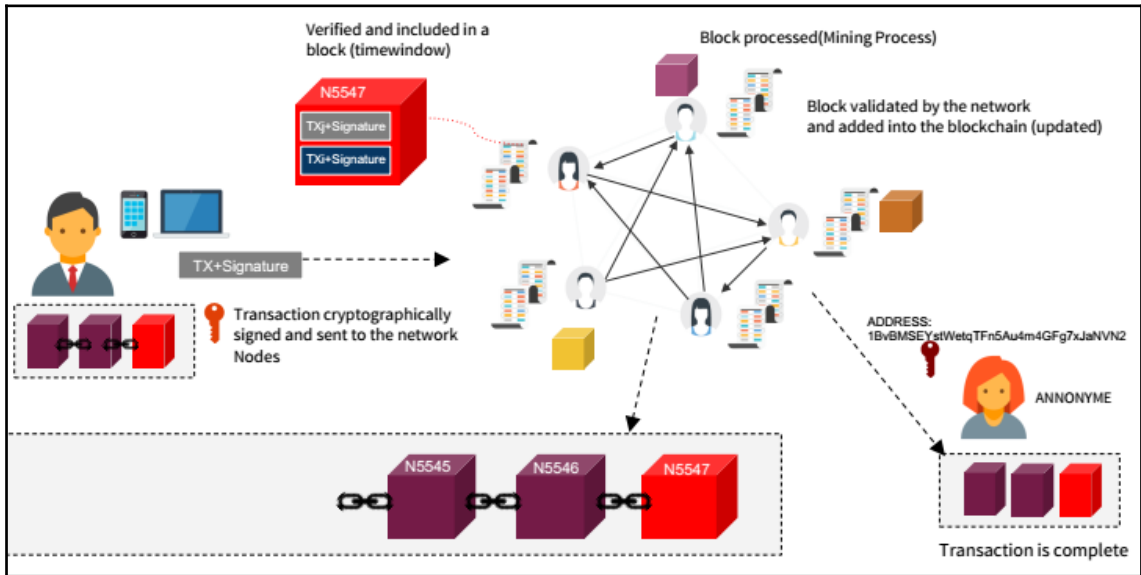
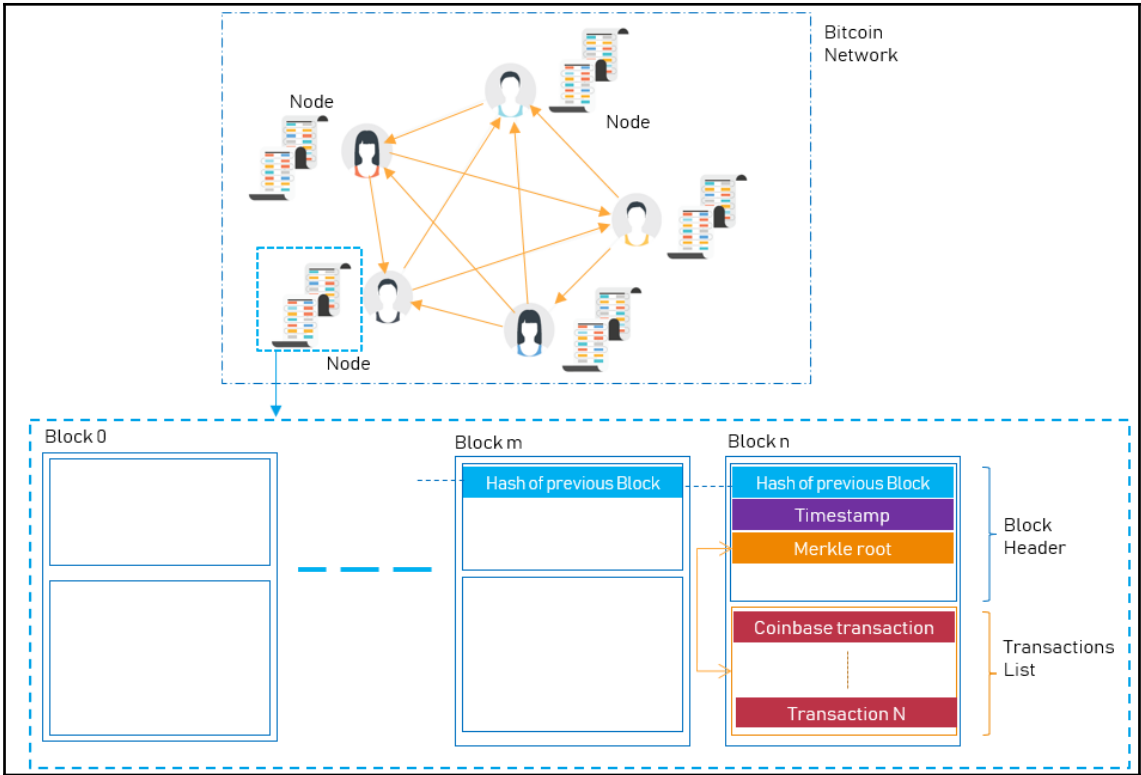
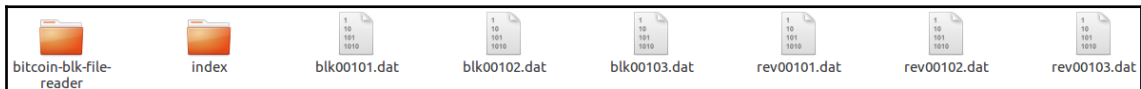
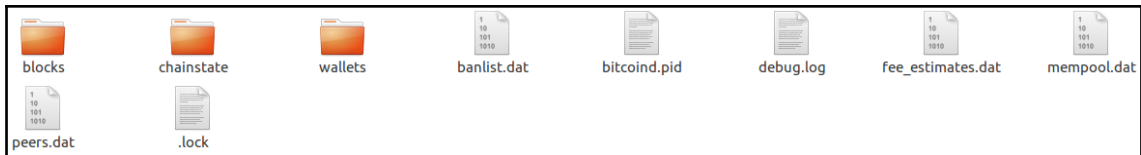
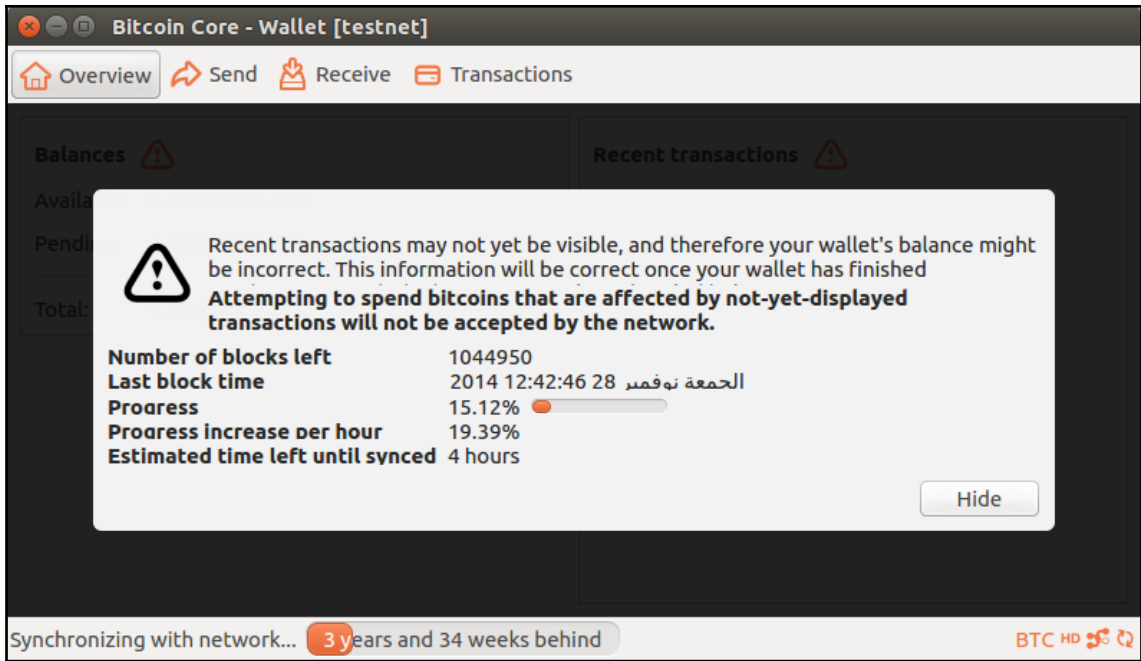


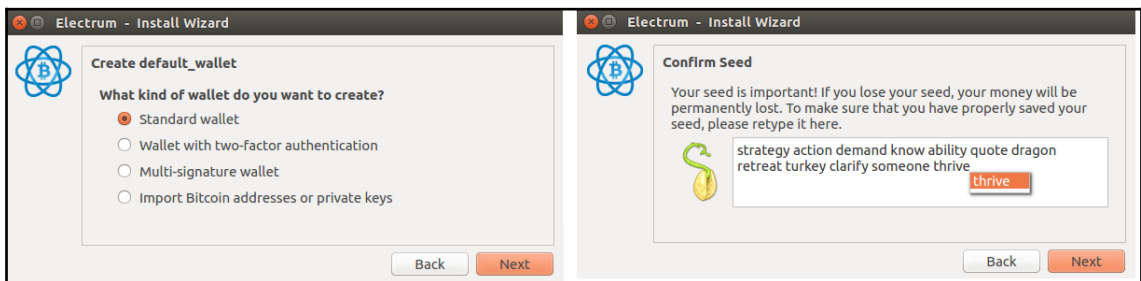
Chapter 1: Say Hello to Blockchain







```
user@ByExample-node:~$ bitcoin-cli getnewaddress
2MsHsi4CHXsaNZSq5krnrpP4WShNgtuRa9U
```



```
user@ByExample-node:~$ electrum --testnet listaddresses
[ecc] warning: libsecp256k1 library not available, falli
[
  "n3CKupfRCJ6Bnmr78mw9eyesZUSkfyHcPy",
  "mhc5YipxN6GhRRXtgakRBjrNUCbz6yppg66",
  "msvrqSHwJFFhS17ReQjMJyd1y4S6n7hirm",
  "mjSiyuBwjS8qeTmK44x97jG7Zmfq3ZB9Ai",
  "mq8izx8q2ydz6P3jhrPjqaPMSurkkwzaTD",
  "myE8qY9MDkRxsuFPUHVZrueMPZxc9TcZBU",
  "mqWMijZC7fdFDWao2KpcGWHgnEviqNN3xu",
  "mWMHczcBcucgMG1E4CmXK2JjGMwbvEF9Mt",

```

Faucet

I'm happy to serve you with TestNet Bitcoins. So take as much as you need to build awesome and secure BTC services. Really, just take them. You need a certain (huge) amount of Testnet Bitcoins? [Contact me](#)

You can get bonus coins:

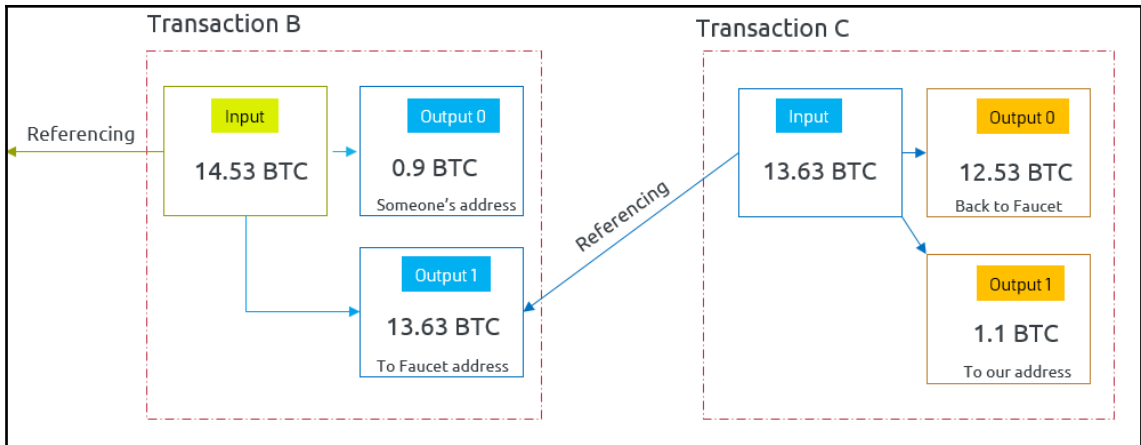
- +10% by using HTTP/2
- +20% by using a non-windows operating system
- +70% by using IPv6

Current wallets balance is **฿45635.17**. You'll get **฿0.5** (+ **฿0.05** bonus)

Sentil TX ID: 0791521362528725683caedf998006cf68b1cd817be1694ef0daca265d9b4252

(Or scan QR code with your camera.)

```
user@ByExample-node:~$ electrum --testnet listunspent
[ecc] warning: libsecp256k1 library not available, falling back to python-ecdsa
[
  {
    "address": "n3CKupfRCJ6Bnmr78mw9eyesZUSkfyHcPy",
    "coinbase": false,
    "height": 1356645,
    "prevout_hash": "0791521362528725683caedf998006cf68b1cd817be1694ef0daca265d9b4252",
    "prevout_n": 1,
    "value": "1.1"
  }
]
```



REPRESENTATION		LENGTH (Bytes)	VALUE
version		4	02000000
input count		1	01
Input 1	previous output ID in little endian (reversed)	32	52429b5d26cadaf04e69e17b81cdb168cf068099dfae3c682587526213529107
	Vout (previous output index)	04	100000000
	ScriptSig length	01	00
	ScriptSig		
	sequence	04	ff ff ff ff
Number of generated outputs		1	02
Output 1	amount of Satoshis (1 Satoshi = 0.00000001 Bitcoin)	8	00000000000000000
	script length	1	0d
	ScriptPubKey: OP_RETURN <Push size> <Payload (hello world in hex)>	13	6a 0b 68656c6c6f20776f726c64
Output 2	Value in Satoshis (hex encoded in little endian order)	8	00e1f50500000000
	Script length	1	17
	ScriptPubKey (Actual output script)	23	a914eb949dbde8d3b1755e7f3c20b6a62c1f1403bd9087
Lock time (the earliest time a transaction can be added to the blockchain)		04	00 00 00 00

```

user@ByExample-node:~$ electrum --testnet deserialize 02000000152429b5d26cadaf04e69e17b81cdb168cf068099dface3c6825875262135291070100000000ffffffff021
a0b68656c6cf20776f726c6400e1f505000000017a914080851b4d96aa26269dfd36af0eb9c2b2fa894568700000000
[ecc] warning: libsecp256k1 library not available, falling back to python-ecdsa
{
  "inputs": [
    {
      "address": null,
      "num_sig": 0,
      "prevout_hash": "0791521362528725683caedf998006cf68b1cd817be1694ef0dca265d9b4252",
      "prevout_n": 1,
      "scriptSig": "",
      "sequence": 4294967295,
      "type": "unknown"
    }
  ],
  "lockTime": 0,
  "outputs": [
    {
      "address": "6a0b68656c6cf20776f726c64",
      "prevout_n": 0,
      "scriptPubKey": "6a0b68656c6cf20776f726c64",
      "type": 2,
      "value": 0
    },
    {
      "address": "2Mshs14CHXsaNZS5q5krnrpP4WshNgtuRa9U",
      "prevout_n": 1,
      "scriptPubKey": "a914080851b4d96aa26269dfd36af0eb9c2b2fa8945687",
      "type": 0,
      "value": 100000000
    }
  ],
  "partial": false,
  "segwit_ser": false,
  "version": 2
}

