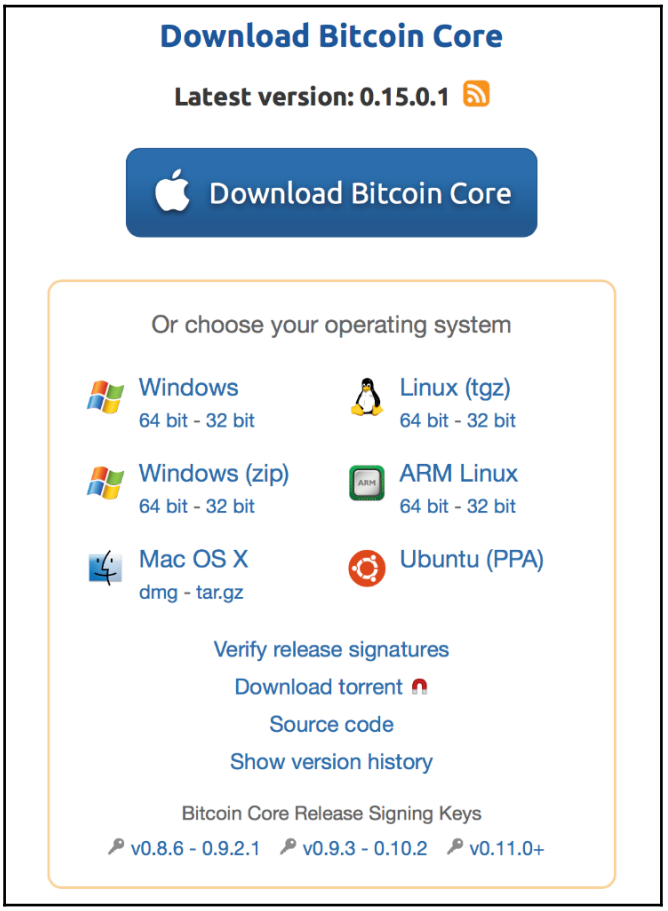
Price per BTC	BTC Amount	Total: (USD)
642.4085	Ƀ0.20450000	$ 131.38
642.4915	Ƀ0.20910000	$ 134.35
643.4470	Ƀ0.05000000	$ 32.18
643.4900	Ƀ0.11944972	$ 76.87
643.5000	Ƀ1.85748652	$ 1195.30
643.6500	Ƀ3.00000000	$ 1930.95
643.6999	Ƀ0.13844181	$ 89.12
643.7000	Ƀ45.80000000	$ 29481.46
643.7487	Ƀ1.22995538	$ 791.79

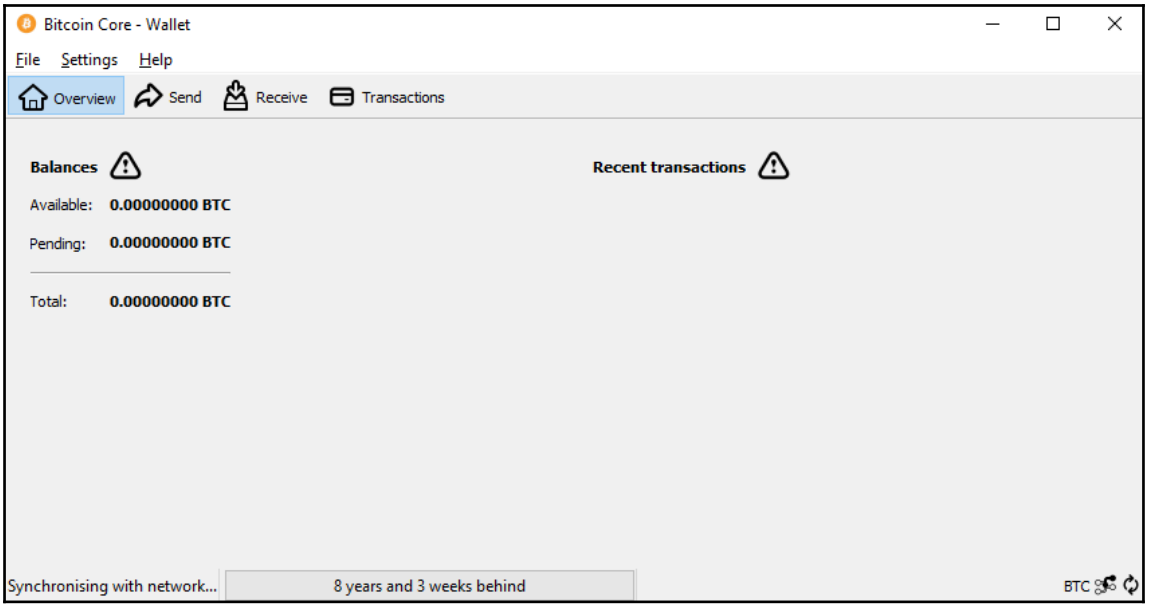
Buy Orders

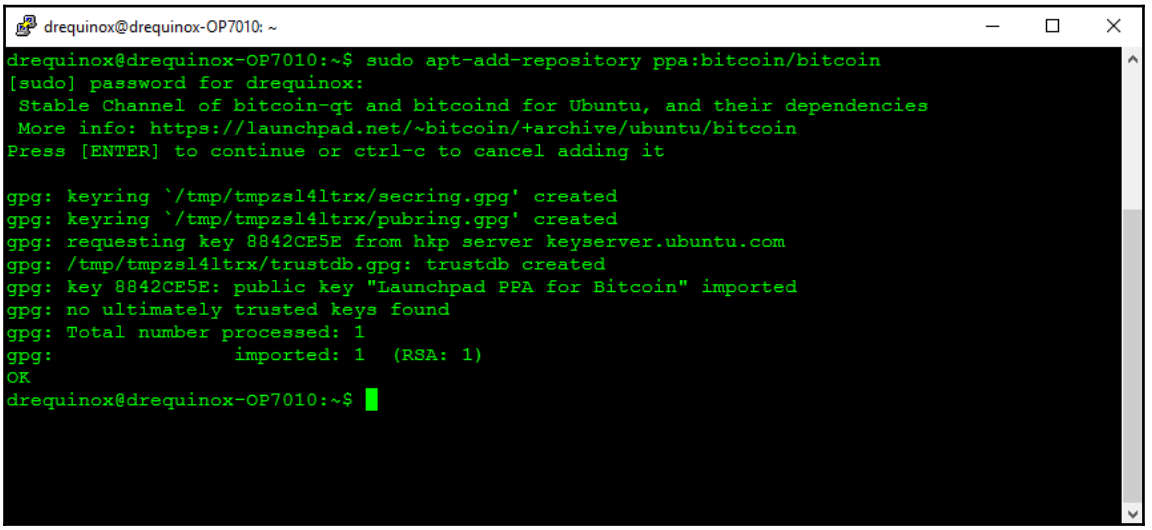
Total USD available: 380739.41

Price per BTC	BTC Amount	Total: (USD)
641.6210	Ƀ0.01390000	$ 8.92
641.6201	Ƀ0.23162780	$ 148.62
641.6200	Ƀ0.12050000	$ 77.32
641.6117	Ƀ1.83477084	$ 1177.22
641.5584	Ƀ0.30000000	$ 192.47
641.5217	Ƀ0.18180000	$ 116.63
641.0217	Ƀ0.10000000	$ 64.11
640.5300	Ƀ0.67323160	$ 431.23
640.5000	Ƀ0.40815400	$ 261.43

Chapter 7: Bitcoin Clients and APIs




Bitcoin Core - Wallet
File Settings Help
Overview Send Receive Transactions
Balances
Available: 0.00000000 BTC
Pending: 0.00000000 BTC
Total: 0.00000000 BTC
Recent transactions
Synchronising with network...
8 years and 3 weeks behind
BTC

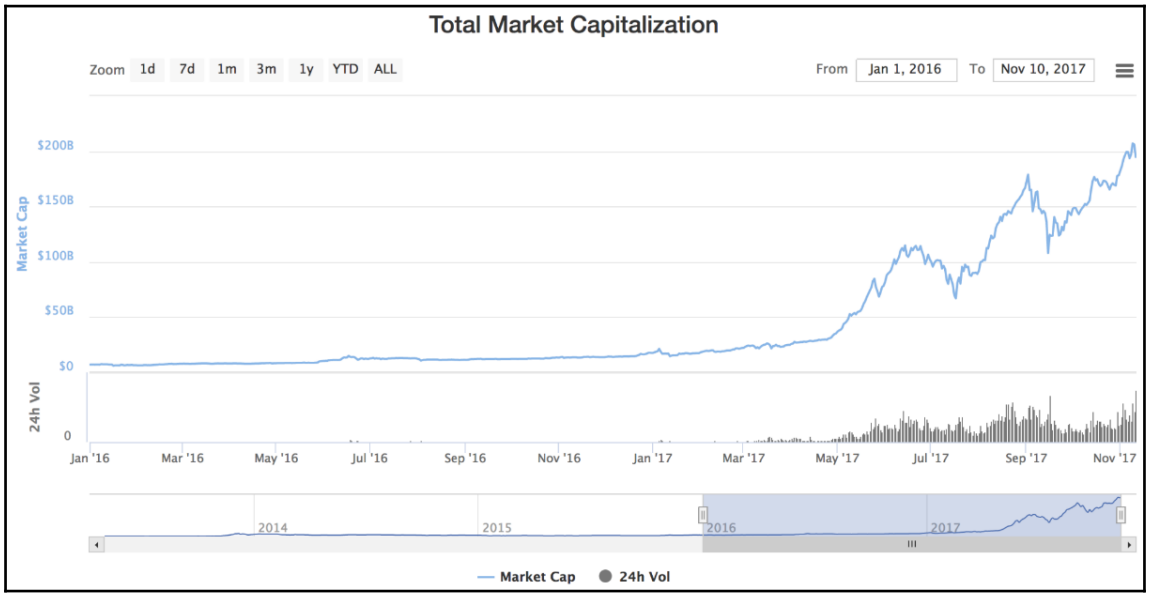

drequinox@drequinox-OP7010: ~
drequinox@drequinox-OP7010:~$ sudo apt-add-repository ppa:bitcoin/bitcoin
[sudo] password for drequinox:
Stable Channel of bitcoin-qt and bitcoind for Ubuntu, and their dependencies
More info: https://launchpad.net/~bitcoin/+archive/ubuntu/bitcoin
Press [ENTER] to continue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

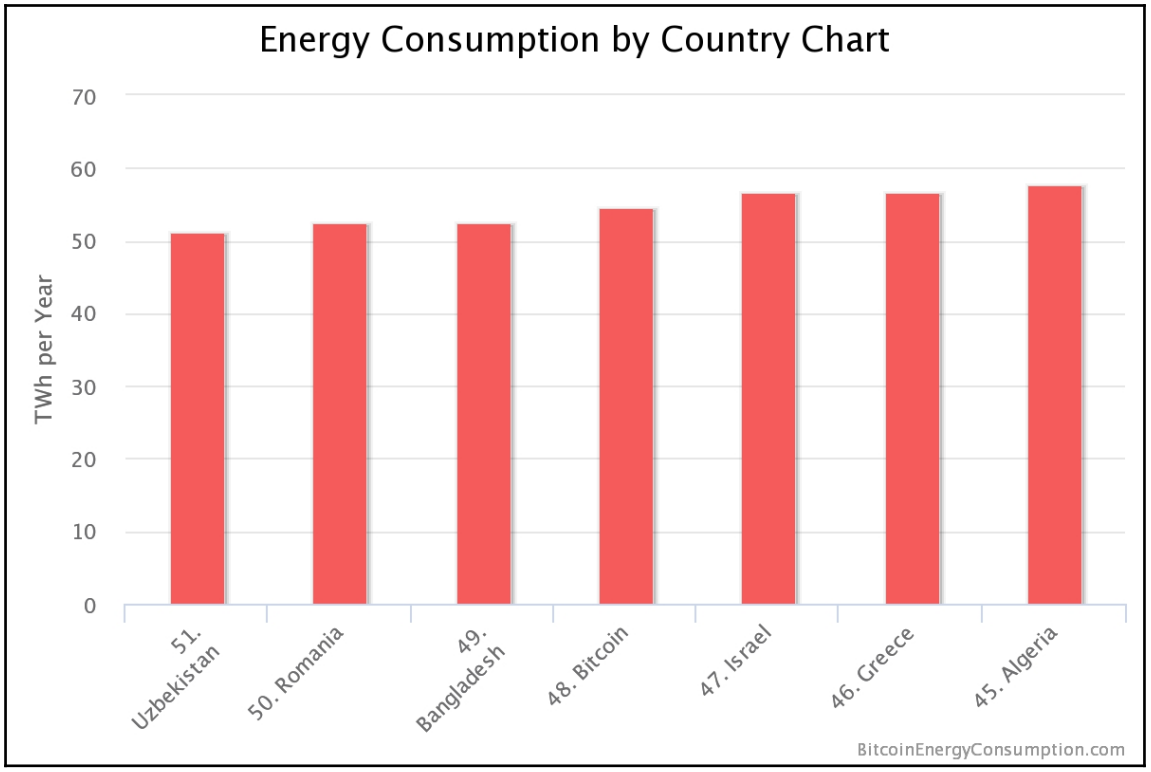
```
drequinox@drequinox-OP7010:~/.bitcoin/regtest$ tail -f debug.log
2016-10-16 15:43:55 AddToWallet d461e1fb162dd6958139a2ab5e4f9993ffbd51b1a4e3a80e5b77e472cd90dd6a  new
2016-10-16 15:43:55 CreateNewBlock(): total size 1000 txs: 0 fees: 0 sigops 400
2016-10-16 15:43:55 UpdateTip: new best=37c1f40299a3724dd2edf63d26925cb580b8c5f27405289ef9204e53fe4e1b87 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
```

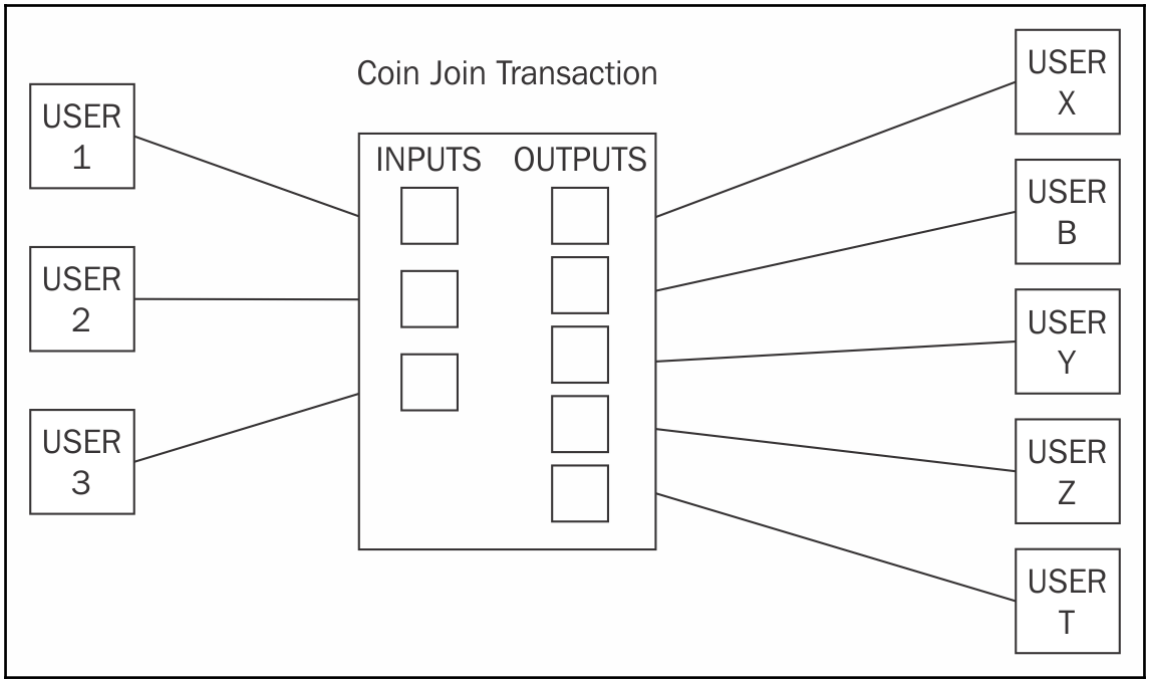
```
drequinox@drequinox-OP7010:~$ bitcoin-cli getinfo
{
  "version": 130000,
  "protocolversion": 70014,
  "walletversion": 130000,
  "balance": 0.00000000,
  "blocks": 433948,
  "timeoffset": 0,
  "connections": 8,
  "proxy": "",
  "difficulty": 258522748404.5154,
  "testnet": false,
  "keypoololdest":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

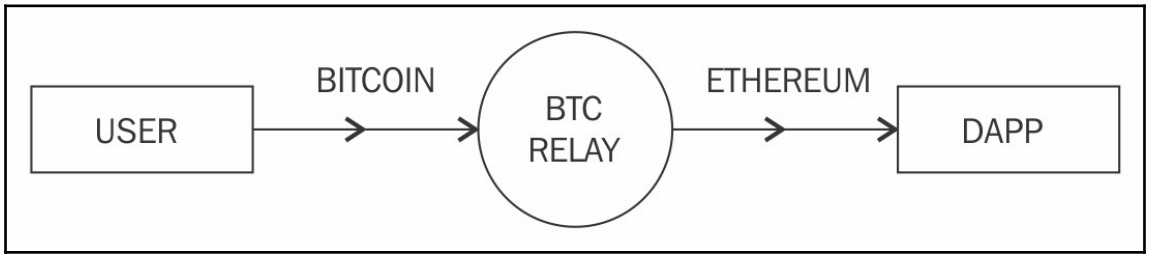
```
drequinox@drequinox-OP7010:~$ bitcoin-cli -testnet help | more
== Blockchain ==
getbestblockhash
getblock "hash" ( verbose )
getblockchaininfo
getblockcount
getblockhash index
getblockheader "hash" ( verbose )
getchaintips
getdifficulty
getmempoolancestors txid (verbose)
getmempooldescendants txid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

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

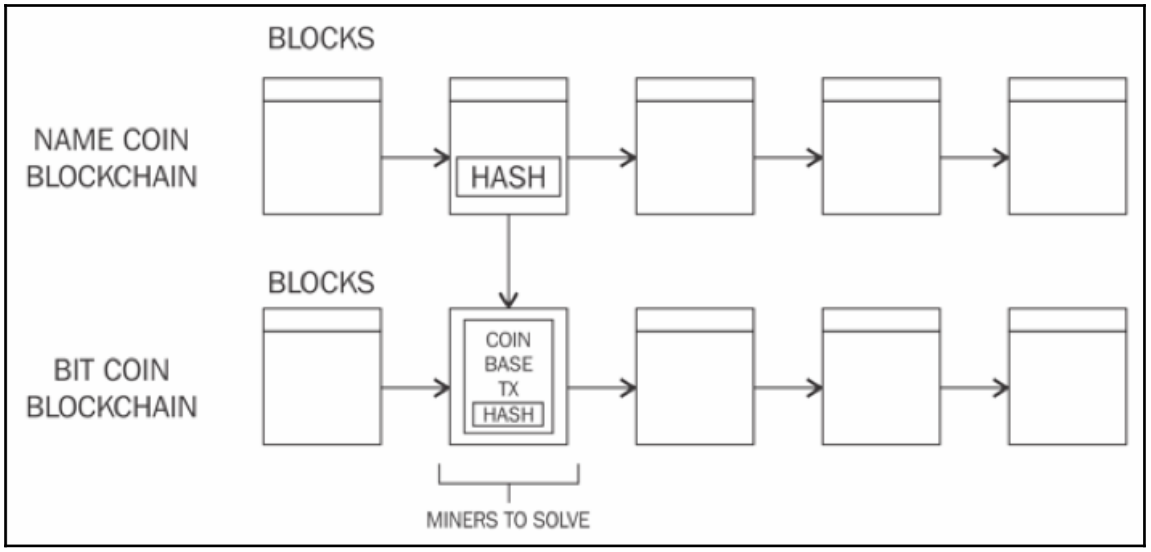
Chapter 8: Alternative Coins



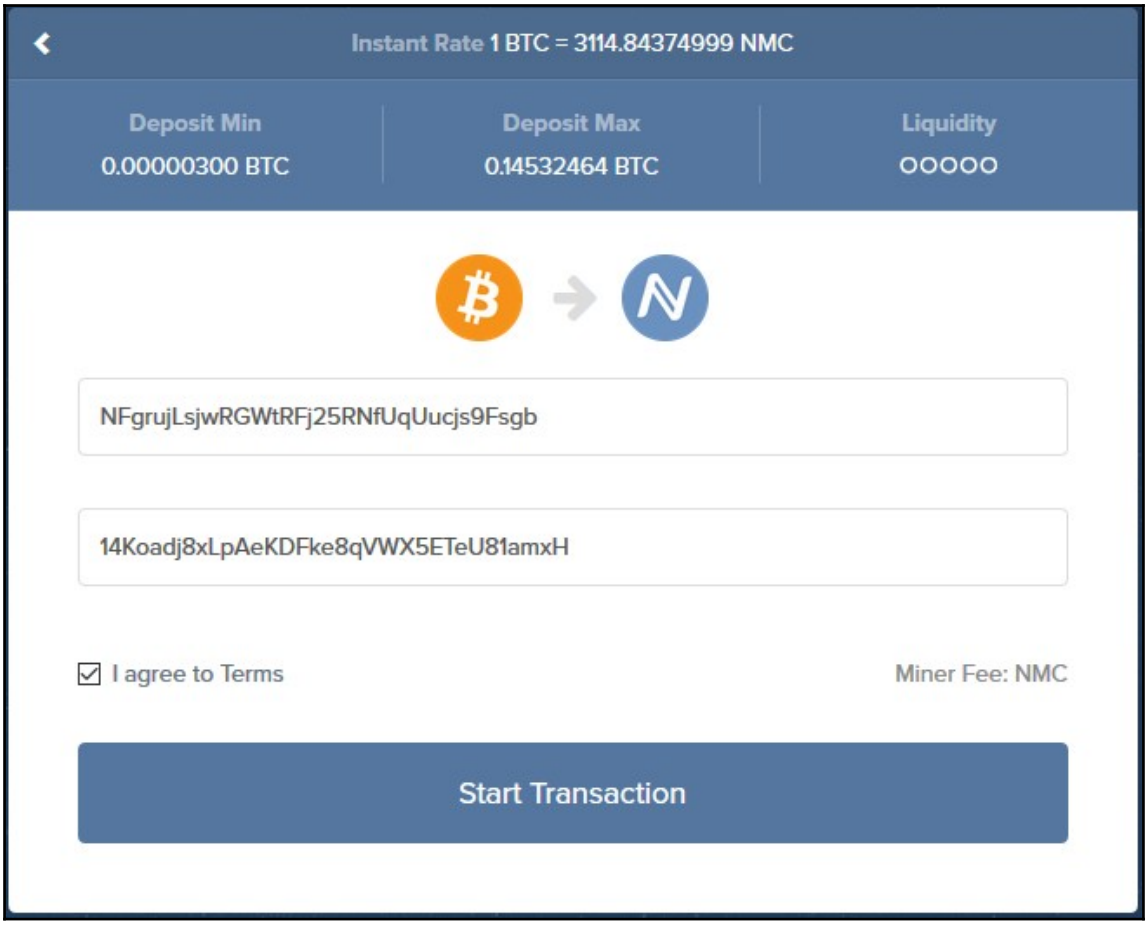

Energy Consumption by Country Chart
TWh per Year
70
60
50
40
30
20
10
0
51. Uzbekistan
50. Romania
49. Bangladesh
48. Bitcoin
47. Israel
46. Greece
45. Algeria
BitcoinEnergyConsumption.com

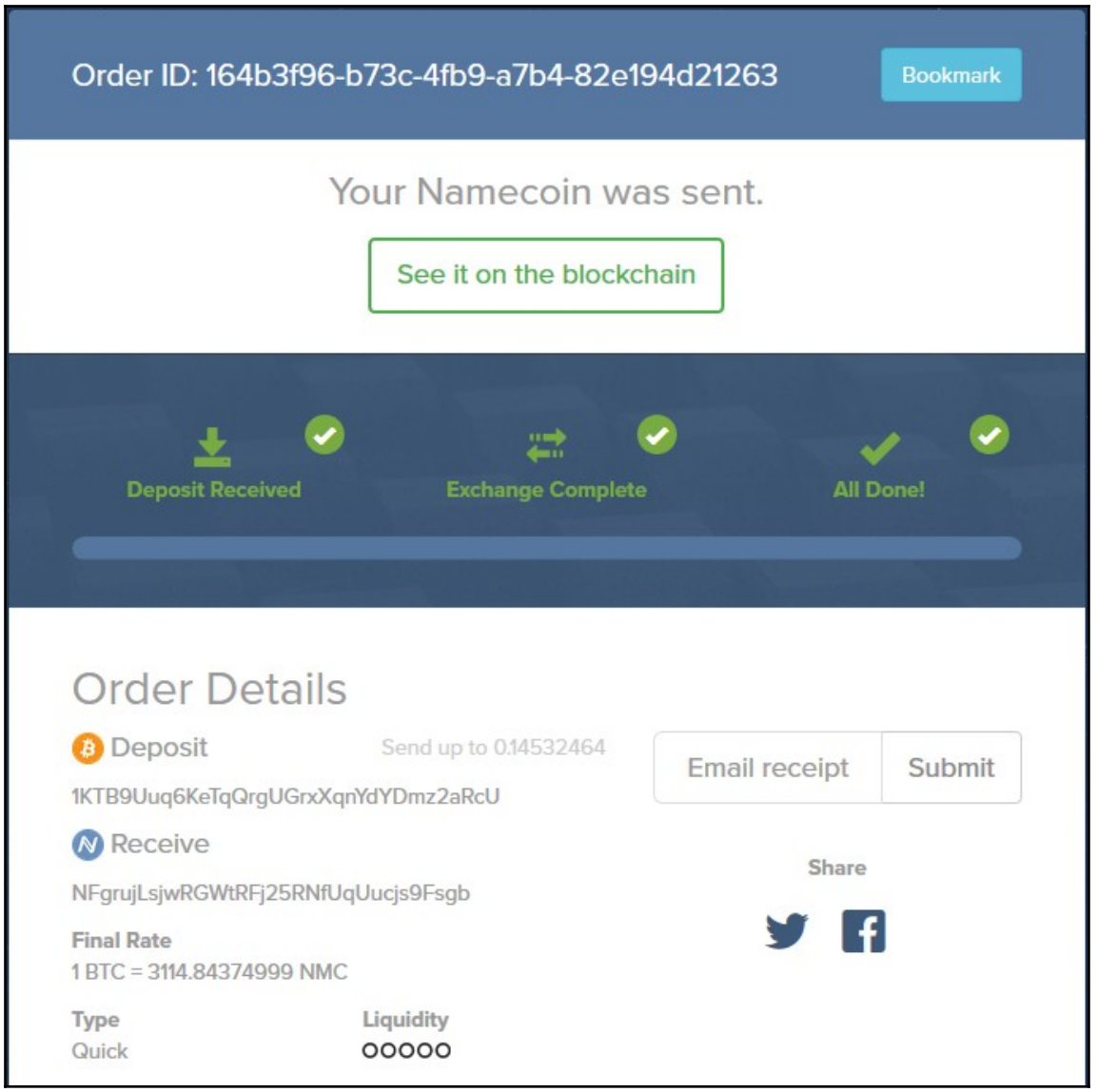

Coin Join Transaction
USER 1
USER 2
USER 3
INPUTS
OUTPUTS
USER X
USER B
USER Y
USER Z
USER T

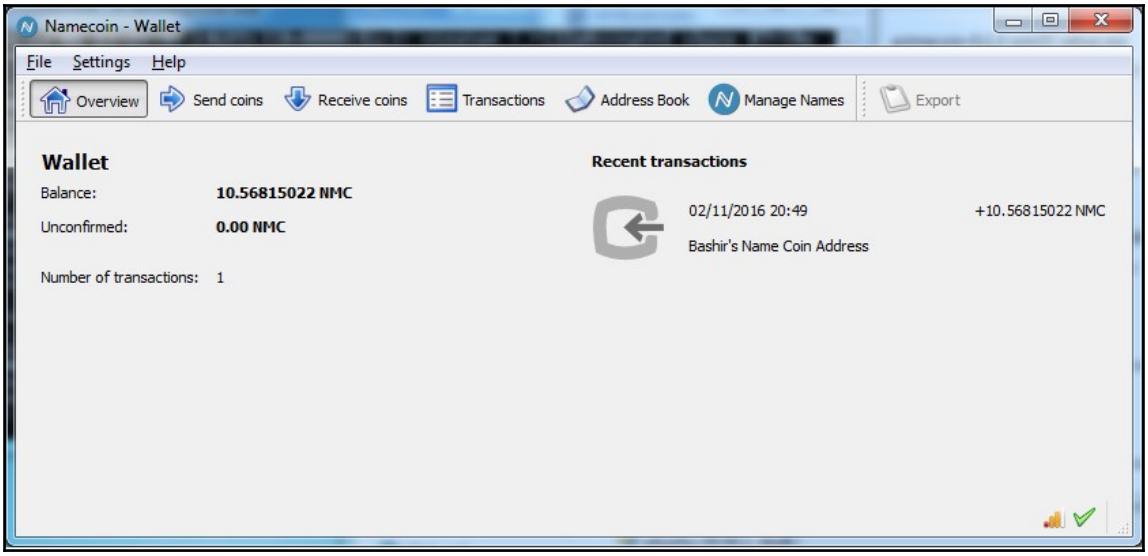

USER
BITCOIN
BTC RELAY
ETHEREUM
DAPP

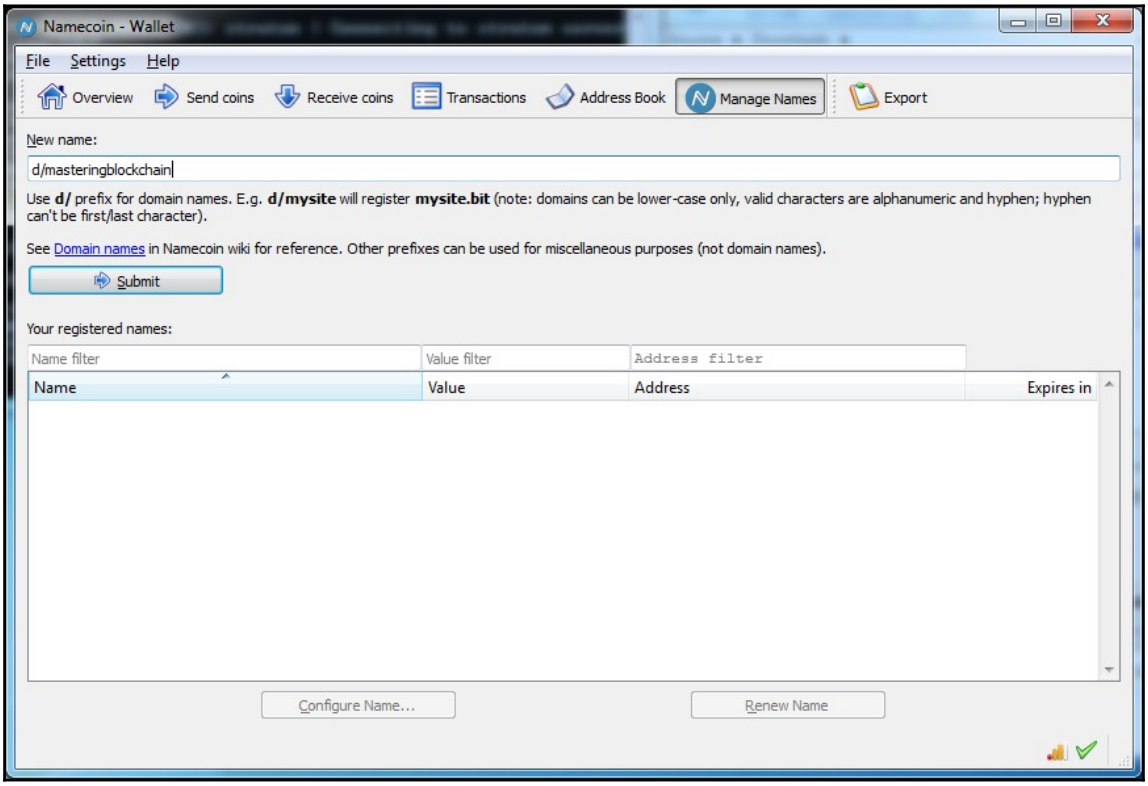

BLOCKS
NAME COIN BLOCKCHAIN
HASH
BLOCKS
BIT COIN BLOCKCHAIN
COIN BASE TX
HASH
MINERS TO SOLVE

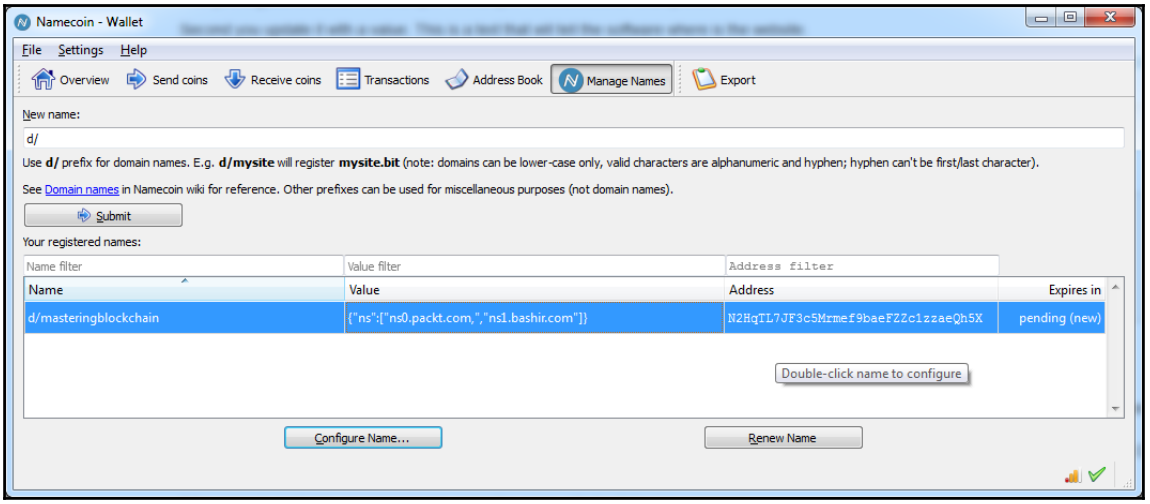

Namecoin - Difficulty
Difficulty
1.2T
1T
800G
600G
400G
200G
Dec 2016
Jan 2017
Feb 2017
Mar 2017
Apr 2017
May 2017
Jun 2017
Jul 2017
Aug 2017
Sep 2017
Oct 2017
Nov 2017

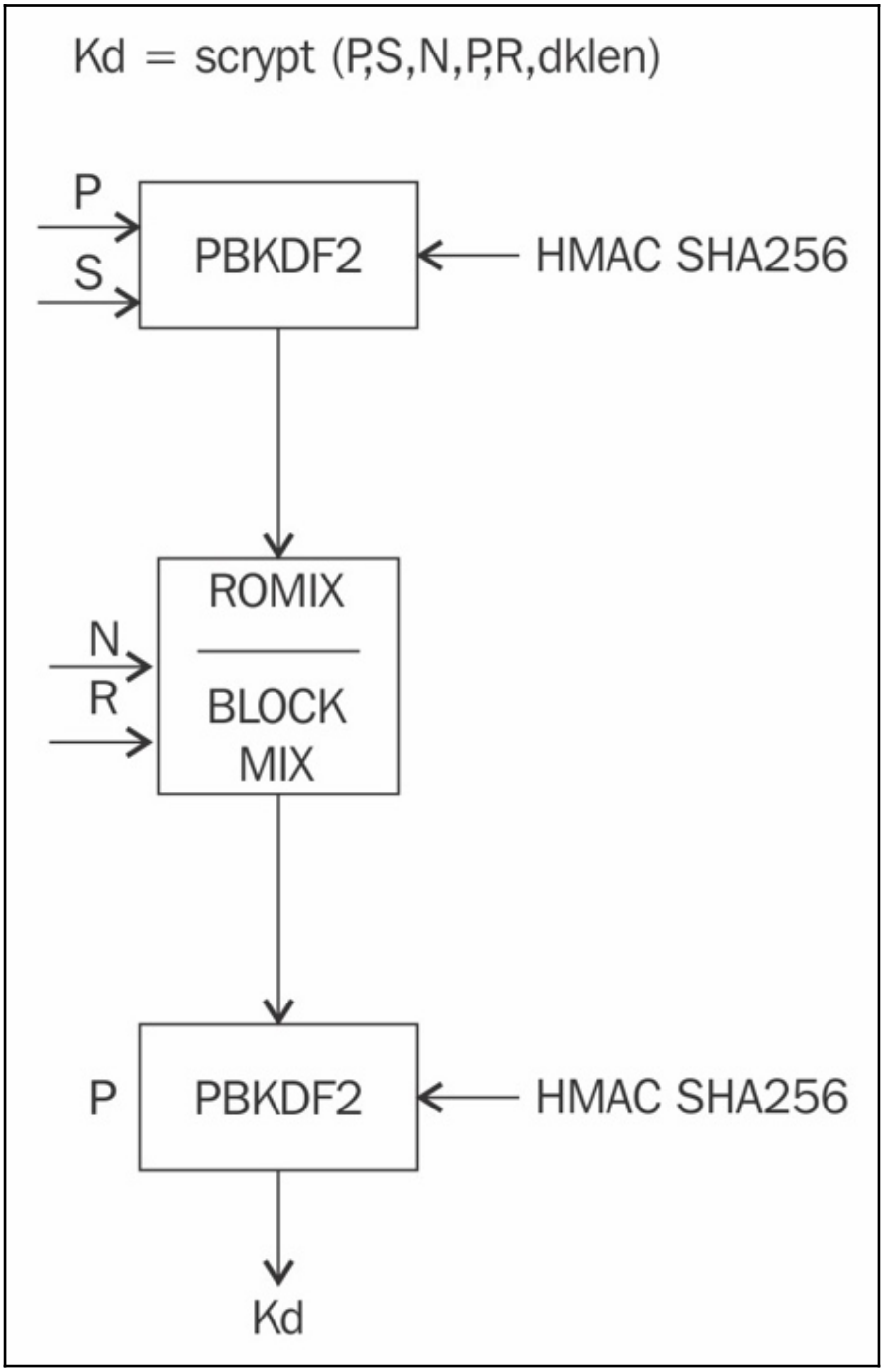

Instant Rate 1 BTC = 3114.84374999 NMC
Deposit Min
0.00000300 BTC
Deposit Max
0.14532464 BTC
Liquidity
OOOOO
NFgrujLsjwRGWtRFj25RNfUqUucjs9Fsgb
14Koadj8xLpAeKDFke8qVWX5ETeU81amxH
I agree to Terms
Miner Fee: NMC
Start Transaction