```

```

user@ByExample-node:~$ electrum --testnet listaddresses | electrum --testnet getprivatekeys -
WARNING: ALL your private keys are secret.
Exposing a single private key can compromise your entire wallet!
In particular, DO NOT use 'redeem private key' services proposed by third parties.
[
  "p2pkh:c0x4Ucd3uXEpa3bNns1JJ84oWn5diChfChtfHskRaDNZOYA1FYnr",
  "p2pkh:cVZn69R4DwrPHVPGk5z63VfPebk3HVqbgCPcDTEd3nw2KRuUSJE",
  "p2pkh:cSkqWniTo7E1bNCmA7QW9FehwX8KZ1HwgMaRH8YocJ44ghz1oYNg",
  "p2pkh:cQFuxDStLrQVCzKkljMhKnSsvsowVEUJwUfowckhd9RWRrPSuKuu",
  "p2pkh:cQL23Vcj4dXXcn42Vc1LrrvZiFijbBaVx4b5GnnSy6cMtVCycV15",
  "p2pkh:cRHUCBnUf5fTWGyq1HdeibqcvTdDzhskTtJkjnxevjrqwrJxAzNW",
  "p2pkh:cRktM73Hvu7EvPNxUQTxz6733h8wiQ81FcbuCovihKcn3RD5GV3R",
  "p2pkh:cSU4oqxniw3TwsA8kzRh5zjQaUYerIDfPhYmEKKoLSDjBBS1NH4L",

```

```

"outputs": [
  {
    "address": "mxPd583YeW6iw3cCgfrmrdcXKG6PLM2fBj",
    "prevout_n": 0,
    "scriptPubKey": "76a914b9172e192d2805ea52fa975847eea0657e38fef888ac",
    "type": 0,
    "value": 1253185750
  },
  {
    "address": "n3CKupfRCj6Bnmr78mw9eyesZUSkyfHcPy",
    "prevout_n": 1,
    "scriptPubKey": "76a914edc8e9f510bf95606ec6a79cb28a745c039e22088ac",
    "type": 0,
    "value": 110000000
  }
],
"partial": false,
"segwit_ser": false,
"version": 2
}

```


blk00100.dat

Block N 1356675

Block Header

Coinbase Transaction

Our Transaction

```

06fdfa15 EC AC F3 22 D3 0D A4 8B 30 C6 2C AD C3 79 5F C6 A0 FF FF FF 02 00 D0 20 00 00 00 00 00 19 76 A9 14 EC ...*.0.,,y_.....v...
06fdfa38 1B D9 39 B5 63 0E 42 C6 CE E1 D7 3B 37 A6 B4 22 38 3C 1A 88 AC 00 00 00 00 00 00 00 00 53 6A 4C 50 00 00 ...9.c.B...;7.*8<.....SjLP..
06fdfa5b B7 D9 00 01 5C 45 B4 F2 8D 84 C1 1A 14 9F 5D 3F 86 6D EC 0E 81 80 50 71 B9 9F BE 80 50 B3 05 D9 12 67 57 ...\.E./.....?m...Eq...P...gW
fa7e E2 A8 42 27 36 82 4B F4 60 9A C1 64 8C F1 09 5B 5E 72 EE 05 60 08 24 BD 9C 2F D4 01 13 7E 2A 59 2C 4D BF ...B*6.R'.d...[^r.'$.//...~*Y,M.
faa1 BB 3B 7A 42 02 C1 FF 43 00 00 00 00 0B 11 09 07 7A 49 0F 00 00 00 00 20 A3 35 BC 1F 92 6A 08 6C D8 8A 56 ...zB..C.....zI.....5...j.l.V
fac6 E9 92 A7 E1 0F EC 04 EF EE 22 D9 FF DC 31 00 00 00 00 00 00 46 C2 90 9D 46 83 59 01 3E 19 20 28 0B 7B ...*.....l.....F...F.V.>. (f
fae7 08 59 ED 80 2F 15 40 77 D2 FE 7F 3D 99 C1 29 D4 35 04 FE 82 63 5B 55 98 49 19 50 72 C6 6F FD C4 08 01 00 01 ...Y./.@w...=.)..5...c[U.I.Pr.o....
fb0a 00 00 00 01 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
fb2d 00 00 FF FF FF FF 24 03 83 B3 14 04 FE 82 63 5B 08 1F FF 60 F5 A8 3F 03 00 0D 2F F0 9F A4 98 F0 9F 98 8E ...
06fdb50 20 4D 72 2E 20 4D 6F 2F 00 00 00 00 02 00 00 00 00 00 00 00 26 6A 24 AA 21 A9 ED 8F 3B B5 2F 68 78 8D ...Mr. Mo/.....6j9!...;/hx.
06fdb73 61 81 B6 90 DB 11 CA 6D 6C 2C 8B DD D7 0C 80 3A 00 F5 80 BC BD 85 01 95 E7 F8 36 9E 16 00 00 00 00 19 76 ...a...ml,.....6.....v
06fdb96 A9 14 48 B5 C6 98 6B 7B C6 39 0B D1 CC 41 61 54 D1 87 4F E1 16 FD 88 AC 01 20 00 00 00 00 00 00 00 00 ...\.H..k[.9..AaT..O.....
06fdbb9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
06fdbdc 5D 26 CA DA F0 4E 69 E1 7B 81 CD E1 68 CF 06 80 99 DF AE 3C 68 25 87 52 62 13 52 91 07 01 00 00 00 6A 47 ...i...Nl.f...h...<bt>8B.R...jG
06fdbff 30 44 02 20 53 7E 19 23 A8 2B 9C 91 0F B5 52 F2 FA CD 45 ED 89 A0 3C 5D D7 FF 66 09 3C 7E 2D 39 97 83 C1 ...0D.S+.#+...R...E...<\.f.<-9...
06fdcf22 B9 02 20 6E DF FB A1 48 DF AE AB EE CE AC E5 1E 06 04 97 14 16 9A E5 D4 C1 CE 09 5A AF A3 07 23 AE C2 93 ...n..n.m.l,.....Z...#.
06dfc45 01 21 02 4E F6 F5 6D CF E9 04 4C FC 6C 10 B7 17 A5 03 E7 F5 A9 10 31 2F 25 56 0A 99 A0 48 A4 A2 1D 33 C5 ...l.N.m...L.l.....1/AV...H...3.
06dfc68 FF FF FF 02 00 00 00 00 00 00 00 00 00 00 6A 08 68 65 6C 6C 6F 20 77 6F 72 6C 64 00 E1 F5 05 00 00 00 00 ...
06dfc8b 17 A9 14 00 80 51 B4 D9 6A A2 62 69 DF D3 6A F0 EB 9C 2B 2F A8 94 56 87 00 00 00 01 00 00 00 01 42 36 ......Q..j.bi..j...+/.V.....B6
06dfcae 26 08 77 25 3A A4 4C 4F 53 3F 3E 8E 10 3E 9A 84 90 7F 2B 39 ED A6 B7 9F CE DB F0 F5 A4 00 00 00 00 6A 47 ...6m.*%Z.LOS78.>.....+Y.....j
06dfcd1 47 30 44 02 20 19 66 00 77 1E 5B B4 2F 9D 60 75 CA DE 56 14 C5 82 90 A9 31 D3 C7 7C 7A 17 E6 93 38 61 15 ...GOD..f.w.[./..u.v.....1..|z...8a.
06dfcf6 64 CD E1 4D 91 35 39 D7 C9 23 C0 85 F4 FE 3B 80 CA 88 C2 38 0E B0 74 67 B0 11 FB 0E dS.ZK...M.59..#...;...8..tg...
06dfd17 FF 01 21 02 4E F6 F5 6D CF E9 04 4C FC 6C 10 B7 17 A5 03 E7 F5 A9 10 31 2F 25 56 0A 99 A0 48 A4 A2 1D 33 C5 ...!.....7..E...l8...9-I...l...
06dfd3a D1 FF FF FF 02 00 00 00 00 00 00 00 00 00 19 76 A9 14 AF F3 AB 2E FE 82 CF A8 8F 06 32 8C 53 B9 72 BB 4C ...!.....v.....2.S.r.L
06dfd5d 99 DB 48 88 AC 00 00 00 00 00 00 00 00 53 6A 4C 50 00 00 DF 82 00 01 4D 2D 41 88 5B 32 1F A4 F8 F3 F7 8A ...H.....SjLP.....M+A.(2.....

```

Search for: 52429b5d26cadaf04e69e17b81cdb168cf068099fae3c682587526213529107 as Hexadecimal Find Next Find Previous

```

user@ByExample-node:~/deletme$ node hello.js
{ txid: '0615fe519f4583546ea9d39d3ca7628eeea56cd3037ea64d1bb0e967f48d93e4',
  output_no: 0,
  script_asm: 'OP_DUP OP_HASH160 edcce89f510bf95606ec6a79cb28a745c039e220 OP_EQU
ALVERIFY OP_CHECKSIG',
  script_hex: '76a914edcce89f510bf95606ec6a79cb28a745c039e22088ac',
  value: '1.10000000',
  confirmations: 0,
  time: 1533938378 }
Transaction ID:
{"status": "success", "data": {"network": "BTCTEST", "txid": "f917abfa314ebd774a4a659c69c924cab3d8e4e9f4f41ccd7620a985b373a2fb"}}

```

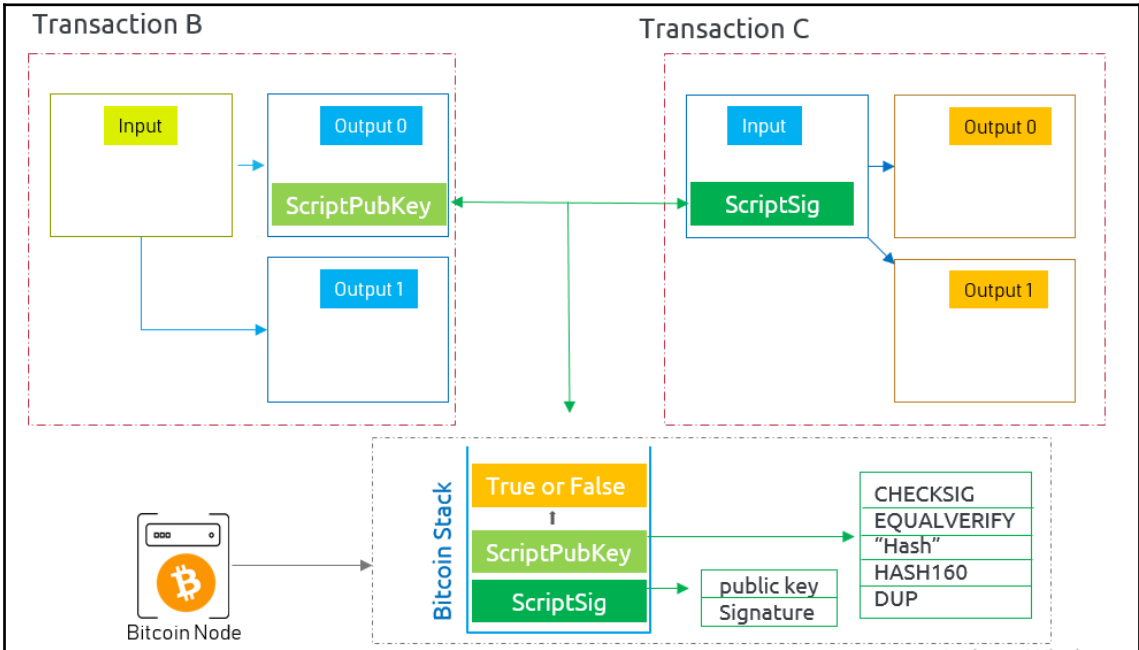

Model	characteristics	Technologies	Strengths
Public blockchain	The general public can join the network and write (under consensus protocol) and read data. This model is a true representation of the original blockchain used in the cryptocurrencies.	Bitcoin, Zcash, Ethereum, Litecoin, NXT, etc..	Full-Decentralization High Security Censorship-resistant Low-trust Anonymity Transparency
Private or internal blockchain	A network under the governance of one organization, which defines the access rules to join its private network. Therefore, only authorized entities can read the transactions data. The organization defines nodes with high trust levels to accept the transaction.	Monax, Symbiont Assembly, Iroha, Kadena, Chain, Quorum, MultiChain.	Confidentiality Authenticated parties Privacy Faster Less expensive
Consortium or hybrid Blockchain	A partly private and permissioned blockchain network operated by known entities such as stakeholders of a given industry regrouped in a consortium or exploiting a shared platform. The network participants have control over who can join the network, and who can participate in the consensus process of the blockchain.	Hyperledger Fabric, Tendermint, Symbiont Assembly, R3 Corda, Iroha, Kadena, Chain, Quorum, MultiChain	Confidentiality Authenticated parties Privacy Faster Less expensive
Blockchain as a service (Baas)	Cloud platform hosted by a service provider to deploy blockchain applications. The service provider manages the blockchain network while the customer defines the business logic.	Bluemix, Azure, Rubix, Stratis, AWS, SAP, Oracle.	Flexibility Scalability Complexity reduction

Chapter 2: Building a Bitcoin Payment System

```

user@ByExample-node:~/deletme$ bitcoin-cli --regtest generate 101
[
  "193a6c217cf7918c1f8b040e415691c131721000746d206e37fc347ede25b1f0",
  "44b3f041bef18fc1265268a752834f5456962b0e7ffe7b2584dd87cd194e0fcc",
  "70edb90d0b3dd510998d15d882b340486dd30eac04bc3650c90d31883f771736",
  "76357d14d35adf2f79b562a6cfa2902defe73fb87efdd115deef2179143aa858",
  "1f1e00f9526fda59632943c96838caed9ee338eef86aa2db2a1ed8dc6e7a794a",
  "347250ca8ed505267dde9f305950dc4e8fd69de37c132f8066a66fa6b0d81168",
  "64f4ca37116dbfbabbdd832a81f469bfc7d83e0856952861344ff05ab2ff1df1",
  "69b3db538b64303c42a8eee7d2ac1d433f03c99803d9623eddc6ebdd8958d65c",
  "07fd1a3186d6bbe7d2613b9ca2ff4ba34dc75205c7992e018d947c10d19aa155",
  "09f31ebf056c4d38070b8dfcd243440de58e299d797464c97e8bb488b49d543b",
  "2d3ed1cad6b92de823f2a7d2f9ed2271f6859a54cf610f856a9bb2fb7e6d0e6c",
  "744db4f8983a5f16c88f723754186289c55a5e985f9f4ac4c5dd71cfe27f7d24",
  "1ac745d9a88a4ef11fd8c64c5ba3a263bcc22694923c32d1483834d60e8df319",
  "31c9709fd9a601688f9ed652dc9034512eb19b956052afd564b16e7b8e57b699",
  "0627f6a23c017f073cb58a0e87acc218aec2fc5ef84cde0f69fadcccbe454630".
]