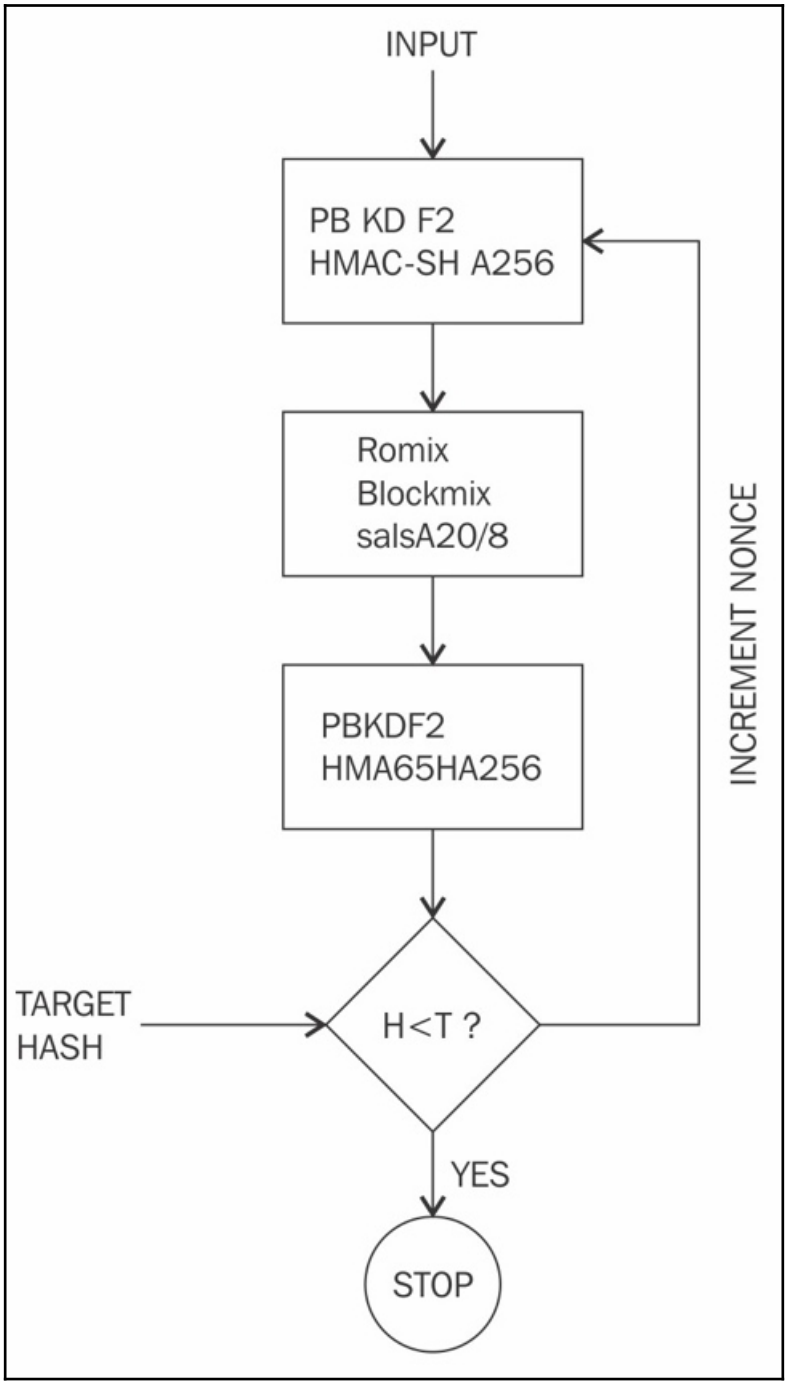

Order ID: 164b3f96-b73c-4fb9-a7b4-82e194d21263
Bookmark
Your Namecoin was sent.
See it on the blockchain
Deposit Received
Exchange Complete
All Done!
Order Details
Deposit
Send up to 0.14532464
1KTB9Uuq6KeTqQrgUGrxXqnYdYDmz2aRcU
Email receipt
Submit
Receive
NFgrujLsjwRGWtRFj25RNfUqUucjs9Fsgb
Share
Final Rate
1 BTC = 3114.84374999 NMC
Type
Quick
Liquidity
OOOOO

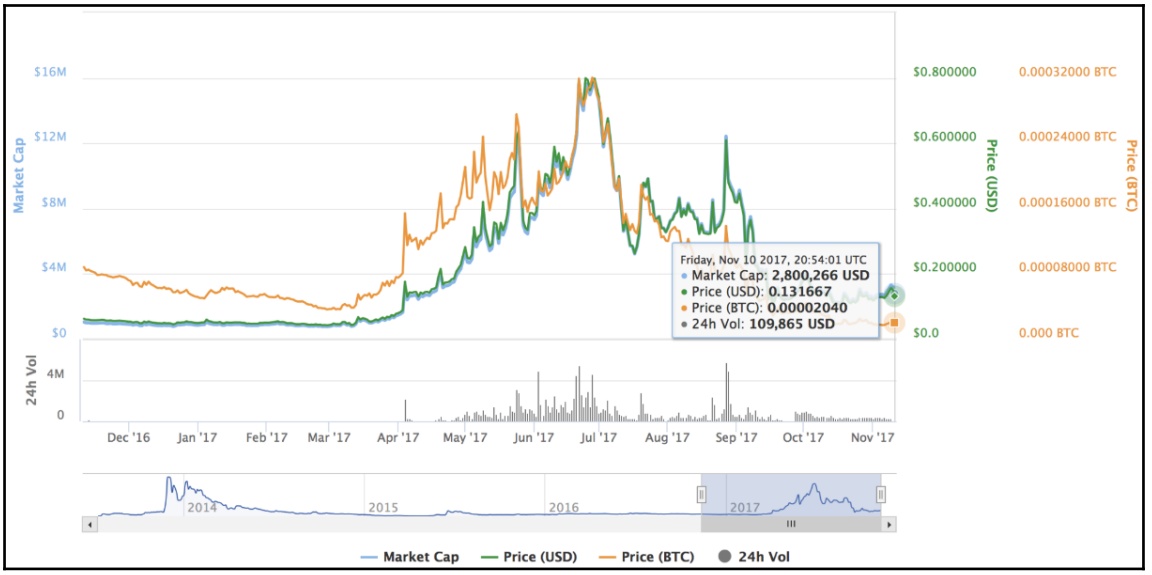

Namecoin - Wallet
File Settings Help
Overview
Send coins
Receive coins
Transactions
Address Book
Manage Names
Export
Wallet
Balance: 10.56815022 NMC
Unconfirmed: 0.00 NMC
Number of transactions: 1
Recent transactions
02/11/2016 20:49
+10.56815022 NMC
Bashir's Name Coin Address

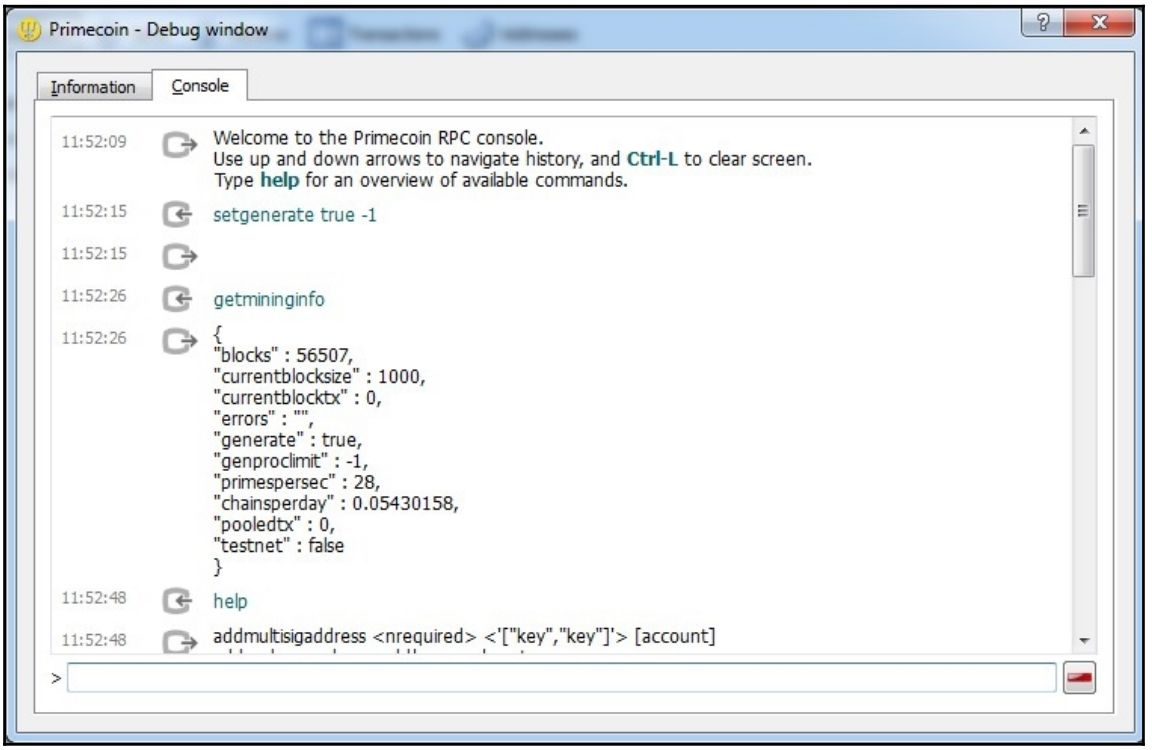

Namecoin - Wallet
File Settings Help
Overview
Send coins
Receive coins
Transactions
Address Book
Manage Names
Export
New name:
d/masteringblockchain
Use d/ prefix for domain names. E.g. d/mysite will register mysite.bit (note: domains can be lower-case only, valid characters are alphanumeric and hyphen; 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).
Submit
Your registered names:
Name filter
Value filter
Address filter
Name
Value
Address
Expires in
Configure Name...
Renew Name

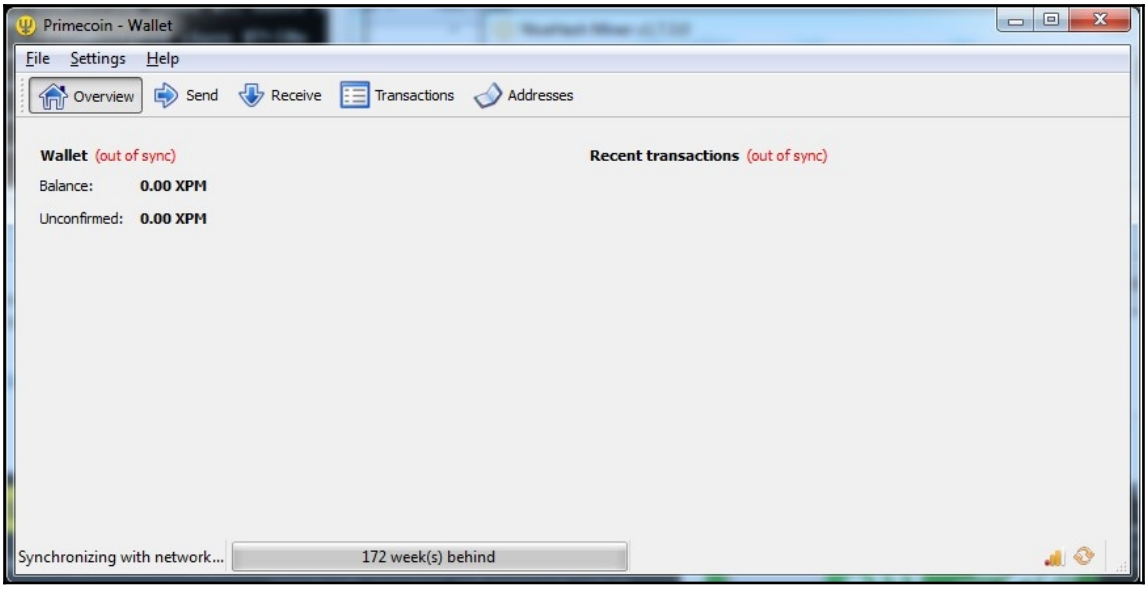

Namecoin - Wallet
File Settings Help
Overview
Send coins
Receive coins
Transactions
Address Book
Manage Names
Export
New name:
d/
Use d/ prefix for domain names. E.g. d/mysite will register mysite.bit (note: domains can be lower-case only, valid characters are alphanumeric and hyphen; hyphen can't be first/last character).
See Domain names in Namecoin wiki for reference. Other prefixes can be used for miscellaneous purposes (not domain names).
Submit
Your registered names:
Name filter
Value filter
Address filter
Name
Value
Address
Expires in
d/masteringblockchain
{"ns":["ns0.packt.com","ns1.bashir.com"]}
N2HqIL7JF3c5Mrmef9baeFZZc1zzaeQh5X
pending (new)
Double-click name to configure
Configure Name...
Renew Name


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

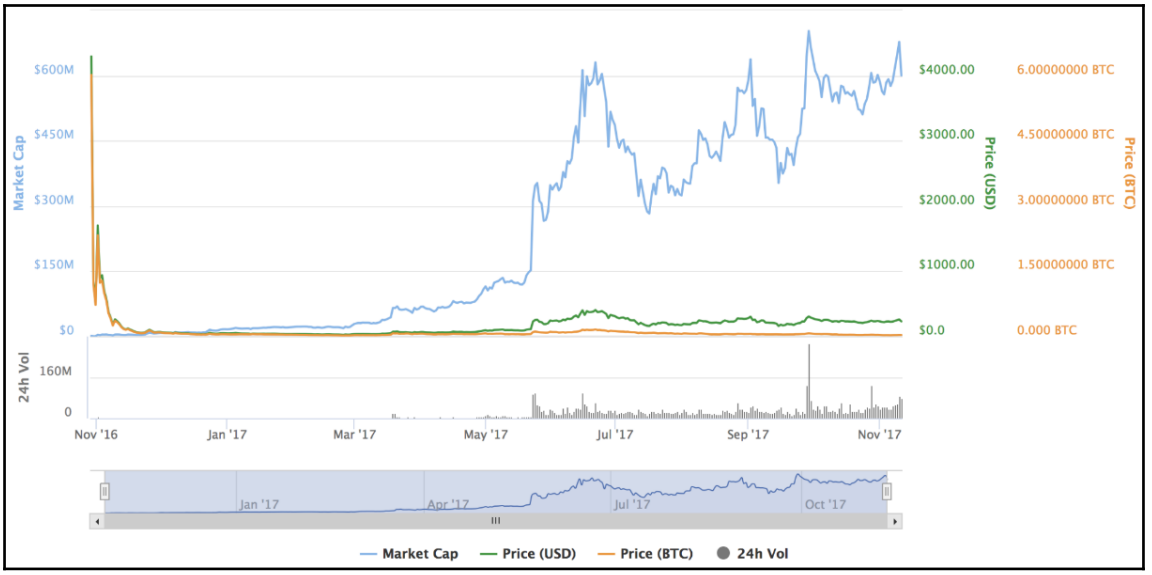

INPUT
PB KD F2
HMAC-SH A256
Romix
Blockmix
salsA20/8
PBKDF2
HMA65HA256
INCREMENT NONCE
TARGET
HASH
H<T ?
YES
STOP


$16M
$12M
$8M
$4M
$0
Market Cap
$0.800000
$0.600000
$0.400000
$0.200000
$0.0
Price (USD)
0.00032000 BTC
0.00024000 BTC
0.00016000 BTC
0.00008000 BTC
0.000 BTC
Price (BTC)
Friday, Nov 10 2017, 20:54:01 UTC
Market Cap: 2,800,266 USD
Price (USD): 0.131667
Price (BTC): 0.00002040
24h Vol: 109,865 USD
24h Vol
4M
0
Dec '16
Jan '17
Feb '17
Mar '17
Apr '17
May '17
Jun '17
Jul '17
Aug '17
Sep '17
Oct '17
Nov '17
2014
2015
2016
2017
Market Cap
Price (USD)
Price (BTC)
24h Vol


Primecoin - Debug window
Information
Console
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
File Settings Help
Overview Send Receive Transactions Addresses
Wallet (out of sync)
Balance: 0.00 XPM
Unconfirmed: 0.00 XPM
Recent transactions (out of sync)
Synchronizing with network...
172 week(s) behind

Attribute	Value
Name	Zcash
Launch date	28/10/16
Main purpose	Currency
Currency Code	ZEC
Maximum coins	21 million
Block time	10 minutes
Consensus facilitation algorithm	Proof of Work (equihash)
Difficulty adjustment algorithm	DigiShield V3 (modified)
Mining hardware	CPU, GPU
Difficulty adjustment period	1 block




```
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
```

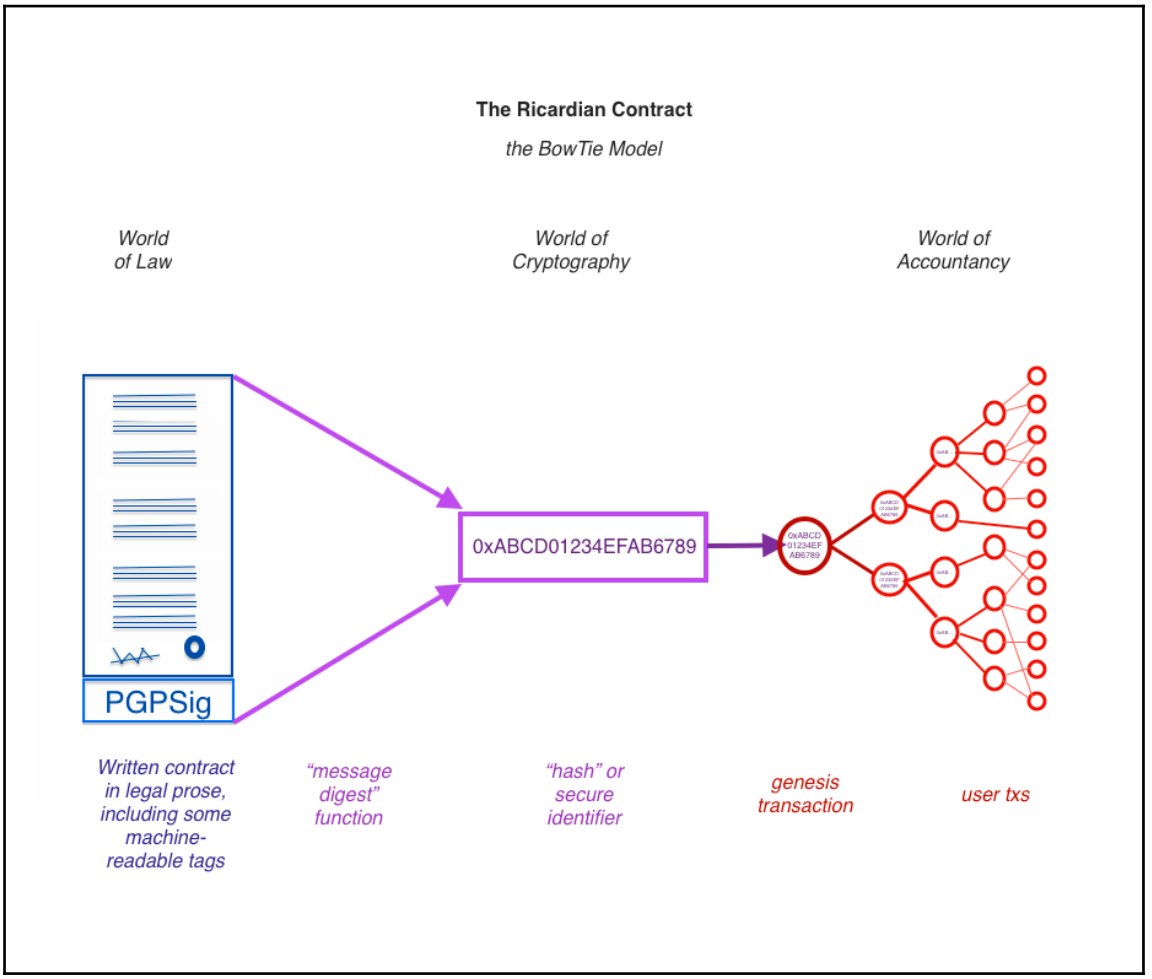
```
drequinox@drequinox-OP7010:~/zcash$ ./zcutil/fetch-params.sh
Zcash - fetch-params.sh

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 ........ ........ ........
```

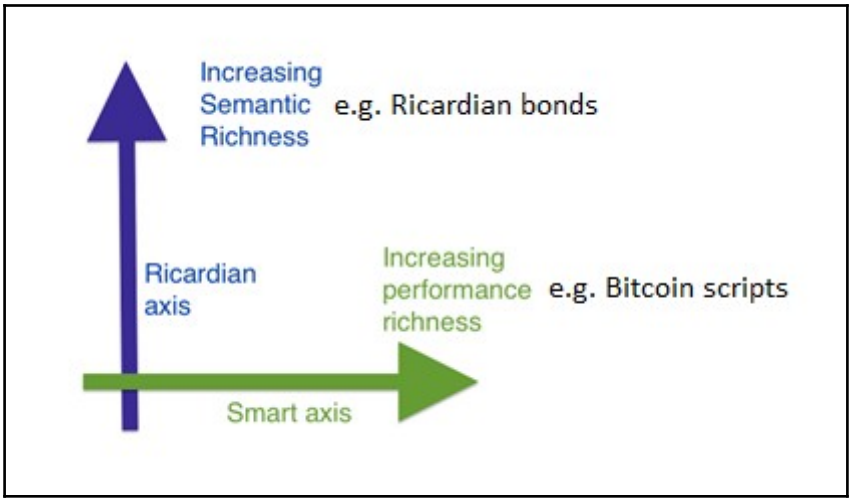
```
drequinox@drequinox-OP7010:~/zcash/src$ ./zcash-cli getinfo
{
    "version" : 1000050,
    "protocolversion" : 170002,
    "walletversion" : 60000,
    "balance" : 0.00000000,
    "blocks" : 601,
    "timeoffset" : 0,
    "connections" : 8,
    "proxy" : "",
    "difficulty" : 13748.56014152,
    "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$
```

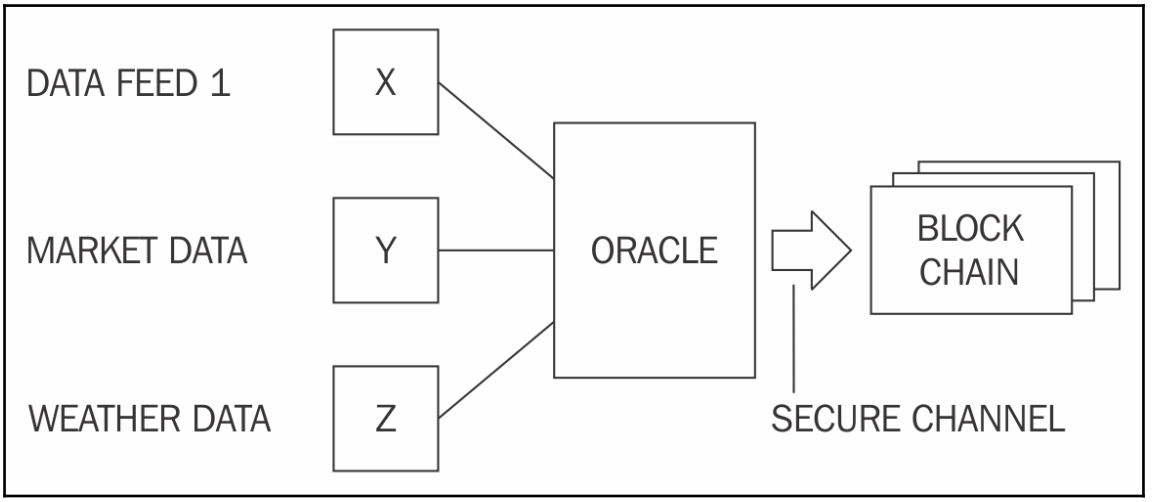
```
drequinox@drequinox-OP7010:~/nheqminer/nheqminer/build$ ./nheqminer -l eu -u 1PL6gsm49xCFMvrXqgGcee5cdrG119GoWN.worker1 -t 6 -od 0
Equihash CPU Miner for NiceHash v0.1c
Thanks to Zcash developers for providing most of the code
Special thanks to tromp for providing optimized CPU equihash solver

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 5000e5b8000000000000000005000e5b9ab
[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
```

```
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 1ffff7da0000000000000001ffff7d9
[2016-10-29 22:37:28.999642][0x00001590]: stratum | ←[35mTarget set to 03c3c3c0000000000000000000000000000000000000000000000000000000←[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 0100000000000000000000000000004
[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
```

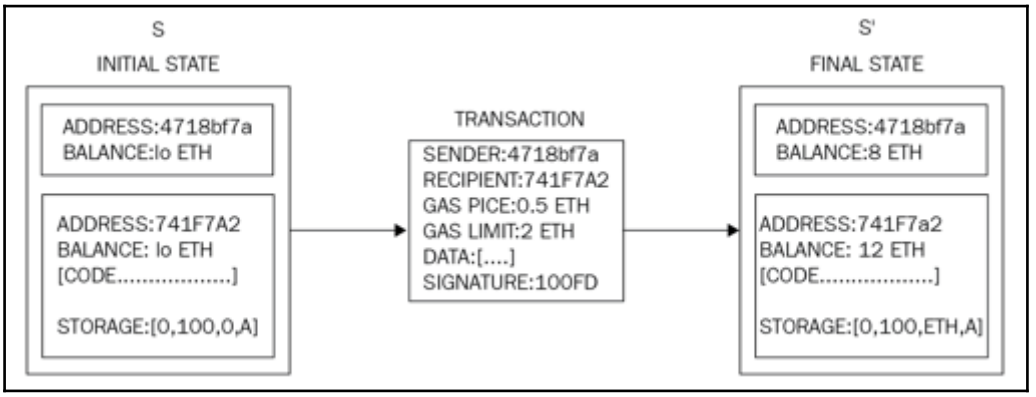
Chapter 9: Smart Contracts



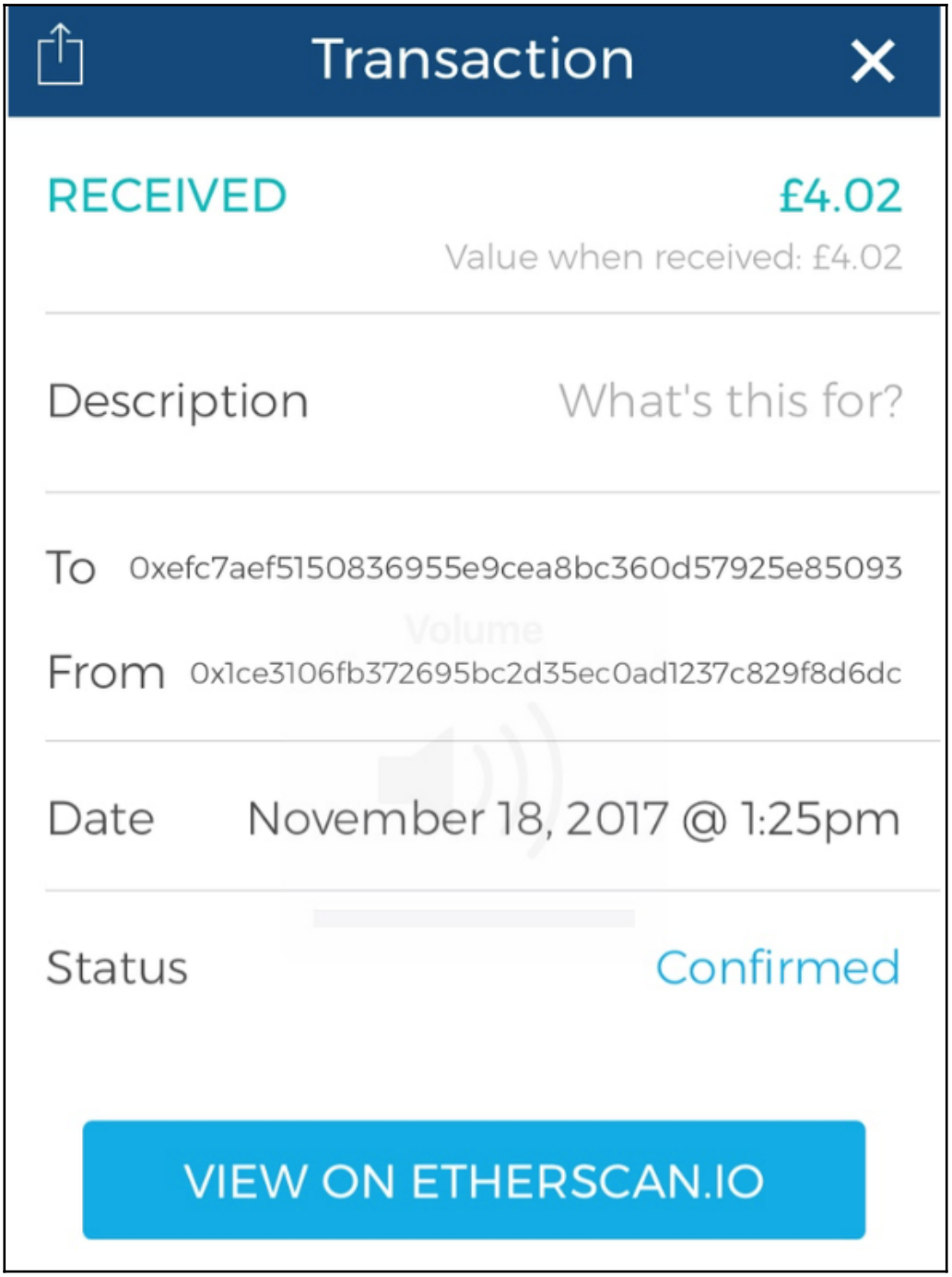

Increasing
Semantic
Richness
e.g. Ricardian bonds
Ricardian
axis
Increasing
performance
richness
e.g. Bitcoin scripts
Smart axis


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

Chapter 10: Ethereum 101




Jaxx
ETH
ZEC
Receive
Send
Your Current Ethereum Address:
0x1ce3106fb372695bc2d35ec0ad1237c829f8d6dc
ETH
0.06785733
£17.04
SEND CONFIRMATION
Send: 4 GBP
Receiving Address
0xeFc7aEF5150836955e9CEa8Bc360D57925e85093
Mining Fee: 0.000441 ETH
CANCEL
CONFIRM


Transaction
RECEIVED
£4.02
Value when received: £4.02
Description
What's this for?
To 0xefc7aef5150836955e9cea8bc360d57925e85093
From 0x1ce3106fb372695bc2d35ec0ad1237c829f8d6dc
Date November 18, 2017 @ 1:25pm
Status Confirmed
VIEW ON ETHERSCAN.IO

TxHash:
0xc63dce6747e1640abd63ee63027c3352aed8cdb92b6a02ae25225666e171009e

TxReceipt Status:
Success

Block Height:
4576084 (20583 block confirmations)

TimeStamp:
3 days 7 hrs ago (Nov-18-2017 01:25:54 PM +UTC)

From:
0x1ce3106fb372695bc2d35ec0ad1237c829f8d6dc

To:
0xefc7aef5150836955e9cea8bc360d57925e85093

Value:
0.015927244142974896 Ether ($5.82)

Gas Limit:
21000

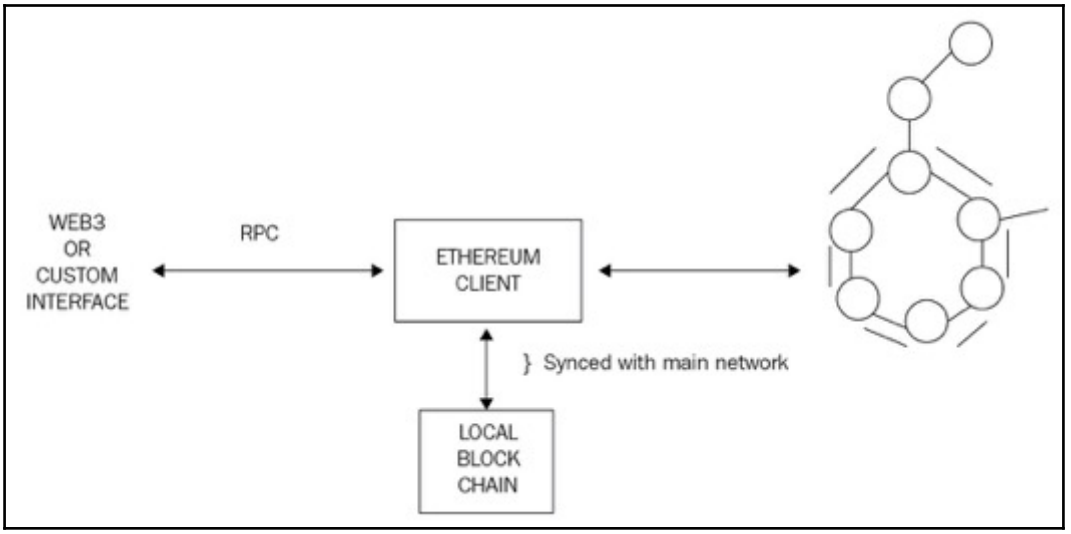
Gas Used By Txn:
21000

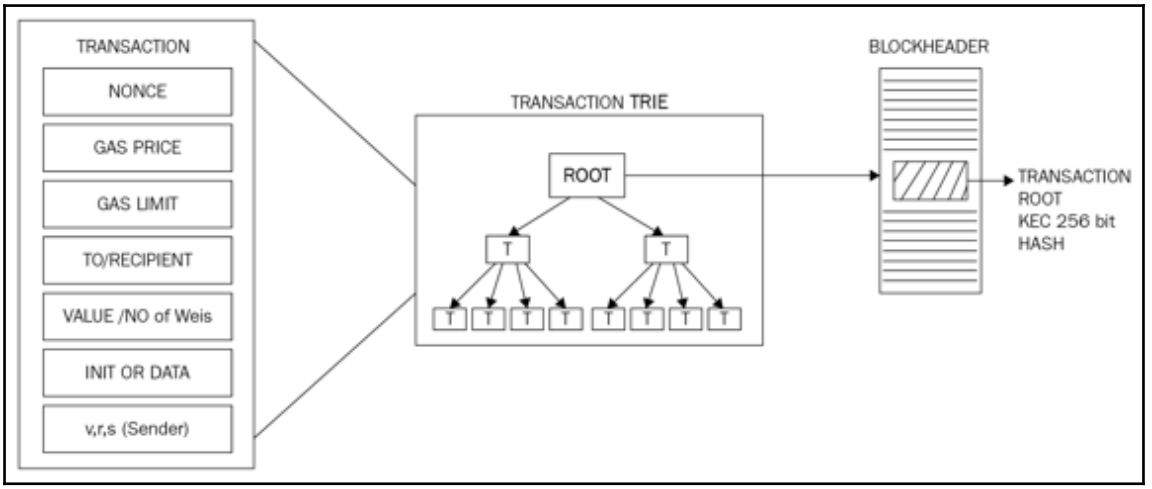
Gas Price:
0.000000021 Ether (21 Gwei)

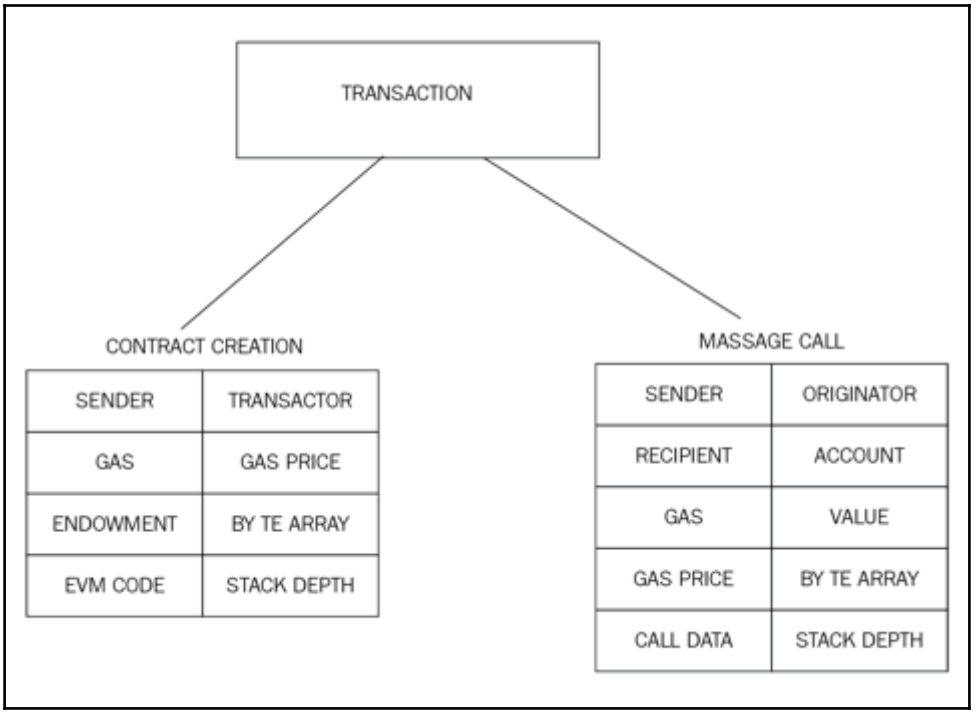
Actual Tx Cost/Fee:
0.000441 Ether ($0.16)