```

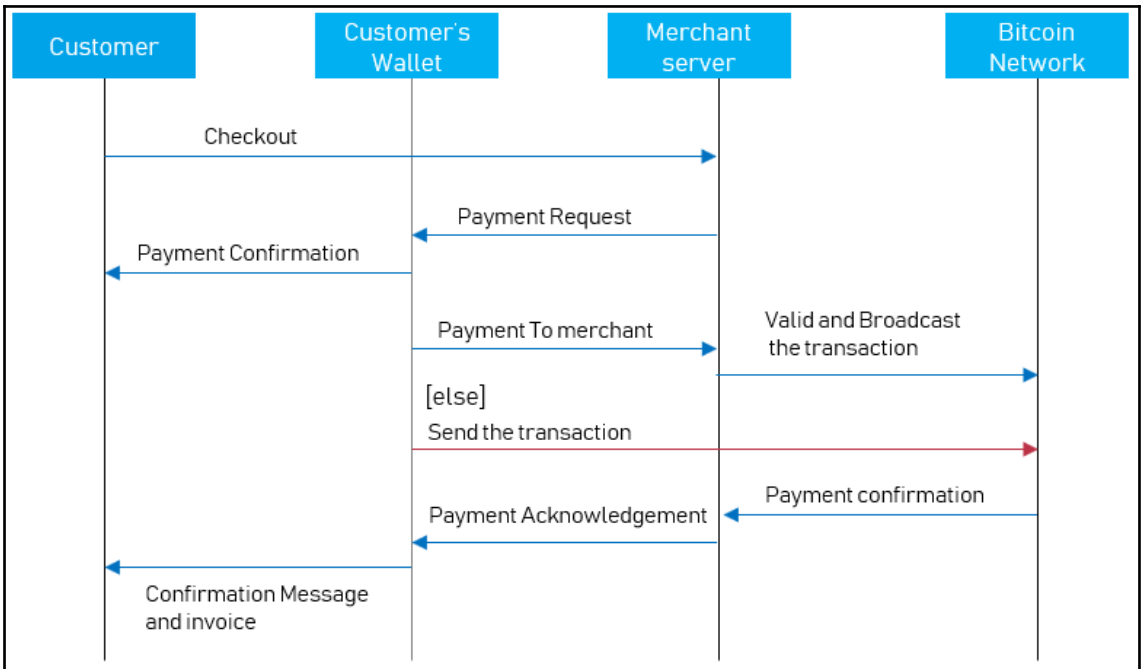
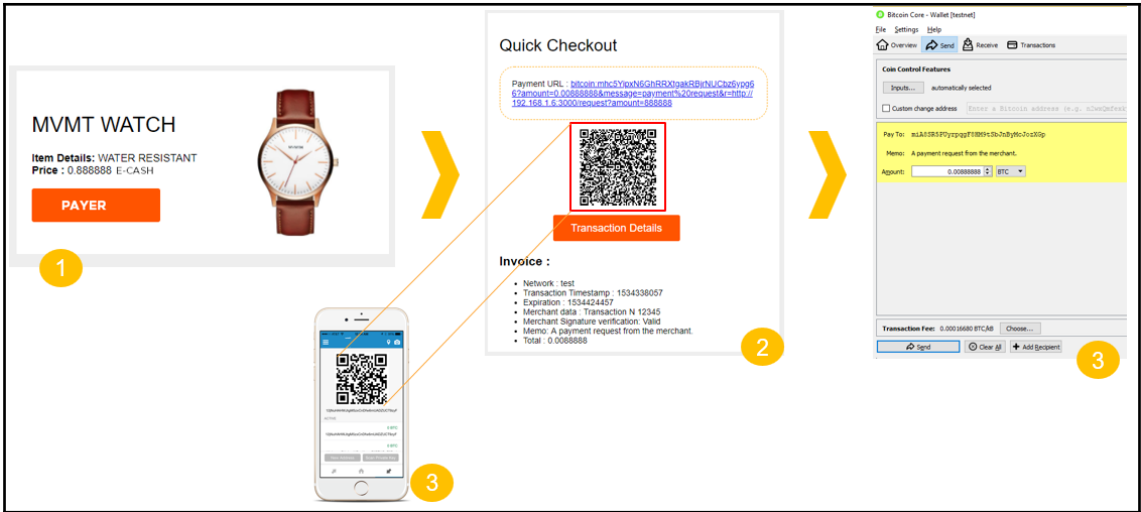


Script Type	Script Format		Description
Pay to PubKey Hash (P2PKH)	ScriptPubKey	OP_DUP OP_HASH160 <PubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	This script is the most popular type in the Bitcoin blockchain. It is used to send Bitcoins to a single address (which is a public key hash encoded in base58check starting with 1).
	ScriptSig	<signature> <PubKey>	
Pay to PubKey (P2PK)	ScriptPubKey	<Public Key> OP_CHECKSIG	This script is usually used by miners to redeem their new mined Bitcoins.
	ScriptSig	<Signature>	
Pay to Script Hash (P2SH)	ScriptPubKey	OP_HASH160 <script Hash> OP_EQUAL	A special script which moves the responsibility for supplying the conditions to redeem a transaction from the creator of the transaction to the receiver(s). This latter must provide a script matching the script hash.
	ScriptSig	<signature> <serialized script>	
Multi-Signature	ScriptPubKey	ScriptPubKey=2 <Public Key A> <Public Key B> <Public Key C> n OP_CHECKMULTISIG	This script locks the output with N public keys, with condition that at least M of those Keys are required. The redeemers should provide M valid signatures corresponding to the N public keys.
	ScriptSig	<Signature1><Signature2>or any permutation of Sig m:n	
P2WSH	ScriptPubKey	zero [32-byte sha256(witness script)]	P2WSH is similar to P2SH but the proof of ownership RedeemScript is moved to the witness instead of ScriptSig (signature + redeem script)
	ScriptSig	Empty (as the signature is located in the witness instead of the ScriptSig)	
Pay-to-Witness-Public-Key-Hash	ScriptPubKey	ScriptPubKey: zero [20-byte hash160(public key)]	P2WPKH is similar to a P2KH but with witness data.
	ScriptSig	Empty	
Null Data:		OP_RETURN OP_DATA_X	This script marks a transaction as provably unspendable and a potential prunable Output. In this case the script is considered as invalid, guaranteeing that there is no corresponding ScriptSig

```

{
  "value": 10.00000000,
  "n": 1,
  "scriptPubKey": {
    "asm": "13 OP_ADD 15 OP_EQUAL",
    "hex": "5d935f87",
    "type": "nonstandard"
  }
}

```



192.168.56.1:3000/checkout

MVMT WATCH

Item Details: WATER RESISTANT
Price : 0.888888 BC.

Pay with BTC



Quick Checkout

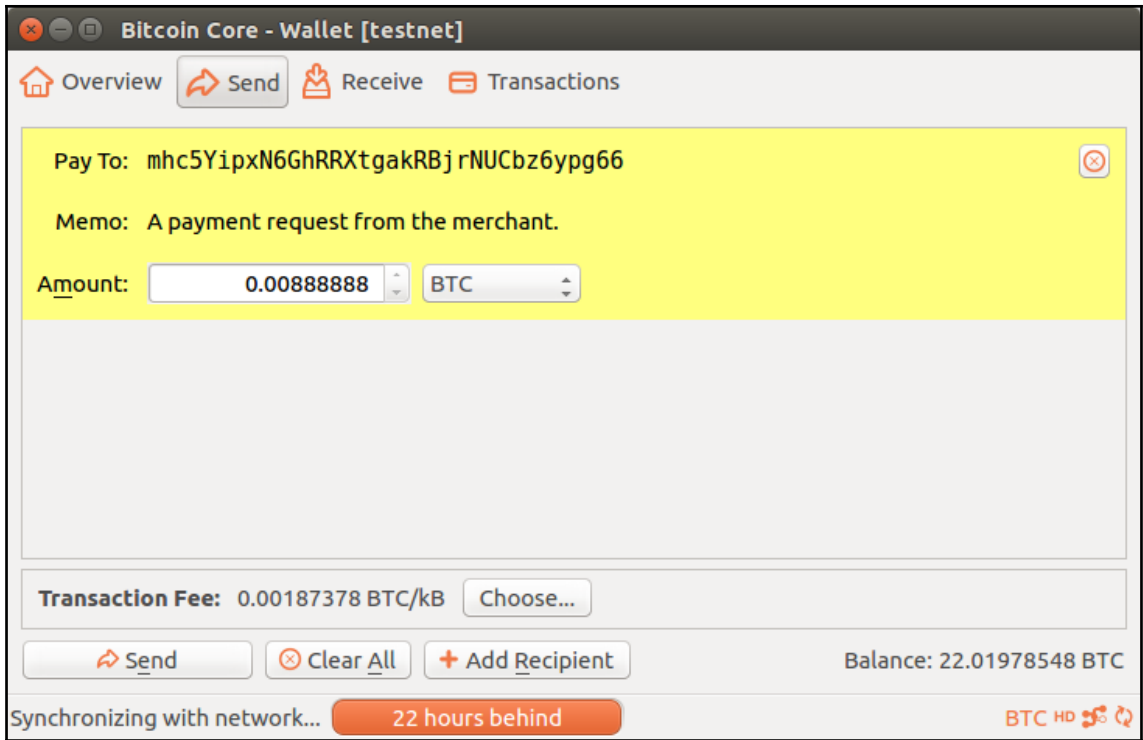
Payment URL : <bitcoin:mhc5YipxN6GhRRXtgakRBjrNUCbz6yppg66?amount=0.00888888&message=payment%20request&r=http://192.168.1.6:3000/request?amount=888888>

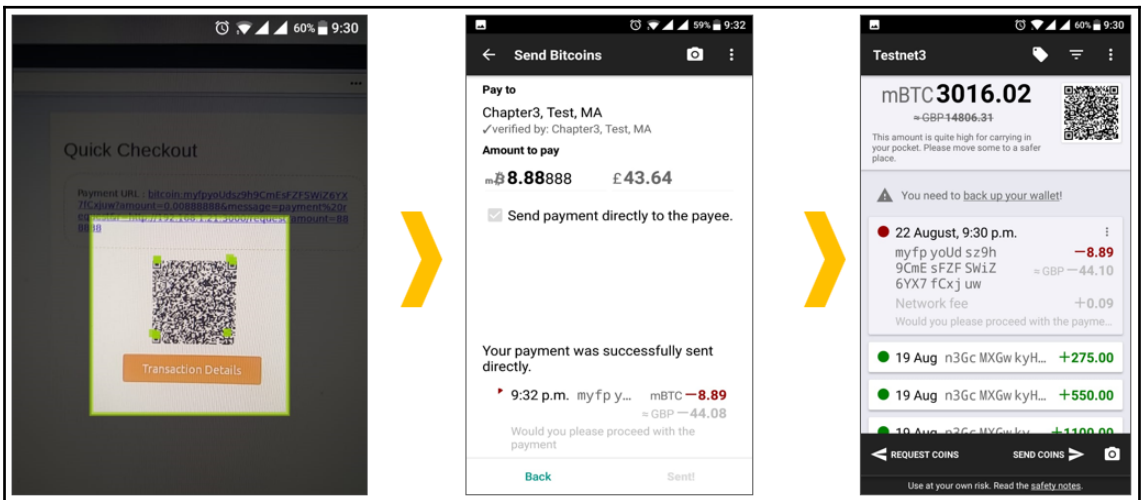
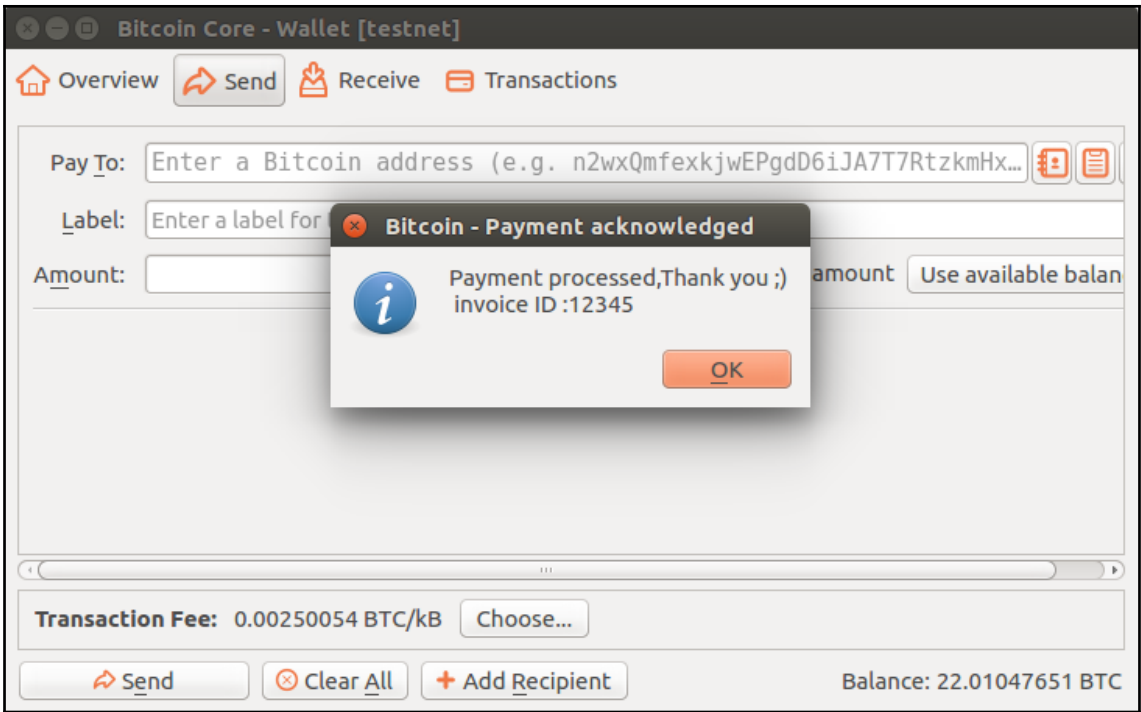


Transaction Details

Invoice :

- Network : test
- Transaction Timestamp : 1534338057
- Expiration : 1534424457
- Merchant data : Transaction N 12345
- Merchant Signature verification: Valid
- Memo: A payment request from the merchant.
- Total : 0.0088888






```
Problems @ Javadoc Declaration Console
<terminated> Cbip70 [Java Application] /usr/lib/jvm/java-8-openjdk-amd64/bin/java (Aug 14, 2018, 2:00:09 PM)
[PeerGroup Inread] INFO org.bitcoinj.core.PeerGroup - waiting 33/5 msec before next connect attempt to [176.9.113.75]:18333
[NioClientManager] INFO org.bitcoinj.net.NioClientManager - Connected to testnet-seed.bitcoin.petertodd.org/82.202.207.182:18333
[NioClientManager] INFO org.bitcoinj.core.Peer - Announcing to testnet-seed.bitcoin.petertodd.org/82.202.207.182:18333 as: /bitcoinj:0
[NioClientManager] INFO org.bitcoinj.net.NioClientManager - Connected to testnet-seed.bitcoin.jonasschnelli.ch/18.222.184.185:18333
[NioClientManager] INFO org.bitcoinj.core.Peer - Announcing to testnet-seed.bitcoin.jonasschnelli.ch/18.222.184.185:18333 as: /bitcoin
[NioClientManager] INFO org.bitcoinj.core.Peer - [195.154.163.75]:18333: Got version=70015, subVer='/Satoshi:0.15.1/', services=0x9, t
[NioClientManager] INFO org.bitcoinj.core.PeerGroup - [195.154.163.75]:18333: New peer (1 connected, 8 pending, 12 max)
[NioClientManager] INFO org.bitcoinj.core.PeerGroup - Setting download peer: [195.154.163.75]:18333
Customer's address : n3UkyjXiy86dChf5nNwD5tJK2AAJ321odQ
Customer's Balance : 165000000
[NioClientManager] INFO org.bitcoinj.net.NioClientManager - Connected to testnet-seed.bluematt.me/198.251.83.19:18333
[NioClientManager] INFO org.bitcoinj.core.Peer - Announcing to testnet-seed.bluematt.me/198.251.83.19:18333 as: /bitcoinj:0.14.7/
[NioClientManager] INFO org.bitcoinj.core.PeerGroup - java.lang.UnsatisfiedLinkError: no secp256k1 in java.library.path
[WalletAppKit STOPPING] INFO org.bitcoinj.core.PeerGroup - Awaiting PeerGroup shutdown ...
```

Run Configurations
Create, manage, and run configurations
Run a Java application

Name: Payment

Main (x) Arguments JRE Classpath Source

Program arguments:

VM arguments:
-Djavax.net.ssl.trustStore=clientkeystore

Revert Apply

Close Run

```

Problems  Javadoc  Declaration  Console  Progress
<terminated> C:\Program Files (x86)\Java\bin\javaw.exe (22 Aug 2018, 19:49:59)
[NioClientManager] INFO org.bitcoinj.core.AbstractBlockchain - Connected orphan 0000000000000000000000000000000000000000000000000000000000000000
[main] INFO org.chapter6.BitcoinClient.Chip7n - Payment Request
[main] INFO org.chapter6.BitcoinClient.Chip7n - Amount to Pay: 0.10888888 BTC
[main] INFO org.chapter6.BitcoinClient.Chip7n - Date: Wed Aug 22 19:50:35 WEST 2018
[main] INFO org.chapter6.BitcoinClient.Chip7n - Message from merchant: Would you please proceed with the payment
[main] INFO org.chapter6.BitcoinClient.Chip7n - Payment requester: Chapter3, Test, Me
[main] INFO org.chapter6.BitcoinClient.Chip7n - Certificate authority: Chapter3, Test, Me
[main] INFO org.bitcoinj.wallet.Wallet - Completing send tx with 1 outputs totalling 0.10888888 BTC and a fee of 0.001 BTC/KB
[main] INFO org.bitcoinj.wallet.Wallet - with 0.9544206 BTC change
[main] INFO org.bitcoinj.wallet.Wallet - completed: 14a0fda370b5dfb88e9aeb5d2b56961ba1df4763adc7e3d2f91ff4ee112a37e
in  PUSHDATA(71)[30440201abb70a242b749ad09c1c40a60f3fc237bc78eb959a3c9713d3f8aac453022020b0c4ab9cee1b40452b3de97e0bdc595ee2d89579453c5b76d0af00d80a2010] PUSHDATA(33)[0330bef1412082360957360f5c97a7905506061e
outpoint:5f04d65b0d6335a8037aba36350949066a26271c691aeeae8c1cd47c4ee11 hash160:d6c9616007808af04793ee33ed6634b20455
out  DUP HASH160 PUSHDATA(20)[0732a2f1672f66143fd9434b9dfcc1cd4b457e] EQUALVERIFY CHECKSIG 0.9544206 BTC
out  DUP HASH160 PUSHDATA(20)[c78fed6a6b23a433aea7038aaaf10f741a4d8fa] EQUALVERIFY CHECKSIG 0.10888888 BTC
fee  0.0010000088 BTC/KB, 0.000227 BTC for 225 bytes
prps USER_PAYMENT

[wallet autosave thread] INFO org.bitcoinj.wallet.WalletFiles - Background saving wallet; last seen block is height 1394677, date 2018-08-22T18:50:33Z, hash 0000000000000000000000000000000000000000000000000000000000000000
[wallet autosave thread] INFO org.bitcoinj.wallet.WalletFiles - Save completed in 977.0 ms
[main] INFO org.bitcoinj.wallet.Wallet - commitTx of 14a0fda370b5dfb88e9aeb5d2b56961ba1df4763adc7e3d2f91ff4ee112a37e
[main] INFO org.bitcoinj.wallet.Wallet - marked 5f04d65b0d6335a8037aba36350949066a26271c691aeeae8c1cd47c4ee11 as spent by 14a0fda370b5dfb88e9aeb5d2b56961ba1df4763adc7e3d2f91ff4ee112a37e
[main] INFO org.bitcoinj.wallet.Wallet - >pending: 14a0fda370b5dfb88e9aeb5d2b56961ba1df4763adc7e3d2f91ff4ee112a37e
[main] INFO org.bitcoinj.wallet.Wallet - Estimated balance is now: 3.02866824 BTC
[main] INFO org.bitcoinj.wallet.KeyChainGroup - Marking key as used: DeterministicKey(pub=0292a6cf4054fbc0f240d333d2ed1cc009e7809765ff7d78211144233557b389, chainCode=11562b0a111a8d2c4b3908e72b9f7c07ae2688794973743d8
[main] INFO org.bitcoinj.wallet.WalletFiles - Saving wallet; last seen block is height 1394678, date 2018-08-22T18:50:34Z, hash 0000000000000000000000000000000000000000000000000000000000000000
[main] INFO org.bitcoinj.wallet.WalletFiles - Save completed in 22.77 ms
[main] INFO org.chapter6.BitcoinClient.Chip7n - Stopping The node...
Memo from merchant :Payment processed,Thank you :)
Invoice ID :12345
Transaction ID : {"status":"success","data":{"network":"BTCTEST","txId":"14a0fda370b5dfb88e9aeb5d2b56961ba1df4763adc7e3d2f91ff4ee112a37e"}}
[PeerGroup Thread] INFO org.bitcoinj.core.PeerGroup - Stopping ...
[walletAppKit STOPPING] INFO org.bitcoinj.core.PeerGroup - Awaiting PeerGroup shutdown ...

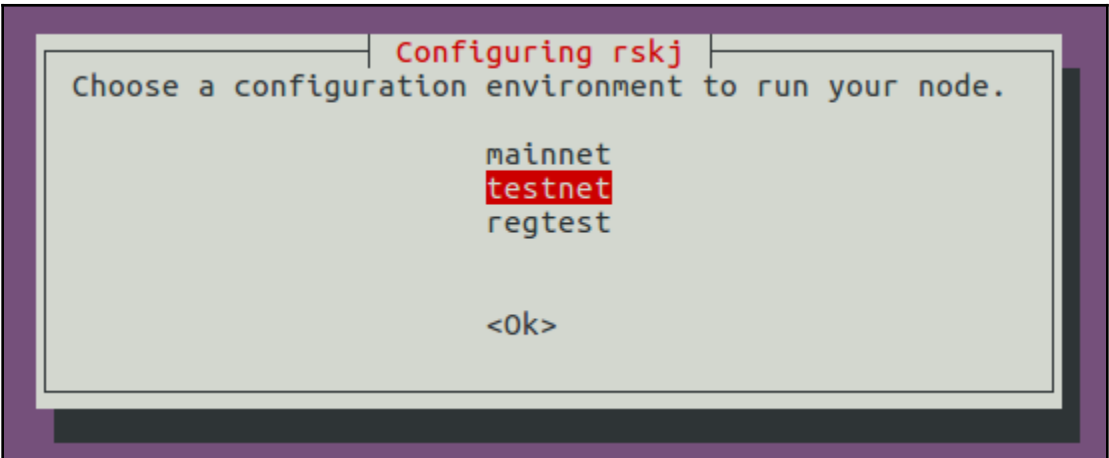
```

Payment request details

Constructed Payment Transaction

Adding Transaction To wallet's Mempool

Confirmation from the server & Transaction and Invoice ID



```

user@ByExample-node:~/Chapter2/utilities/console$ node console.js -server localhost:4444
RSK > web3.personal.newAccount("pwd1234")
0x6dcb977df8fc8b3b82b84bb62d39135b0cb821a9
RSK > web3.eth.getBalance("0xe009f56c37526809bc54089b128c071429938368").toNumber()
0
RSK > web3.eth.blockNumber
17612

```

Compile Run Analysis Testing Debugger Settings Support

Environment Web3 Provider VM (-) ⓘ

Account + 0xca3...a733c (9) 📄 ✎

Gas limit 3000000

Value 0 wei ▾

store ▾ ⓘ

Deploy

or

At Address Load contract from Address

Transactions recorded: ⓘ ▾

Deployed Contracts 🗑️

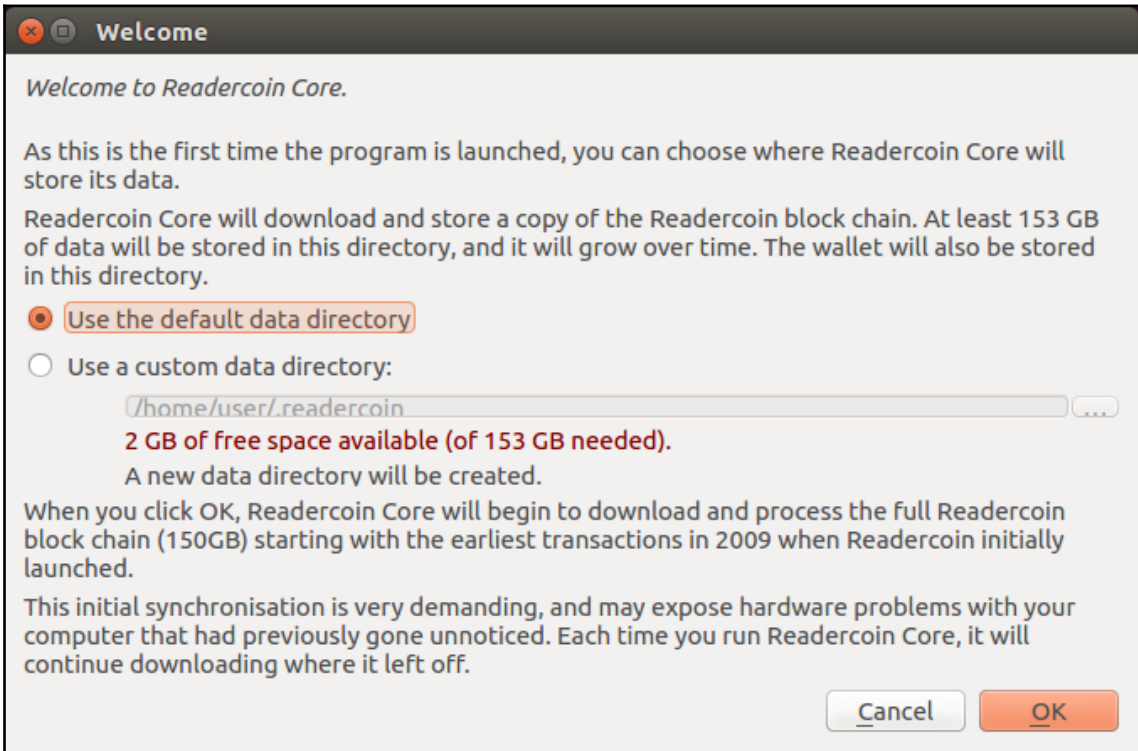
store at 0xef5...46e41 📄 ✕

set "hello" ▾

Message

0: string: hello

Chapter 3: Building Your Own Cryptocurrency



Coin's Name	Readercoin
Con's Symbol	RDC
Block Time	2.5 minute
Initial block reward	10
Halving interval	Every 100000 blocks (174 days)
Ports	RPC port: 19333 P2P port: 9333
Total supply	2000000 units
difficulty readjustment	After 576 blocks
Block size	Up to 8 Mb

Network	Magic value	Sent over wire as
main	0xD9B4BEF9	F9 BE B4 D9
testnet	0xDAB5BFFA	FA BF B5 DA
testnet3	0x0709110B	0B 11 09 07
namecoin	0xFEB4BEF9	F9 BE B4 FE

```

static CBlock CreateGenesisBlock(const char* pszTimestamp, const CScript genesisOutputScript, uint32_t nTime, uint32_t nNonce, uint32_t nBits, int32_t nVersion, const CAmount genesisReward)
{
    CMutableTransaction txNew;
    txNew.nVersion = 1;
    txNew.vin.resize(1);
    txNew.vout.resize(1);
    txNew.vin[0].scriptSig = CScript() << 486604799 << CScriptNum(1) << std::vector<unsigned char>((const unsigned char*)pszTimestamp, (const unsigned char*)pszTimestamp + strlen(pszTimestamp));
    txNew.vout[0].nValue = genesisReward;
    txNew.vout[0].scriptPubKey = genesisOutputScript;

    CBlock genesis;
    genesis.nTime = nTime;
    genesis.nBits = nBits;
    genesis.nNonce = nNonce;
    genesis.nVersion = nVersion;
    genesis.vtx.push_back(MakeTransactionRef(std::move(txNew)));
    genesis.hashPrevBlock.SetNull();
    genesis.hashMerkleRoot = BlockMerkleRoot(genesis);
    return genesis;
}

```

```

user@ByExample-node: ~/GenesisH0
user@ByExample-node:~/GenesisH0$ python genesis.py -z "Blockchain by example 2018" -n 1 -t 1529321830 -v 1000000000 -b 0x1e0ffff0
04ffff001d01041a426c6f636b636861696e206279206578616d706c652032303138
algorithm: SHA256
merkle hash: 6bc2585d63185ac63868cc34e0b017b3fb41c00938eb09bc52a3cf73a31ec6a8
pszTimestamp: Blockchain by example 2018
pubkey: 04678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5f
time: 1529321830
bits: 0x1e0ffff0
Searching for genesis hash..
genesis hash found!
nonce: 490987
genesis hash: 000001a9bbae8bb141c6941838bdacdbcf474b6ed28a0b18b2120b60a68f00ee
user@ByExample-node:~/GenesisH0$

```

```

static CBlock CreateGenesisBlock(uint32_t nTime, uint32_t nNonce, uint32_t nBits, int32_t nVersion, const CAmount genesisReward)
{
    const char* pszTimestamp = "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks";
    const CScript genesisOutputScript = CScript() << ParseHex("04678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5f") << OP_CHECKSIG;
    return CreateGenesisBlock(pszTimestamp, genesisOutputScript, nTime, nNonce, nBits, nVersion, genesisReward);
}

```



```

CAmount GetBlockSubsidy(int nHeight, const Consensus::Params& consensusParams)
{
    int halvings = nHeight / consensusParams.nSubsidyHalvingInterval;
    // Force block reward to zero when right shift is undefined.
    if (halvings >= 64)
        return 0;

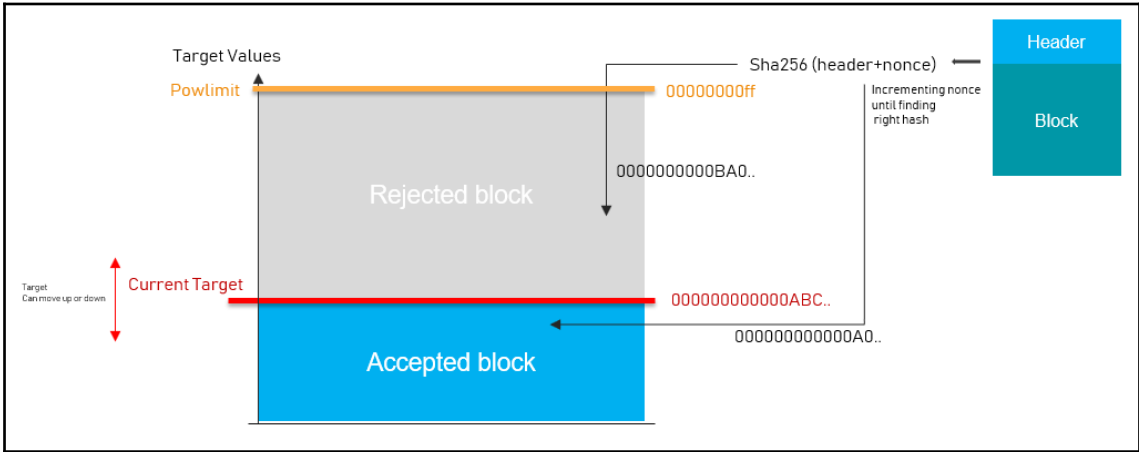
    CAmount nSubsidy = 50 * COIN;
    // Subsidy is cut in half every 210,000 blocks which will occur approximately every 4 years.
    nSubsidy >>= halvings;
    return nSubsidy;
}

```

```

/** No amount larger than this (in satoshi) is valid.
 *
 * Note that this constant is *not* the total money supply, which in Bitcoin
 * currently happens to be less than 21,000,000 BTC for various reasons, but
 * rather a sanity check. As this sanity check is used by consensus-critical
 * validation code, the exact value of the MAX_MONEY constant is consensus
 * critical; in unusual circumstances like a(nother) overflow bug that allowed
 * for the creation of coins out of thin air modification could lead to a fork.
 */
static const CAmount MAX_MONEY = 21000000 * COIN;
inline bool MoneyRange(const CAmount& nValue) { return (nValue >= 0 && nValue <= MAX_MONEY); }