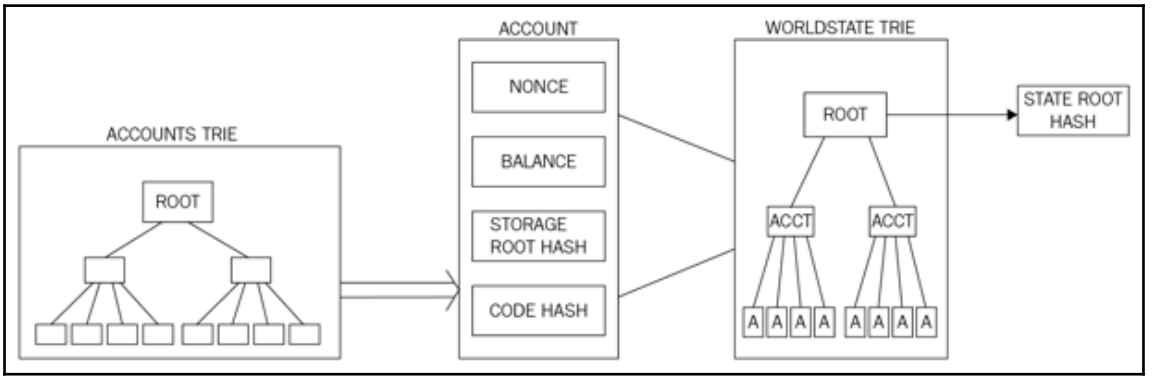
Cumulative Gas Used:
156148

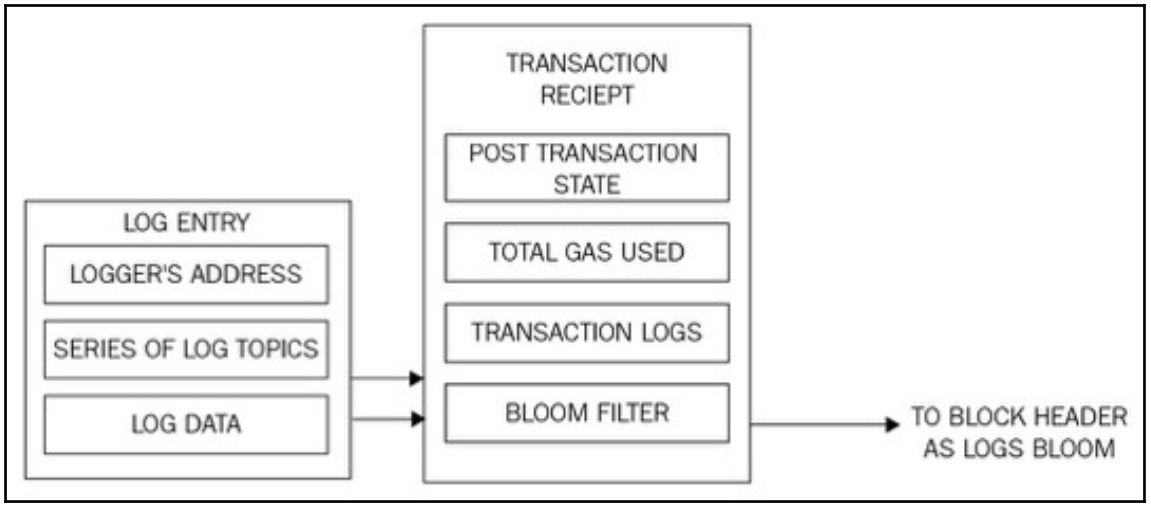
Nonce:
1

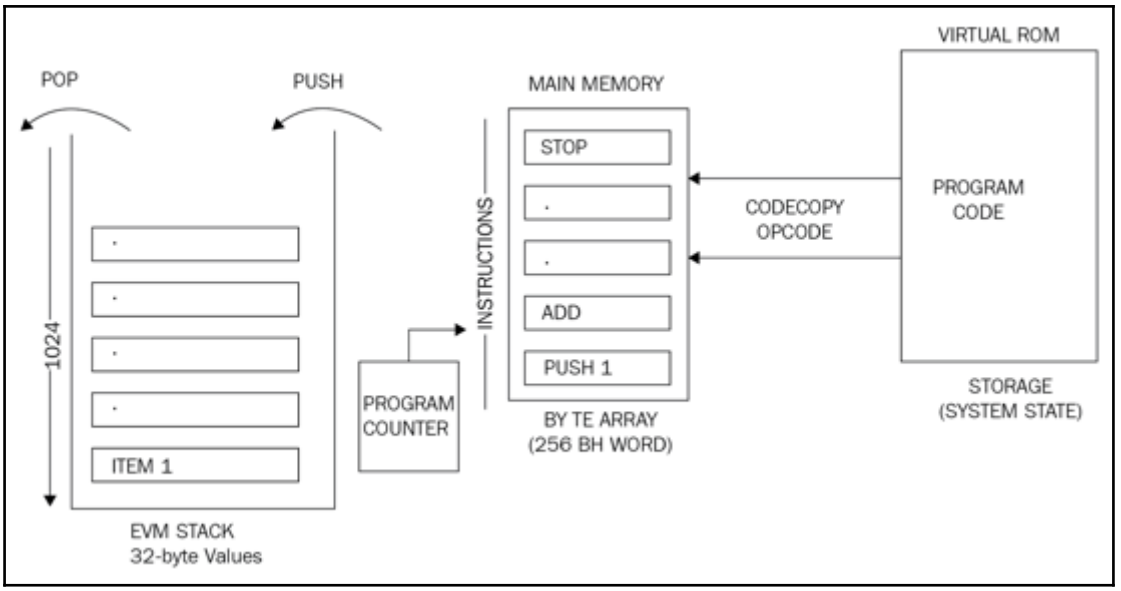

WEB3
OR
CUSTOM
INTERFACE
RPC
ETHEREUM
CLIENT
} Synced with main network
LOCAL
BLOCK
CHAIN

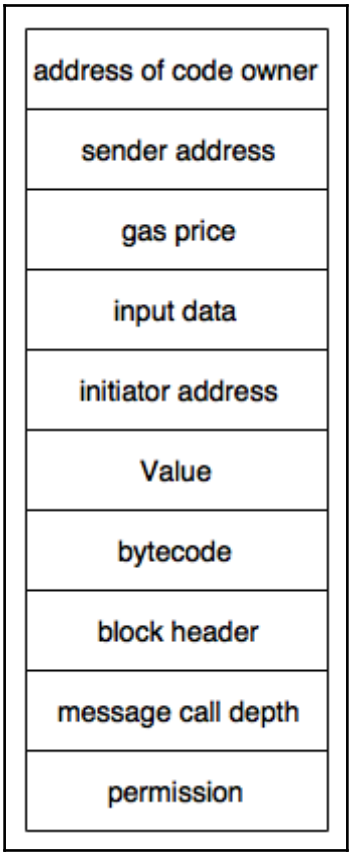

TRANSACTION
NONCE
GAS PRICE
GAS LIMIT
TO/RECIPIENT
VALUE /NO of Weis
INIT OR DATA
v,r,s (Sender)
TRANSACTION TRIE
ROOT
T
BLOCKHEADER
TRANSACTION
ROOT
KEC 256 bit
HASH


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


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


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

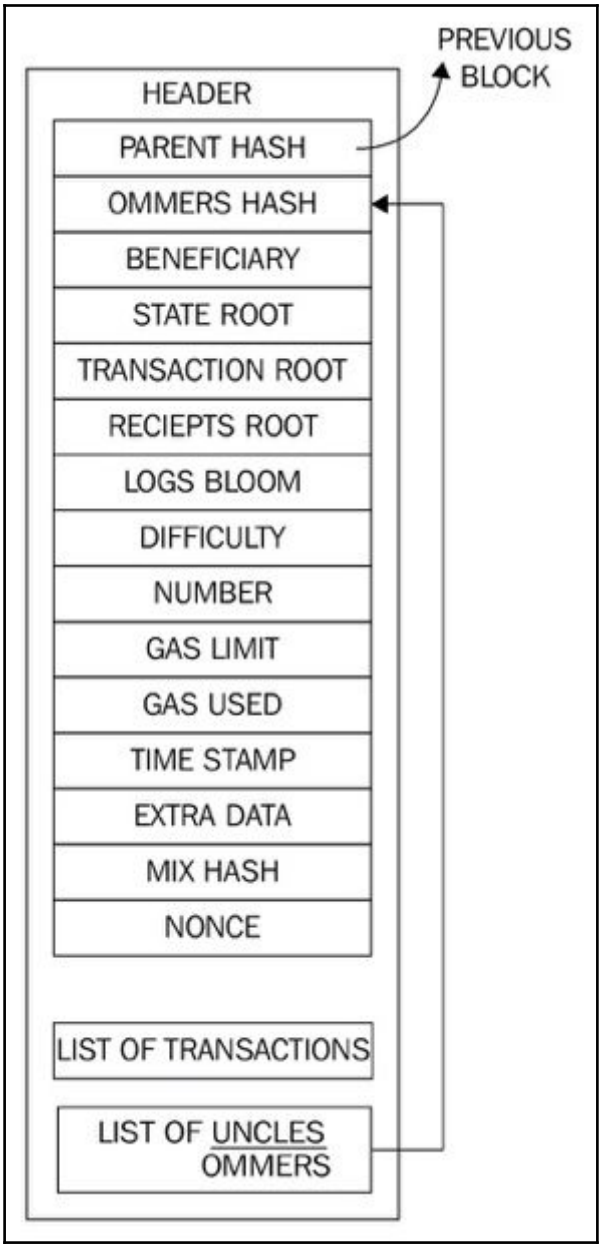

POP
PUSH
1024
ITEM 1
EVM STACK
32-byte Values
PROGRAM
COUNTER
INSTRUCTIONS
MAIN MEMORY
STOP
ADD
PUSH 1
BY TE ARRAY
(256 BH WORD)
CODECOPY
OPCODE
VIRTUAL ROM
PROGRAM
CODE
STORAGE
(SYSTEM STATE)


address of code owner
sender address
gas price
input data
initiator address
Value
bytecode
block header
message call depth
permission

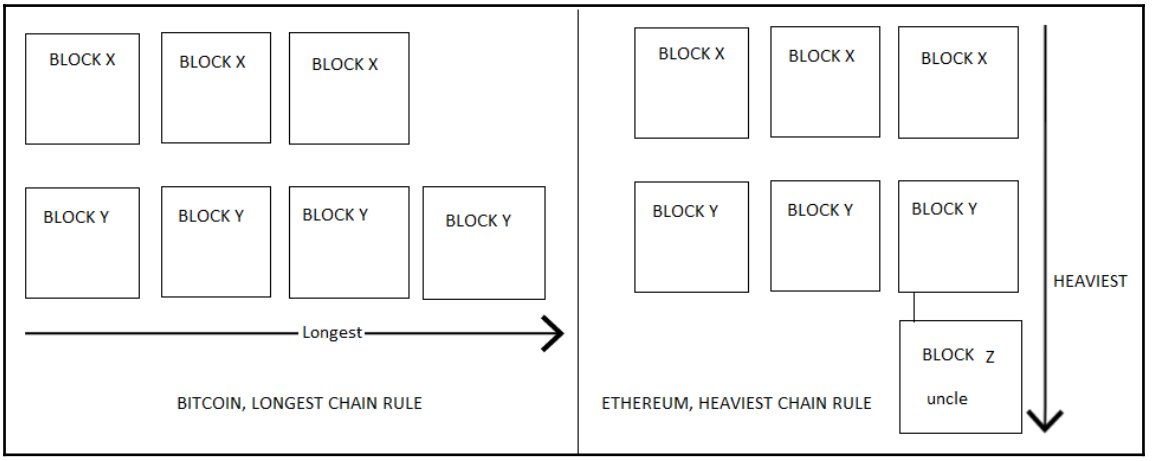

MACHINE STATE
AVAILABLE GAS
PROGRAM COUNTER
MEMORY CONTENTS
NUMBER OF WORDS
STACK CONTENTS

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.

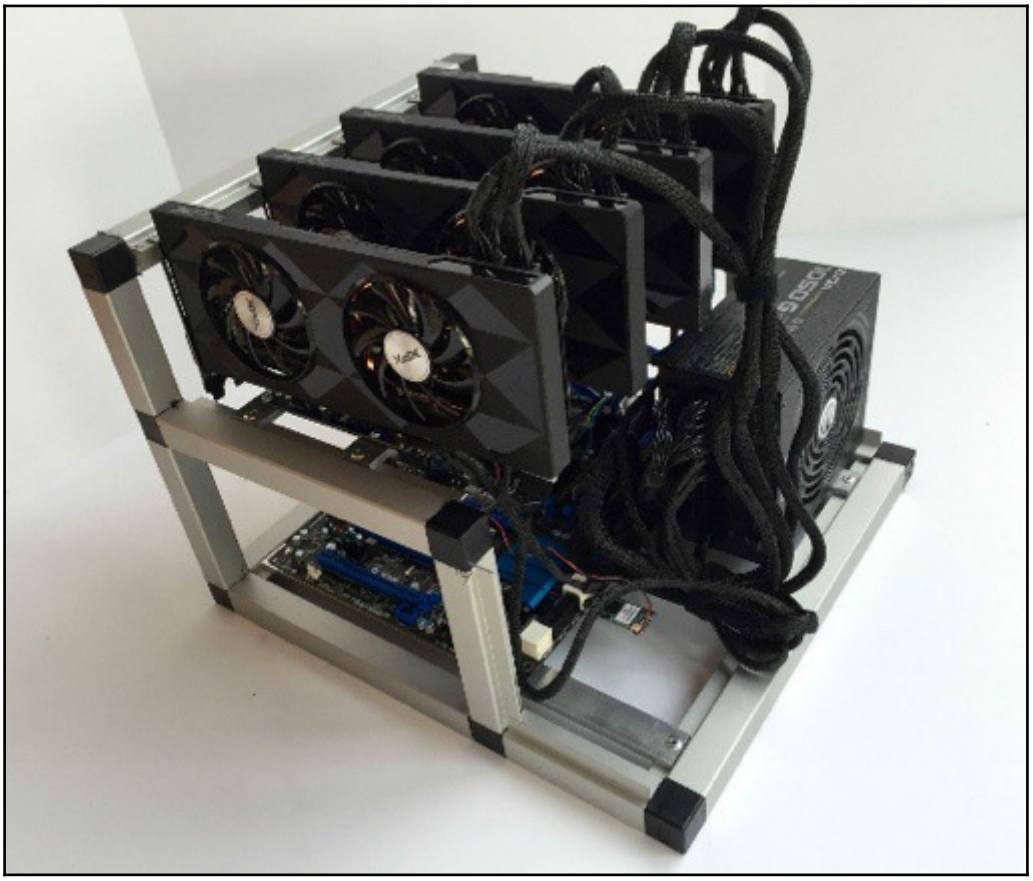

PREVIOUS
BLOCK
HEADER
PARENT HASH
OMMERS HASH
BENEFICIARY
STATE ROOT
TRANSACTION ROOT
RECIEPTS ROOT
LOGS BLOOM
DIFFICULTY
NUMBER
GAS LIMIT
GAS USED
TIME STAMP
EXTRA DATA
MIX HASH
NONCE
LIST OF TRANSACTIONS
LIST OF UNCLES
OMMERS

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

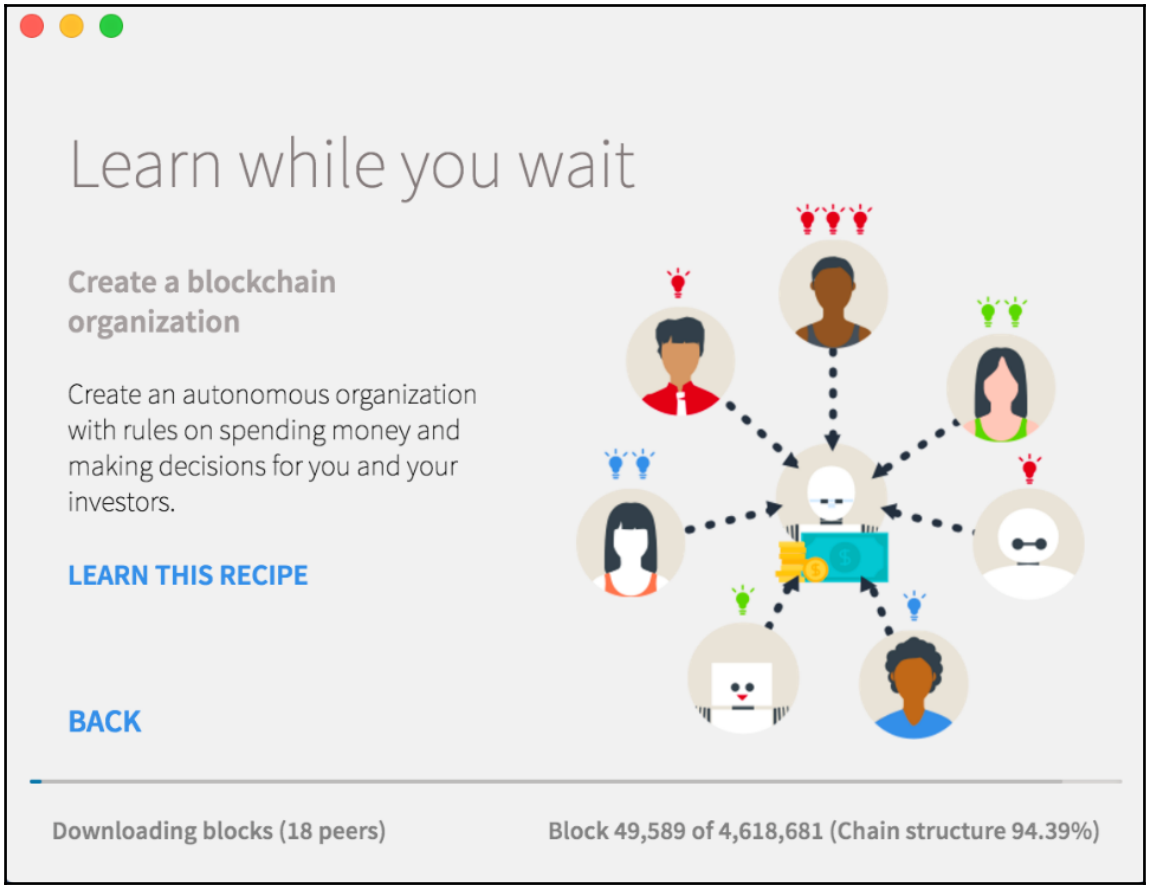


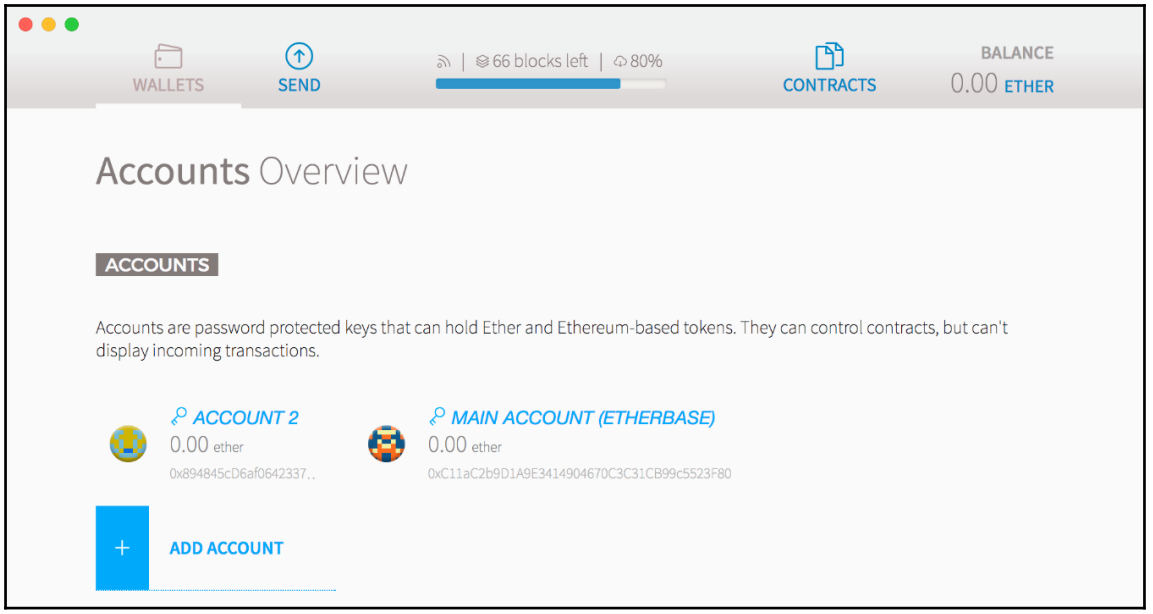

```
drequinox@drequinox-OP7010:~$ ethminer -G
[OPENCL]:No OpenCL platforms found
No GPU device with sufficient memory was found. Can't GPU mine. Remove the -G argument
drequinox@drequinox-OP7010:~$
```

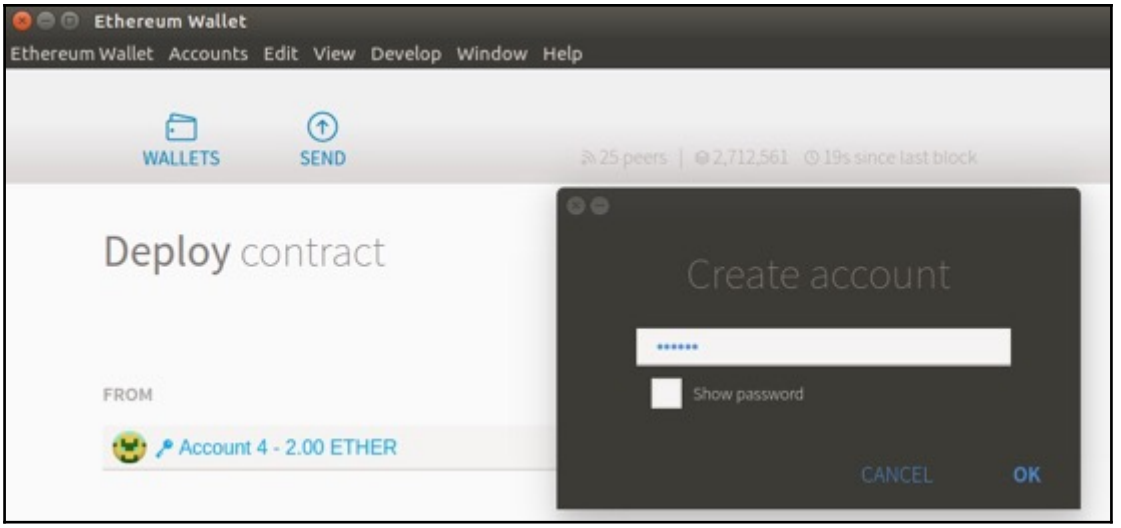
```
drequinox@drequinox-OP7010:~$ ethminer -M -C
  ◇  22:43:30.560 ethminer  #00004000…
Benchmarking on platform: 8-thread CPU
Preparing DAG...
  □  22:43:30.561 miner0  Loading full DAG of seedhash: #00000000…
Warming up...
Trial 1... 0
Trial 2... DAG  22:43:38.310 miner0  Generating DAG file. Progress: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



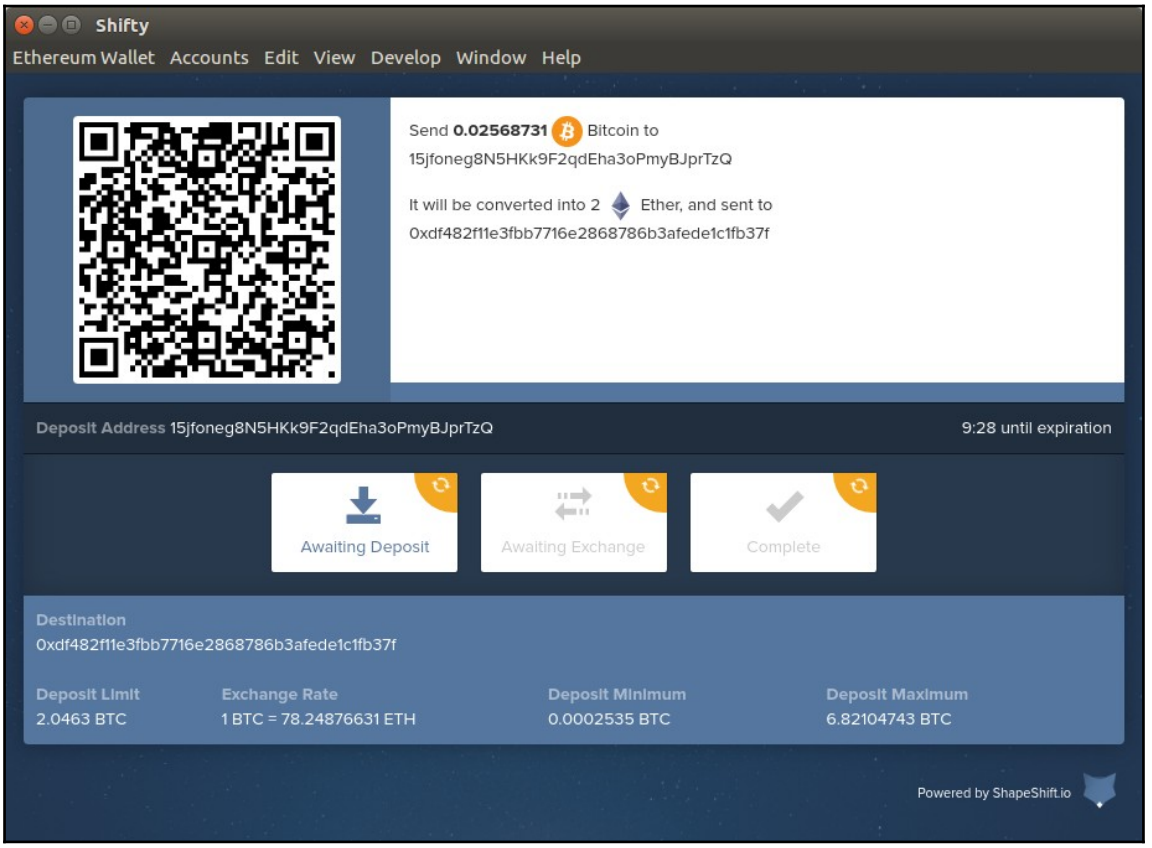
```
drequinox@drequinox-OP7010:~$  ethminer -C -F http://ethereumpool.co/?miner=0.1@0x024a20cc5feba7f3dc3776075b3e60c20eb1459c@DrEquinox
miner  23:50:52.046 ethminer  Getting work package...
```

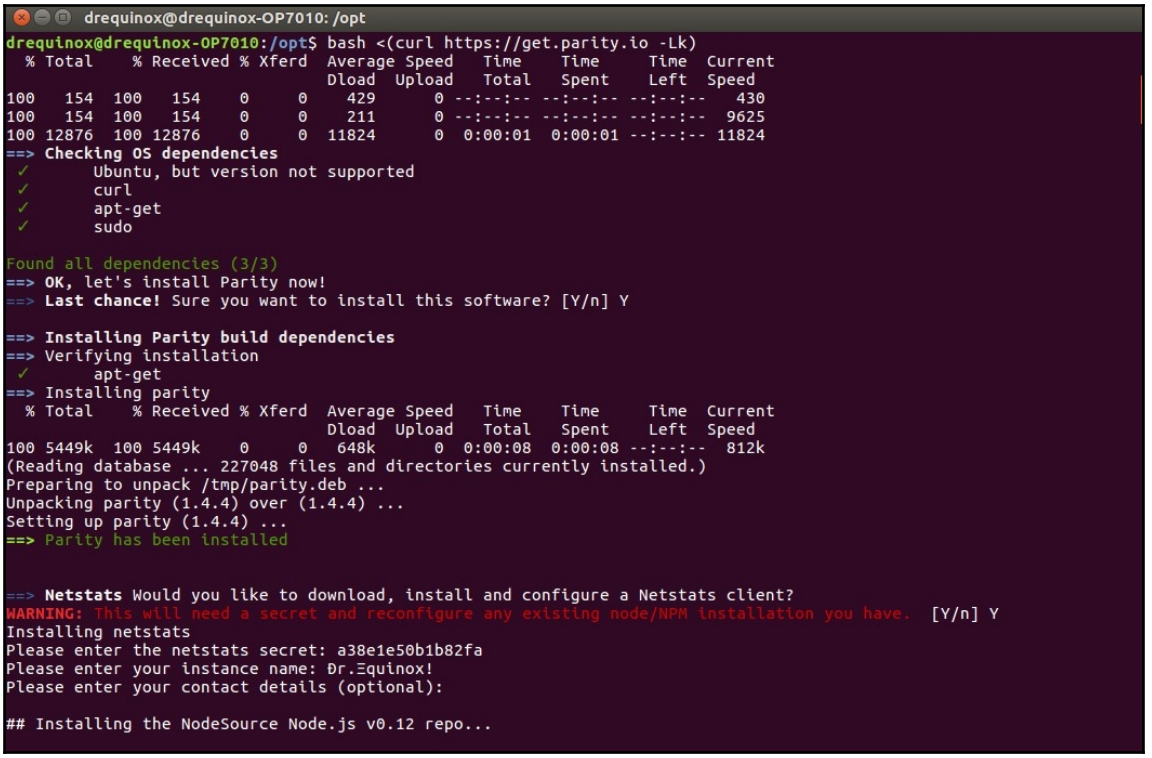

Learn while you wait
Create a blockchain organization
Create an autonomous organization with rules on spending money and making decisions for you and your investors.
LEARN THIS RECIPE
BACK
Downloading blocks (18 peers)
Block 49,589 of 4,618,681 (Chain structure 94.39%)

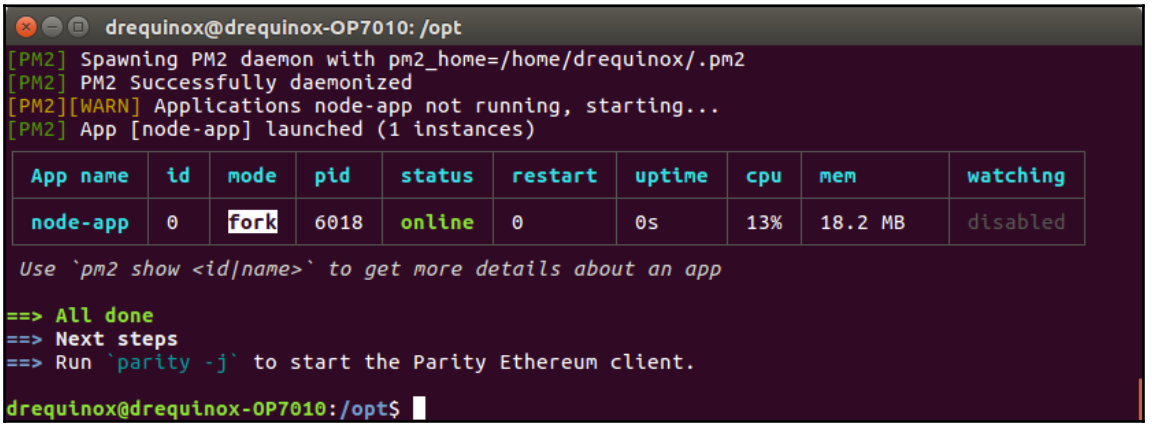

WALLETS
SEND
66 blocks left | 80%
CONTRACTS
BALANCE
0.00 ETHER
Accounts Overview
ACCOUNTS
Accounts are password protected keys that can hold Ether and Ethereum-based tokens. They can control contracts, but can't display incoming transactions.
ACCOUNT 2
0.00 ether
0x894845cD6af0642337..
MAIN ACCOUNT (ETHERBASE)
0.00 ether
0xC11aC2b9D1A9E3414904670C3C31CB99c5523F80
ADD ACCOUNT


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
CANCEL
OK

```
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

>
```

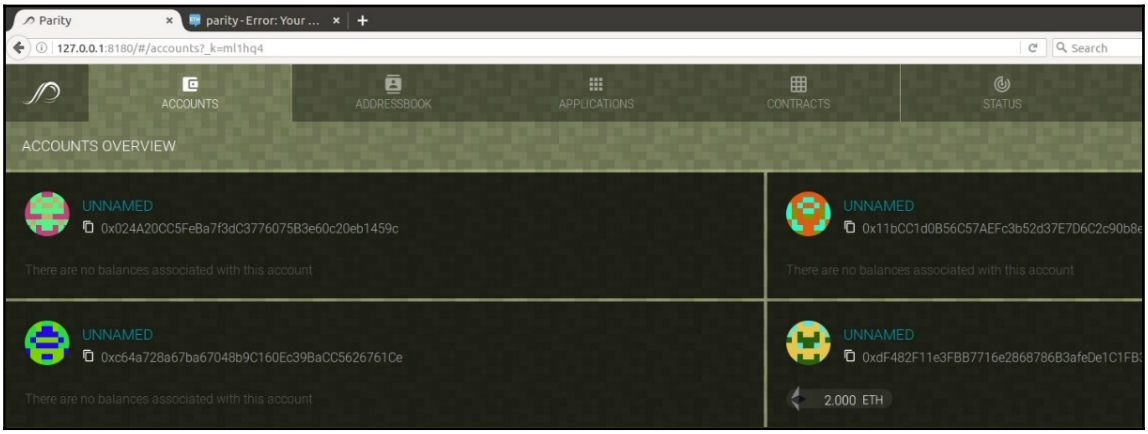


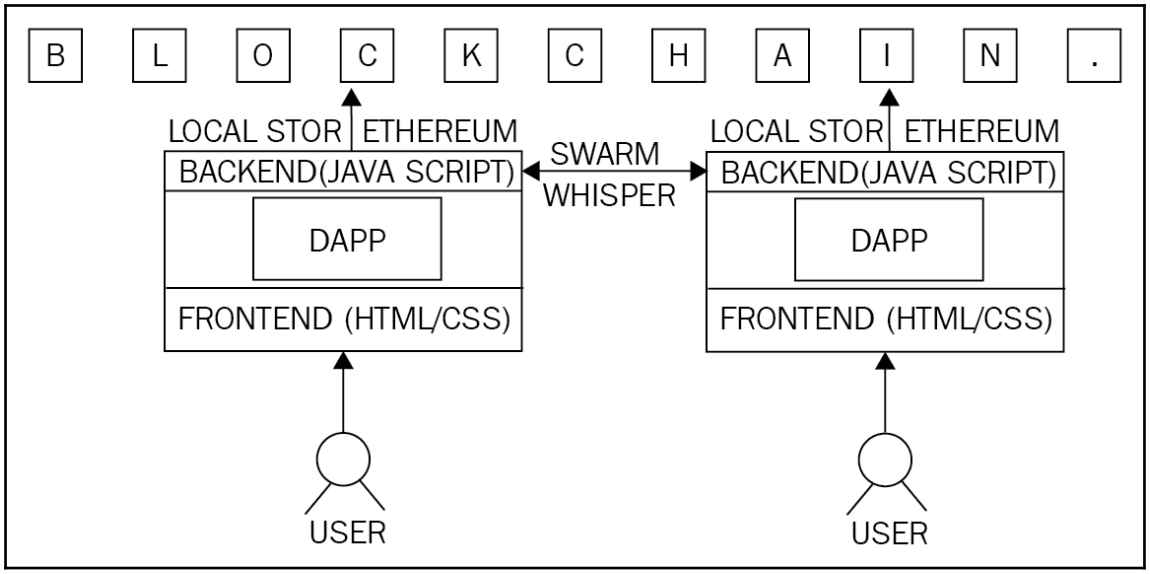

drequinox@drequinox-OP7010: /opt
drequinox@drequinox-OP7010:/opt$ bash <(curl https://get.parity.io -Lk)
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 154 100 154 0 0 429 0 --:--:-- --:--:-- --:--:-- 430
100 154 100 154 0 0 211 0 --:--:-- --:--:-- --:--:-- 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: Ðr.Ξquinox!
Please enter your contact details (optional):
Installing the NodeSource Node.js v0.12 repo...


drequinox@drequinox-OP7010: /opt
[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$


BEST BLOCK
#2,700,281
UNCLES
1/5
LAST BLOCK
0s ago
AVG BLOCK TIME
15.37s
AVG NETWORK HASHRATE
5.1 TH/s
DIFFICULTY
66.74 TH
ACTIVE NODES
37/39
GAS PRICE
25 gwei
GAS LIMIT
3300000 gas
PAGE LATENCY
293 ms
UPTIME
100%
BLOCK TIME
DIFFICULTY
BLOCK PROPAGATION
LAST BLOCKS MINERS
UNCLE COUNT
TRANSACTIONS
GAS SPENDING
GAS LIMIT
ATTENTION!
This page does not represent the entire state of the ethereum network - listing a node on this page is a voluntary process.


Bootnode-SG Geth/v1.8.1-stable/linux-amd64/go1.7 123 ms 510
Bootnode-IE Geth/v1.8.1-stable/linux-amd64/go1.7 43 ms 499
sphinxRust Parity//v1.8.11-stable-21522ff86-20180227/x86_64-linux-gnu/rustc1.24.1 46 ms 328
Bootnode-NORCAL Geth/v1.8.1-stable/linux-amd64/go1.10 36 ms 256
Zetabit2 Parity//v1.8.10-stable-78acefd-20180219/x86_64-linux-gnu/rustc1.24.0 50 ms 239
FunFair-01 Geth/v1.8.2-stable-b8b9f7f4/linux-amd64/go1.9.4 60 ms 239
Bootnode-AU Geth/v1.8.1-stable/linux-amd64/go1.7 100 ms 232
Bootnode-BR Geth/v1.8.2-stable/linux-amd64/go1.10 59 ms 229
ethpool.maxhash.org (US) Parity//v1.8.9-stable-1952d05-20180201/x86_64-linux-gnu/rustc1.23.0 8 ms 0 KH/s 199
CIMS FARM CRYPTO. INVEST. Geth/v1.8.2-stable-b8b9f7f4/linux-amd64/go1.9.4 4 ms 161


Parity
parity - Error: Your ...
127.0.0.1:8180/#/accounts?_k=ml1hq4
Search
ACCOUNTS
ADDRESSBOOK
APPLICATIONS
CONTRACTS
STATUS
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
0xdF482F11e3FBB7716e2868786B3afeDe1C1FB
2.000 ETH


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


Ether Historical Market Capitalization Chart (USD)
Source: Etherscan.io
Click and drag in the plot area to zoom in
150 B
125 B
100 B
75 B
50 B
25 B
0 B
Ether Market Cap (USD)
Apr '17
Jul '17
Oct '17
Jan '18

Chapter 12: Ethereum Development Environment

```
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
```

```
WARN [12-13|19:19:11] No etherbase set and no accounts found as default
INFO [12-13|19:19:11] Allocated cache and file handles         database=/Users/drequinox/etherprivate/geth/chaindata cache=16 handles=16
INFO [12-13|19:19:11] Writing custom genesis block
INFO [12-13|19:19:11] Successfully wrote genesis state         database=chaindata                                    hash=6650a0…b5c158
INFO [12-13|19:19:11] Allocated cache and file handles         database=/Users/drequinox/etherprivate/geth/lightchaindata cache=16 handles=16
INFO [12-13|19:19:11] Writing custom genesis block
INFO [12-13|19:19:11] Successfully wrote genesis state         database=lightchaindata                               hash=6650a0…b5c158
```

```
WARN [12-13|19:20:11] No etherbase set and no accounts found as default
INFO [12-13|19:20:11] Starting peer-to-peer node               instance=Geth/v1.7.3-stable-4bb3c89d/darwin-amd64/go1.9.2
INFO [12-13|19:20:11] Allocated cache and file handles         database=/Users/drequinox/etherprivate/geth/chaindata cach
WARN [12-13|19:20:11] Upgrading database to use lookup entries
INFO [12-13|19:20:11] Initialised chain configuration          config="{ChainID: 786 Homestead: 0 DAO: <nil> DAOSupport:
INFO [12-13|19:20:11] Disk storage enabled for ethash caches   dir=/Users/drequinox/etherprivate/geth/ethash count=3
INFO [12-13|19:20:11] Disk storage enabled for ethash DAGs     dir=/Users/drequinox/.ethash                  count=2
INFO [12-13|19:20:11] Initialising Ethereum protocol           versions="[63 62]" network=786
INFO [12-13|19:20:11] Database deduplication successful        deduped=0
INFO [12-13|19:20:11] Loaded most recent local header          number=0 hash=6650a0…b5c158 td=1024
INFO [12-13|19:20:11] Loaded most recent local full block      number=0 hash=6650a0…b5c158 td=1024
INFO [12-13|19:20:11] Loaded most recent local fast block      number=0 hash=6650a0…b5c158 td=1024
INFO [12-13|19:20:11] Regenerated local transaction journal    transactions=0 accounts=0
INFO [12-13|19:20:11] Starting P2P networking
INFO [12-13|19:20:13] UDP listener up                          self=enode://5c53ec0755806bc92432728f22a55f169a8c63df307fc
7a55d635@86.15.44.209:30303
INFO [12-13|19:20:13] RLPx listener up                         self=enode://5c53ec0755806bc92432728f22a55f169a8c63df307fc
7a55d635@86.15.44.209:30303
INFO [12-13|19:20:13] IPC endpoint opened: /Users/drequinox/etherprivate/geth.ipc
INFO [12-13|19:20:14] Mapped network port                      proto=udp extport=30303 intport=30303 interface="UPNP IGDv
INFO [12-13|19:20:14] Mapped network port                      proto=tcp extport=30303 intport=30303 interface="UPNP IGDv
```

```
Welcome to the Geth JavaScript console!

instance: Geth/v1.7.3-stable-4bb3c89d/darwin-amd64/go1.9.2
 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

>
```

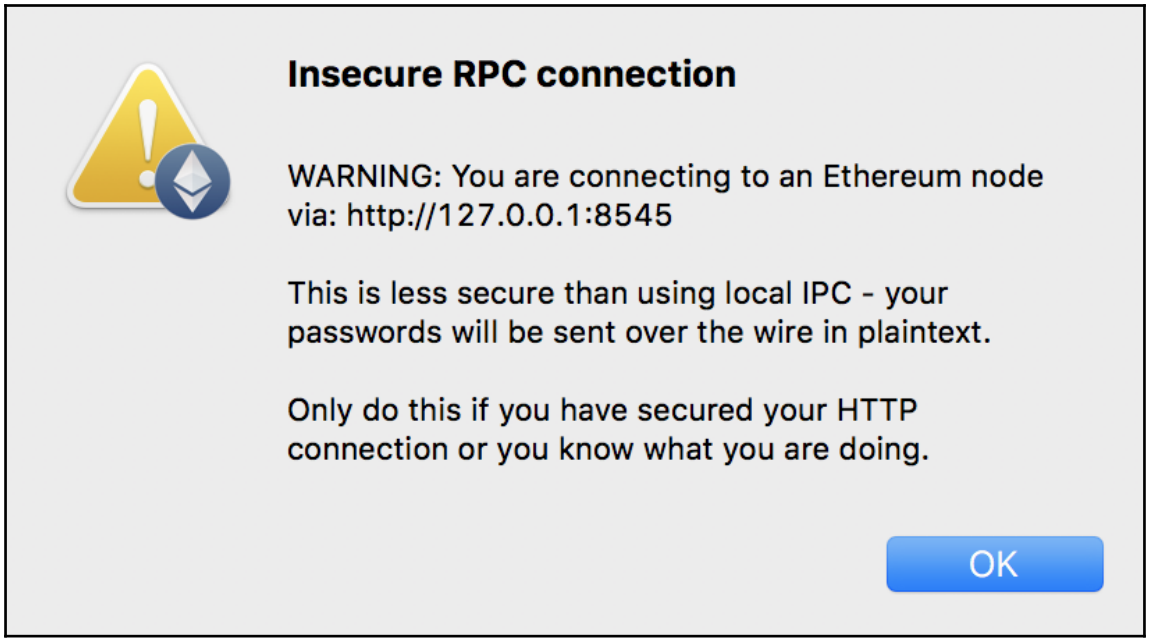
```
I0211 23:58:50.380089 eth/backend.go:479] Automatic pregeneration of ethash DAG ON (ethash dir: /home/imran/.e
thash)
I0211 23:58:50.380097 miner/miner.go:136] Starting mining operation (CPU=2 TOT=3)
I0211 23:58:50.380138 eth/backend.go:486] checking DAG (ethash dir: /home/imran/.ethash)
I0211 23:58:50.380257 miner/worker.go:542] commit new work on block 1 with 0 txs & 0 uncles. Took 139.49µs
I0211 23:58:50.380292 vendor/github.com/ethereum/ethash/ethash.go:259] Generating DAG for epoch 0 (size 107373
9904) (0000000000000000000000000000000000000000000000000000000000000000)
I0211 23:58:51.166755 vendor/github.com/ethereum/ethash/ethash.go:276] Done generating DAG for epoch 0, it too
k 786.458657ms
```

```
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
```

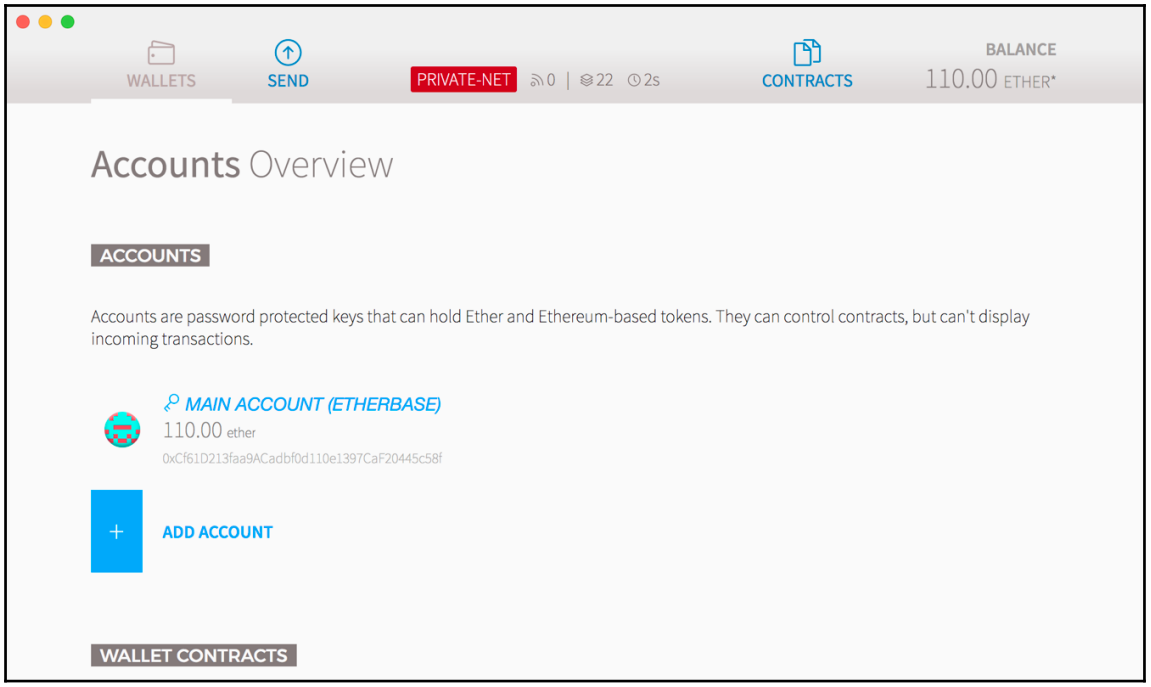
```
>
Array               Math                TypeError           constructor         hasOwnProperty      parseFloat          toString
BigNumber           NaN                 URIError            debug               inspect             parseInt            txpool
Boolean             Number              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
>
```

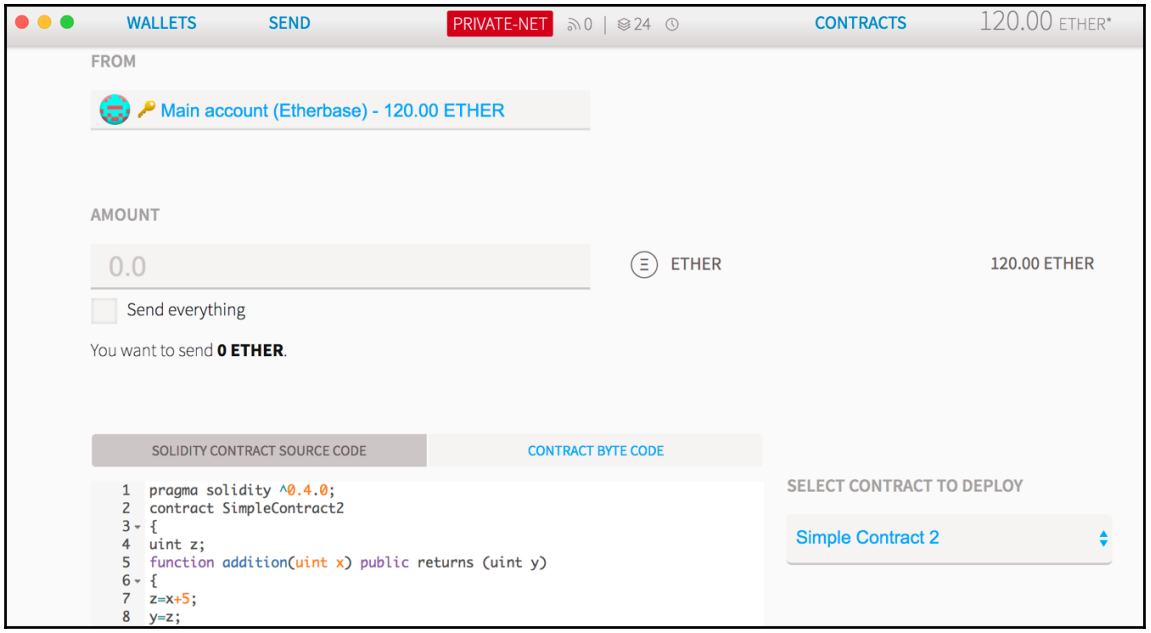
```
> personal.
personal._requestManager personal.getListAccounts personal.lockAccount     personal.sign
personal.constructor     personal.importRawKey     personal.newAccount      personal.unlockAccount
personal.ecRecover       personal.listAccounts     personal.sendTransaction
> net.
net._requestManager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

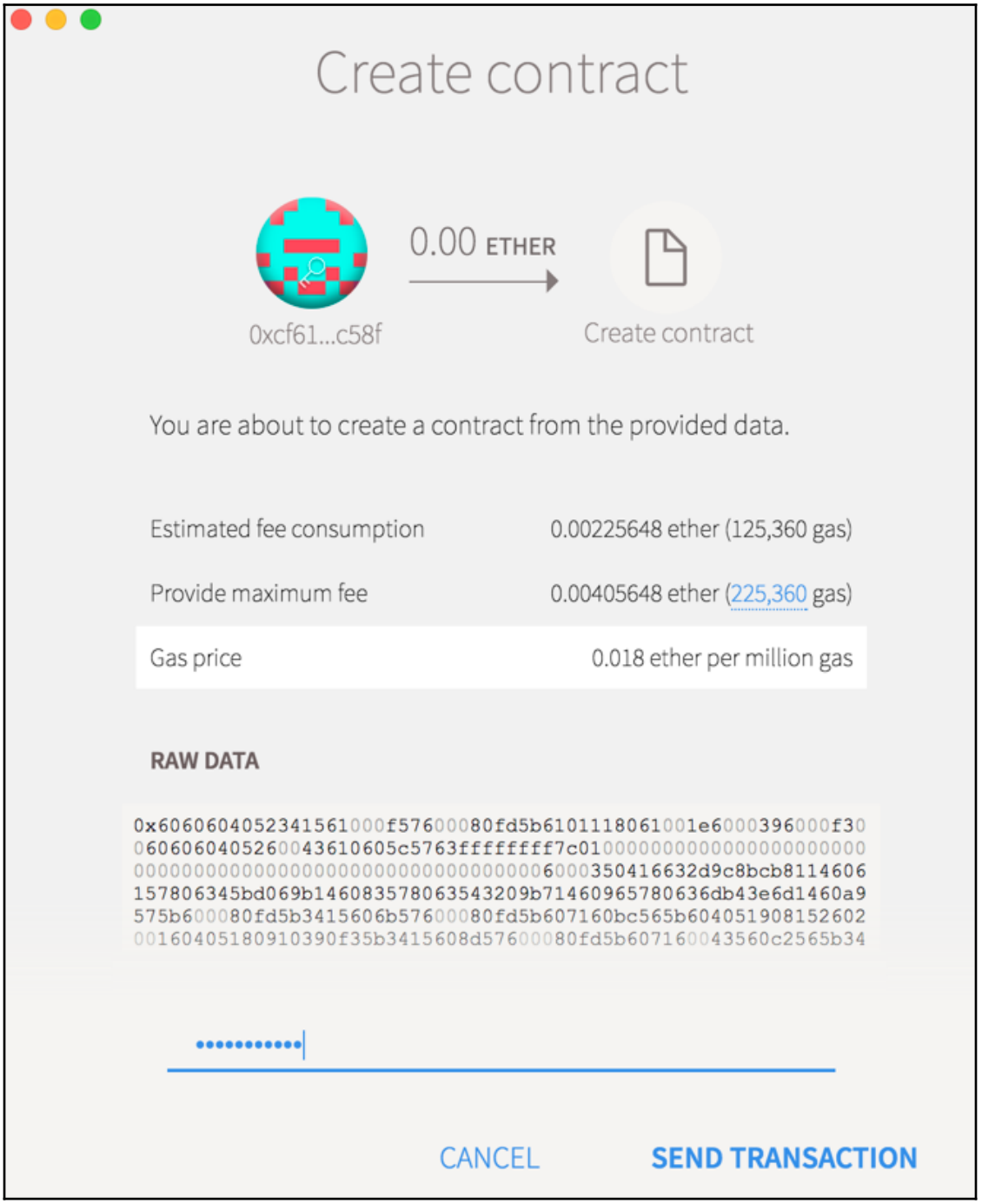
```
> net;
{
  listening: true,
  peerCount: 0,
  version: "786",
  getListening: function(callback),
  getPeerCount: function(callback),
  getVersion: function(callback)
}
>
```

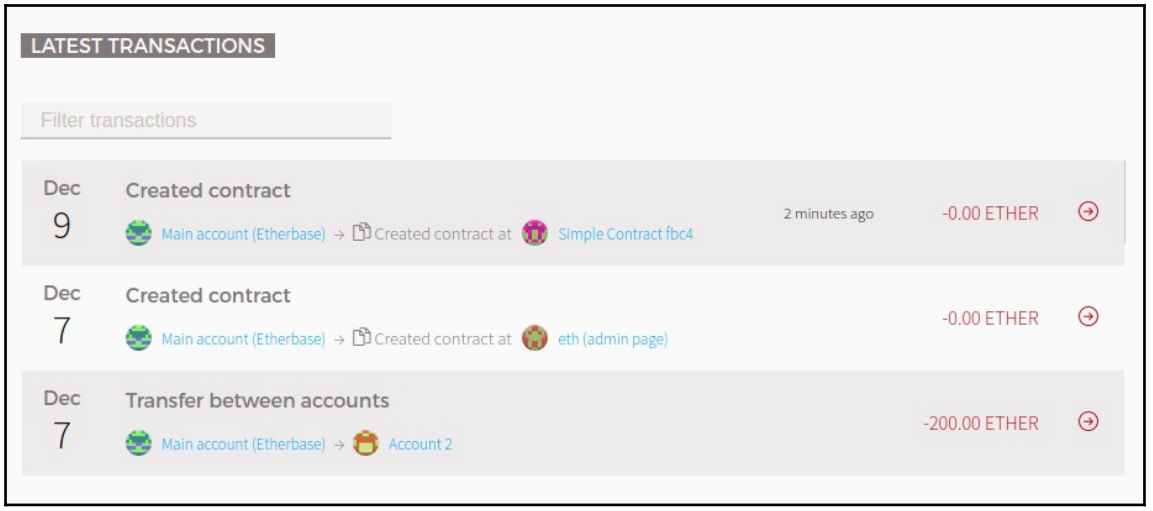


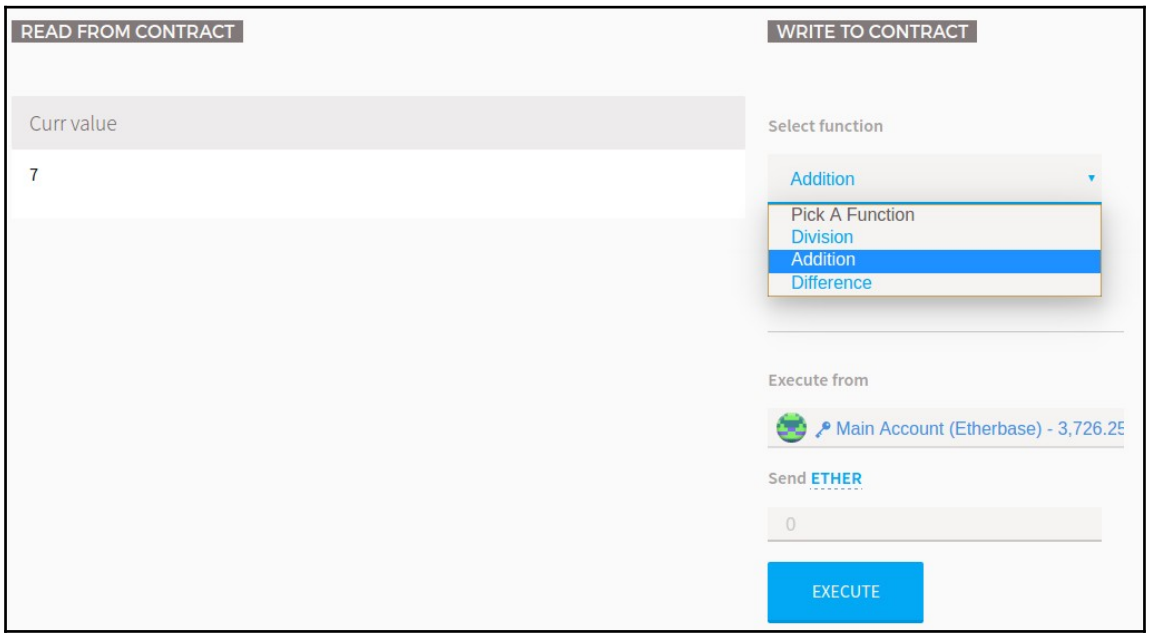

```
imran@drequinox-OP7010: /opt/Ethereum Wallet
imran@drequinox-OP7010:/opt/Ethereum Wallet$ ./Ethereum\ Wallet --rpc /home/imran/.ethereum/privatenet/geth.ipc
[2016-12-06 07:58:08.706] [INFO] main - Running in production mode: true
Secp256k1 bindings are not compiled. Pure JS implementation will be 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.
```

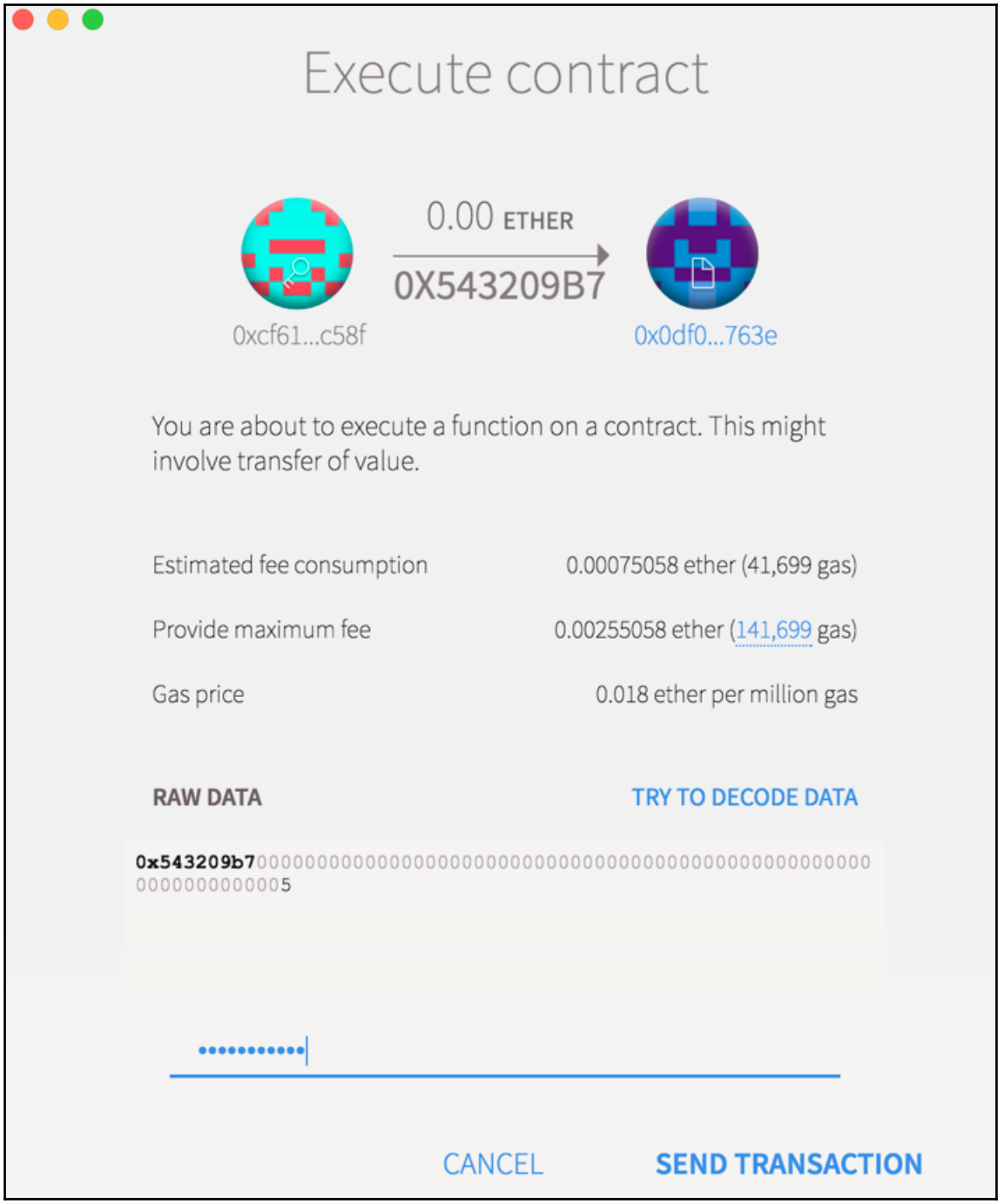

WALLETS
SEND
PRIVATE-NET
0 | 22 2s
CONTRACTS
BALANCE
110.00 ETHER*
Accounts Overview
ACCOUNTS
Accounts are password protected keys that can hold Ether and Ethereum-based tokens. They can control contracts, but can't display incoming transactions.
MAIN ACCOUNT (ETHERBASE)
110.00 ether
0xCf61D213faa9ACadbf0d110e1397CaF20445c58f
ADD ACCOUNT
WALLET CONTRACTS


WALLETS
SEND
PRIVATE-NET
0 | 24
CONTRACTS
120.00 ETHER*
FROM
Main account (Etherbase) - 120.00 ETHER
AMOUNT
0.0
ETHER
120.00 ETHER
Send everything
You want to send 0 ETHER.
SOLIDITY CONTRACT SOURCE CODE
CONTRACT BYTE CODE
1 pragma solidity ^0.4.0;
2 contract SimpleContract2
3 {
4 uint z;
5 function addition(uint x) public returns (uint y)
6 {
7 z=x+5;
8 y=z;
SELECT CONTRACT TO DEPLOY
Simple Contract 2

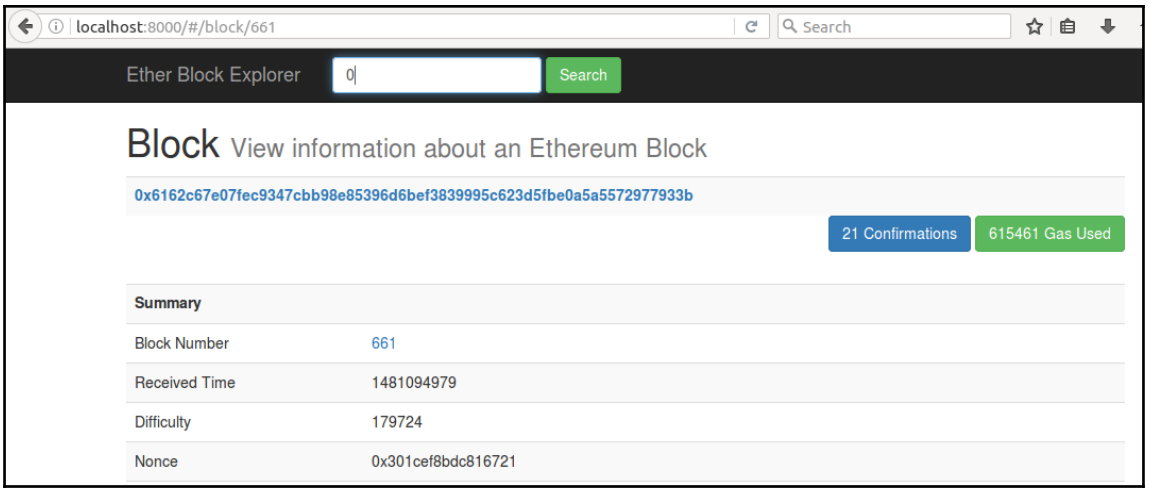

Create contract
0.00 ETHER
0xcf61...c58f
Create contract
You are about to create a contract from the provided data.
Estimated fee consumption
0.00225648 ether (125,360 gas)
Provide maximum fee
0.00405648 ether (225,360 gas)
Gas price
0.018 ether per million gas
RAW DATA
0x6060604052341561000f576000 80fd5b6101118061001e6000396000f30
06060604052600436106 05c5763ffffffff7c01000000000000000000000
0000000000000000000000000000000000006000350416632d9c8bcb8114606
157806345bd069b14608357806354320 9b71460965780636db43e6d1460a9
575b6000 80fd5b3415606b576000 80fd5b607160bc565b604051908152602
0016040518091039 0f35b3415608d576000 80fd5b607160043560c2565b34
CANCEL
SEND TRANSACTION


LATEST TRANSACTIONS
Filter 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
Pick A Function
Division
Addition
Difference
Execute from
Main Account (Etherbase) - 3,726.25
Send ETHER
0
EXECUTE

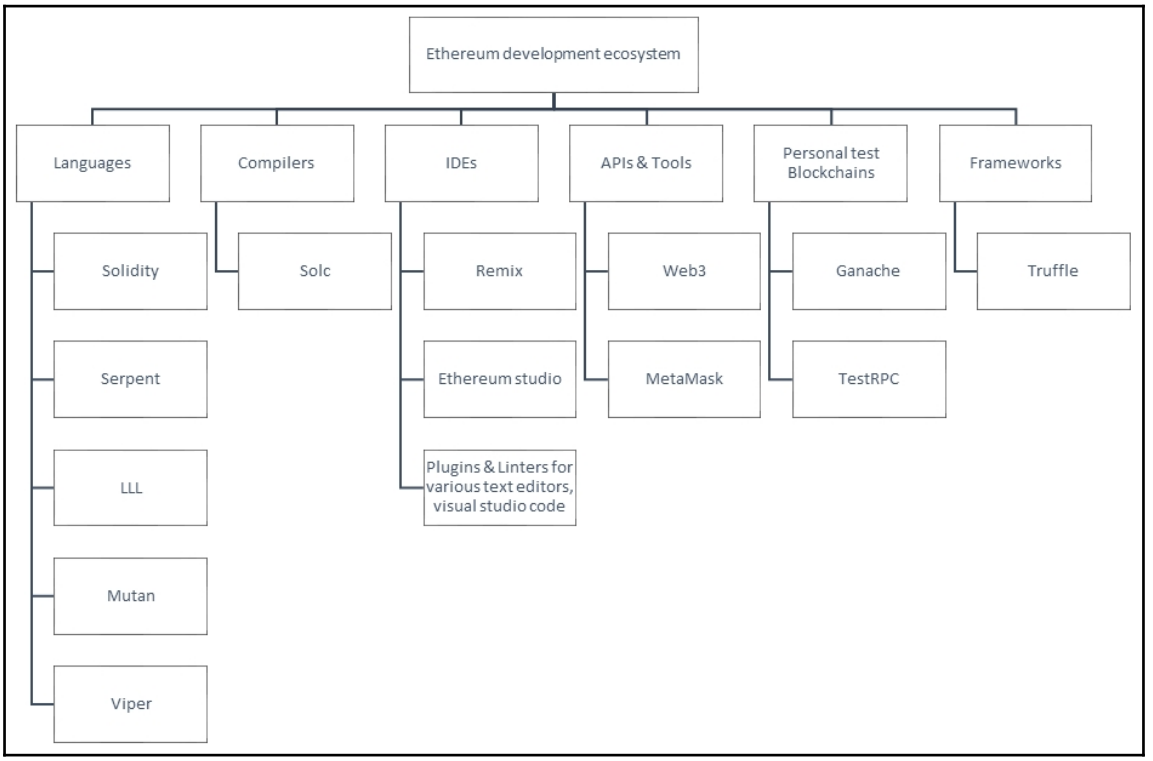

Execute contract
0.00 ETHER
0X543209B7
0xcf61...c58f
0x0df0...763e
You are about to execute a function on a contract. This might involve transfer of value.
Estimated fee consumption
0.00075058 ether (41,699 gas)
Provide maximum fee
0.00255058 ether (141,699 gas)
Gas price
0.018 ether per million gas
RAW DATA
TRY TO DECODE DATA
0x543209b70000000000000000000000000000000000000000000000000000000000000005
CANCEL
SEND TRANSACTION


explorer — node ◂ npm TERM_PROGRAM=Apple_Terminal SHELL=/bin/bash — 121×34
node-uuid@1.4.8
oauth-sign@0.8.2
qs@3.1.0
stringstream@0.0.5
tough-cookie@2.3.3
punycode@1.4.1
tunnel-agent@0.4.3
saucelabs@1.0.1
https-proxy-agent@1.0.0
agent-base@2.1.1
semver@5.0.3
extend@3.0.1
selenium-webdriver@2.47.0
tmp@0.0.24
ws@0.8.1
bufferutil@1.2.1
bindings@1.2.1
options@0.0.6
ultron@1.0.2
utf-8-validate@1.2.2
nan@2.4.0
xml2js@0.4.4
sax@0.6.1
xmlbuilder@9.0.4
source-map-support@0.2.10
source-map@0.1.32
shelljs@0.2.6
> EthereumExplorer@0.1.0 start /Users/drequinox/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


localhost:8000/#/block/661
Search
Ether Block Explorer
0
Search
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"

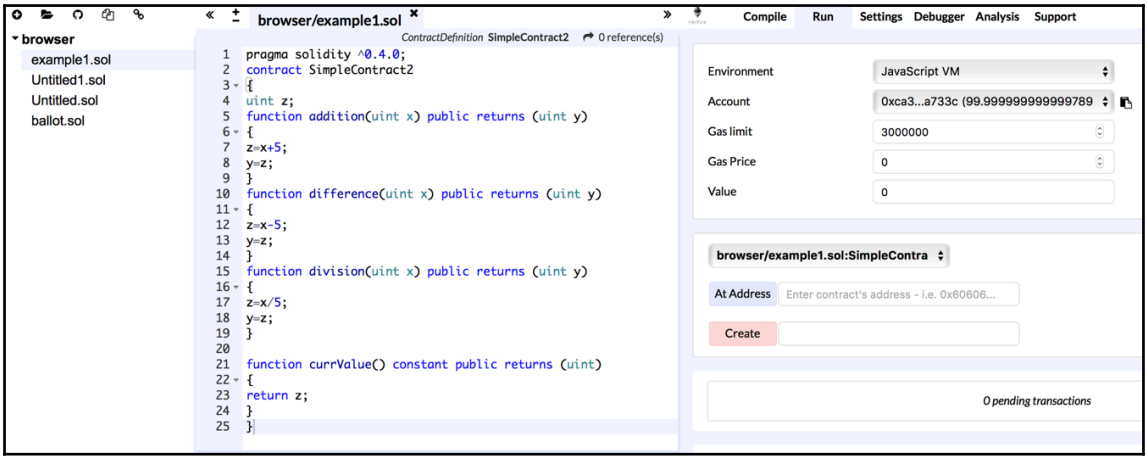
Chapter 13: Development Tools and Frameworks