```



```

unsigned int CalculateNextWorkRequired(const CBlockIndex* pindexLast, int64_t nFirstBlockTime, const Consensus::Params& params)
{
    if (params.fPowNoRetargeting)
        return pindexLast->nBits;

    // Limit adjustment step
    int64_t nActualTimespan = pindexLast->GetBlockTime() - nFirstBlockTime;
    if (nActualTimespan < params.nPowTargetTimespan/4)
        nActualTimespan = params.nPowTargetTimespan/4;
    if (nActualTimespan > params.nPowTargetTimespan*4)
        nActualTimespan = params.nPowTargetTimespan*4;

    // Retarget
    const arith_uint256 bnPowLimit = UintToArith256(params.powLimit);
    arith_uint256 bnNew;
    bnNew.SetCompact(pindexLast->nBits);
    bnNew *= nActualTimespan;
    bnNew /= params.nPowTargetTimespan;

    if (bnNew > bnPowLimit)
        bnNew = bnPowLimit;

    return bnNew.GetCompact();
}

```

```

// Size limits
if (block.vtx.empty() || block.vtx.size() * WITNESS_SCALE_FACTOR > MAX_BLOCK_WEIGHT || ::GetSerializeSize(block, SER_NETWORK, PROTOCOL_VERSION |
SERIALIZE_TRANSACTION_NO_WITNESS) * WITNESS_SCALE_FACTOR > MAX_BLOCK_WEIGHT)
    return state.DoS(100, false, REJECT_INVALID, "bad-blk-length", false, "size limits failed");

```

```

/** The maximum allowed size for a serialized block, in bytes (only for buffer size limits) */
static const unsigned int MAX_BLOCK_SERIALIZED_SIZE = 4000000;
/** The maximum allowed weight for a block, see BIP 141 (network rule) */
static const unsigned int MAX_BLOCK_WEIGHT = 4000000;
/** The maximum allowed number of signature check operations in a block (network rule) */
static const int64_t MAX_BLOCK_SIGOPS_COST = 80000;
static const int WITNESS_SCALE_FACTOR = 4;

```

```

consensus.BIP34Height = 227931;
consensus.BIP34Hash = uint256S("0x000000000000024b89b42a942fe0d9fea3bb44ab7bd1b19115dd6a759c0808b8");
consensus.BIP65Height = 388381; // 0000000000000004c2b624ed5d7756c508d90fd0da2c7c679febfa6c4735f0
consensus.BIP66Height = 363725; // 000000000000000379eaa19dce8c9b722d46ae6a57c2f1a988119488b50931

```



```

consensus.nRuleChangeActivationThreshold = 1916; // 95% of 2016
consensus.nMinerConfirmationWindow = 2016; // nPowTargetTimespan / nPowTargetSpacing
consensus.vDeployments[Consensus::DEPLOYMENT_TESTDUMMY].bit = 28;
consensus.vDeployments[Consensus::DEPLOYMENT_TESTDUMMY].nStartTime = 1199145601; // January 1, 2008
consensus.vDeployments[Consensus::DEPLOYMENT_TESTDUMMY].nTimeout = 1230767999; // December 31, 2008

// Deployment of BIP68, BIP112, and BIP113.
consensus.vDeployments[Consensus::DEPLOYMENT_CSV].bit = 0;
consensus.vDeployments[Consensus::DEPLOYMENT_CSV].nStartTime = 1462060800; // May 1st, 2016
consensus.vDeployments[Consensus::DEPLOYMENT_CSV].nTimeout = 1493596800; // May 1st, 2017

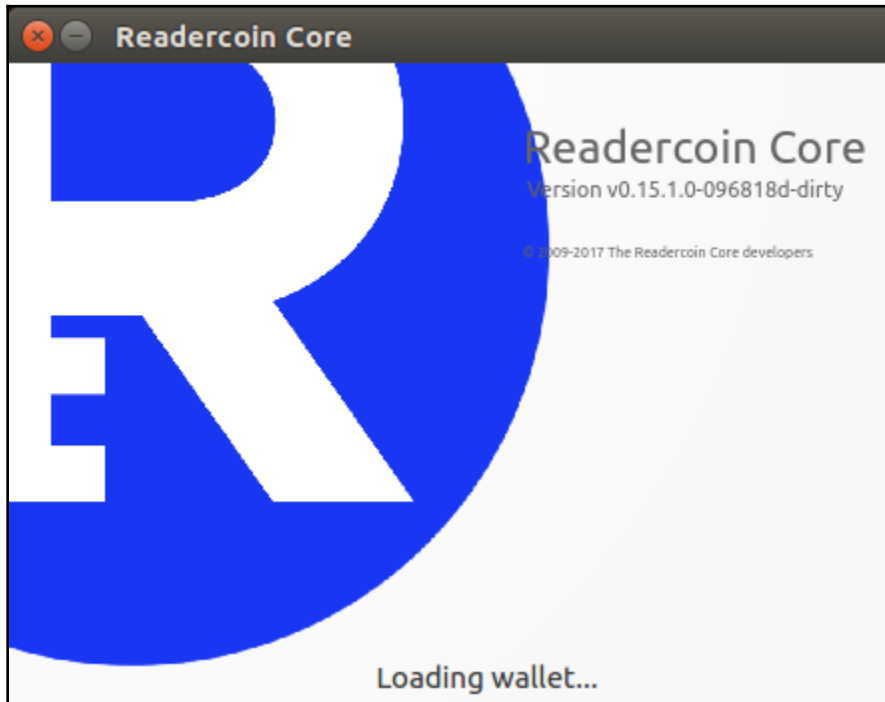
// Deployment of SegWit (BIP141, BIP143, and BIP147)
consensus.vDeployments[Consensus::DEPLOYMENT_SEGWIT].bit = 1;
consensus.vDeployments[Consensus::DEPLOYMENT_SEGWIT].nStartTime = 1479168000; // November 15th, 2016.
consensus.vDeployments[Consensus::DEPLOYMENT_SEGWIT].nTimeout = 1510704000; // November 15th, 2017.

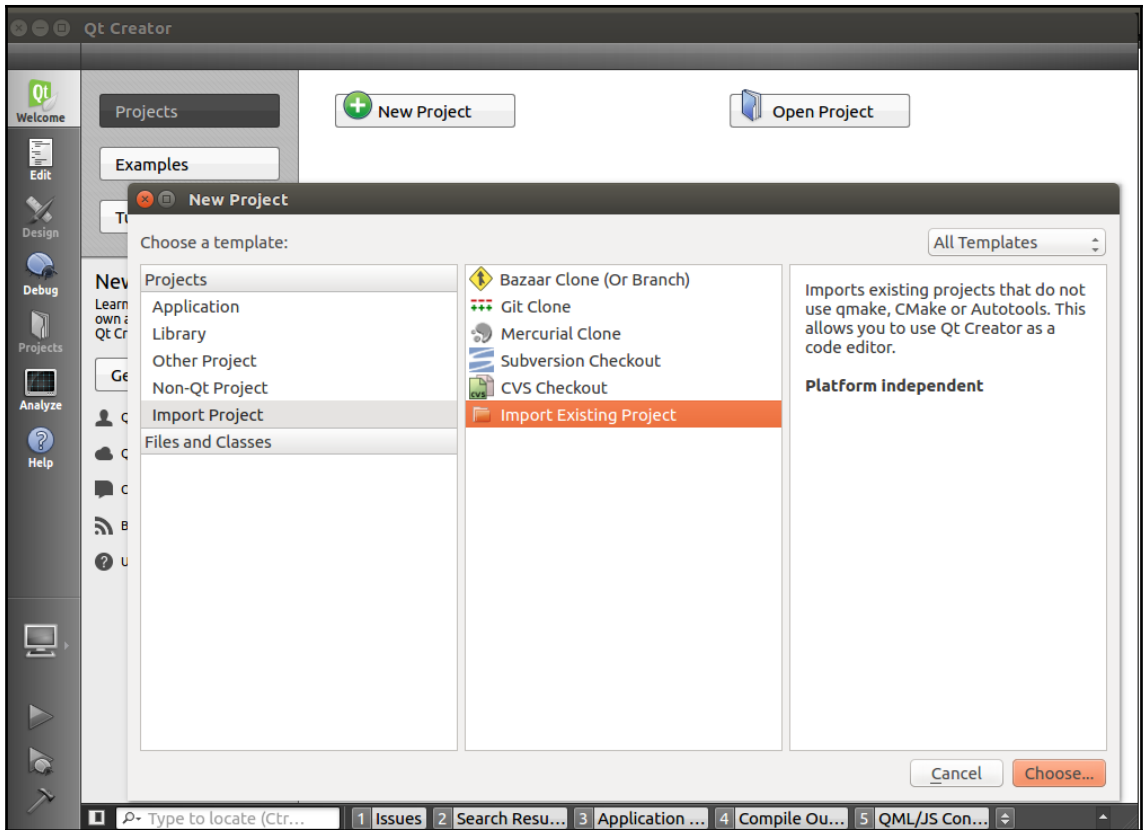
```

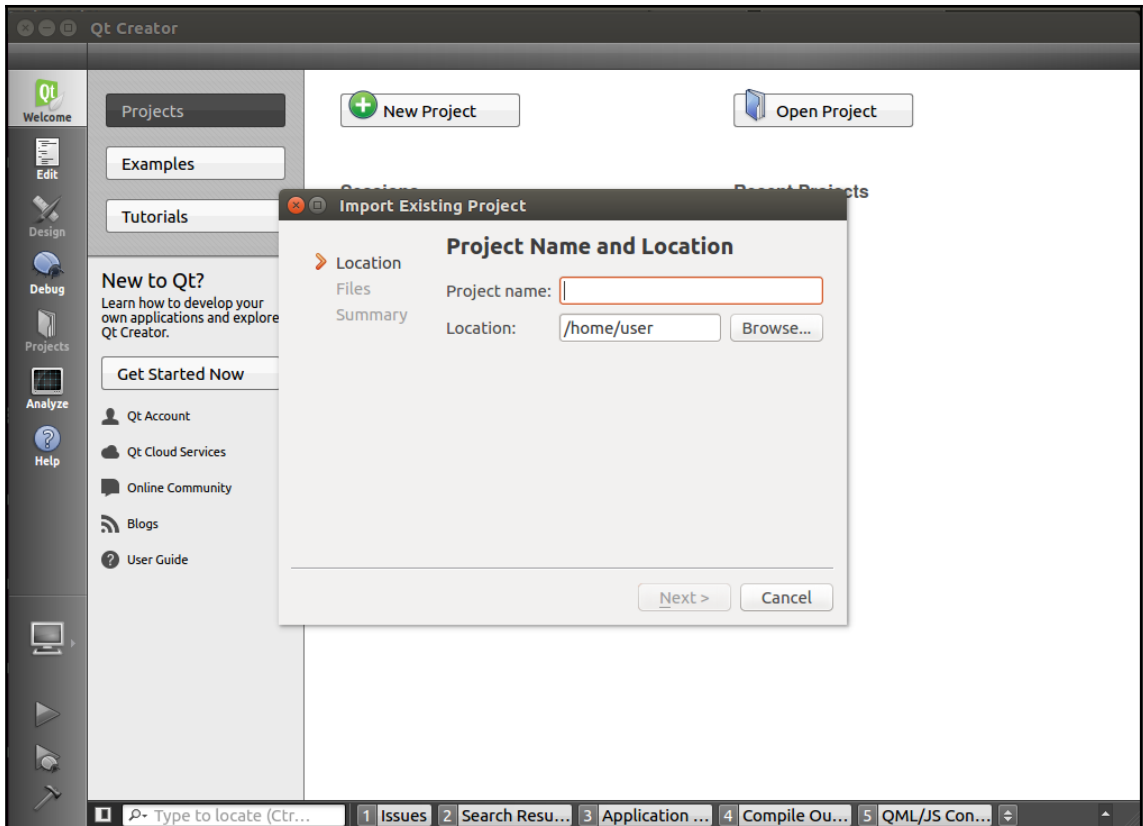
```

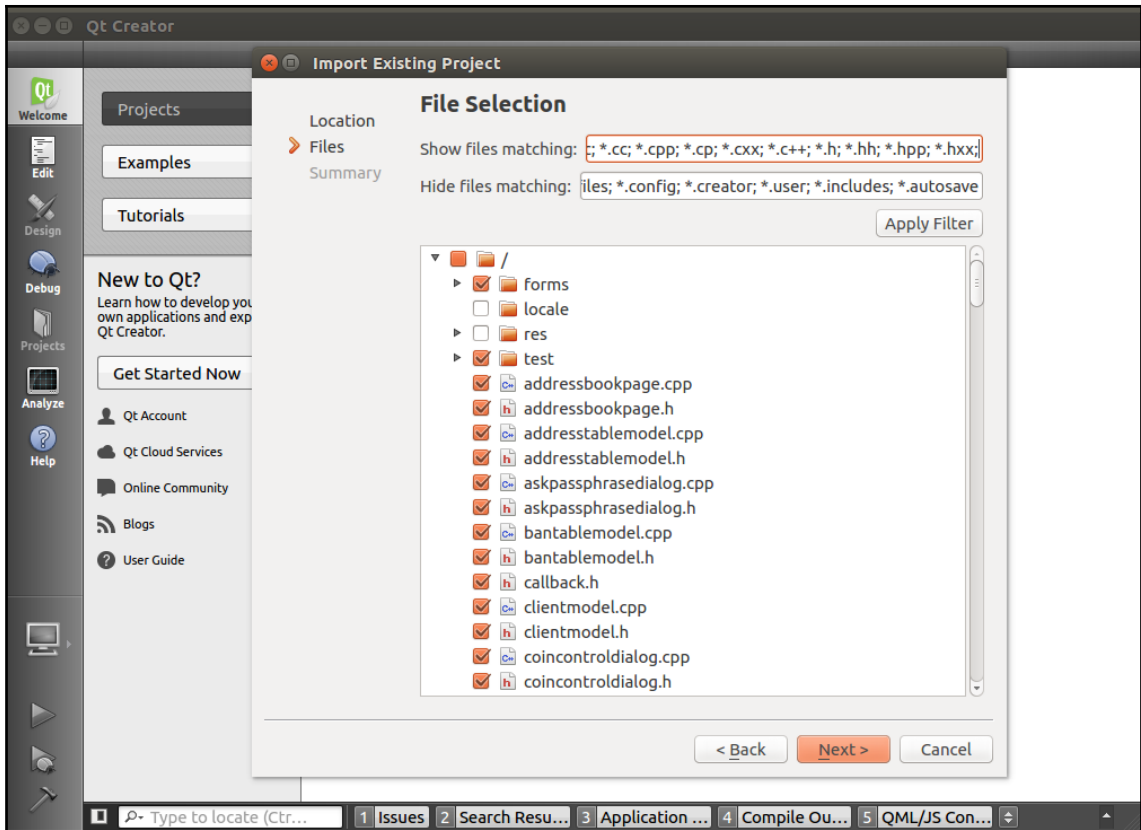
user@ByExample-node:~/workspace/readercoin/src$ ./readercoin-cli addnode 192.168.1.4 onetry
user@ByExample-node:~/workspace/readercoin/src$ ./readercoin-cli getblockchaininfo
{
  "chain": "main",
  "blocks": 187,
  "headers": 187,
  "bestblockhash": "00000b6242a3f38d6635be95badbda19263e1cc657de6ad62f67e113b22d186d",
  "difficulty": 0.000244140625,
  "mediantime": 1528732541,
  "verificationprogress": 0.9894736842105263,
  "chainwork": "00000000000000000000000000000000000000000000000000000000bc00bc0",
  "pruned": false,
  "softforks": [
    {
      "id": "bip34",
      "version": 2,
      "reject": {
        "status": false
      }
    },
    {
      "id": "bip66",
      "version": 3,
      "reject": {
        "status": false
      }
    },
    {
      "id": "bip65",
      "version": 4,
      "reject": {
        "status": false
      }
    }
  ],
  "bip9_softforks": {
    "csv": {
      "status": "defined",
      "startTime": 1528707955,
      "timeout": 1528707955,
      "since": 0
    },
    "segwit": {
      "status": "defined",
      "startTime": 1528707955,

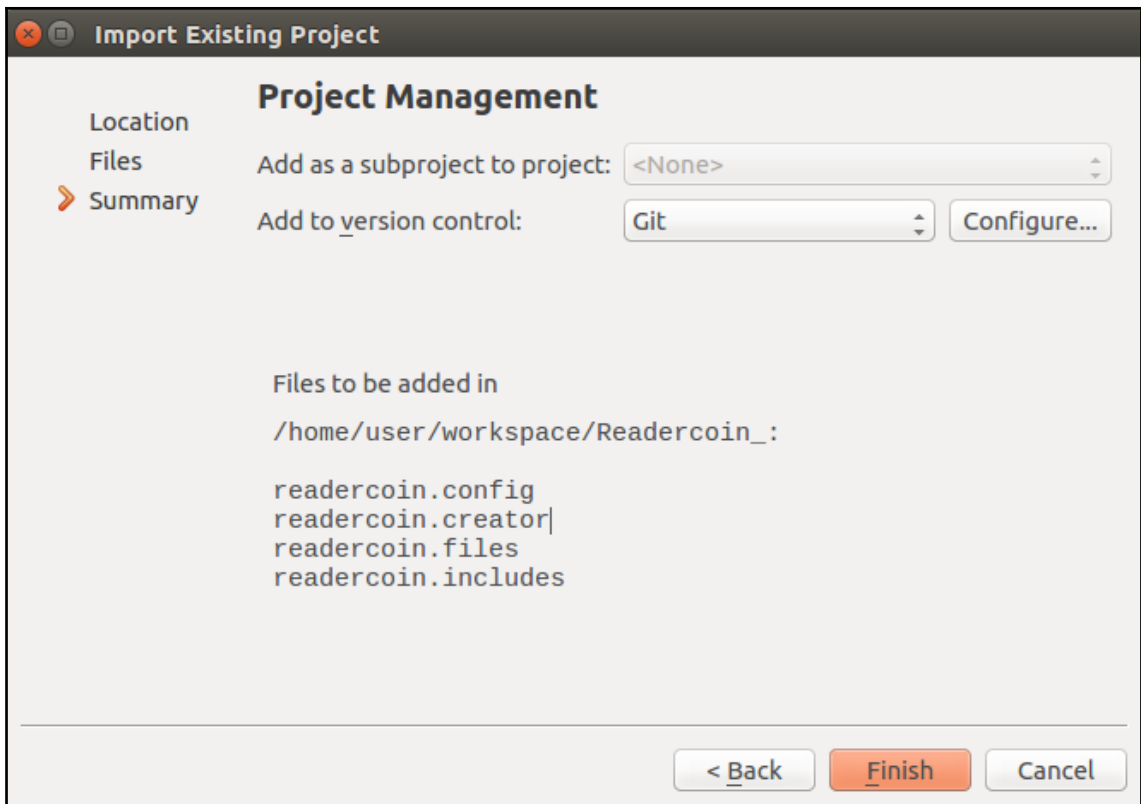
```