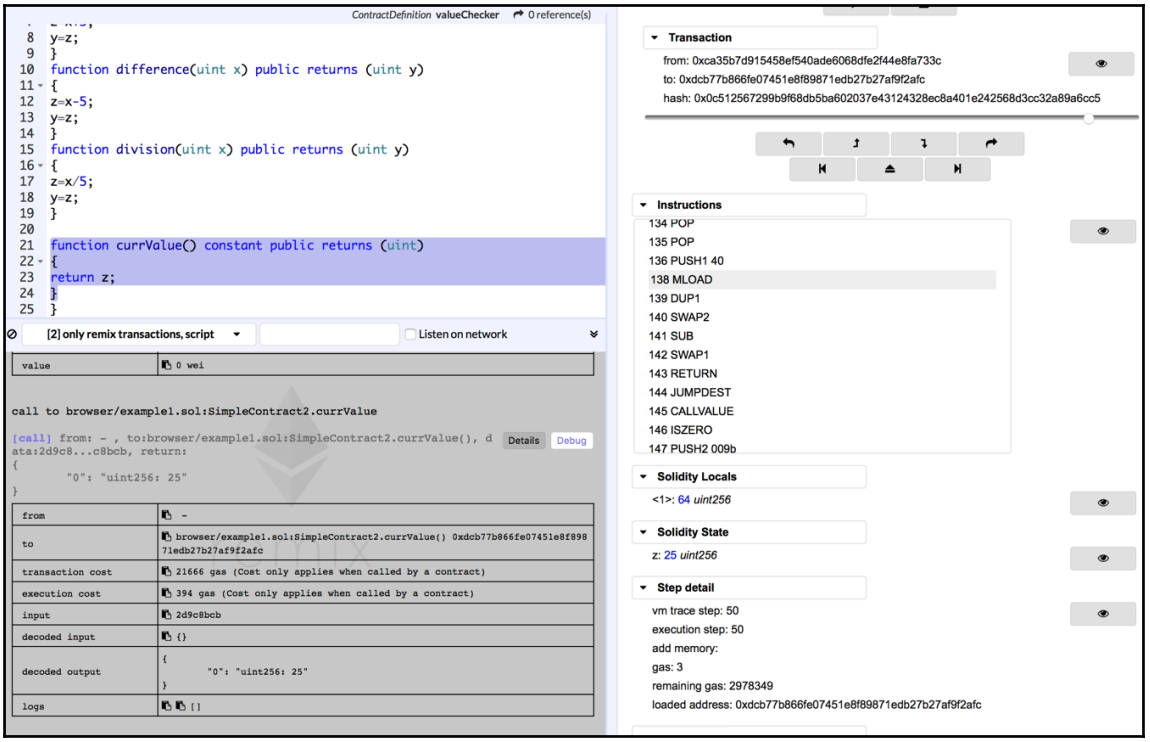


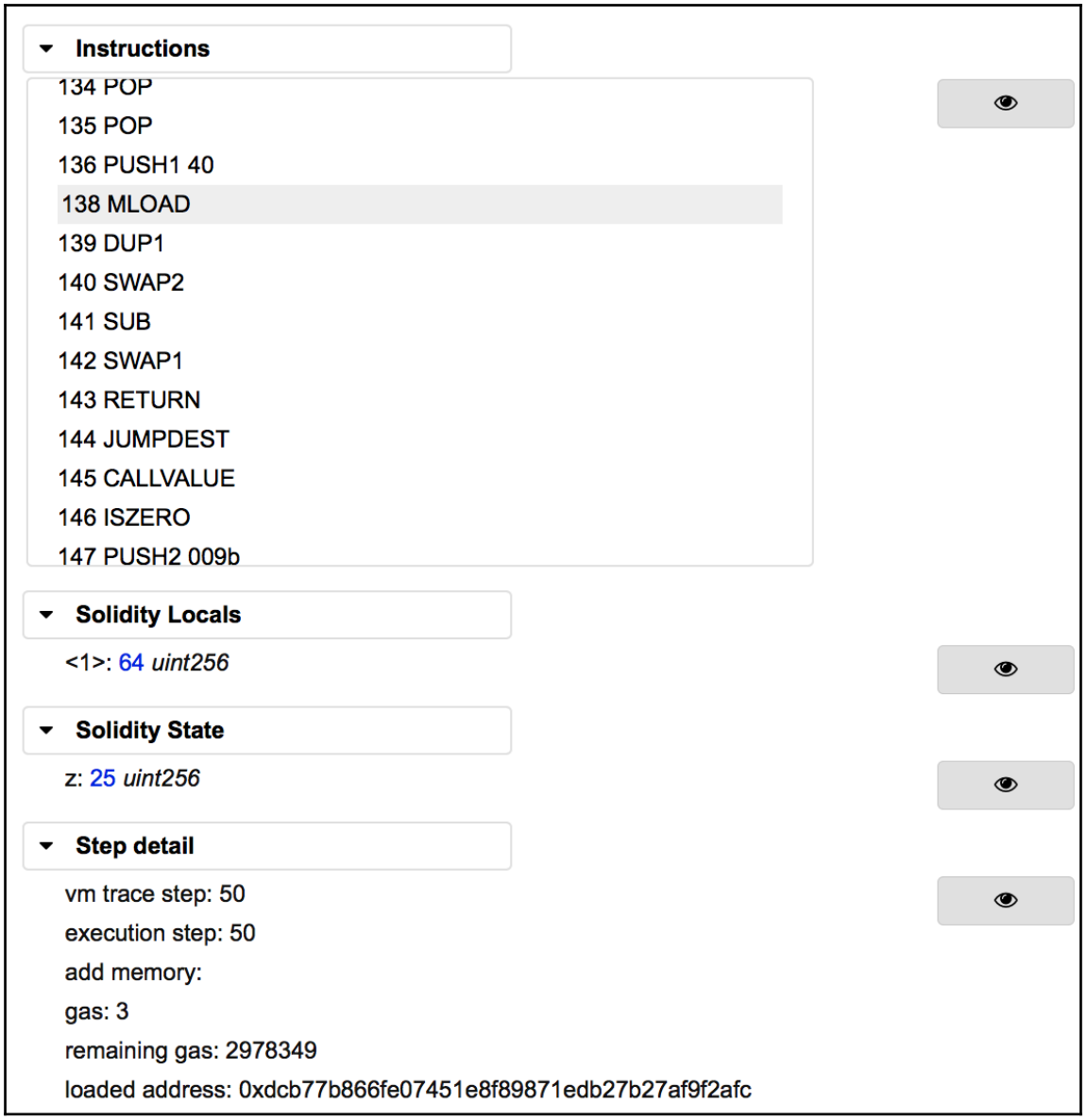

```
imrans-MacBook-Pro:~ drequinox$ solc --bin Addition.sol

======= Addition.sol:Addition =======
Binary:
6060604052341561000f57600080fd5b61010b8061001e6000396000f300606060405260043610604957600035 7c01000000
0000000000000000000000000000000000000000000000000000900463ffffffff16806336718d8014604e578063ac04e0a014
607d575b600080fd5b3415605857600080fd5b607b600480803560ff16906020019091908035 60ff16906020019091905050
60a9565b005b3415608757600080fd5b608d60c9565b604051808260ff1660ff16815260200191505060405180910390f35b
8082016000806101000a81548160ff021916908360ff160217905550505056 5b60008060009054906101000a900460ff1690
50905600a165627a7a7230582037bbf1721ae442876d01fa64f7feee6baac85d550db40825cf6dea392487369e0029
imrans-MacBook-Pro:~ drequinox$
```

```
imrans-MacBook-Pro:~ drequinox$ solc --gas Addition.sol

======= Addition.sol:Addition =======
Gas estimation:
construction:
   100 + 53400 = 53500
external:
   addx(uint8,uint8):   20475
   retrievex(): 464
imrans-MacBook-Pro:~ drequinox$
```

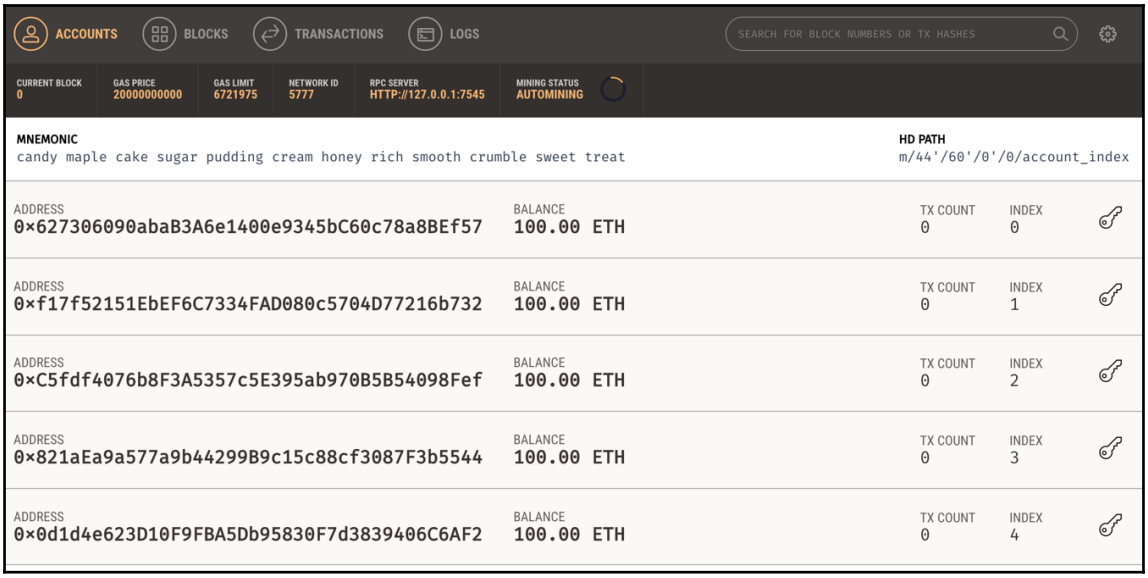
```
imrans-MacBook-Pro:bin drequinox$ cat Addition.abi
[{"constant":false,"inputs":[{"name":"y","type":"uint8"},{"name":"z","type":"uint8"}],"name":"addx","outputs":[]
,"payable":false,"stateMutability":"nonpayable","type":"function"},{"constant":true,"inputs":[],"name":"retrieve
x","outputs":[{"name":"","type":"uint8"}],"payable":false,"stateMutability":"view","type":"function"}]imrans-Mac
Book-Pro:bin drequinox$
imrans-MacBook-Pro:bin drequinox$
imrans-MacBook-Pro:bin drequinox$ cat Addition.bin
6060604052341561000f57600080fd5b60da8061001d6000396000f300606060405260043610604857763ffffffff7c0100000000000000000
0000000000000000000000000000000000000000000600035041663367 18d808114604d578063ac04e0a014606b575b600080fd5b3415605757
600080fd5b606960ff6004358116906024356091565b005b34156075576000080fd5b607b60a5565b60405160ff9091168152602001604 0
5180910390f35b6000805460ff19169190920160ff16179055565b60005460ff16905600a165627a7a72305820f7ca91776882f1c97964c8
29324591eb96e72adb62b5548a67f4ea22e9daf2b80029imrans-MacBook-Pro:bin drequinox$
imrans-MacBook-Pro:bin drequinox$
imrans-MacBook-Pro:bin drequinox$
```

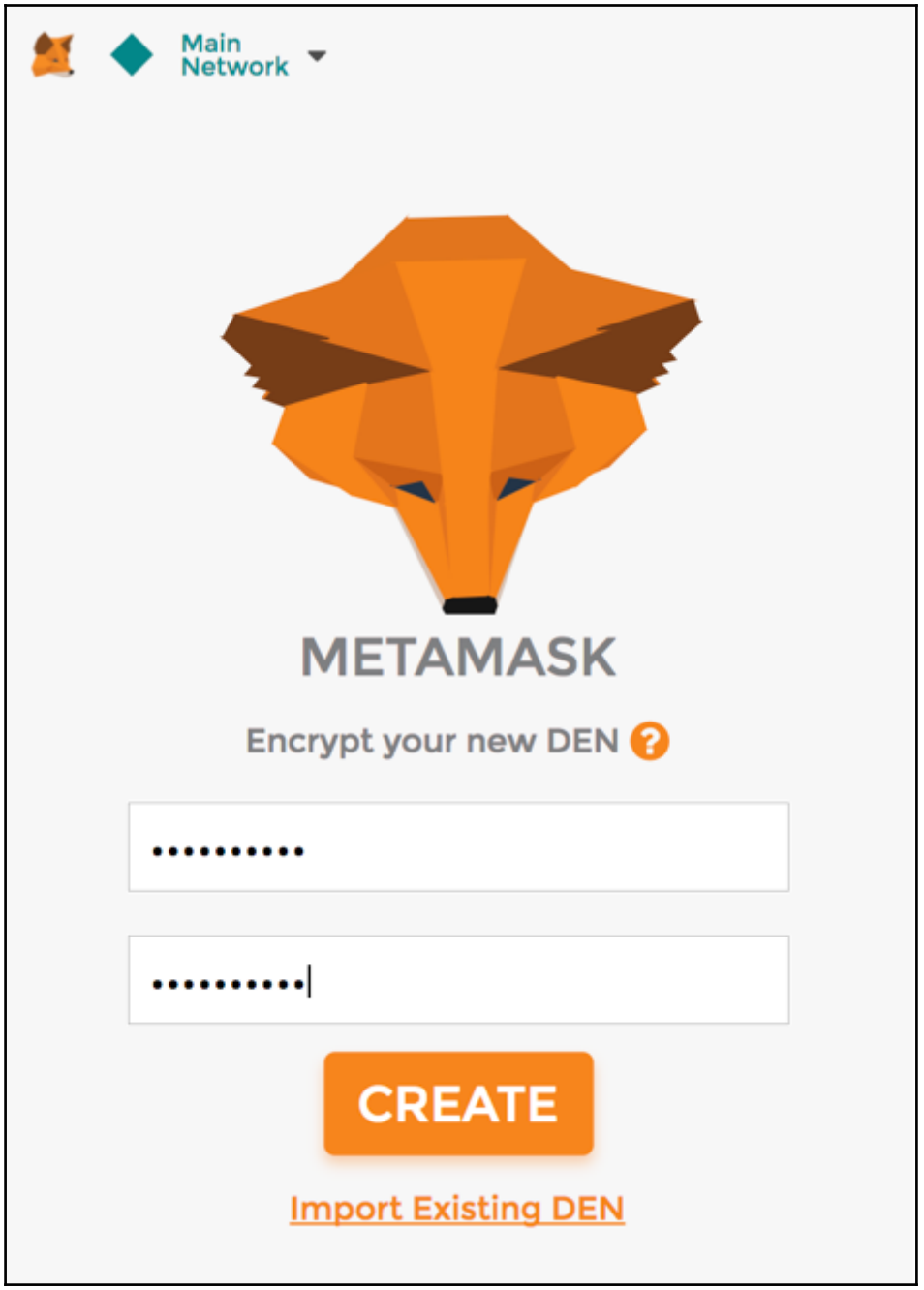


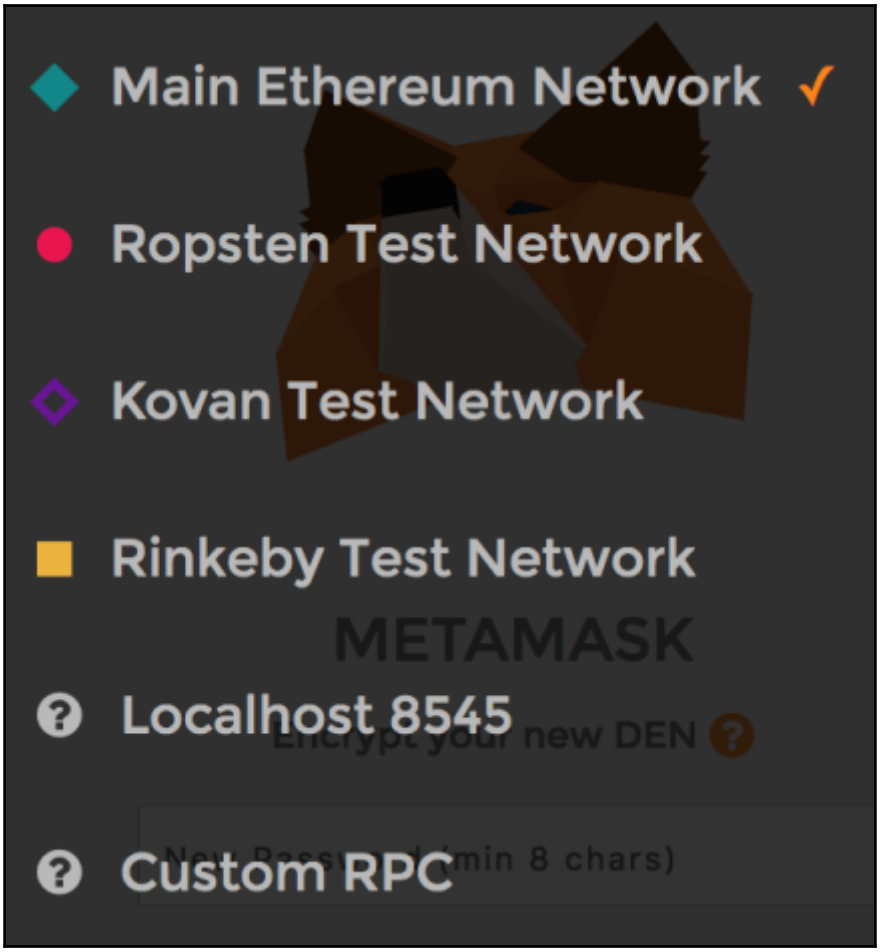

ContractDefinition valueChecker
0 reference(s)
y=z;
}
function difference(uint x) public returns (uint y)
{
z=x-5;
y=z;
}
function division(uint x) public returns (uint y)
{
z=x/5;
y=z;
}
function currValue() constant public returns (uint)
{
return z;
}
}
[2] only remix transactions, script
Listen on network
value
0 wei
call to browser/example1.sol:SimpleContract2.currValue
[call] from: - , to:browser/example1.sol:SimpleContract2.currValue(), data:2d9c8...c8bcb, return:
{
"0": "uint256: 25"
}
Details
Debug
from
-
to
browser/example1.sol:SimpleContract2.currValue() 0xdcb77b866fe07451e8f8987 1edb27b27af9f2afc
transaction cost
21666 gas (Cost only applies when called by a contract)
execution cost
394 gas (Cost only applies when called by a contract)
input
2d9c8bcb
decoded input
{}
decoded output
{
"0": "uint256: 25"
}
logs
[]
Transaction
from: 0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to: 0xdcb77b866fe07451e8f89871edb27b27af9f2afc
hash: 0x0c512567299b9f68db5ba602037e43124328ec8a401e242568d3cc32a89a6cc5
Instructions
134 POP
135 POP
136 PUSH1 40
138 MLOAD
139 DUP1
140 SWAP2
141 SUB
142 SWAP1
143 RETURN
144 JUMPDEST
145 CALLVALUE
146 ISZERO
147 PUSH2 009b
Solidity Locals
<1>: 64 uint256
Solidity State
z: 25 uint256
Step detail
vm trace step: 50
execution step: 50
add memory:
gas: 3
remaining gas: 2978349
loaded address: 0xdcb77b866fe07451e8f89871edb27b27af9f2afc

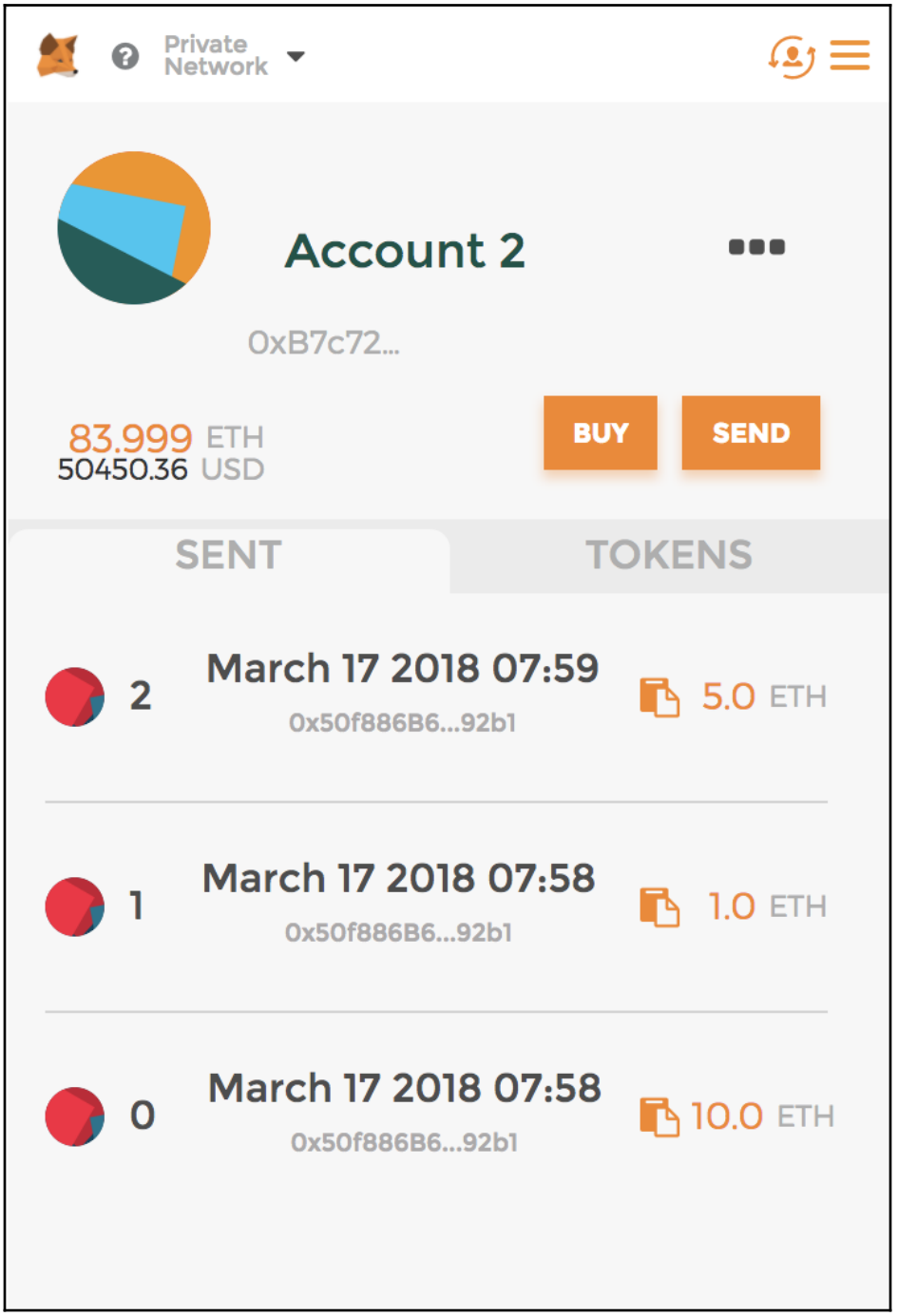

Instructions
134 POP
135 POP
136 PUSH1 40
138 MLOAD
139 DUP1
140 SWAP2
141 SUB
142 SWAP1
143 RETURN
144 JUMPDEST
145 CALLVALUE
146 ISZERO
147 PUSH2 009b
Solidity Locals
<1>: 64 uint256
Solidity State
z: 25 uint256
Step detail
vm trace step: 50
execution step: 50
add memory:
gas: 3
remaining gas: 2978349
loaded address: 0xdcb77b866fe07451e8f89871edb27b27af9f2afc

```
EthereumJS TestRPC v6.0.3 (ganache-core: 2.0.2)

Available Accounts
==================
(0) 0x6ca19d903eb53e00bb73622d275c965f2abad3d8
(1) 0x1f192daefa61ae050332e6a965e71fcf4621e887
(2) 0x97c0b2ea19a5b496e314e55d1e5a3a5d41b5ad21
(3) 0x3a04fbc6f8eb34b89918628a5a5fde4267e32e28
(4) 0x43e03d85a8a9328f510732be594993ac7011335c
(5) 0x6dfe1a7059df7a625c1ffaed0e97c42384b68446
(6) 0xb9992f167e68dc4bd4a1ce79c07b6193c4e72f37
(7) 0x46243dfcfb6d2d4ec60aa97ebbceac0f96aa33ab
(8) 0xe5b9c05dcb55ad987a504da7fb3dde4281d73bc4
(9) 0x37f6576fd633d95cbc29db28bbae4a272fe5594c

Private Keys
==================
(0) c82c6a860eeb57c8eedbd2e8bc59dc7c800f99118b7f1ef5540c41cdb10805dc
(1) 144271a65d21c59bd6f321659798b42e3d1a22feeb45c2c44f823db0477f330d
(2) d2a55f4406b23c8c18c55a6d30f4b4982ab17a01a6125f0d091e0d4807346905
(3) 1c16608a159b52ba84a0ae170d7642f3166712514693498109640dccf4cae8b9
(4) b7dea27d5bd105bb3e4fbf69598b561563557d343d4c89ea2d7d689f5a160554
(5) 10d6467570c50e103ade3694ef85cf9ae0f14cf331ddcd9faaae1f752ed766c5
(6) 7571ece88840db22a09d8e6062292c1e3d106c9e9d8d634f05d4524e75bfa50a
(7) 15e215703ba63d52c870392086f3474b78b5a1b0b6f276fe48c9aae6061f478d
(8) 5dd1fd136b3ba917922b011daaf55ce2b5fd3e332a1f0d39ad5bef664190ebdb
(9) 30e1850a76ee65fcfd565caf81fa7310ff239679816be51f0b04149afe4407e1

HD Wallet
==================
Mnemonic:      prepare flavor identify liquid twice tip bullet blanket vast vivid hunt now
Base HD Path:  m/44'/60'/0'/0/{account_index}

Listening on localhost:8545
```

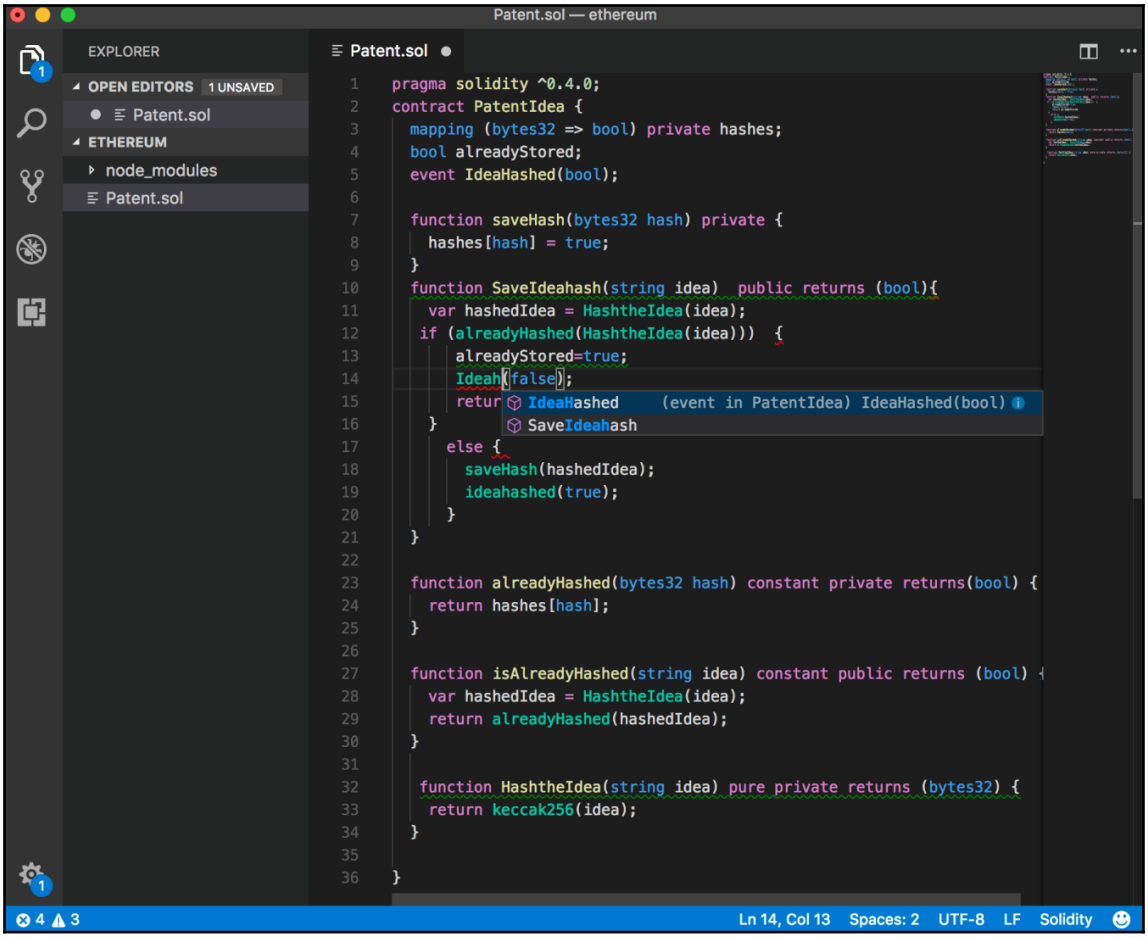

ACCOUNTS
BLOCKS
TRANSACTIONS
LOGS
SEARCH FOR BLOCK NUMBERS OR TX HASHES
CURRENT BLOCK 0
GAS PRICE 20000000000
GAS LIMIT 6721975
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
MNEMONIC
candy maple cake sugar pudding cream honey rich smooth crumble sweet treat
HD PATH
m/44'/60'/0'/0/account_index
ADDRESS 0x627306090abaB3A6e1400e9345bC60c78a8BEf57 BALANCE 100.00 ETH TX COUNT 0 INDEX 0
ADDRESS 0xf17f52151EbEF6C7334FAD080c5704D77216b732 BALANCE 100.00 ETH TX COUNT 0 INDEX 1
ADDRESS 0xC5fdf4076b8F3A5357c5E395ab970B5B54098Fef BALANCE 100.00 ETH TX COUNT 0 INDEX 2
ADDRESS 0x821aEa9a577a9b44299B9c15c88cf3087F3b5544 BALANCE 100.00 ETH TX COUNT 0 INDEX 3
ADDRESS 0x0d1d4e623D10F9FBA5Db95830F7d3839406C6AF2 BALANCE 100.00 ETH TX COUNT 0 INDEX 4


Main
Network
METAMASK
Encrypt your new DEN
CREATE
Import Existing DEN


Main Ethereum Network
Ropsten Test Network
Kovan Test Network
Rinkeby Test Network
METAMASK
Localhost 8545
Custom RPC


Private Network
Account 2
0xB7c72...
83.999 ETH
50450.36 USD
BUY
SEND
SENT
TOKENS
2
March 17 2018 07:59
0x50f886B6...92b1
5.0 ETH
1
March 17 2018 07:58
0x50f886B6...92b1
1.0 ETH
0
March 17 2018 07:58
0x50f886B6...92b1
10.0 ETH

```
Truffle v4.0.1 - a development framework for Ethereum

Usage: truffle <command> [options]

Commands:
  init      Initialize new Ethereum project with example contracts and tests
  compile   Compile contract source files
  migrate   Run migrations to deploy contracts
  deploy    (alias for migrate)
  build     Execute build pipeline (if configuration present)
  test      Run Mocha and Solidity tests
  debug     Interactively debug any transaction on the blockchain (experimental)
  opcode    Print the compiled opcodes for a given contract
  console   Run a console with contract abstractions and commands available
  develop   Open a console with a local TestRPC
  create    Helper to create new contracts, migrations and tests
  install   Install a package from the Ethereum Package Registry
  publish   Publish a package to the Ethereum Package Registry
  networks  Show addresses for deployed contracts on each network
  watch     Watch filesystem for changes and rebuild the project automatically
  serve     Serve the build directory on localhost and watch for changes
  exec      Execute a JS module within this Truffle environment
  unbox     Unbox Truffle project
  version   Show version number and exit

See more at http://truffleframework.com/docs
```


Patent.sol — ethereum
EXPLORER
OPEN EDITORS 1 UNSAVED
Patent.sol
ETHEREUM
node_modules
Patent.sol
Patent.sol
pragma solidity ^0.4.0;
contract PatentIdea {
mapping (bytes32 => bool) private hashes;
bool alreadyStored;
event IdeaHashed(bool);
function saveHash(bytes32 hash) private {
hashes[hash] = true;
}
function SaveIdeahash(string idea) public returns (bool){
var hashedIdea = HashtheIdea(idea);
if (alreadyHashed(HashtheIdea(idea))) {
alreadyStored=true;
Ideah(false);
retur
IdeaHashed (event in PatentIdea) IdeaHashed(bool)
SaveIdeahash
}
else {
saveHash(hashedIdea);
ideahashed(true);
}
}
function alreadyHashed(bytes32 hash) constant private returns(bool) {
return hashes[hash];
}
function isAlreadyHashed(string idea) constant public returns (bool) {
var hashedIdea = HashtheIdea(idea);
return alreadyHashed(hashedIdea);
}
function HashtheIdea(string idea) pure private returns (bytes32) {
return keccak256(idea);
}
}
4 3
Ln 14, Col 13
Spaces: 2
UTF-8
LF
Solidity

FUNCTIONHASHES

```
{
    "f9d55e21": "Matcher(uint8)"
}
```

```
pragma solidity ^0.4.0; //specify the 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 declare and initialized with value 10
    event valueEvent(bool returnValue);
    function Matcher (uint8 x) returns (bool)
    {
        if ( x >= price)
        {
            valueEvent(true);
            return true;
        }
    }
}
```

Chapter 14: Introducing Web3

```
> 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)
}
>
```

```
1  pragma solidity ^0.4.0;
2  contract valueChecker
3  {
4      uint price=10;
5  event valueEvent(bool returnValue);
6  function Matcher (uint8 x) public returns (bool)
7  {
8      if (x>=price){valueEvent(true);
9      return true;
10
11     }}}
```

Start to compile Auto compile

valueChecker Details Publish on Swarm

valueChecker

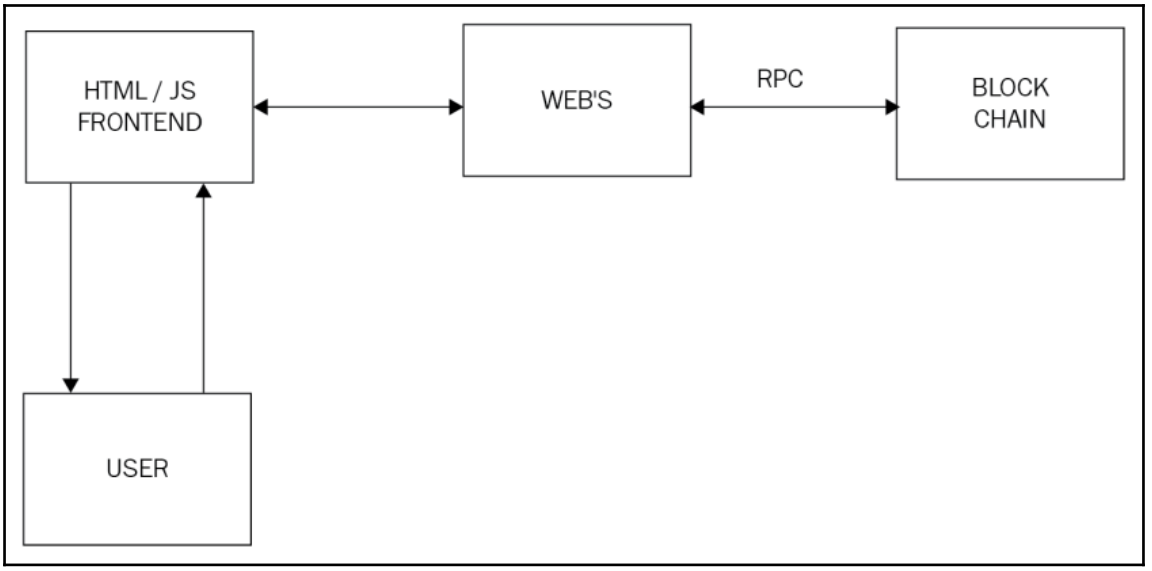
WEB3DEPLOY

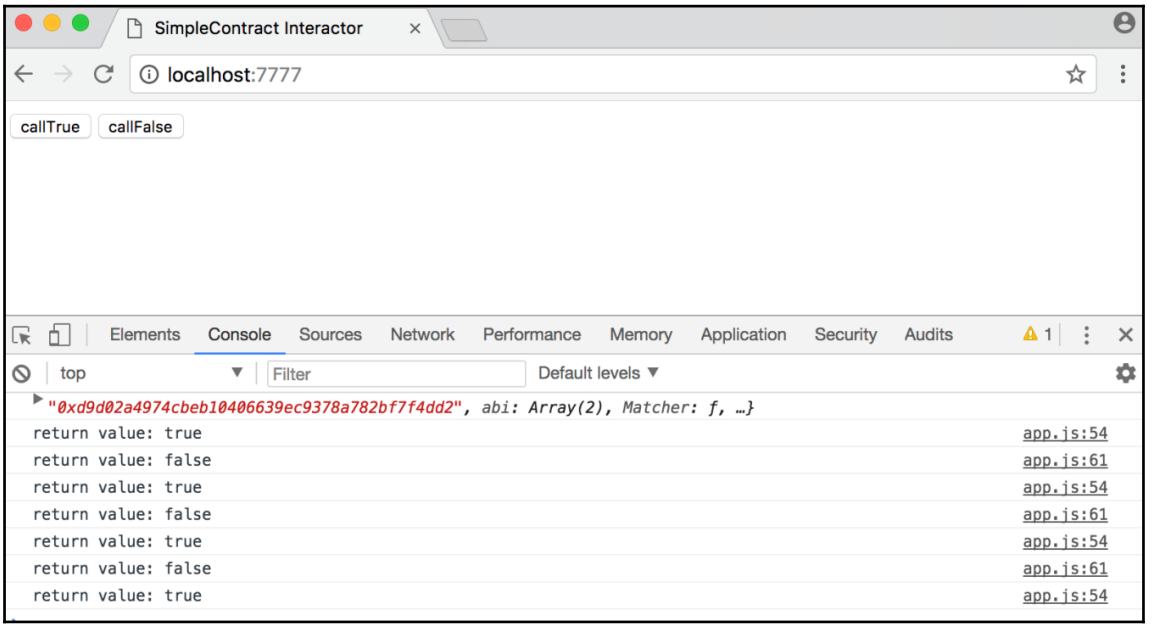
Copy value to clipboard

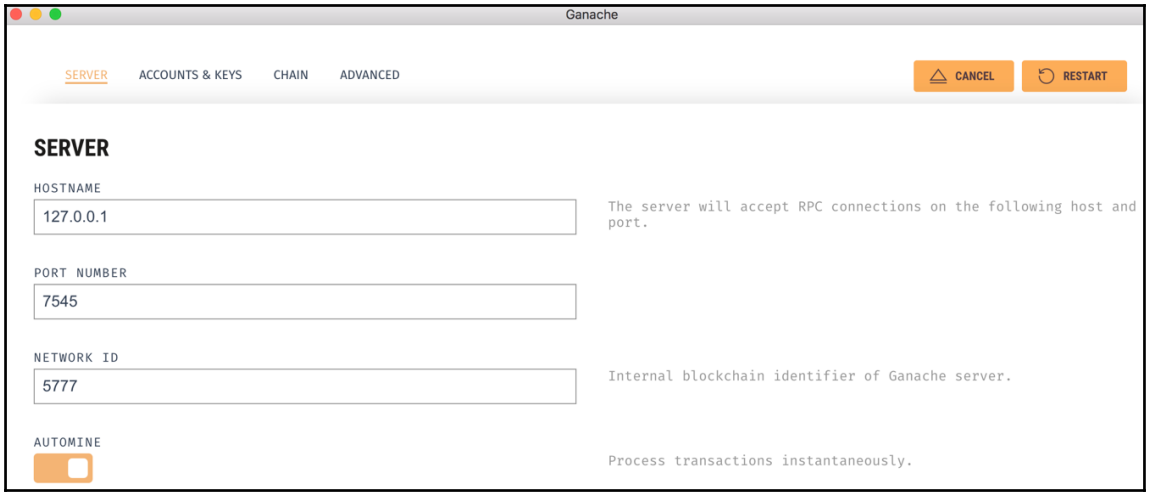
```
var valuecheckerContract = web3.eth.contract([{"constant":false,"inpu
ts":[{"name":"x","type":"uint8"}],"name":"Matcher","outputs":[{"name"
:"","type":"bool"}],"payable":false,"stateMutability":"nonpayable","t
ype":"function"},{"anonymous":false,"inputs":[{"indexed":false,"name"
:"returnValue","type":"bool"}],"name":"valueEvent","type":"event"}]);
var valuechecker = valuecheckerContract.new(
   {
     from: web3.eth.accounts[0],
     data: '0x6060604052600a60005534156100145760008fd5b6101038061002
36000396000f300606060405260043610603f576000357c010000000000000000000
000000000000000000000000000000000000000900463ffffffff168063f9d55e2114604
4575b600080fd5b3415604e57600080fd5b6065600480803560ff1690602001909190
5050607f565b604051808215151515815260200191505060405180910390f35b60008
0548260ff1610151560d1577f3eb1a229ff7995457774a4bd31ef7b13b6f4491ad1eb
b8961af120b8b4b6239c60016040518082151515158152602001915050604051809010
390a16001905060d2565b5b9190505600a165627a7a723058205b1d9d0f31b39806b7
782fdb9360af93d5b5f66a36f6f4023ee1aa9ca12782b70029',
     gas: '4700000'
   }, function (e, contract){
    console.log(e, contract);
    if (typeof contract.address !== 'undefined') {
         console.log('Contract mined! address: ' + contract.address +
 ' transactionHash: ' + contract.transactionHash);
    }
 })
```

```
> personal.unlockAccount(personal.listAccounts[0])
Unlock account 0xcf61d213faa9acadbf0d110e1397caf20445c58f
Passphrase:
true
> var valuecheckerContract = web3.eth.contract([{"constant":false,"inputs":[{"name":"x","type":"uint8"}],"name":"Matcher","ou
tputs":[{"name":"","type":"bool"}],"payable":false,"stateMutability":"nonpayable","type":"function"},{"anonymous":false,"inpu
ts":[{"indexed":false,"name":"returnValue","type":"bool"}],"name":"valueEvent","type":"event"}]);
undefined
> var valuechecker = valuecheckerContract.new(
...    {
......      from: web3.eth.accounts[0],
......      data: '0x6060604052600a600055341561001457600080fd5b6101038061002360003960000f300606060405260043610603f576000357c01
0000000000000000000000000000000000000000000000000000000000900463ffffffff168063f9d55e21146044575b600080fd5b3415604e57600080fd5b6
065600480803560ff16906020019091905050607f565b60405180821515151581526020019150506040518091039035b600080548260ff1610151560d157
7f3eb1a229ff7995457774a4bd31ef7b13b6f4491ad1ebb8961af120b8b4b6239c60016040518082151515158152602001915050604051809103903a160019
05060d2565b5b9190505600a165627a7a723058205b1d9d0f31b39806b7782fdb9360af93d5b5f66a36f6f4023ee1aa9ca12782b70029',
......      gas: '4700000'
......    }, function (e, contract){
......     console.log(e, contract);
......     if (typeof contract.address !== 'undefined') {
.........          console.log('Contract mined! address: ' + contract.address + ' transactionHash: ' + contract.transactionHa
sh);
.........     }
......  })
null [object Object]
undefined
```

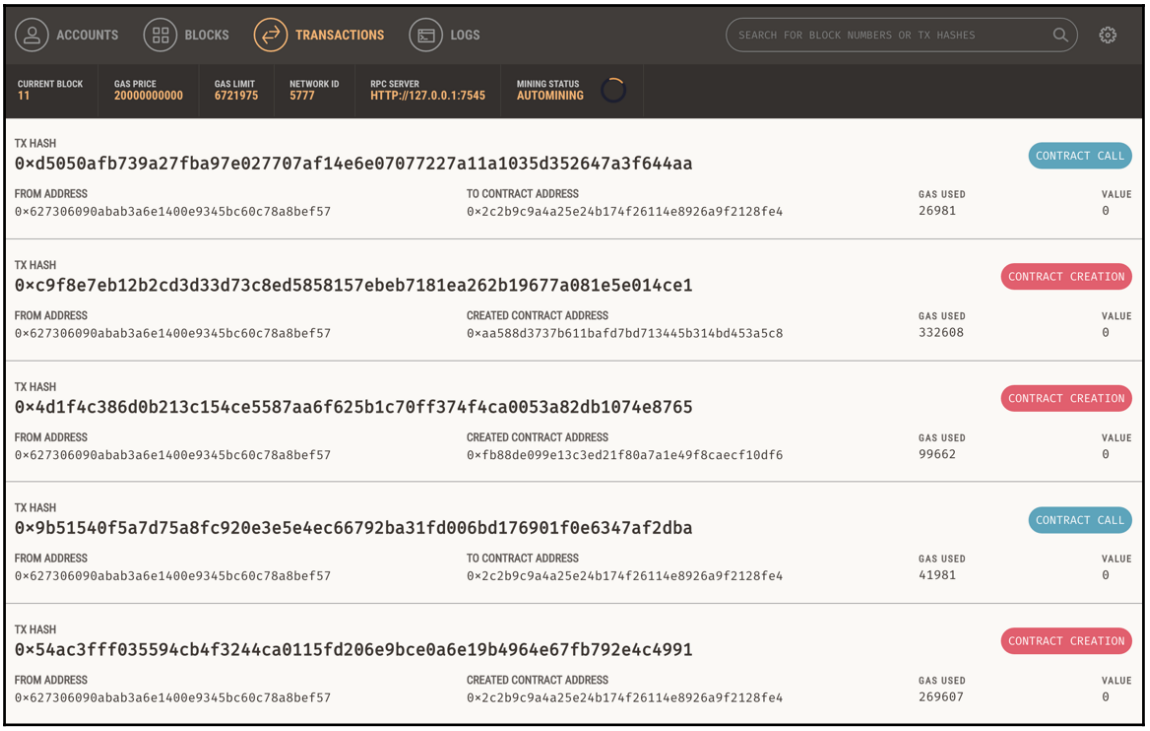
```
> valuechecker.
valuechecker.Matcher         valuechecker.abi             valuechecker.allEvents       valuechecker.transactionHash
valuechecker._eth            valuechecker.address         valuechecker.constructor     valuechecker.valueEvent
> valuechecker.abi
[{
    constant: false,
    inputs: [{
        name: "x",
        type: "uint8"
    }],
    name: "Matcher",
    outputs: [{
        name: "",
        type: "bool"
    }],
    payable: false,
    stateMutability: "nonpayable",
    type: "function"
}, {
    anonymous: false,
    inputs: [{
        indexed: false,
        name: "returnValue",
        type: "bool"
    }],
    name: "valueEvent",
    type: "event"
}]
> valuechecker.address
"0xbd663c5136155cb6d7ed55446888271dcd5092bc"
>
```

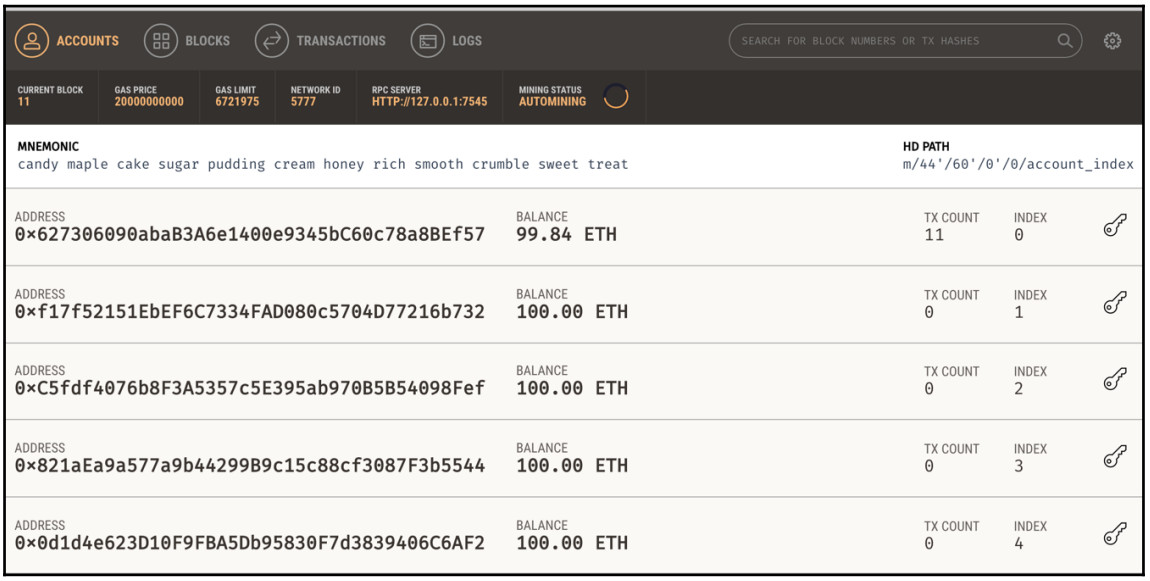

HTML / JS
FRONTEND
WEB'S
RPC
BLOCK
CHAIN
USER


SimpleContract Interactor
localhost:7777
callTrue
callFalse
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
top
Filter
Default levels
"0xd9d02a4974cbeb10406639ec9378a782bf7f4dd2", abi: Array(2), Matcher: f, …}
return value: true app.js:54
return value: false app.js:61
return value: true app.js:54
return value: false app.js:61
return value: true app.js:54
return value: false app.js:61
return value: true app.js:54




```
Using network 'development'.

Running migration: 1_initial_migration.js
  Deploying Migrations...
  ... 0x54ac3fff035594cb4f3244ca0115fd206e9bce0a6e19b4964e67fb792e4c4991
  Migrations: 0x2c2b9c9a4a25e24b174f26114e8926a9f2128fe4
Saving successful migration to network...
  ... 0x9b51540f5a7d75a8fc920e3e5e4ec66792ba31fd006bd176901f0e6347af2dba
Saving artifacts...
Running migration: 2_deploy_contracts.js
  Deploying ConvertLib...
  ... 0x4d1f4c386d0b213c154ce5587aa6f625b1c70ff374f4ca0053a82db1074e8765
  ConvertLib: 0xfb88de099e13c3ed21f80a7a1e49f8caecf10df6
  Linking ConvertLib to MetaCoin
  Deploying MetaCoin...
  ... 0xc9f8e7eb12b2cd3d33d73c8ed5858157ebeb7181ea262b19677a081e5e014ce1
  MetaCoin: 0xaa588d3737b611bafd7bd713445b314bd453a5c8
Saving successful migration to network...
  ... 0xd5050afb739a27fba97e027707af14e6e07077227a11a1035d352647a3f644aa
Saving artifacts...
```


ACCOUNTS
BLOCKS
TRANSACTIONS
LOGS
SEARCH FOR BLOCK NUMBERS OR TX HASHES
CURRENT BLOCK 11
GAS PRICE 20000000000
GAS LIMIT 6721975
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
TX HASH
0×d5050afb739a27fba97e027707af14e6e07077227a11a1035d352647a3f644aa
CONTRACT CALL
FROM ADDRESS
0×627306090abab3a6e1400e9345bc60c78a8bef57
TO CONTRACT ADDRESS
0×2c2b9c9a4a25e24b174f26114e8926a9f2128fe4
GAS USED
26981
VALUE
0
TX HASH
0×c9f8e7eb12b2cd3d33d73c8ed5858157ebeb7181ea262b19677a081e5e014ce1
CONTRACT CREATION
FROM ADDRESS
0×627306090abab3a6e1400e9345bc60c78a8bef57
CREATED CONTRACT ADDRESS
0×aa588d3737b611bafd7bd713445b314bd453a5c8
GAS USED
332608
VALUE
0
TX HASH
0×4d1f4c386d0b213c154ce5587aa6f625b1c70ff374f4ca0053a82db1074e8765
CONTRACT CREATION
FROM ADDRESS
0×627306090abab3a6e1400e9345bc60c78a8bef57
CREATED CONTRACT ADDRESS
0×fb88de099e13c3ed21f80a7a1e49f8caecf10df6
GAS USED
99662
VALUE
0
TX HASH
0×9b51540f5a7d75a8fc920e3e5e4ec66792ba31fd006bd176901f0e6347af2dba
CONTRACT CALL
FROM ADDRESS
0×627306090abab3a6e1400e9345bc60c78a8bef57
TO CONTRACT ADDRESS
0×2c2b9c9a4a25e24b174f26114e8926a9f2128fe4
GAS USED
41981
VALUE
0
TX HASH
0×54ac3fff035594cb4f3244ca0115fd206e9bce0a6e19b4964e67fb792e4c4991
CONTRACT CREATION
FROM ADDRESS
0×627306090abab3a6e1400e9345bc60c78a8bef57
CREATED CONTRACT ADDRESS
0×2c2b9c9a4a25e24b174f26114e8926a9f2128fe4
GAS USED
269607
VALUE
0


ACCOUNTS
BLOCKS
TRANSACTIONS
LOGS
SEARCH FOR BLOCK NUMBERS OR TX HASHES
CURRENT BLOCK 11
GAS PRICE 20000000000
GAS LIMIT 6721975
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
MNEMONIC
candy maple cake sugar pudding cream honey rich smooth crumble sweet treat
HD PATH
m/44'/60'/0'/0/account_index
ADDRESS
0×627306090abaB3A6e1400e9345bC60c78a8BEf57
BALANCE
99.84 ETH
TX COUNT
11
INDEX
0
ADDRESS
0×f17f52151EbEF6C7334FAD080c5704D77216b732
BALANCE
100.00 ETH
TX COUNT
0
INDEX
1
ADDRESS
0×C5fdf4076b8F3A5357c5E395ab970B5B54098Fef
BALANCE
100.00 ETH
TX COUNT
0
INDEX
2
ADDRESS
0×821aEa9a577a9b44299B9c15c88cf3087F3b5544
BALANCE
100.00 ETH
TX COUNT
0
INDEX
3
ADDRESS
0×0d1d4e623D10F9FBA5Db95830F7d3839406C6AF2
BALANCE
100.00 ETH
TX COUNT
0
INDEX
4

```
> truffle-init-webpack@0.0.2 dev /Users/drequinox/dapp1
> webpack-dev-server

Project is running at http://localhost:8080/
webpack output is served from /
Hash: 157d6514272a12586aba
Version: webpack 2.7.0
Time: 6702ms
     Asset       Size  Chunks                    Chunk Names
    app.js    1.65 MB       0  [emitted]  [big]  main
index.html  925 bytes          [emitted]
chunk    {0} app.js (main) 1.63 MB [entry] [rendered]
   [71] ./app/javascripts/app.js 3.64 kB {0} [built]
   [72] (webpack)-dev-server/client?http://localhost:8080 7.95 kB {0} [built]
   [73] ./build/contracts/MetaCoin.json 23.8 kB {0} [built]
  [111] ./~/loglevel/lib/loglevel.js 7.86 kB {0} [built]
  [117] ./~/querystring-es3/index.js 127 bytes {0} [built]
  [119] ./~/strip-ansi/index.js 161 bytes {0} [built]
  [122] ./app/stylesheets/app.css 905 bytes {0} [built]
  [163] ./~/truffle-contract/index.js 2.64 kB {0} [built]
  [197] ./~/url/url.js 23.3 kB {0} [built]
  [199] ./~/web3/index.js 193 bytes {0} [built]
  [233] (webpack)-dev-server/client/overlay.js 3.73 kB {0} [built]
  [234] (webpack)-dev-server/client/socket.js 1.05 kB {0} [built]
  [235] (webpack)/hot nonrecursive ^\.\/log$ 160 bytes {0} [built]
  [236] (webpack)/hot/emitter.js 77 bytes {0} [built]
  [237] multi (webpack)-dev-server/client?http://localhost:8080 ./app/javascripts/app.js 40 bytes {0} [built]
    + 223 hidden modules
webpack: Compiled successfully.
```

MetaCoin Example Truffle Dapp

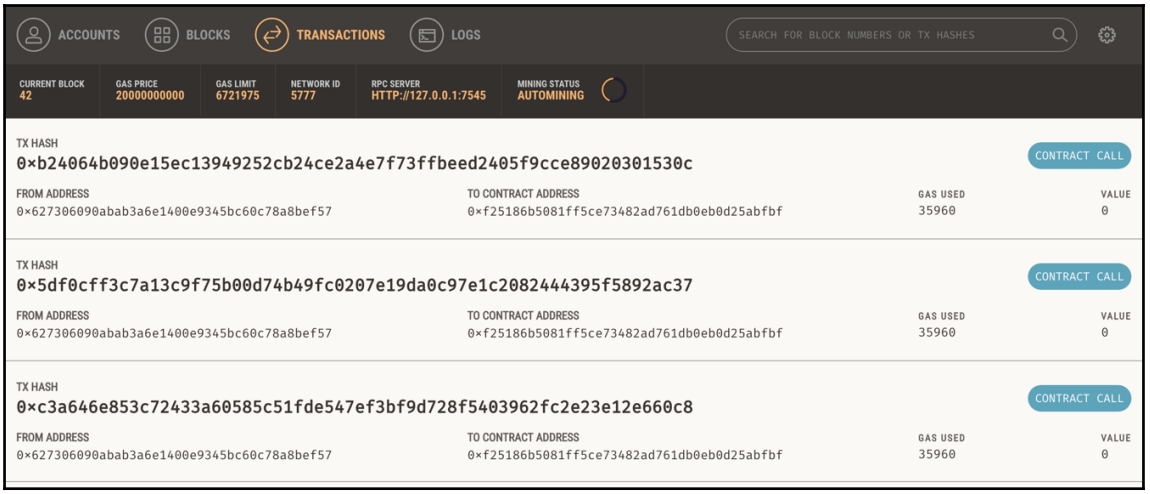
You have 8680 META

Send MetaCoin

Amount: 55

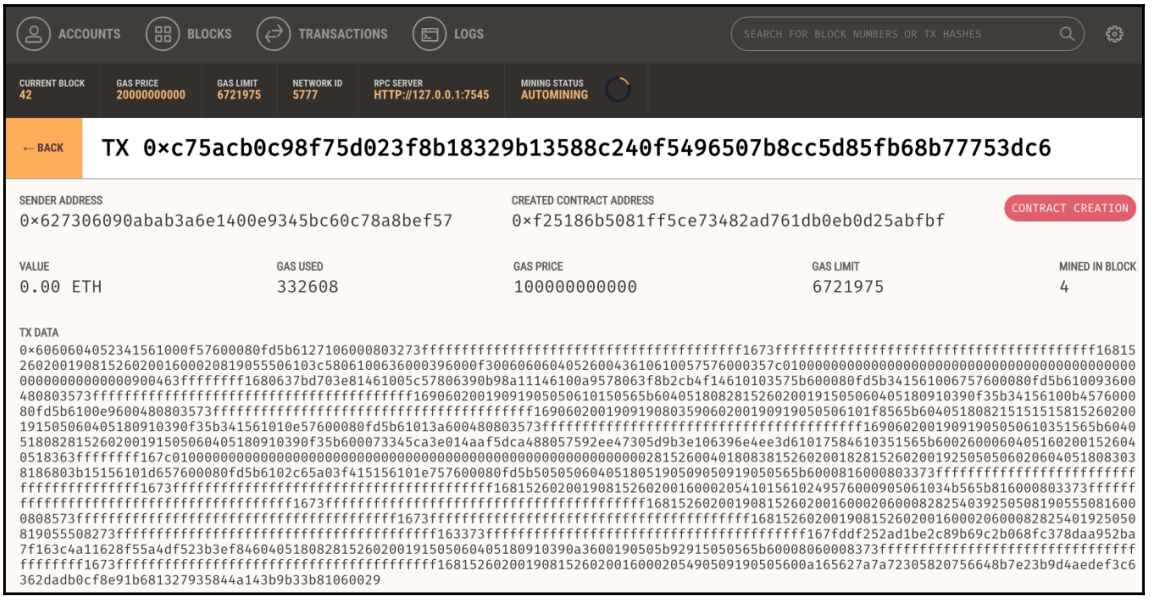
To Address: 0xf17f52151EbEF6C7334FAD080c5704D77216b732

Send MetaCoin

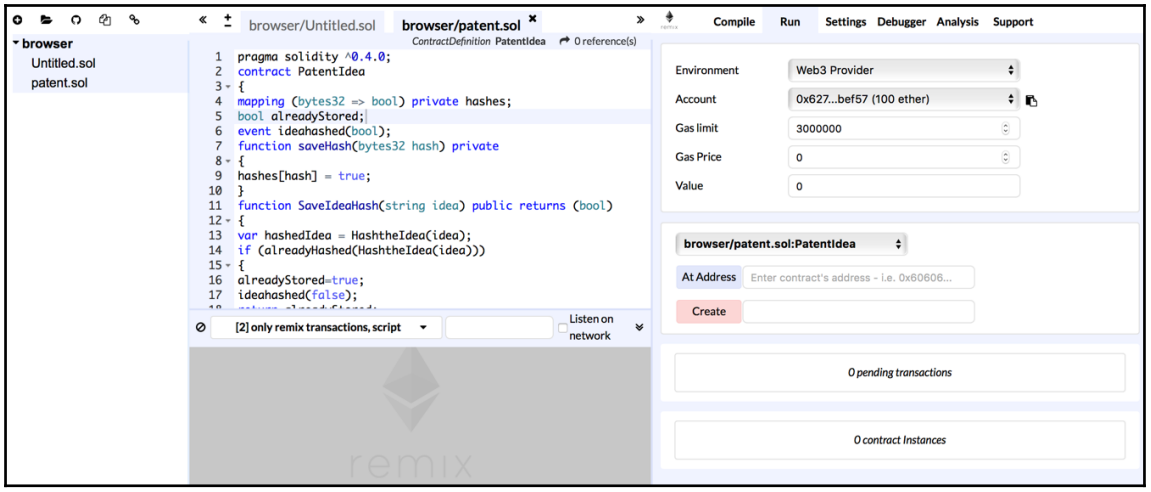


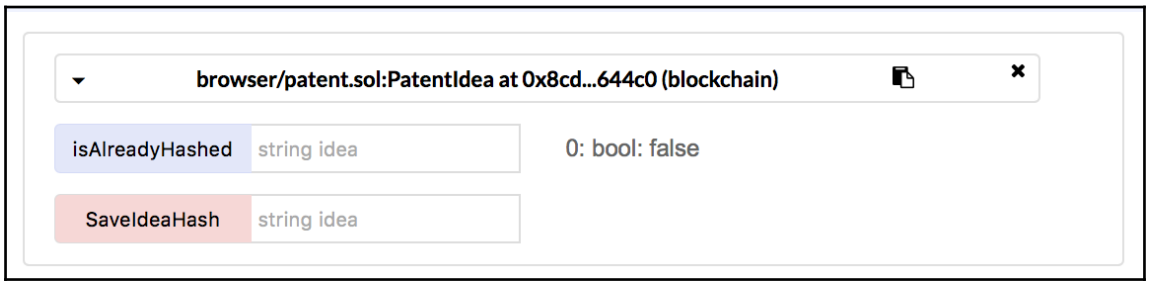

```
drequinox@drequinox-OP7010:~/testdapp$ truffle console
truffle(default)>
```

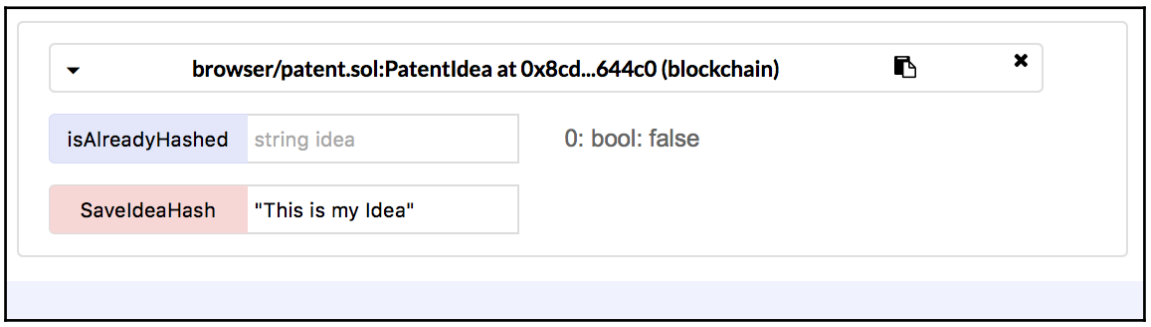
```
drequinox@drequinox-OP7010:~/testdapp$ truffle console
truffle(default)> MetaCoin.
MetaCoin.__defineGetter__      MetaCoin.__defineSetter__      MetaCoin.__lookupGetter__      MetaCoin.__lookupSetter__
MetaCoin.__proto__             MetaCoin.constructor           MetaCoin.hasOwnProperty        MetaCoin.isPrototypeOf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