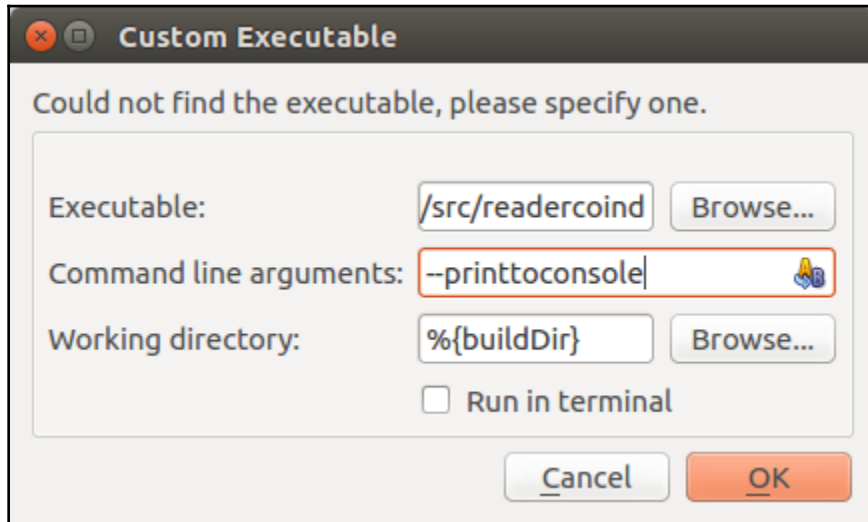
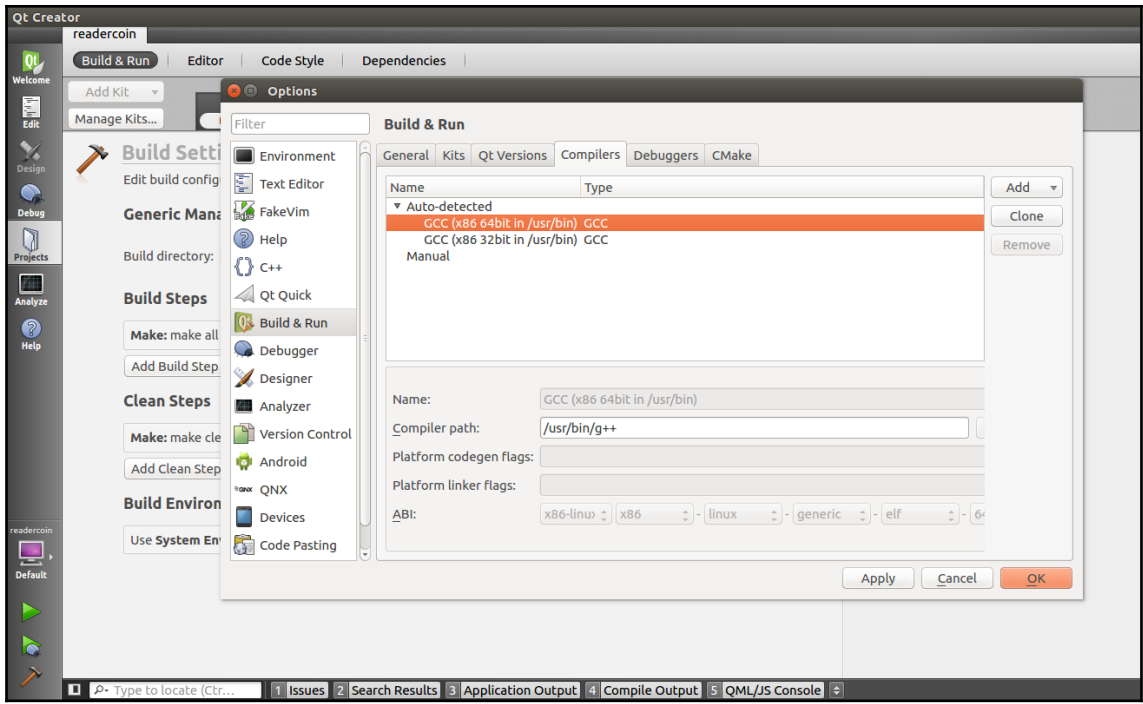


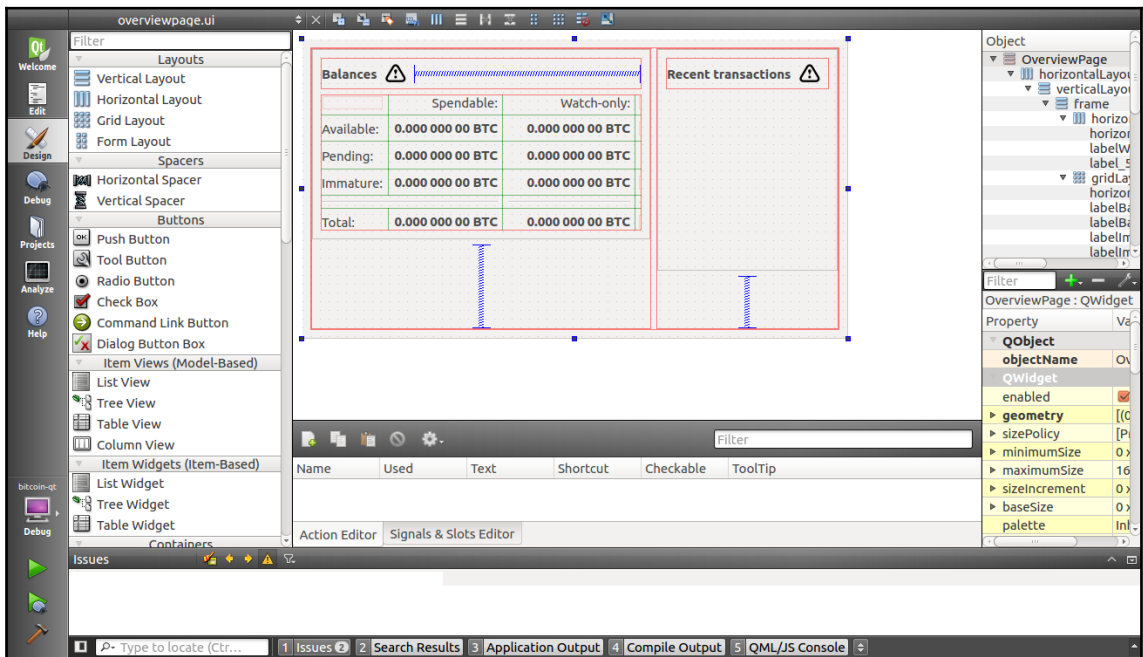
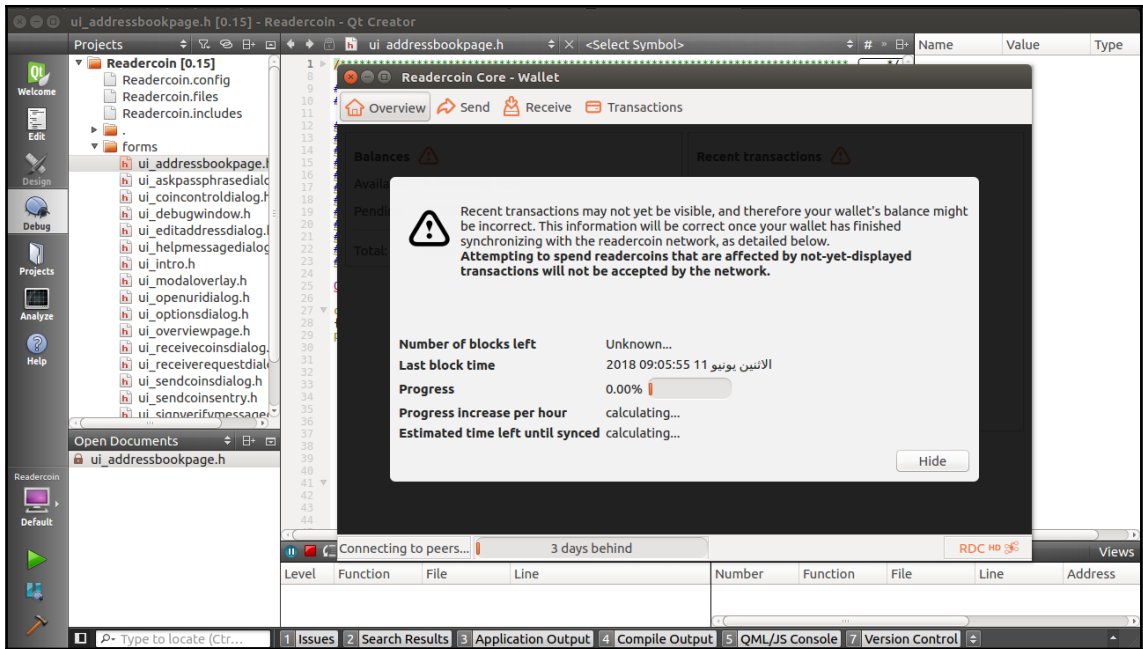