```
truffle(development)> Addition.at(Addition.address).addx(100,100)
{ tx: '0xd58f346b76c1d878b67e7318bd4f2f4acb53418d4632efafa35bf939f0181cac',
  receipt:
   { transactionHash: '0xd58f346b76c1d878b67e7318bd4f2f4acb53418d4632efafa35bf939f0181cac',
     transactionIndex: 0,
     blockHash: '0x9215c0d4f7e5f2861b68bc8d097e017c65751dbaf4fe73c1a5729f97ac4315de',
     blockNumber: 41,
     gasUsed: 27131,
     cumulativeGasUsed: 27131,
     contractAddress: null,
     logs: [],
     status: 1 },
  logs: [] }
truffle(development)> Addition.at(Addition.address).retrievex()
{ [String: '200'] s: 1, e: 2, c: [ 200 ] }
truffle(development)>
```

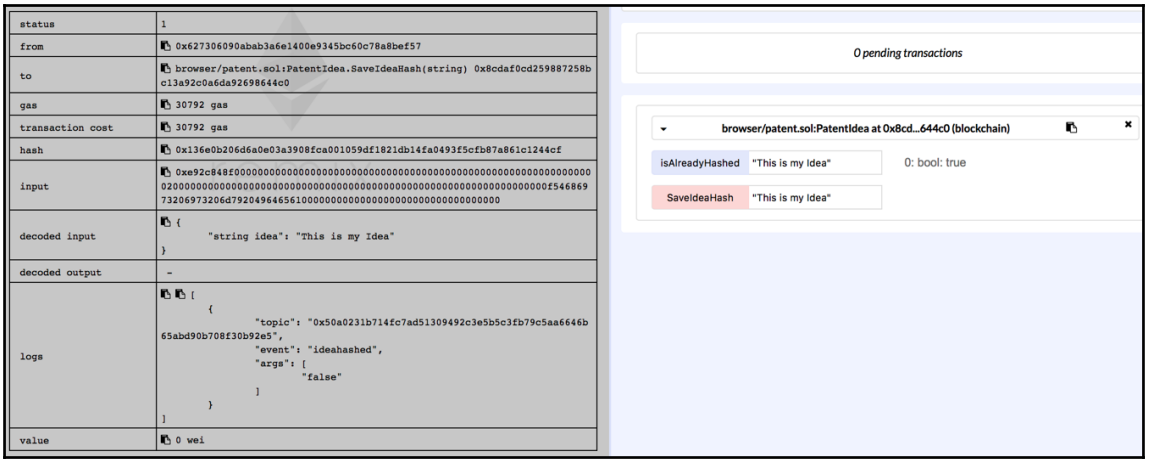

browser
Untitled.sol
patent.sol
browser/Untitled.sol
browser/patent.sol
ContractDefinition PatentIdea
0 reference(s)
pragma solidity ^0.4.0;
contract PatentIdea
{
mapping (bytes32 => bool) private hashes;
bool alreadyStored;
event ideahashed(bool);
function saveHash(bytes32 hash) private
{
hashes[hash] = true;
}
function SaveIdeaHash(string idea) public returns (bool)
{
var hashedIdea = HashtheIdea(idea);
if (alreadyHashed(HashtheIdea(idea)))
{
alreadyStored=true;
ideahashed(false);
[2] only remix transactions, script
Listen on network
Compile
Run
Settings
Debugger
Analysis
Support
Environment
Web3 Provider
Account
0x627...bef57 (100 ether)
Gas limit
3000000
Gas Price
0
Value
0
browser/patent.sol:PatentIdea
At Address
Enter contract's address - i.e. 0x60606...
Create
0 pending transactions
0 contract Instances


browser/patent.sol:PatentIdea at 0x8cd...644c0 (blockchain)
isAlreadyHashed
string idea
0: bool: false
SaveIdeaHash
string idea

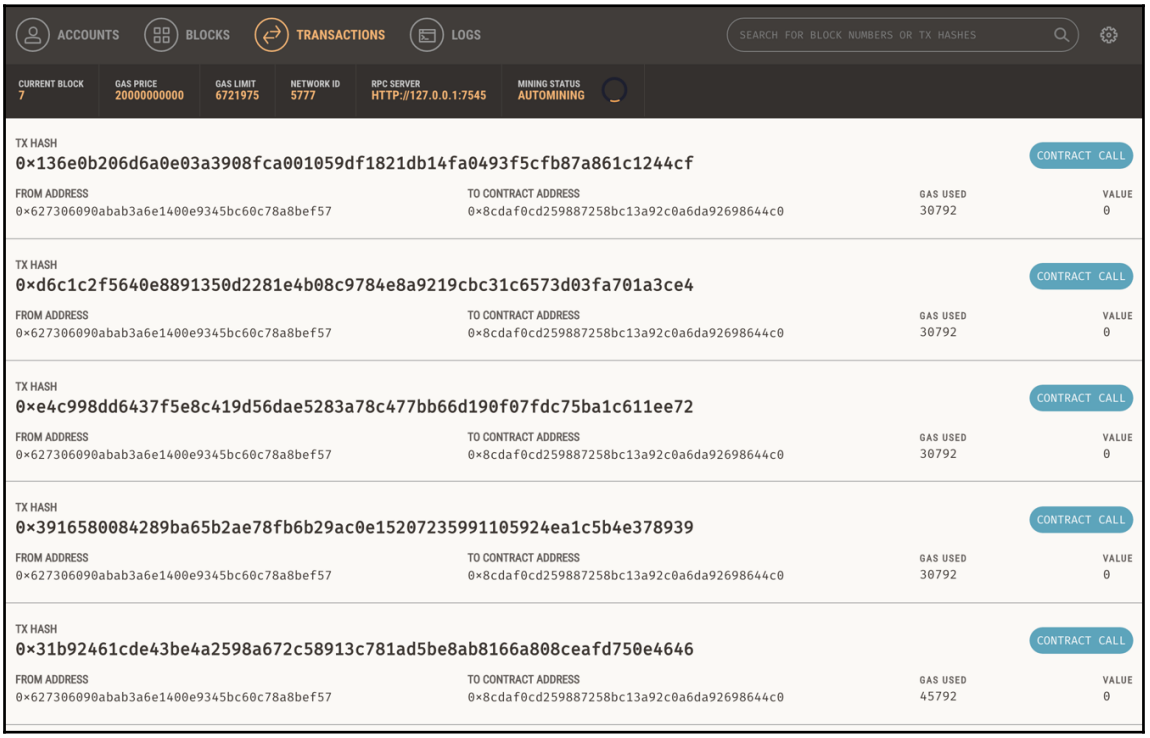

browser/patent.sol:PatentIdea at 0x8cd...644c0 (blockchain)
isAlreadyHashed
string idea
0: bool: false
SaveIdeaHash
"This is my Idea"

[block:2 txIndex:0] from:0x627...bef57, to:browser/patent.sol:PatentIdea.SaveIdeaHash(string) 0x8cd...644c0, value:0 wei, 1 logs, data:0xe92...00000, hash:0x783...0a2fc Details Debug

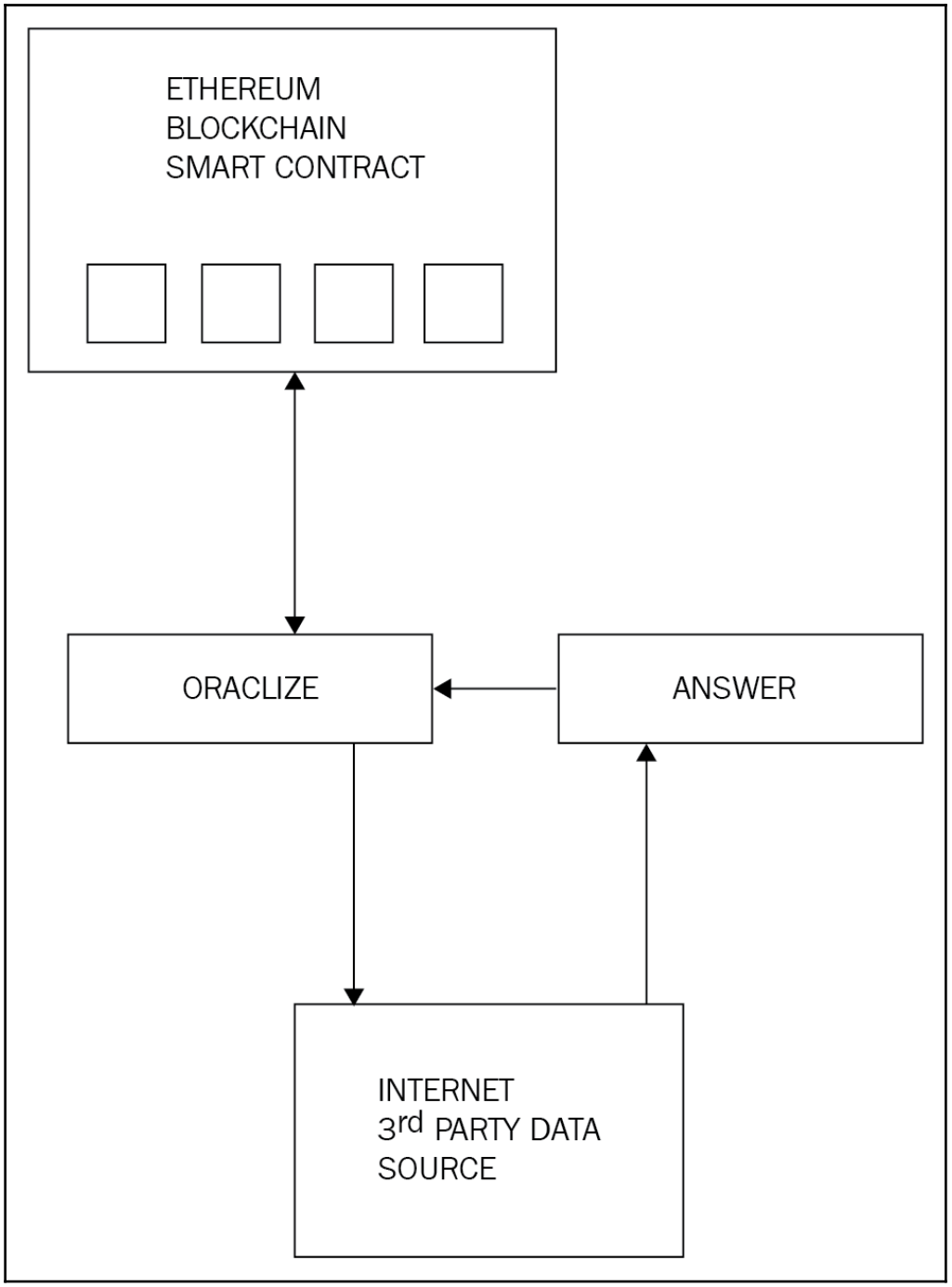
status	1
from	0x627306090abab3a6e1400e9345bc60c78a8bef57
to	browser/patent.sol:PatentIdea.SaveIdeaHash(string) 0x8cdaf0cd259887258bc13a92c0a6da92698644c0
gas	45663 gas
transaction cost	45663 gas
hash	0x7834e933d99861237281906f7f9b92ae8f0ee7c3e9c3005942e4a5efc330a2fc
input	0xe92c848f0000000000000000000000000000000000000000000000000000000000000020000000000000000000000000000000000000000000000000000000000000000f54686973206973206d7920496465610000000000000000000000000000000000
decoded input	{ "string idea": "This is my Idea" }
decoded output	-
logs	[{ "topic": "0x50a0231b714fc7ad51309492c3e5b5c3fb79c5aa6646b65abd90b708f30b92e5", "event": "ideahashed", "args": ["true"] }]
value	0 wei



status	1
from	0x627306090abab3a6e1400e9345bc60c78a8bef57
to	browser/patent.sol:PatentIdea.SaveIdeaHash(string) 0x8cdaf0cd259887258bc13a92c0a6da92698644c0
gas	30792 gas
transaction cost	30792 gas
hash	0x136e0b206d6a0e03a3908fca001059df1821db14fa0493f5cfb87a861c1244cf
input	0xe92c848f0000000000000000000000000000000000000000000000000000000000000020000000000000000000000000000000000000000000000000000000000000000f5468697320697320d792049646561000000000000000000000000000000000000
decoded input	{ "string idea": "This is my Idea" }
decoded output	-
logs	[{ "topic": "0x50a0231b714fc7ad51309492c3e5b5c3fb79c5aa6646b65abd90b708f30b92e5", "event": "ideahashed", "args": ["false"] }]
value	0 wei

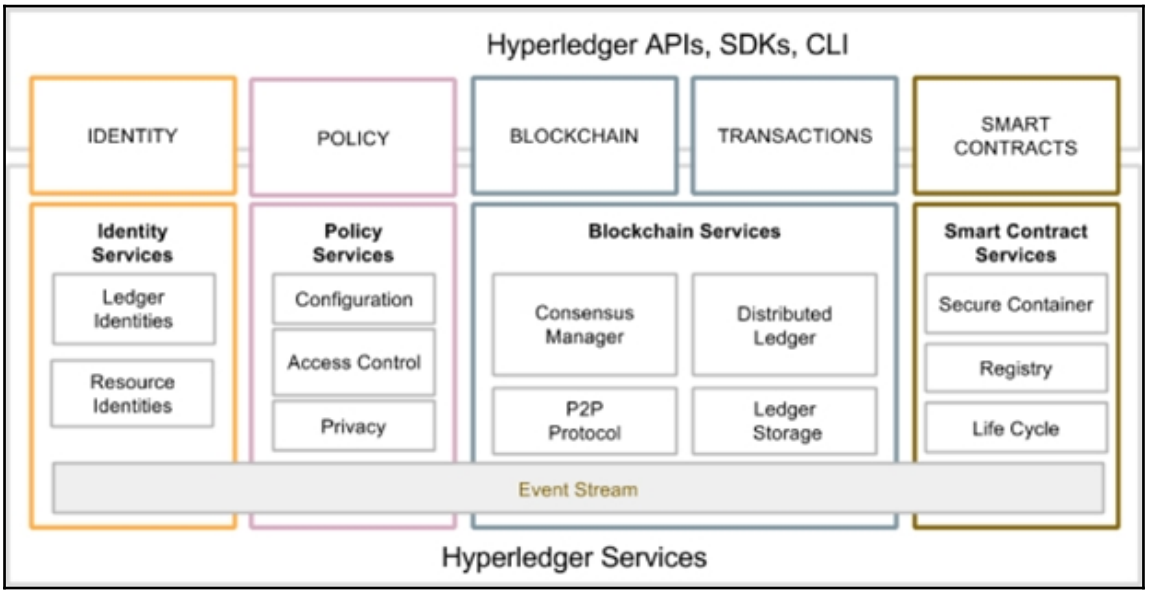


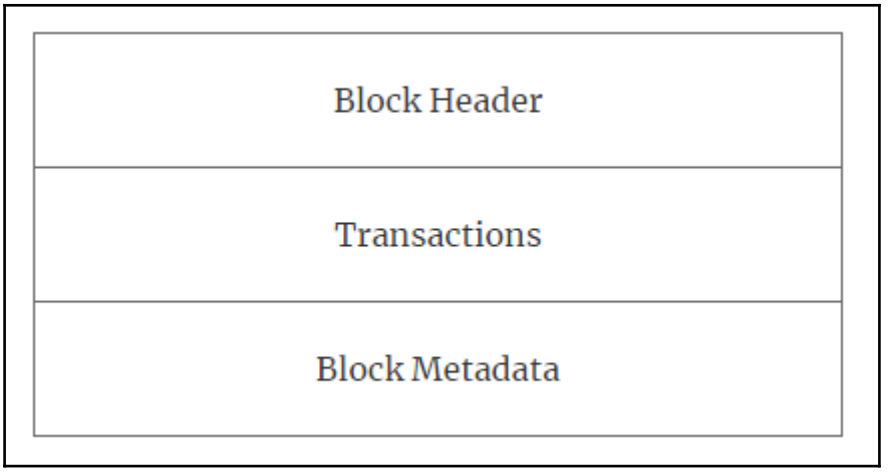
```
truffle(development)> PatentIdea.deployed().then(function(instance){app = instance})
undefined
truffle(development)> app.SaveIdeaHash("hello1")
{ tx: '0x597fffed0f859877676b158077c402b09a0ba1cd213c1ba28298e72a1f48af80',
  receipt:
   { blockHash: '0xaf21334ea79cc7f507eca9e6c93f043253fd371d987f0d3593ef3e270e4c77d6',
     blockNumber: 4046,
     contractAddress: null,
     cumulativeGasUsed: 45634,
     from: '0xcf61d213faa9acadbf0d110e1397caf20445c58f',
     gasUsed: 45634,
     logs: [ [Object] ],
     logsBloom: '0x00000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000400000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000400000200000000000000000000000000000000000000000000000000
     root: '0xc9b84ede2a53eefa6e933d697068230565e16570bffeb3ad21fe71c6ee62454b',
     to: '0x0694d9db791803c83e10175163d8a58df76a2a84',
     transactionHash: '0x597fffed0f859877676b158077c402b09a0ba1cd213c1ba28298e72a1f48af80',
     transactionIndex: 0 },
  logs:
   [ { address: '0x0694d9db791803c83e10175163d8a58df76a2a84',
       blockNumber: 4046,
       transactionHash: '0x597fffed0f859877676b158077c402b09a0ba1cd213c1ba28298e72a1f48af80',
       transactionIndex: 0,
       blockHash: '0xaf21334ea79cc7f507eca9e6c93f043253fd371d987f0d3593ef3e270e4c77d6',
       logIndex: 0,
       removed: false,
       event: 'ideahashed',
       args: [Object] } ] }
```

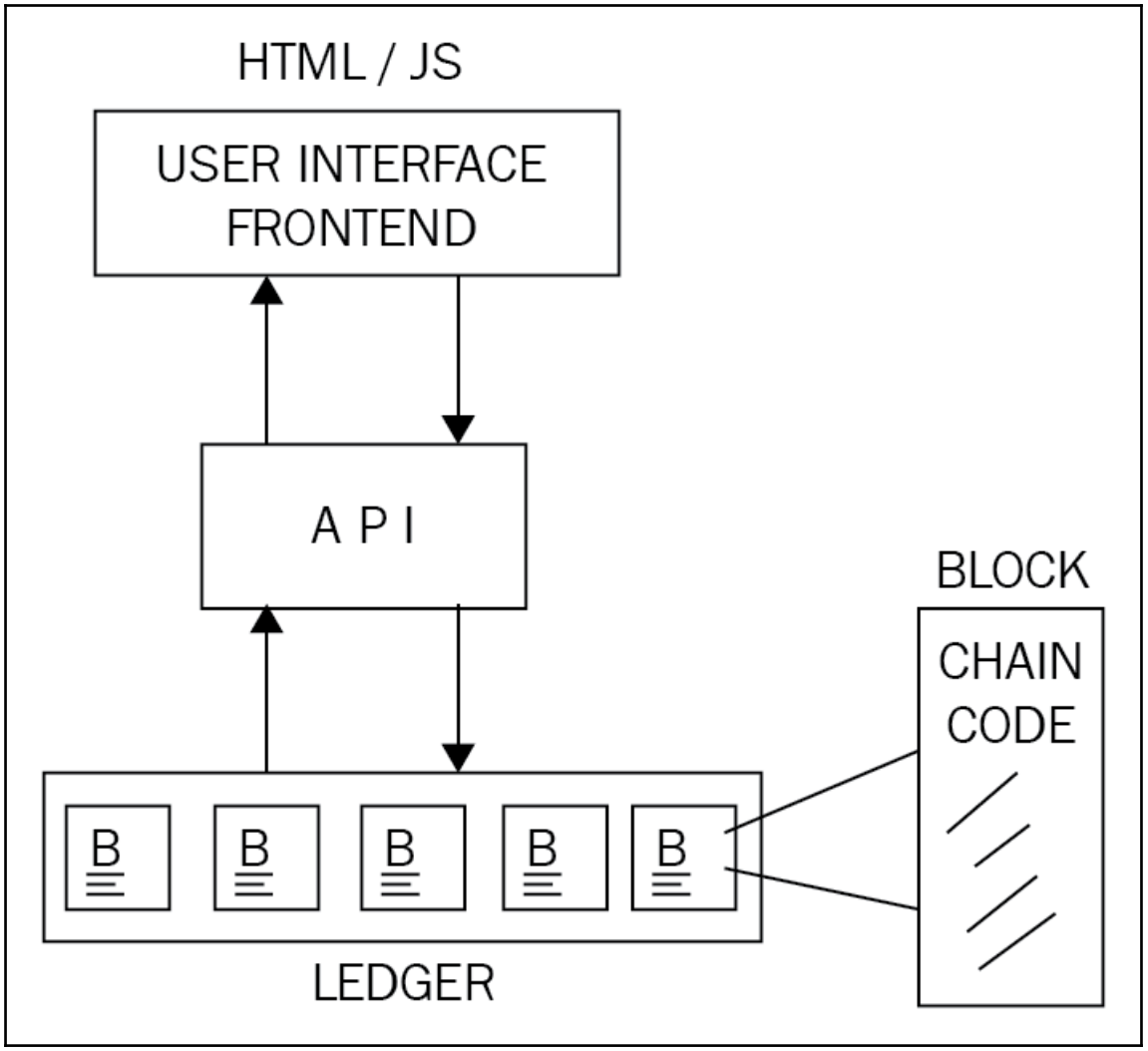

ETHEREUM
BLOCKCHAIN
SMART CONTRACT
ORACLIZE
ANSWER
INTERNET
3rd PARTY DATA
SOURCE

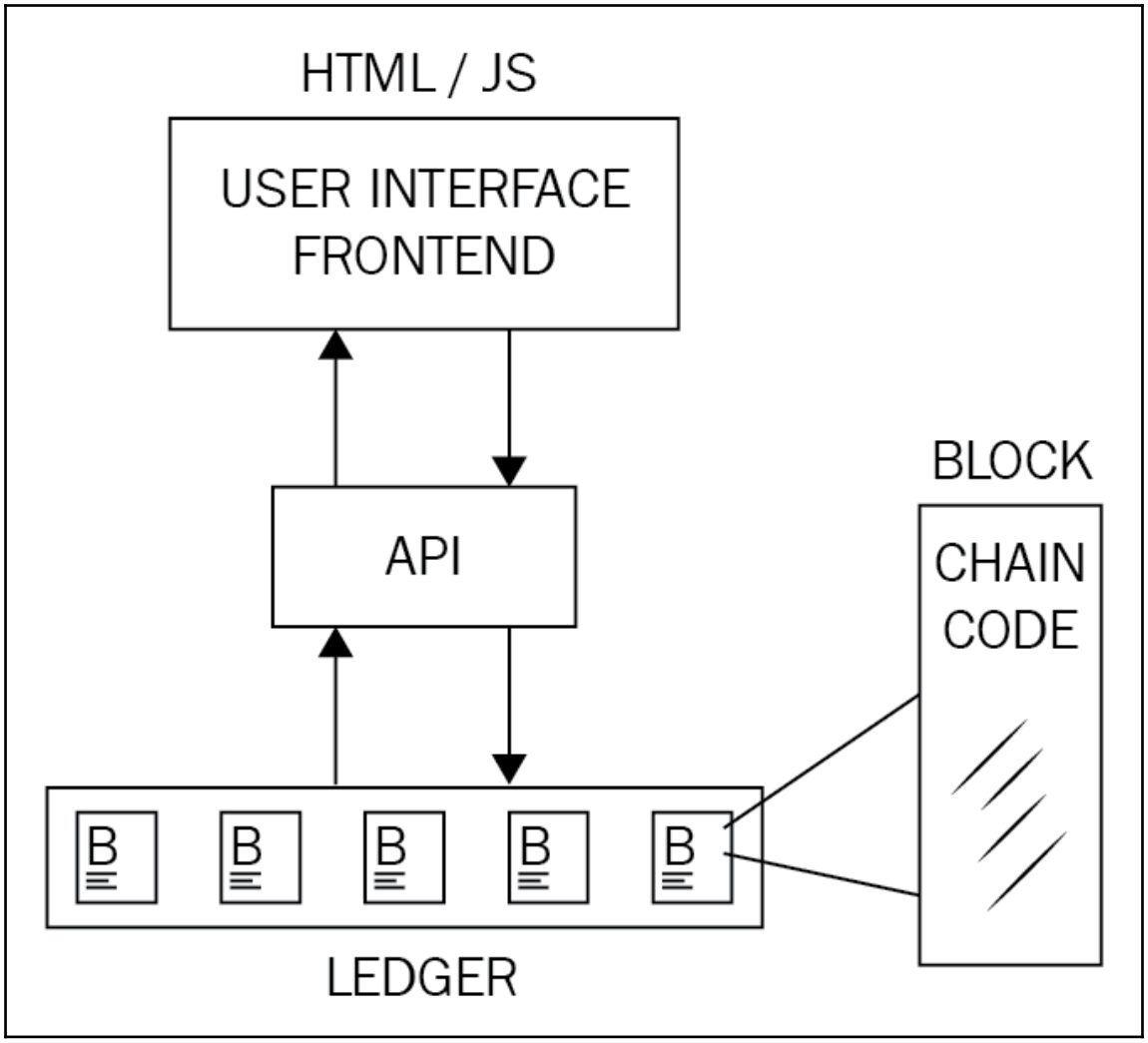
```
imran@drequinox-OP7010:~$  ipfs cat /ipfs/QmYwAPJzv5CZsnA625s3Xf2nemtYgPpHdWEz79ojWnPbdG/readme
Hello and Welcome to IPFS!

                   ██╗██████╗ ███████╗███████╗
                   ██║██╔══██╗██╔════╝██╔════╝
                   ██║██████╔╝█████╗  ███████╗
                   ██║██╔═══╝ ██╔══╝  ╚════██║
                   ██║██║     ██║     ███████║
                   ╚═╝╚═╝     ╚═╝     ╚══════╝

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

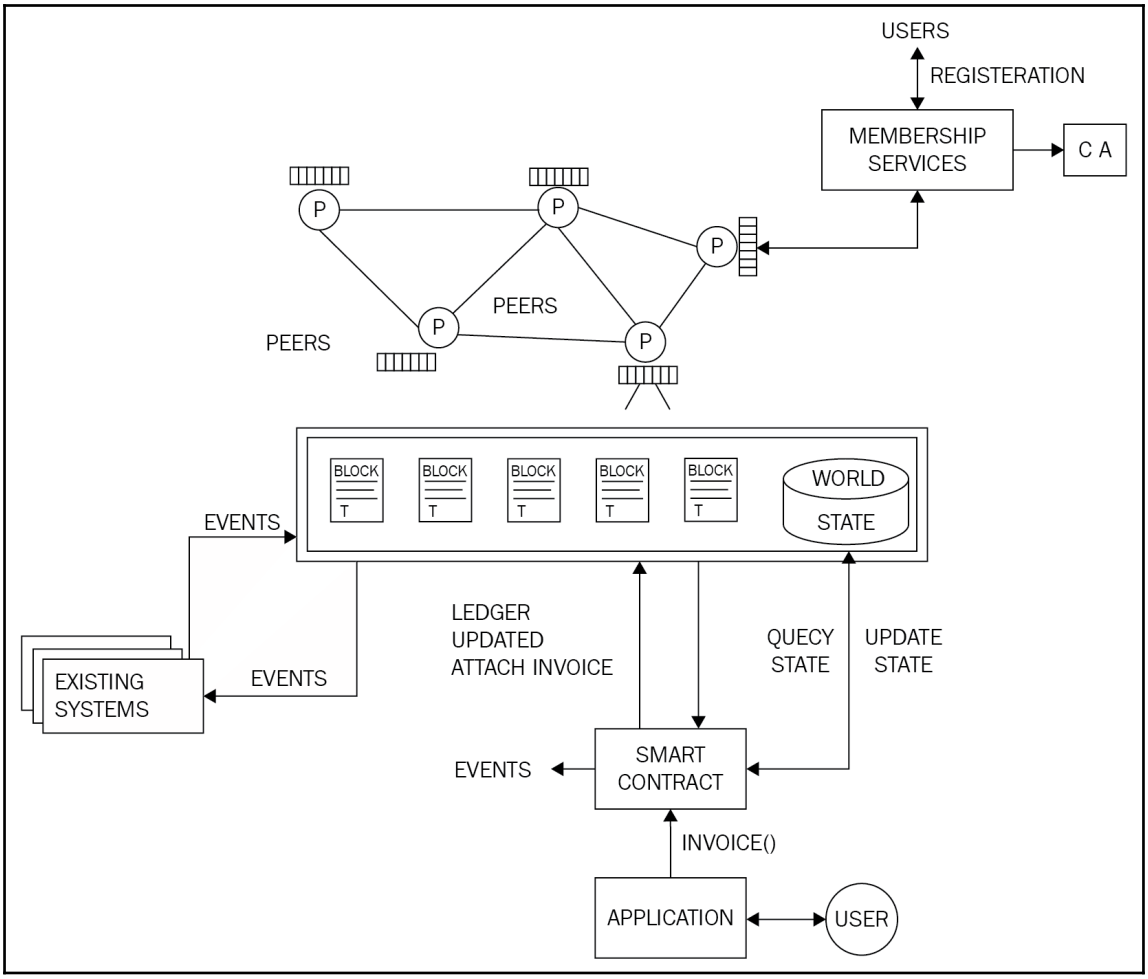
Chapter 15: Hyperledger

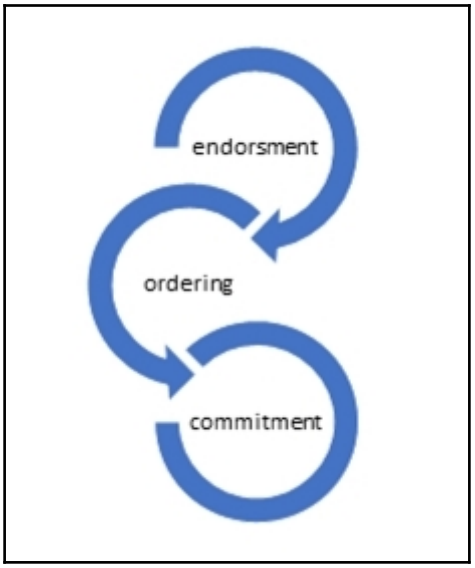




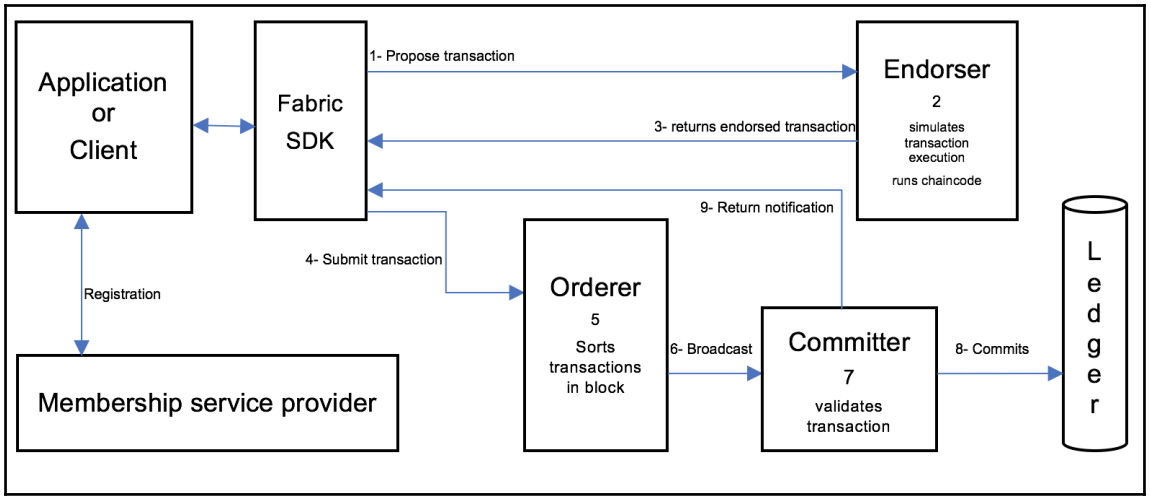

HTML / JS
USER INTERFACE
FRONTEND
A P I
BLOCK
CHAIN
CODE
B
B
B
B
B
LEDGER

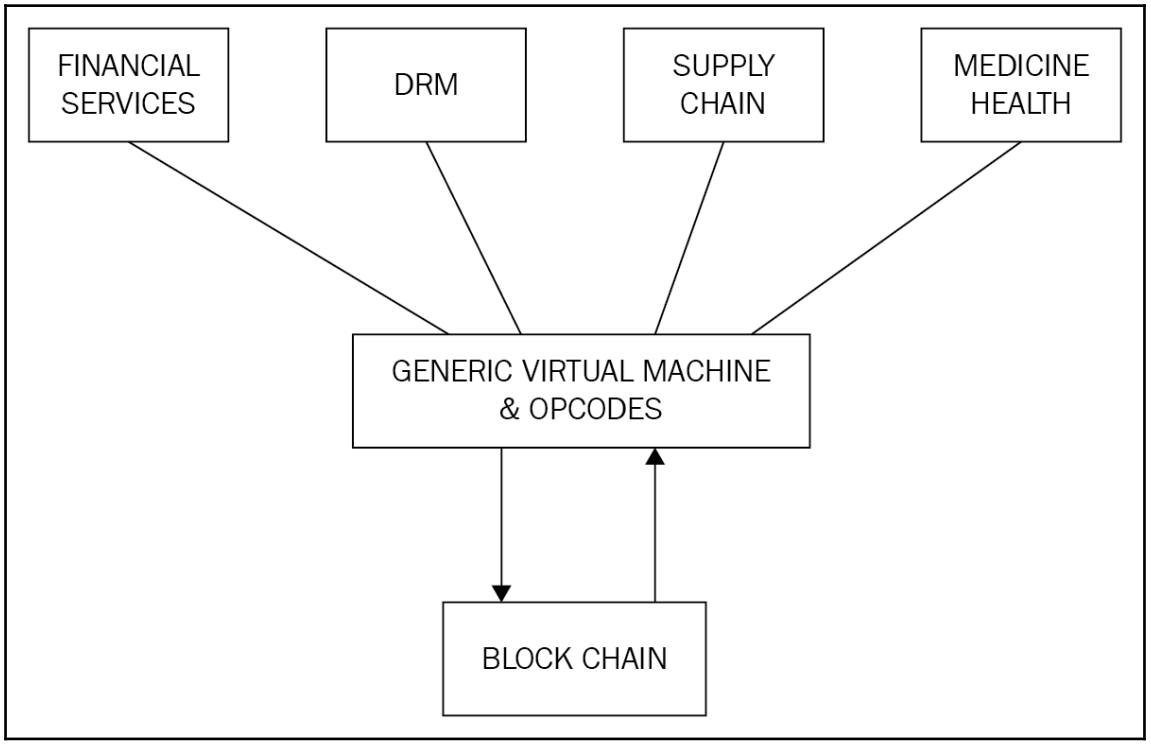

HTML / JS
USER INTERFACE
FRONTEND
API
BLOCK
CHAIN
CODE
B
B
B
B
B
LEDGER

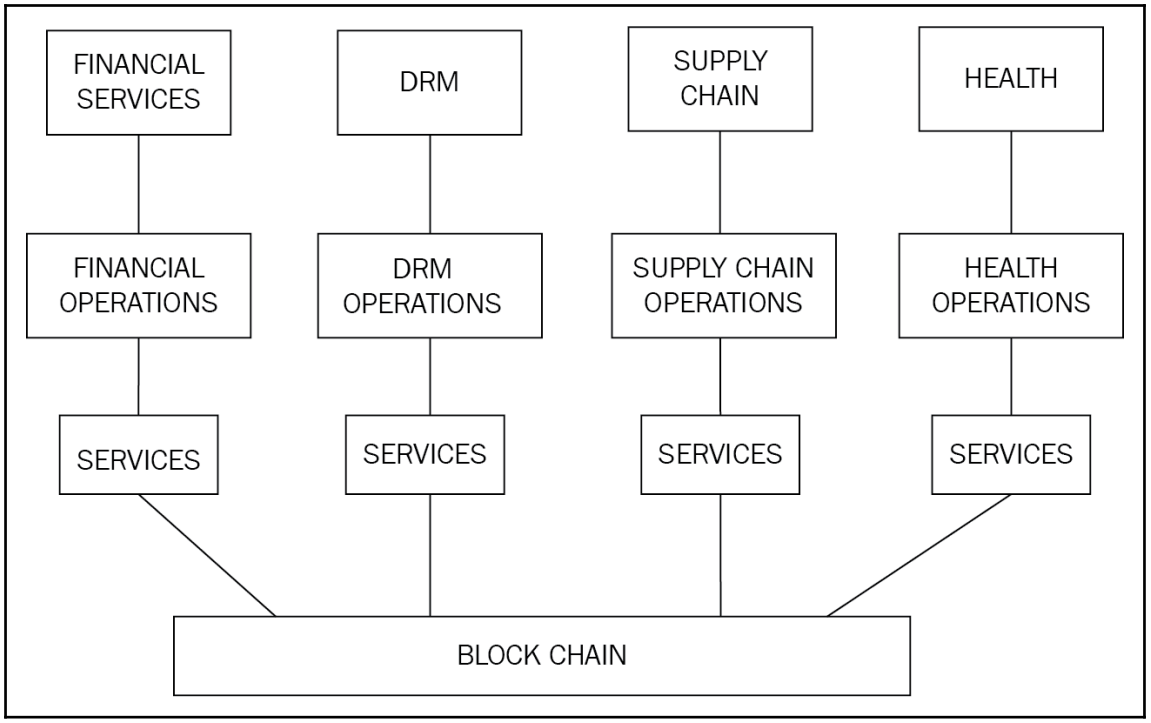

USERS
REGISTERATION
MEMBERSHIP SERVICES
C A
P
P
P
P
P
PEERS
PEERS
BLOCK
T
BLOCK
T
BLOCK
T
BLOCK
T
BLOCK
T
WORLD
STATE
EVENTS
LEDGER
UPDATED
ATTACH INVOICE
QUECY
STATE
UPDATE
STATE
EXISTING SYSTEMS
EVENTS
EVENTS
SMART CONTRACT
INVOICE()
APPLICATION
USER



- **MSP** • enrolls the users and applications
- **App** • Submits proposal
- **endorser** • simulates transactions and responds back
- **App** • submit transaction to orderers
- **Orderer** • sort transactions, assemble blocks, send to committer
- **Committer** • validate transaction and update ledger


Application or Client
Fabric SDK
1- Propose transaction
Endorser
2
simulates transaction execution
runs chaincode
3- returns endorsed transaction
9- Return notification
Registration
4- Submit transaction
Orderer
5
Sorts transactions in block
6- Broadcast
Committer
7
validates transaction
8- Commits
Ledger
Membership service provider


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



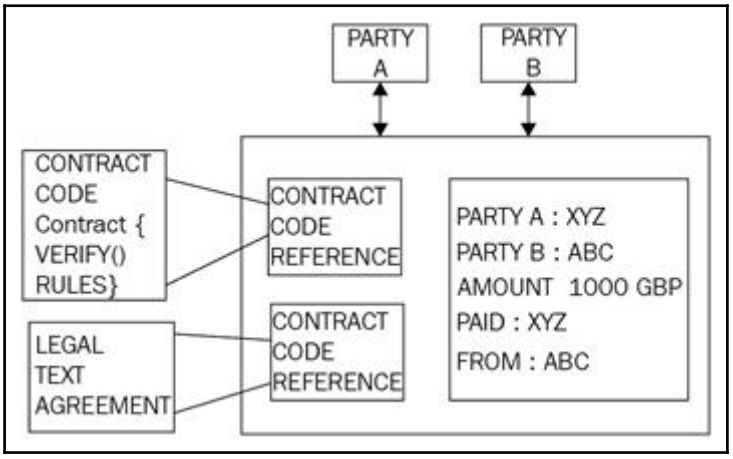

```
drequinox@drequinox-OP7010:~/project$ git clone https://github.com/IntelLedger/sawtooth-core.git
Cloning into 'sawtooth-core'...
remote: Counting objects: 12527, done.
remote: Compressing objects: 100% (964/964), done.
remote: Total 12527 (delta 452), reused 0 (delta 0), pack-reused 11515
Receiving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

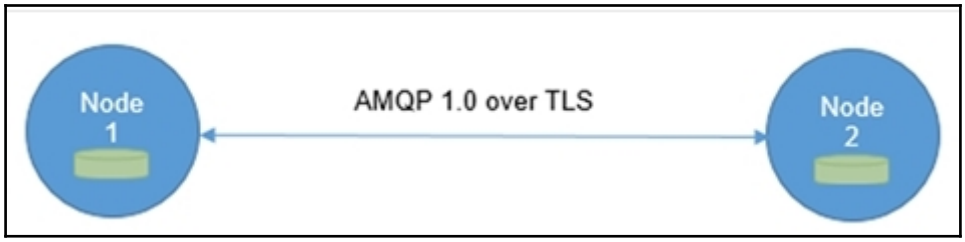
```
drequinox@drequinox-OP7010:~/project/sawtooth-core/tools$ vagrant up
Could not determine vagrant user.
VAGRANT_BOX = ubuntu/xenial64
VAGRANT_FORWARD_PORTS = true
VAGRANT_MEMORY = 2048
VAGRANT_CPUS = 2
Proxyconf plugin not found
Install: vagrant plugin install vagrant-proxyconf
Bringing machine 'default' 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
```

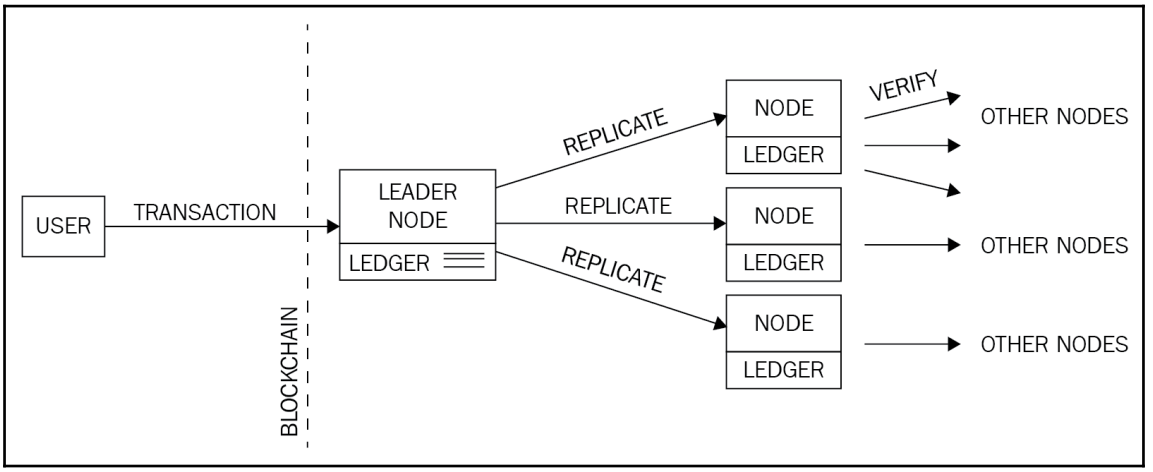
```
ubuntu@ubuntu-xenial:/project/sawtooth-core$ ./bin/txnvalidator -v -F ledger.transaction.integer_key --config /home/ubuntu/sawto
oth/v0.json
[22:08:22 INFO    validator_cli] validator started with arguments: ['./bin/txnvalidator', '-v', '-F', 'ledger.transaction.intege
r_key', '--config', '/home/ubuntu/sawtooth/v0.json']
[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>
```




Node
1
AMQP 1.0 over TLS
Node
2

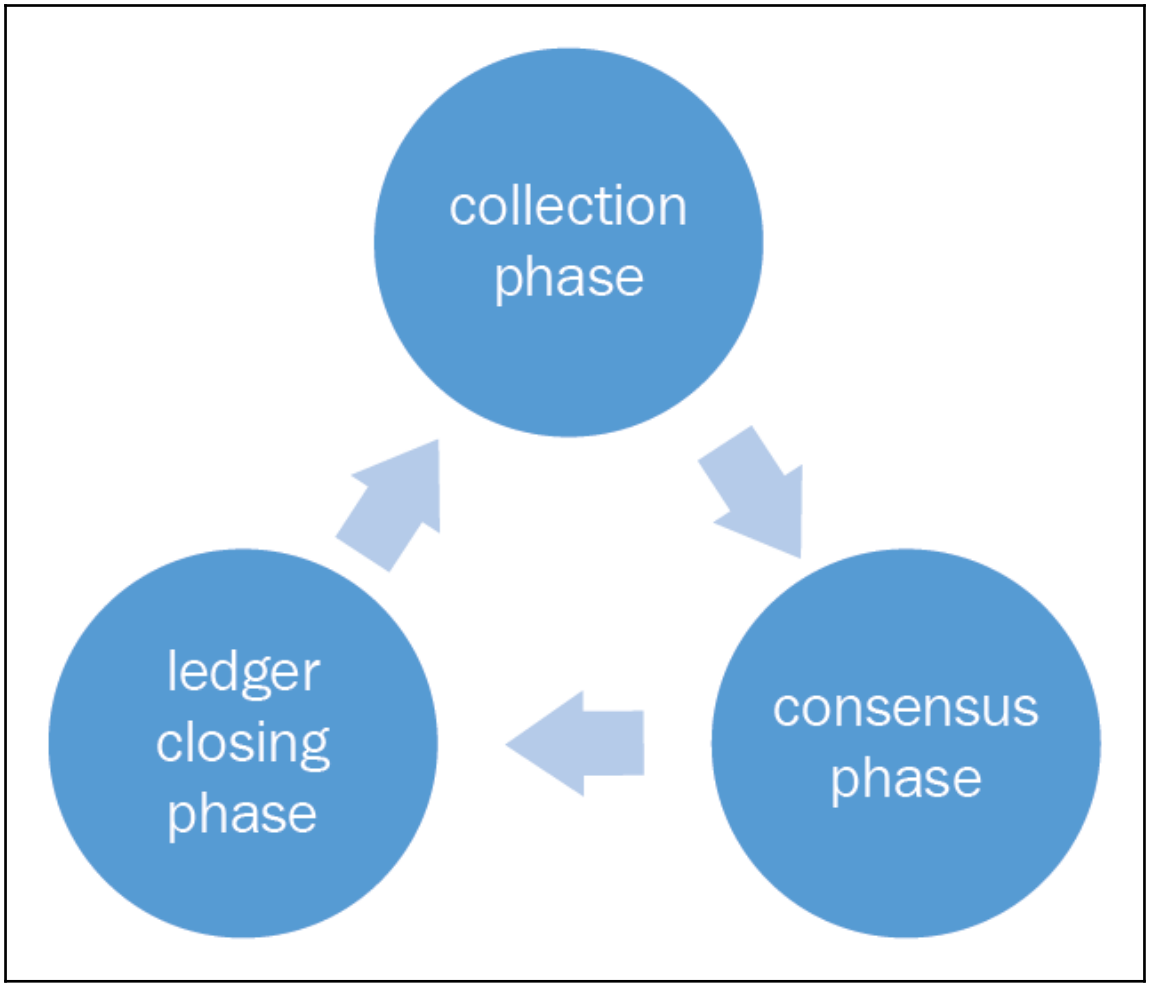
Chapter 16: Alternative Blockchains



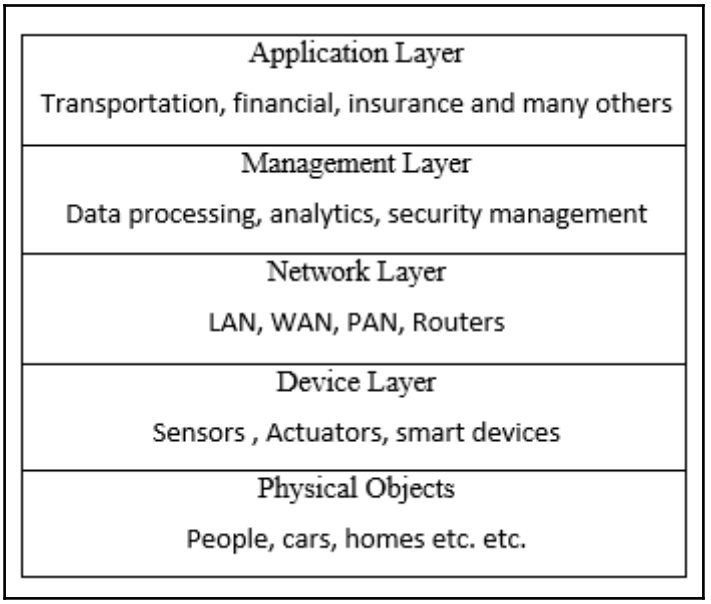

```
drequinox@drequinox-OP7010:~/Downloads$ ./pact
pact> 1234
1234
pact> (+ 1 2)
3
pact> (if (= (+ 1 2) 3 "OK" "ERROR")
(interactive):1:31: error: unexpected
    EOF, expected: ")", ";", "{",
    Boolean false, Boolean true,
    Decimal literal, Integer literal,
    String literal, Symbol literal,
 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