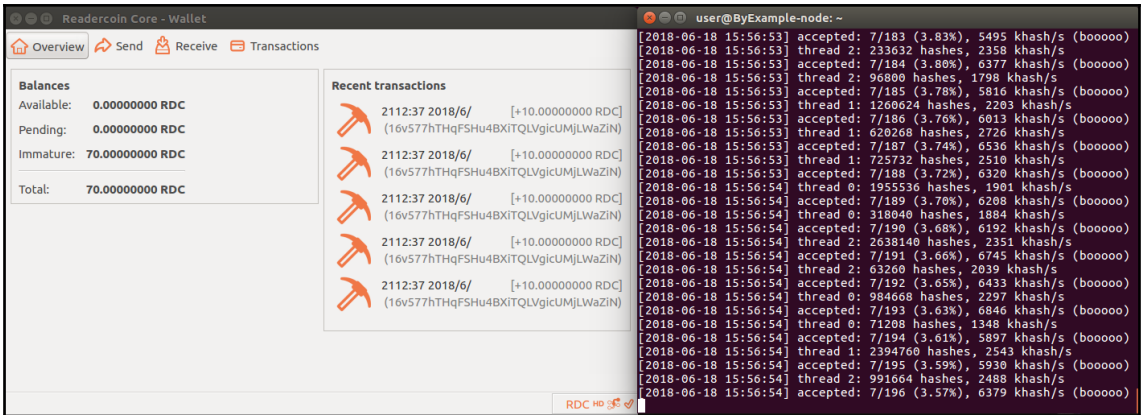
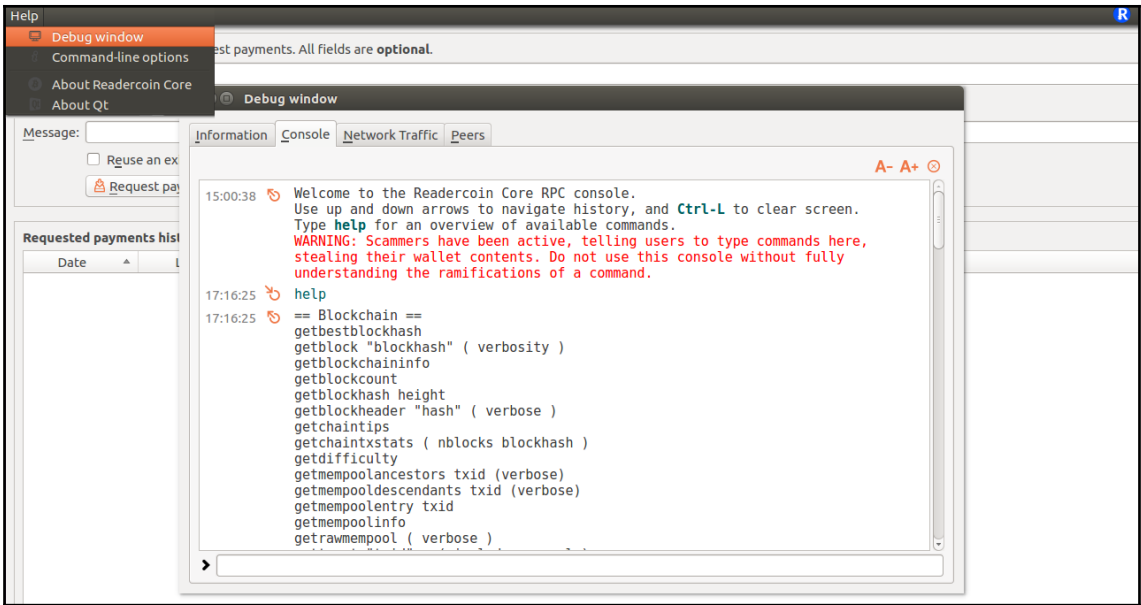





```
user@ByExample-node: ~/workspace/readercoin/src
2018-06-15 21:42:22 Readercoin version v0.15.1.0-unk
2018-06-15 21:42:22 InitParameterInteraction: parameter interaction: -whitelistedforcerelay=1 -> setting -whitelistrelay=1
Readercoin hashGenesisBlock:00000375b8aa3b506e2d5b2aa4f5c7510608f50d37bfbdb55d2ff581425adc
Readercoin merkle:dbc2585d63185acf3868cc34e0b017b3fb41c0938eb09bc52a3cf73a31ec6a8
Readercoin hashGenesisBlock:00000375b8aa3b506e2d5b2aa4f5c7510608f50d37bfbdb55d2ff581425adc
Readercoin merkle:dbc2585d63185acf3868cc34e0b017b3fb41c0938eb09bc52a3cf73a31ec6a8
2018-06-15 21:42:22 Assuming ancestors of block 00000375b8aa3b506e2d5b2aa4f5c7510608f50d37bfbdb55d2ff581425adc have valid signatures.
2018-06-15 21:42:22 Setting nMinimumChainWork=0000000000000000000000000000000000000000000000000000000000000000
2018-06-15 21:42:22 Using the 'standard' SHA256 implementation
2018-06-15 21:42:22 Using Rnd as an additional entropy source
2018-06-15 21:42:22 Default data directory /home/user/.readercoin
2018-06-15 21:42:22 Using data directory /home/user/.readercoin
2018-06-15 21:42:22 Using config file /home/user/.readercoin/readercoin.conf
2018-06-15 21:42:22 Using at most 125 automatic connections (1024 file descriptors available)
2018-06-15 21:42:22 Using 16 MiB out of 32/2 requested for signature cache, able to store 524288 elements
2018-06-15 21:42:22 Using 16 MiB out of 32/2 requested for script execution cache, able to store 524288 elements
2018-06-15 21:42:22 Using 3 threads for script verification
2018-06-15 21:42:22 HTTP: creating work queue of depth 16
2018-06-15 21:42:22 Config options rpcuser and rpcpassword will soon be deprecated. Locally-run instances may remove rpcuser to use cookie-based auth, or may be replaced with rpcauth. Please see share/rpcuser for rpcauth generation.
2018-06-15 21:42:22 HTTP: starting 4 worker threads
2018-06-15 21:42:22 init message: Verifying wallet(s)...
2018-06-15 21:42:22 Using BerkeleyDB version Berkeley DB 4.8.30: (April 9, 2010)
2018-06-15 21:42:22 Using wallet wallet.dat
2018-06-15 21:42:22 CDBEnv::Open: LogDir=/home/user/.readercoin/database ErrorFile=/home/user/.readercoin/db.log
2018-06-15 21:42:22 scheduler thread start
2018-06-15 21:42:22 Cache configuration:
2018-06-15 21:42:22 * Using 2.0MiB for block index database
2018-06-15 21:42:22 * Using 8.0MiB for chain state database
2018-06-15 21:42:22 * Using 440.0MiB for in-memory UTXO set (plus up to 286.1MiB of unused mempool space)
2018-06-15 21:42:22 scheduler thread start
2018-06-15 21:42:22 init message: Loading block index...
2018-06-15 21:42:22 Opening LevelDB in /home/user/.readercoin/blocks/index
2018-06-15 21:42:22 Opened LevelDB successfully
2018-06-15 21:42:22 Using obfuscation key for /home/user/.readercoin/blocks/index: 0000000000000000
2018-06-15 21:42:22 LoadBlockIndexDB: last block file = 0
2018-06-15 21:42:22 LoadBlockIndexDB: last block file info: CBlockFileInfo(blocks=1, size=250, heights=0...0, time=2018-06-11...2018-06-11)
2018-06-15 21:42:22 Checking all blk files are present...
2018-06-15 21:42:22 LoadBlockIndexDB: transaction index disabled
2018-06-15 21:42:22 Opening LevelDB in /home/user/.readercoin/chainstate
2018-06-15 21:42:22 Opened LevelDB successfully
2018-06-15 21:42:22 Using obfuscation key for /home/user/.readercoin/chainstate: 55e071fdc67e0441
2018-06-15 21:42:22 Loaded best chain: hashBestChain=00000375b8aa3b506e2d5b2aa4f5c7510608f50d37bfbdb55d2ff581425adc height=0 date=2018-06-11 09:05:55 progress=0.00003
2018-06-15 21:42:22 init message: Rewinding blocks...
```

```
user@ByExample-node: ~
2018-06-18 14:06:11 Bound to [::]:7333
2018-06-18 14:06:11 Bound to 0.0.0.0:7333
2018-06-18 14:06:11 init message: Loading P2P addresses...
2018-06-18 14:06:11 Loaded 0 addresses from peers.dat 0ms
2018-06-18 14:06:11 init message: Loading banlist...
2018-06-18 14:06:11 init message: Starting network threads...
2018-06-18 14:06:11 init message: Done loading
2018-06-18 14:06:11 torcontrol thread start
2018-06-18 14:06:11 net thread start
2018-06-18 14:06:11 dnsseed thread start
2018-06-18 14:06:11 Loading addresses from DNS seeds (could take a while)
2018-06-18 14:06:11 msghand thread start
2018-06-18 14:06:11 0 addresses found from DNS seeds
2018-06-18 14:06:11 dnsseed thread exit
2018-06-18 14:06:11 Imported mempool transactions from disk: 0 successes, 0 failed, 0 expired
2018-06-18 14:06:11 opencon thread start
2018-06-18 14:06:11 adcon thread start
2018-06-18 14:06:14 connect() to 192.168.1.7:9333 failed after select(): No route to host (113)
2018-06-18 14:06:14 Leaving InitialBlockDownload (latching to false)
2018-06-18 14:06:14 receive version message: /Satoshi:0.15.1/: version 70015, blocks=0, us=[::]:0, peer=0
```

```
user@ByExample-node: ~/bitcoin
user@ByExample-node:~/bitcoin$ ./src/bitcoin-cli getconnectioncount
2
user@ByExample-node:~/bitcoin$ ./src/bitcoin-cli getpeerinfo
[
  {
    "id": 23,
    "addr": "192.168.1.3:8333",
    "services": "0000000000000005",
    "relaytxes": true,
    "lastsend": 1511116445,
    "lastrecv": 1511116478,
    "bytessent": 355,
    "bytesrecv": 5636,
    "conntime": 1511116445,
    "timeoffset": 0,
    "pingtime": 0.015793,
    "minping": 0.015793,
    "version": 70012,
    "subver": "/Satoshi:0.12.1/",
    "inbound": false,
    "startingheight": 0,
    "banscore": 0,
    "synced_headers": -1,
    "synced_blocks": -1,
    "inflight": [
    ],
    "whitelisted": false
  }
]
```



```

user@ByExample-node:~/workspace/readercoin/src$ ./readercoin-cli addnode 192.168.1.4 onetry
user@ByExample-node:~/workspace/readercoin/src$ ./readercoin-cli getblockchaininfo
{
  "chain": "main",
  "blocks": 187,
  "headers": 187,
  "bestblockhash": "00000b6242a3f38d6635be95badbda19263e1cc657de6ad62f67e113b22d186d",
  "difficulty": 0.000244140625,
  "mediantime": 1528732541,
  "verificationprogress": 0.9894736842105263,
  "chainwork": "00000000000000000000000000000000000000000000000000000000bc00bc0",
  "pruned": false,
  "softforks": [
    {
      "id": "bip34",
      "version": 2,
      "reject": {
        "status": false
      }
    },
    {
      "id": "bip66",
      "version": 3,
      "reject": {
        "status": false
      }
    },
    {
      "id": "bip65",
      "version": 4,
      "reject": {
        "status": false
      }
    }
  ],
  "bip9_softforks": {
    "csv": {
      "status": "defined",
      "startTime": 1528707955,
      "timeout": 1528707955,
      "since": 0
    },
    "segwit": {
      "status": "defined",
      "startTime": 1528707955,

```

```
Terminal File Edit View Search Terminal Help
user@ByExample-node:~$ readercoin-cli getblockhash 0
000003758b8aa3b5066e2d5b2aa4f5c7516868f50d37bfd55d52ff581425adc
user@ByExample-node:~$ readercoin-cli getblock 000003758b8aa3b5066e2d5b2aa4f5c7516868f50d37bfd55d52ff581425adc
{
  "hash": "000003758b8aa3b5066e2d5b2aa4f5c7516868f50d37bfd55d52ff581425adc",
  "confirmations": 1,
  "strippedsize": 242,
  "size": 242,
  "weight": 968,
  "height": 0,
  "version": 1,
  "versionHex": "00000001",
  "merkleroot": "6bc2585d63185acf3868cc34e0b017b3fb41c00938eb09bc52a3cf73a31ec6a8",
  "tx": [
    "6bc2585d63185acf3868cc34e0b017b3fb41c00938eb09bc52a3cf73a31ec6a8"
  ],
  "time": 1528707955,
  "mediantime": 1528707955,
  "nonce": 690552,
  "bits": "1e0ffff0",
  "difficulty": 0.000244140625,
  "chainwork": "00000000000000000000000000000000000000000000000000000000000000000000100010"
}
user@ByExample-node:~$
```

The screenshot shows the 'Readercoin Core - Wallet' application window. At the top, there are navigation tabs: Overview, Send, Receive, and Transactions. The 'Send' tab is active. The main area contains a form for creating a transaction:

- Pay To:** 125GsQaXzP9p5pvw1ofL7EK9ArnQvQu7x6
- Label:** test
- Amount:** 1.00000000 RDC
- Subtract fee from amount

Below the form, there is a section for **Transaction Fee** with a warning: "Warning: Fee estimation is currently not possible." A dropdown menu is open, showing various fee estimation options:

- Recommended: 0.00020000 RDC/kB (Sm...)
- Confirmation time target: 15 minutes (6 blocks) (highlighted)
- Custom: per kilobyte 0.00...
- Request Replace-By-Fee

Other options in the dropdown include: 5 minutes (2 blocks), 10 minutes (4 blocks), 30 minutes (12 blocks), 60 minutes (24 blocks), 2 hours (48 blocks), 6 hours (144 blocks), 21 hours (504 blocks), and 42 hours (1008 blocks). The interface also shows a 'Balance: 710.00000000 RDC' and a 'Send' button.

127.0.0.1:3001/block/000003758b8aa3b506e2d5b2aa4f5c7516868f50d37bfb55d52f581425adc

IQUIDUS Explorer Movement Network Top 100 Markets API

Network (GH/s): 0.0000 Difficulty: 0.000244140625 Coin Supply (RDC): 0 BTC Price: 0.00000000

You may enter a block height, block hash, tx hash or address. Search

RDC Block: 000003758b8aa3b506e2d5b2aa4f5c7516868f50d37bfb55d52f581425adc

Height	Difficulty	Confirmations	Size (kB)	Bits	Nonce	Timestamp
0	0.0002	1	0.24	1e0ff1f0	690552	11th Jun 2018 09:05:55

GENESIS

192.168.1.12:3000/funds#/deposits/btc


PEATIO Trade Funds Solvency History test@readercoin.com

Funds

\$ 0.00000 USD 0.0	Deposit Withdraw
3.00000 BTC 0.0	Deposit Withdraw
0.00000 ETH 0.0	Deposit Withdraw
10.00000 RDC 10.0	Deposit Withdraw

RDC Deposit

- Please use your common wallet services, local wallet, mobile terminal or online wallet, select a payment and send.
- Please paste the address blow in your wallet, and fill in the amount you want to deposit, then confirm and send.



Address: 1HtknsgEWpMp,y1chxHLwHxe11qS9oc9fm New Address

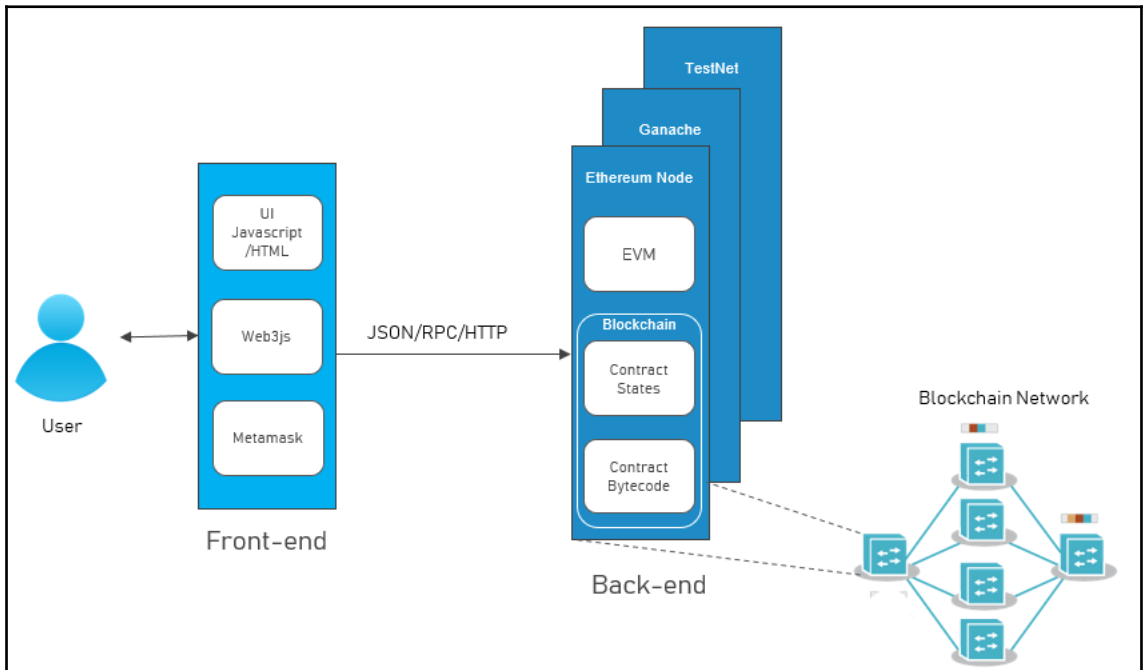
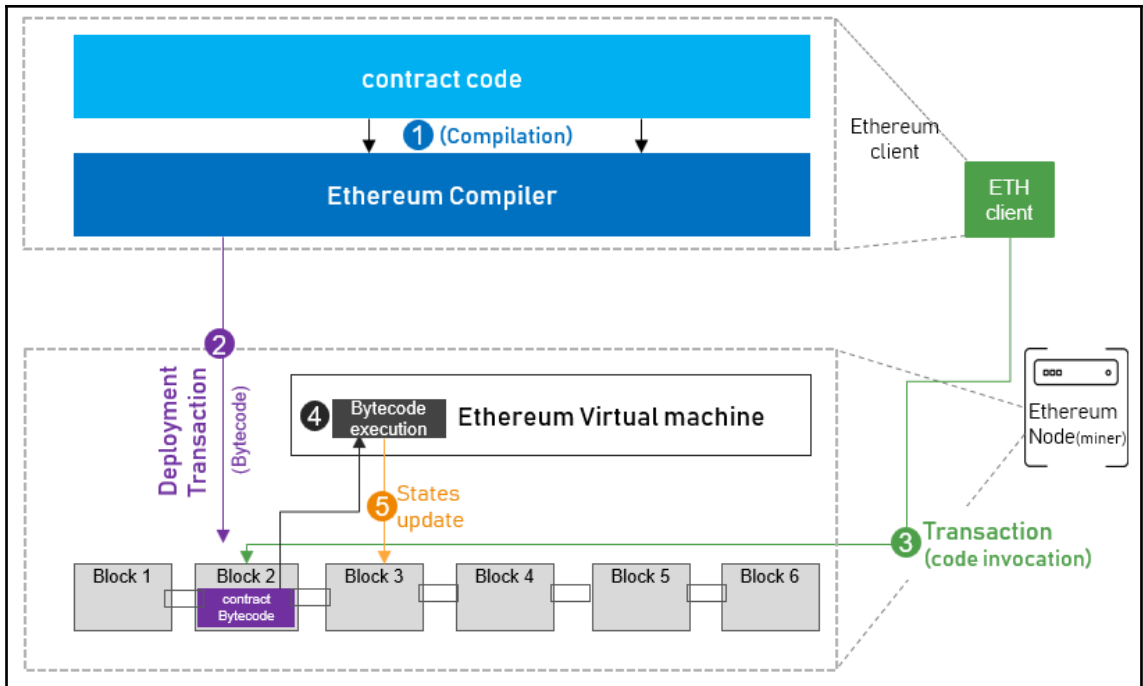
Scanning QR code to Pay for in the mobile terminal wallet.
- Once you complete sending, you can check the status of your new deposit below.