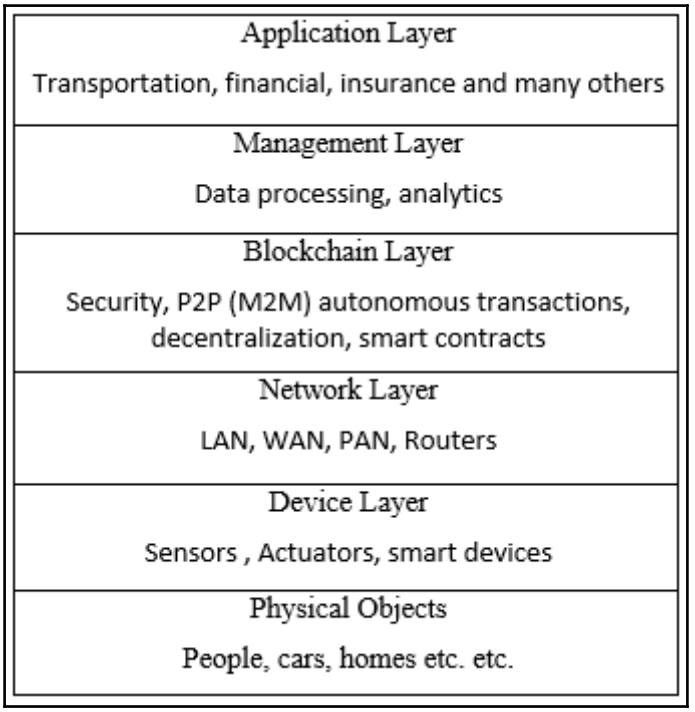
```
;Begin transaction with optinal NAME.
(begin-tx) 'testTransaction
;Set transaction data in JSON format or pact types
(env-data { "keyset": {"keys": ["admin"], "pred": "keys-any"}})
;Define keyset as NAME with KEYSET
(define-keyset 'admin-keyset (read-keyset "keyset"))
;Set transaction signature KEYS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

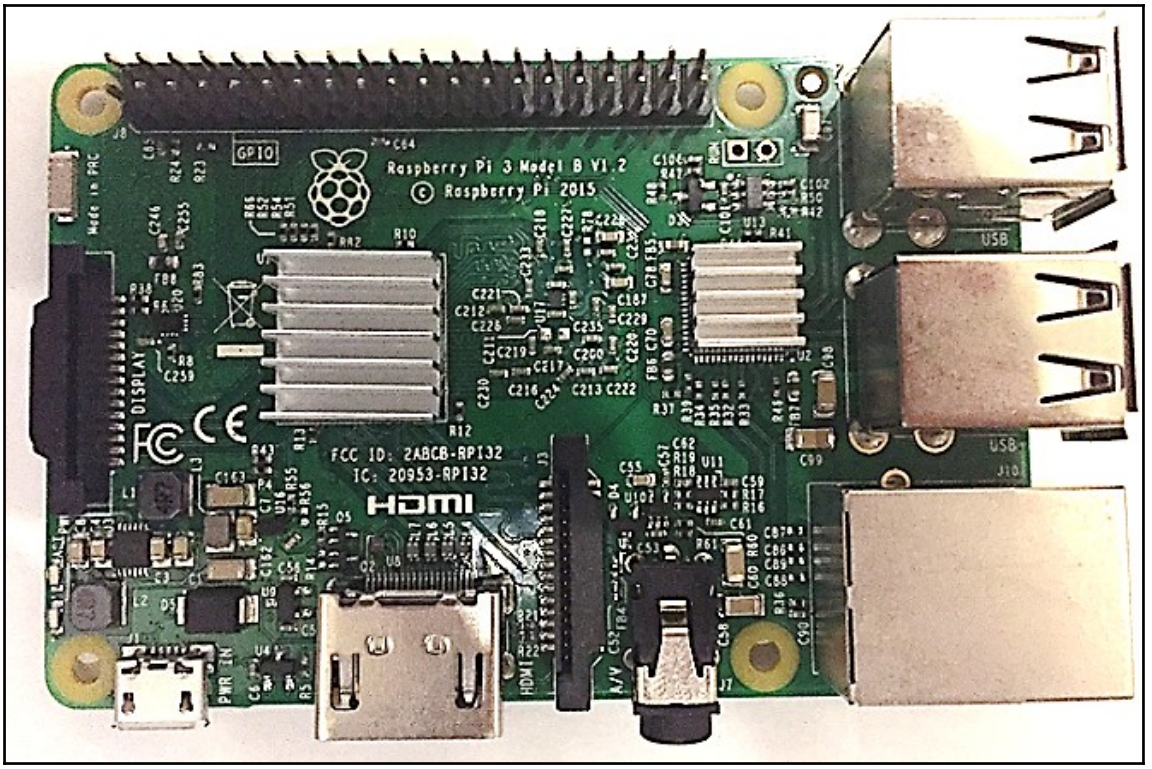
```
Begin Tx Just 1
testTransaction
Setting transaction data
Keyset defined
Setting transaction keys
Loaded module "additionModule"
  , hash "eaf647f843b2e88b5009253fe4eeca6f8890a646da76b4
Commit Tx Just 1
Using "additionModule"
Result : 600
```


collection phase
consensus phase
ledger closing phase

Chapter 17: 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: ~
File  Edit  Tabs  Help
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 $ ./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://44352ede5b9e792e437c1c0431c1578ce3676
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
      }
    }
}]
```

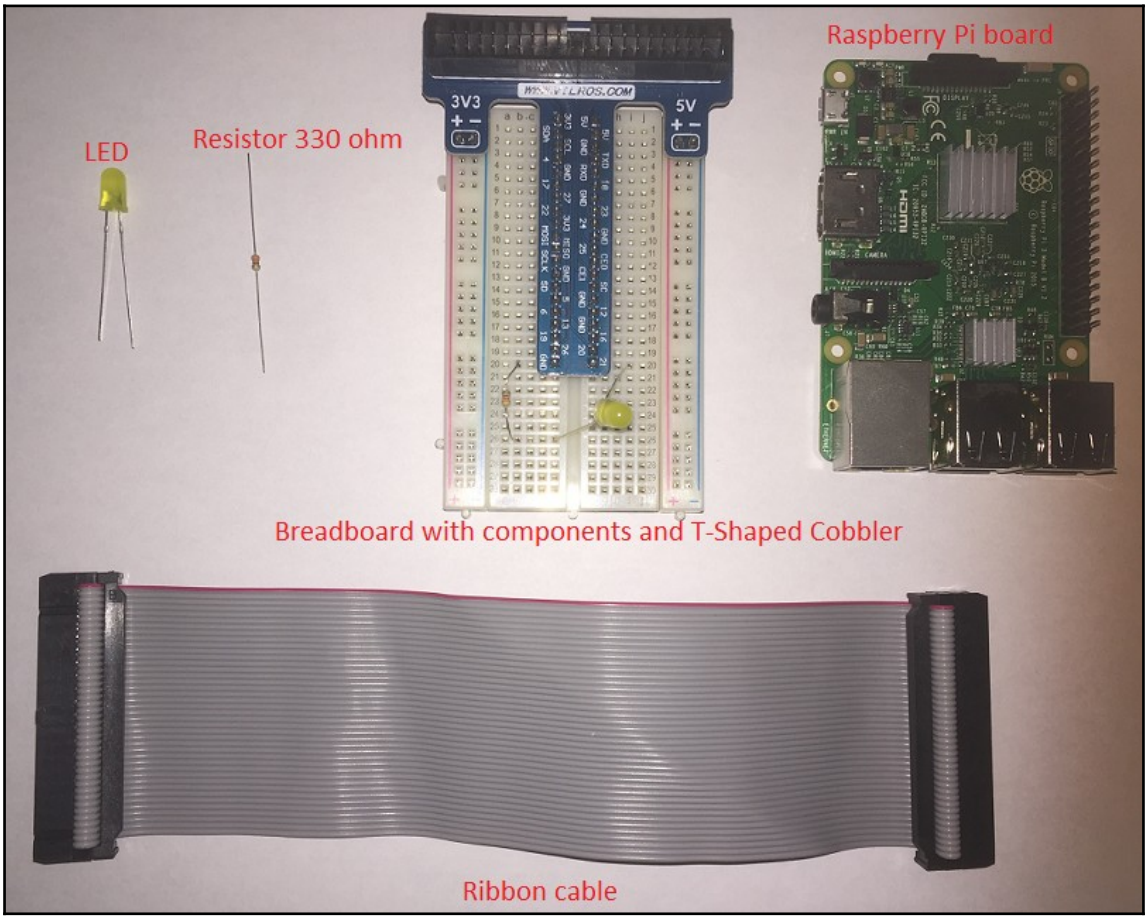
```
> admin.peers
[{
    caps: ["eth/62", "eth/63"],
    id: "98ba36ecea7ff011803d634da45752abd25101f20a62f23427afc3f280017bc134833dd5ba400bb195ac6ed59c3b01
ca2a3f14638a52697a1bb1bf967fc84274",
    name: "Geth/raspberry/v1.5.6-stable-2a609af5/linux/go1.7.4",
    network: {
      localAddress: "192.168.0.19:30301",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

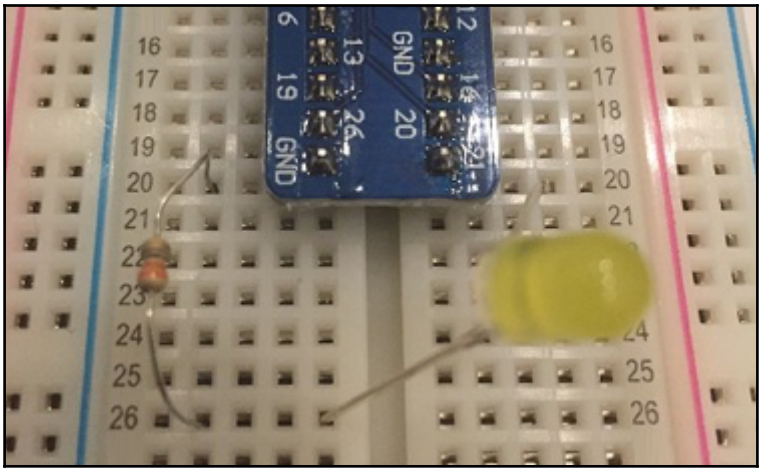
```
pi@raspberrypi:~/testled $ curl -sL https://deb.nodesource.com/setup_7.x | sudo -E bash -

## 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]
```

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

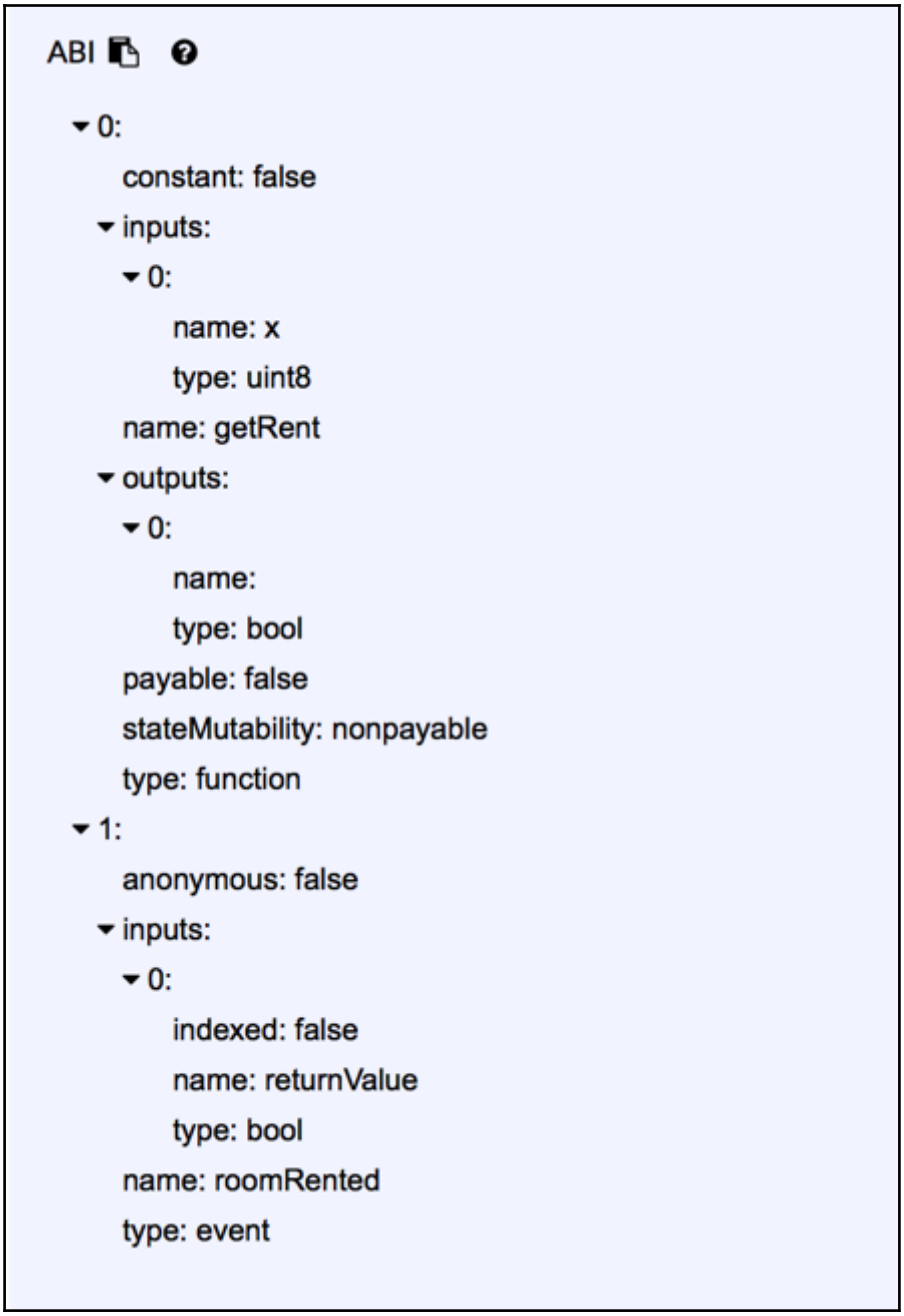
```
pi@raspberrypi:~/testled $ npm install web3
testled@1.0.0 /home/pi/testled
└─┬ web3@0.18.0
  └── bignumber.js@2.0.7  (git+https://github.com/debris/bignumber.js.git#94d7146671b9719e00a09c29b01a691bc85048c2)

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

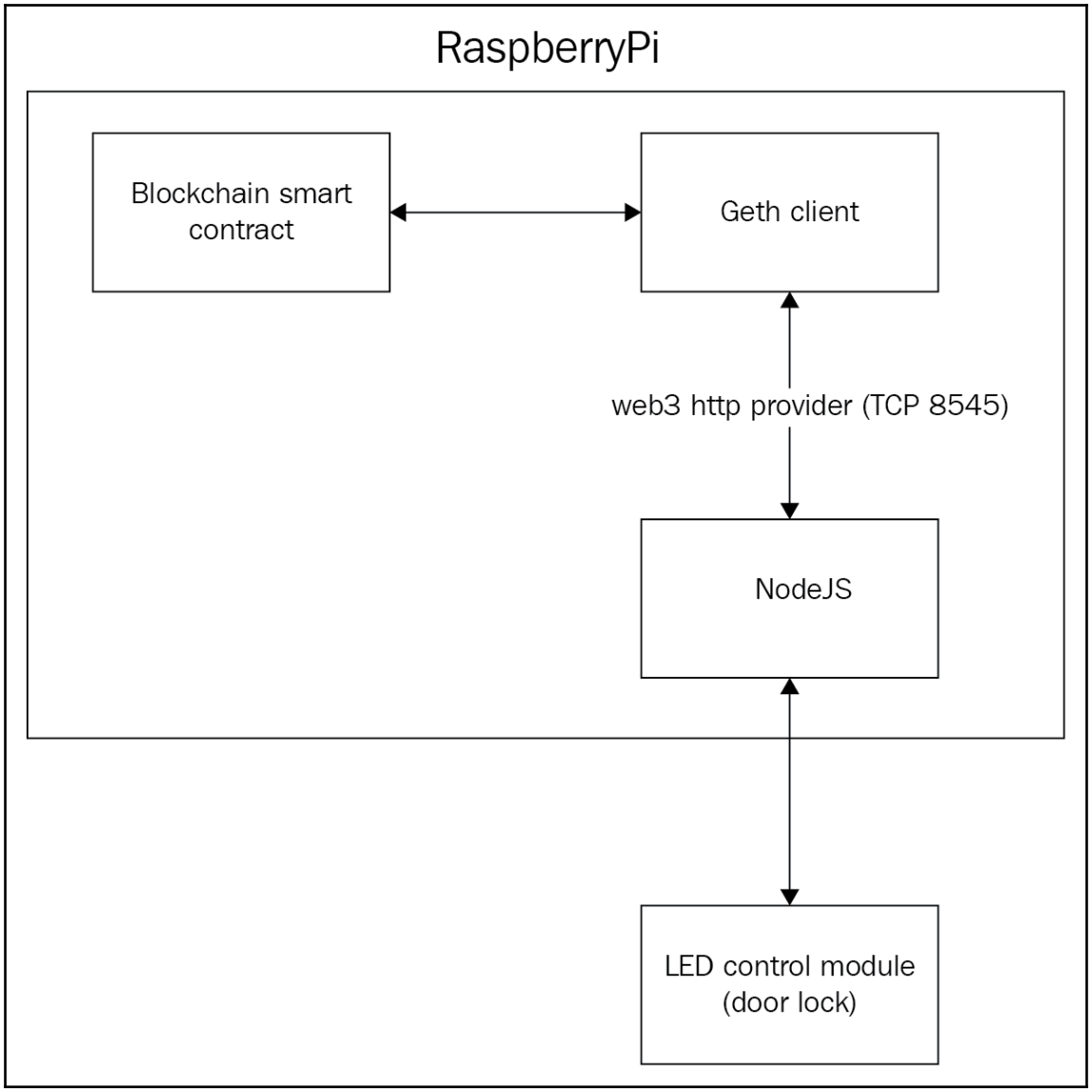
```
pi@raspberrypi:~/testled $ npm install onoff --save
testled@1.0.0 /home/pi/testled
└── onoff@1.1.1

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

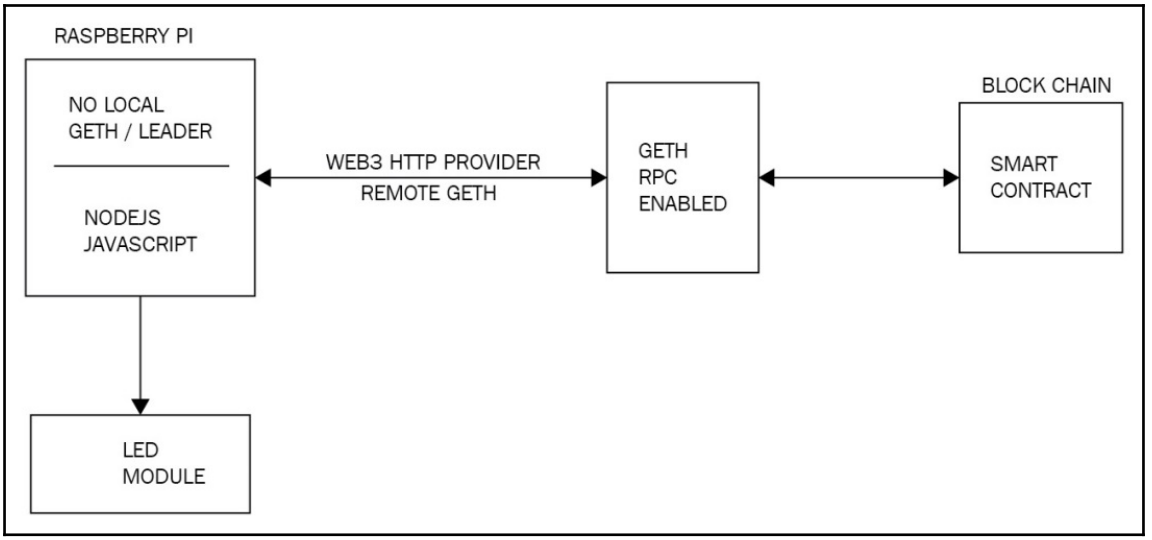





```
pragma solidity ^0.4.0;
contract simpleIOT {
    uint roomrent = 10;
    event roomRented(bool returnValue);
    function getRent (uint8 x) public returns (bool) {
        if (x==roomrent) {
            roomRented(true);
            return true;
        }
    }
}
```

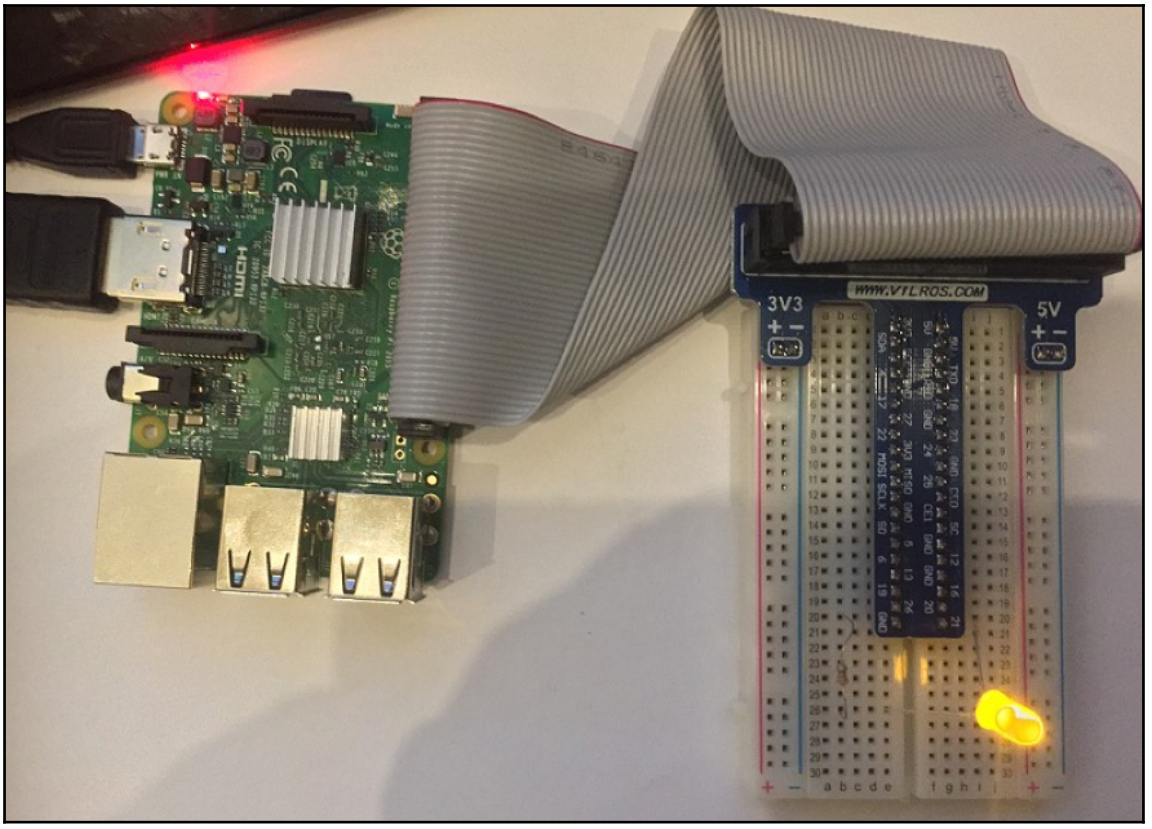

ABI
0:
constant: false
inputs:
0:
name: x
type: uint8
name: getRent
outputs:
0:
name:
type: bool
payable: false
stateMutability: nonpayable
type: function
1:
anonymous: false
inputs:
0:
indexed: false
name: returnValue
type: bool
name: roomRented
type: event

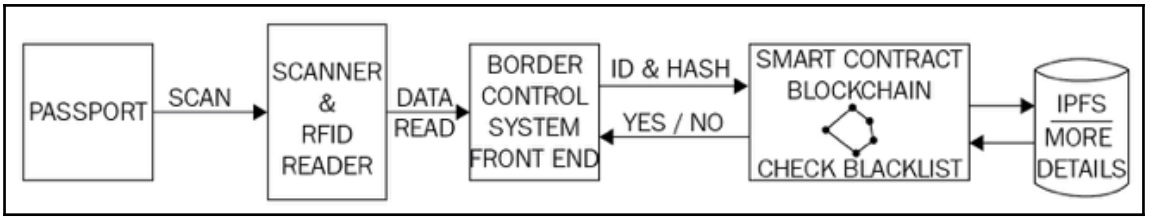

RaspberryPi
Blockchain smart contract
Geth client
web3 http provider (TCP 8545)
NodeJS
LED control module (door lock)



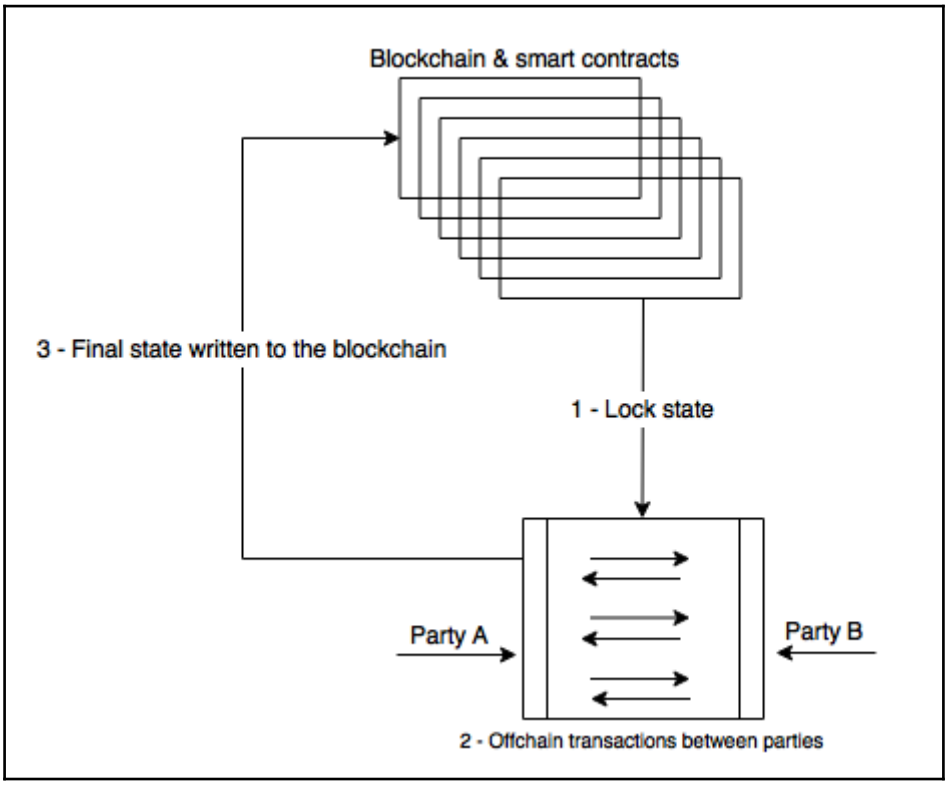

```
imran@drequinox-OP7010:~/iotcontract$ truffle migrate --reset
Running migration: 1_initial_migration.js
  Deploying Migrations...
  Migrations: 0xdd8a88072aa4ff49b62c25d6f6f2207b731aee76
Saving successful migration to network...
Saving artifacts...
Running migration: 2_deploy_contracts.js
  Deploying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

```
truffle(development)> simpleiot.getRent(10)
'0x71f550949a4c5168af7b9f7f84fada99bccc20a123779642e5e8c0c0127266ee'
```


WWW.VTLROS.COM
3V3
5V


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 18: Scalability and Other Challenges



Security

- [x] Transaction origin: Warn if tx.origin is used
- [x] Check effects: Avoid potential reentrancy bugs
- [x] Inline assembly: Use of Inline Assembly
- [x] Block timestamp: Semantics maybe unclear
- [x] Low level calls: Semantics maybe unclear
- [x] Block.blockhash usage: Semantics maybe unclear
- [x] Selfdestruct: Be aware of caller contracts.

Gas & Economy

- [x] Gas costs: Warn if the gas requirements of functions are too high.
- [x] This on local calls: Invocation of local functions via this

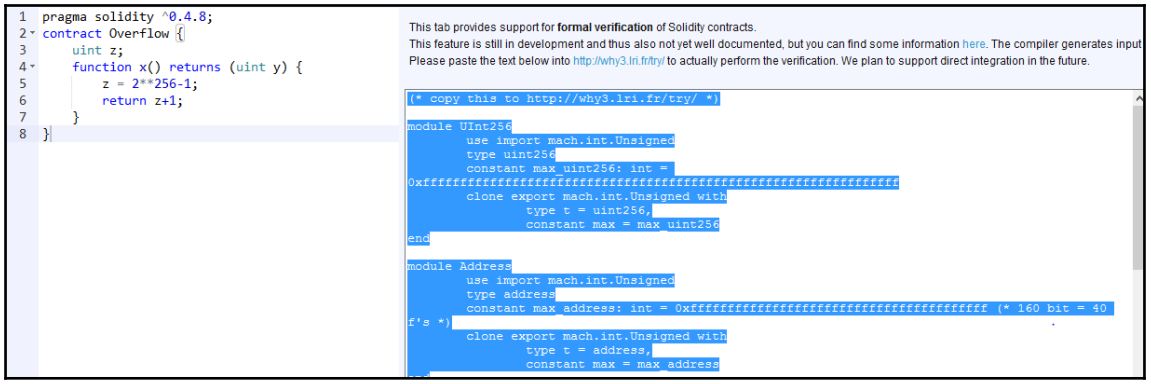
Miscellaneous

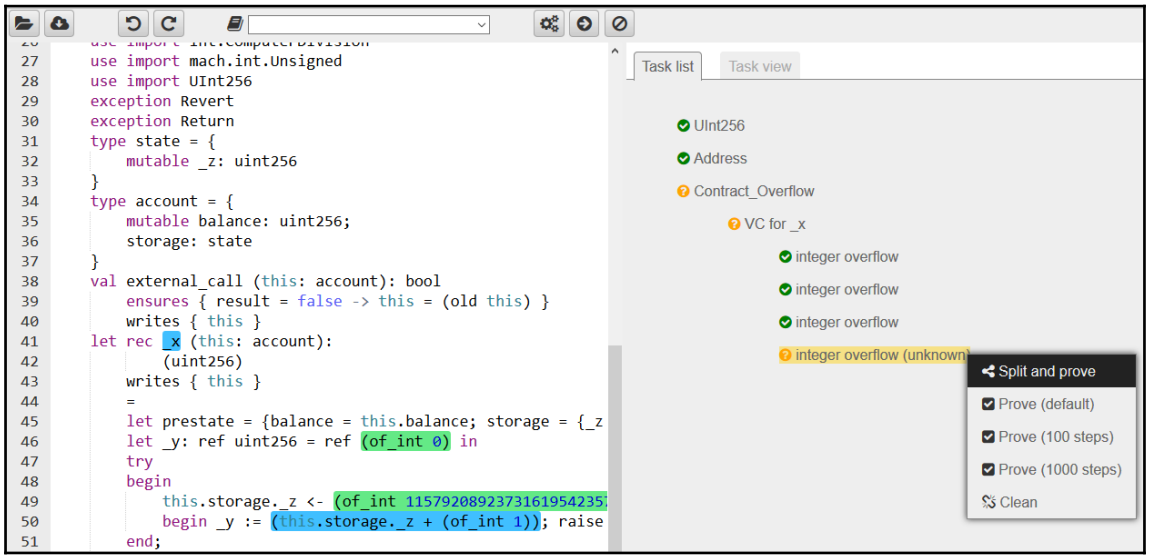
- [x] Constant functions: Check for potentially constant functions
- [x] Similar variable names: Check if variable names are too similar
- [x] no return: Function with return type is not returning
- [x] Guard Conditions: Use require and appropriately

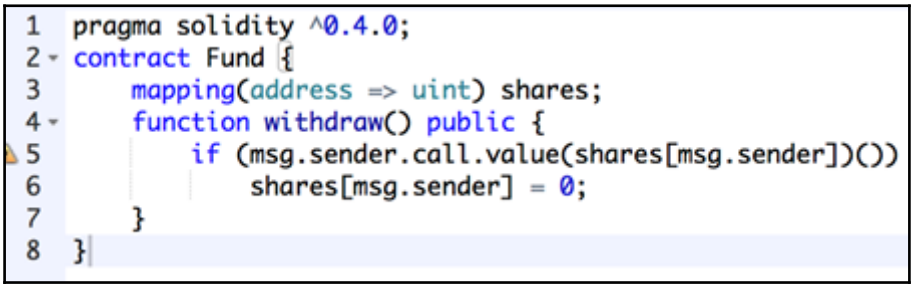
Run [ ] Auto run

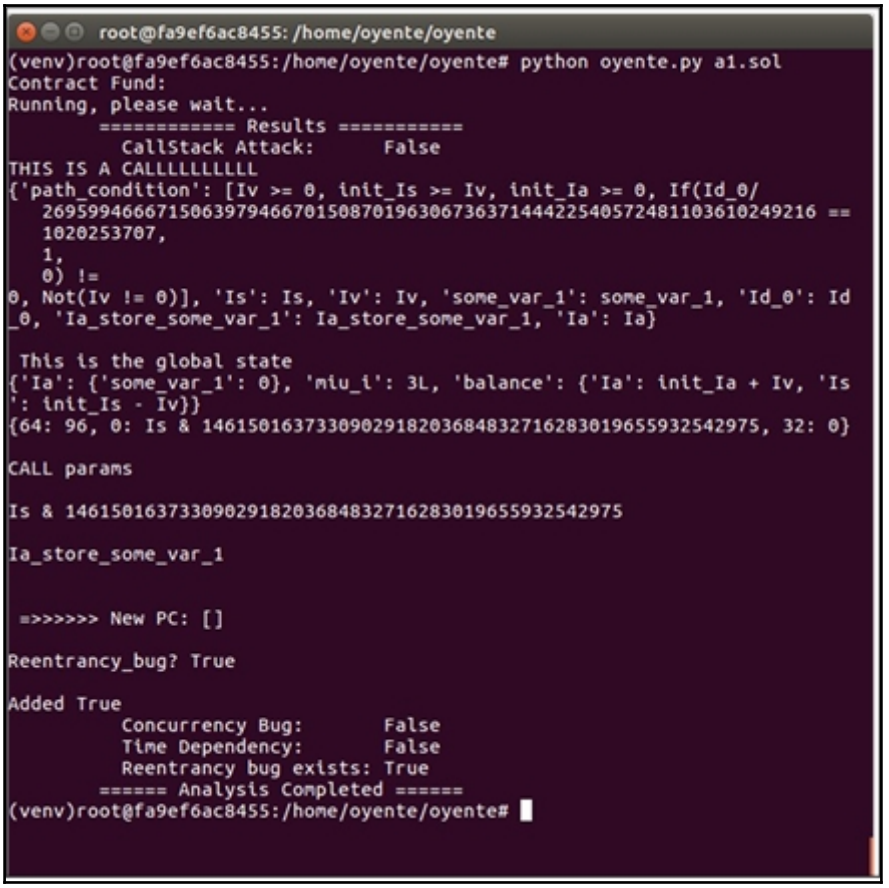
Potential Violation of Checks-Effects-Interaction pattern in Fund.withdraw(): Could potentially lead to re-entrancy vulnerability.

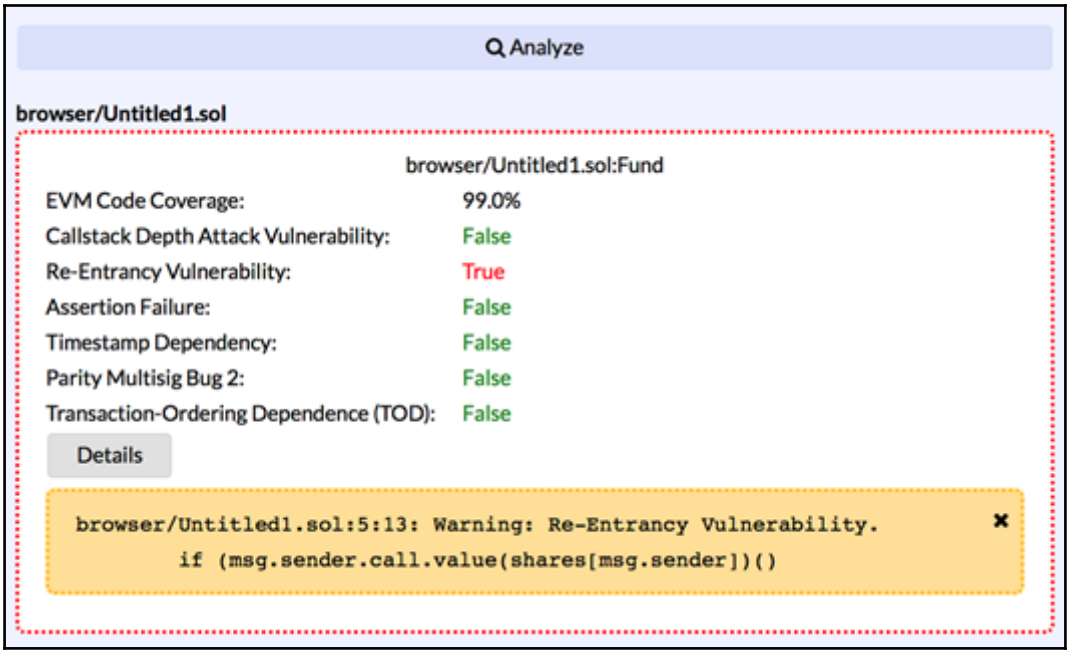
more


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
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 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;
Task list
Task view
UInt256
Address
Contract_Overflow
VC for _x
integer overflow
integer overflow
integer overflow
integer overflow (unknown
Split and prove
Prove (default)
Prove (100 steps)
Prove (1000 steps)
Clean


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


root@fa9ef6ac8455: /home/oyente/oyente
(venv)root@fa9ef6ac8455:/home/oyente/oyente# python oyente.py a1.sol
Contract Fund:
Running, please wait...
========== Results ==========
CallStack Attack: False
THIS IS A CALLLLLLLLL
{'path_condition': [Iv >= 0, init_Is >= Iv, init_Ia >= 0, If(Id_0/
269599466671506397946670150870196306736371444225405724811036102492 16 ==
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#


Analyze
browser/Untitled1.sol
browser/Untitled1.sol:Fund
EVM Code Coverage: 99.0%
Callstack Depth Attack Vulnerability: False
Re-Entrancy Vulnerability: True
Assertion Failure: False
Timestamp Dependency: False
Parity Multisig Bug 2: False
Transaction-Ordering Dependence (TOD): False
Details
browser/Untitled1.sol:5:13: Warning: Re-Entrancy Vulnerability.
if (msg.sender.call.value(shares[msg.sender])()