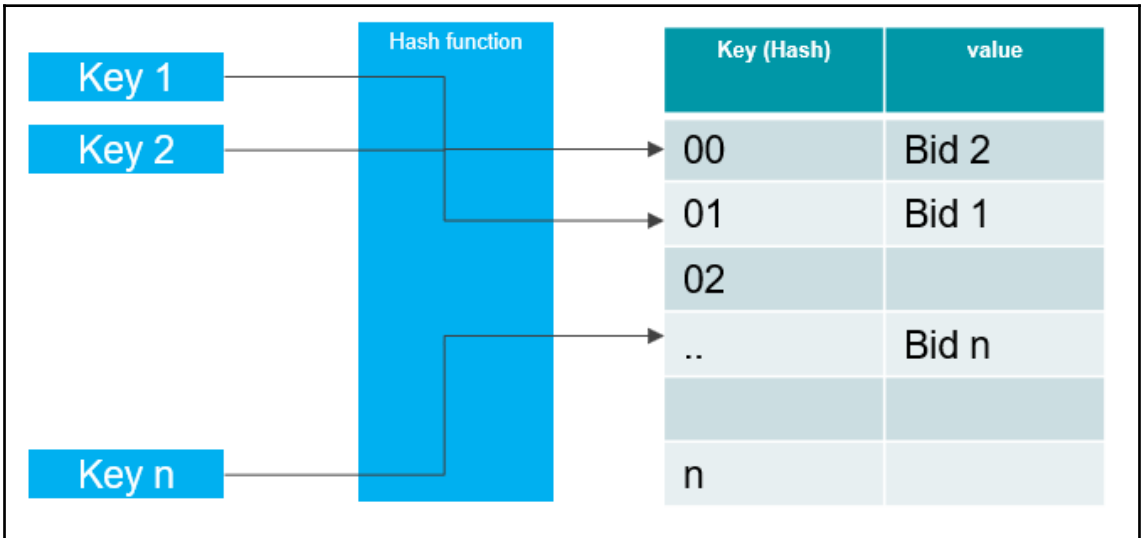
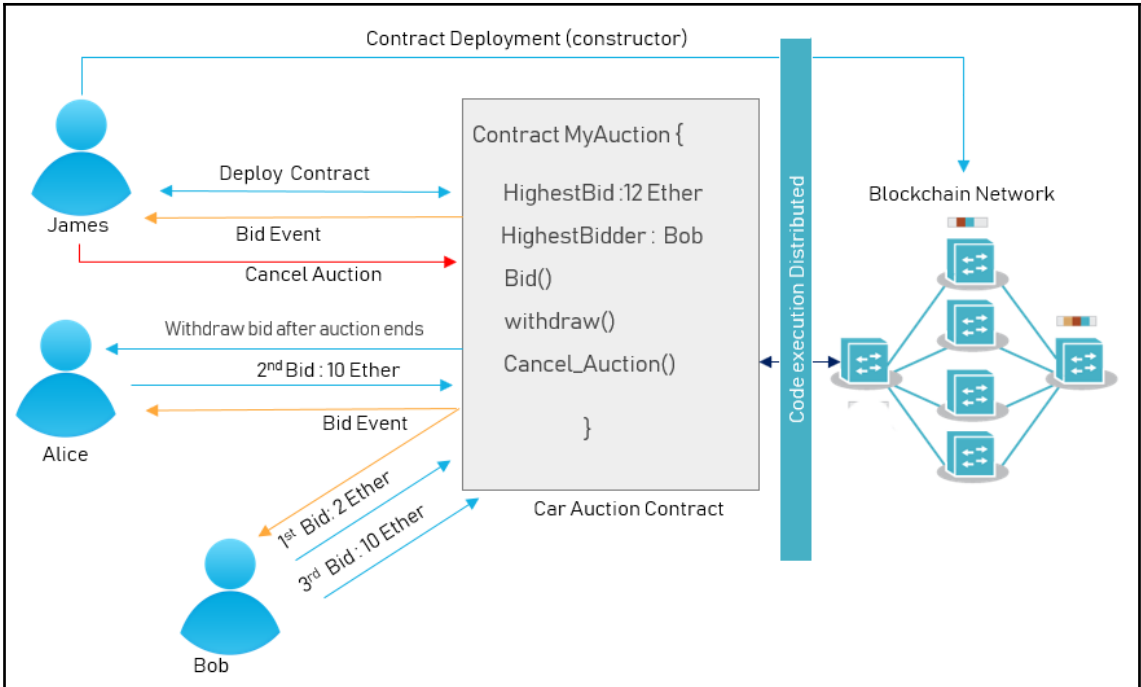
Deposit History

Time	Transaction ID	Amount	Confirmations	State/Action
------	----------------	--------	---------------	--------------

Chapter 4: Peer-to-Peer Auctions in Ethereum

	Ethereum	Bitcoin
Smart Contracting	Universal and Turing-complete scripting language.	Forth-like language Locking unlocking scripts.
Mining algorithm	Ethash PoW, specialized hardware resistant.	PoW based on SHA-256, non-specialized hardware resistant
Cryptocurrency Generation	3 Ethers per block after Byzantium Fork (It will be reduced in near future to 2 Ethers)	Initially 50 Bitcoin, which halves every 210,000 blocks (currently 12,5 Bitcoin)
Average confirmation time	GHOST (fast block confirmation time, 3 ~ 30 sec)	Slow block confirmation (an average of 10 minutes)
stale blocks	Uncles and nephews blocs are accepted	Orphaned blocks are rejected
Blockchain Model	Account model with two types: <ul style="list-style-type: none">• External accounts• Contract accounts	UTXO model.





```
require(msg.sender == owner);
```

```
if(msg.sender != owner) { throw; }  
if(msg.sender != owner) { revert(); }  
assert(msg.sender == owner);
```

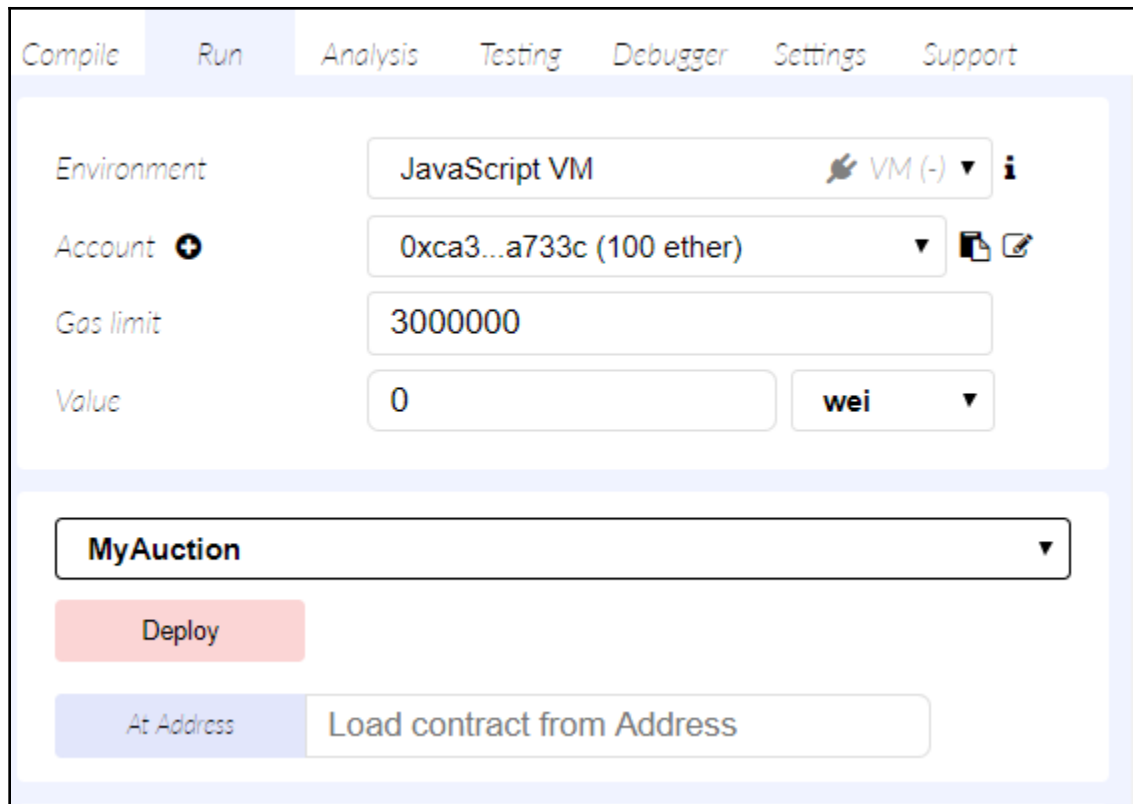
The screenshot shows a Solidity IDE with a contract named 'Auction' and its deployment details. The contract code is as follows:

```
1 pragma solidity ^0.4.11;  
2  
3  
4 contract Auction {  
5     address internal auction_owner;  
6     uint256 public auction_start;  
7     uint256 public auction_end;  
8     uint256 public highestBid;  
9     address public highestBidder;  
10  
11  
12  
13     enum auction_state {  
14         CANCELLED, STARTED  
15     }  
16  
17     struct car {  
18         string brand;  
19         string number;  
20     }  
21  
22     address[] bidders;  
23  
24     mapping(address => uint) public bids;  
25  
26     auction_state public STATE;  
27  
28     --  
29     modifier an_ongoing_auction(){  
30         require(now <= auction_end);  
31         _;  
32     }  
33  
34
```

The deployment details on the right show the contract is named 'MyAuction' and is being deployed to the 'Web3 Provider' environment. The account used is '0x256...2b23d' with a gas limit of 3000000. The contract is being deployed to the address '10...9a2568e49...02177b32d9a082026817a7fa'. The contract is currently in a 'pending' state.

The screenshot shows a Solidity IDE with a warning message for a function signature. The warning is as follows:

```
browser/Untitled1.sol:75:1: Warning: No visibility specified. Defaulting to "x"  
function cancel_auction() only_owner an_ongoing_auction{  
^ (Relevant source part starts here and spans across multiple lines).
```



MyAuction at 0x591...ee3be (blockchain) 

(fallback)

bid

cancel_auction

destruct_auction

withdraw

auction_end

auction_start

bids

get_owner

O: address:

0x0e9FD1369729B91E72c3C9d6287b02FF23E4734d

highestBid

highestBidder

Mycar

STATE

Ganache

ACCOUNTS BLOCKS TRANSACTIONS LOGS UPDATE AVAILABLE SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK: 0 GAS PRICE: 2000000000 GAS LIMIT: 6721975 NETWORK ID: 5777 RPC SERVER: HTTP://127.0.0.1:7545 MINING STATUS: AUTOMINING

MNEMONIC: sponsor desk arm derive sense parrot reason punch maze lumber urban daughter HD PATH: m/44'/60'/0'/0/account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0x256C8C46c92177b32d9a082026817EF7C6f2B23d	100.00 ETH	0	0
0xd722DBF01888377bDaB6695b5258274C89B1A5DB	100.00 ETH	0	1
0x440E87613FC25fcFb78cBa0E9063517a48A7dc55	100.00 ETH	0	2

Compile Run Settings Analysis Debugger Support

Environment: Injected Web3 (can't detect network)

Account: JavaScript VM, Injected Web3, Web3 Provider

Gas limit: 3000000

Value: 0 wei

Web3 Provider Endpoint: http://localhost:7545

OK Cancel

Genache
— □ ×

ACCOUNTS
BLOCKS
TRANSACTIONS
LOGS

🔍
⚙️

CURRENT BLOCK
5

GAS PRICE
2000000000

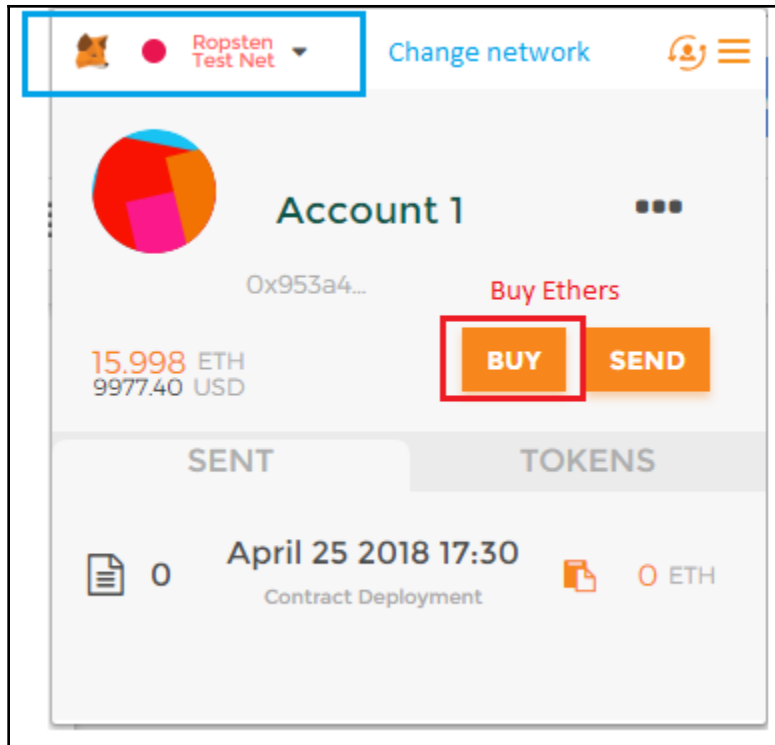
GAS LIMIT
6721975

NETWORK ID
5777

RPC SERVER
HTTP://127.0.0.1:7545

MINING STATUS
AUTOMINING

TX HASH 0xa723f95e435ec07952a59515f95f4b0e7430b9f8b2c5ec93dc89739830a9f82f CONTRACT CALL			
FROM ADDRESS 0xab1683a378aedadc6f07d567593e216a9428ed32	TO CONTRACT ADDRESS 0x8666dd71c06201accf43db58bdcEaFC88483Cd9b	GAS USED 21855	VALUE 0
TX HASH 0x341e6a5c741a0b21337336e3a22d1dd7a9d4ef9a7af1293bddbca596e57bab45 VALUE TRANSFER			
FROM ADDRESS 0xab1683a378aedadc6f07d567593e216a9428ed32	TO CONTRACT ADDRESS 0x8666dd71c06201accf43db58bdcEaFC88483Cd9b	GAS USED 80328	VALUE 15000000000000000000
TX HASH 0x18d3cb8442bf976f1e0a6b1e4225eb8f49e85e6c749f747ee0b608ba8d0c16da VALUE TRANSFER			
FROM ADDRESS 0x256c8c46c92177b32d9a082026817EF7C6f2B23d	TO CONTRACT ADDRESS 0x8666dd71c06201accf43db58bdcEaFC88483Cd9b	GAS USED 125328	VALUE 12000000000000000000
TX HASH 0xae0af4e6d7b056ba2910d0be4af62ca806fc10d440c16bfeec90b0cea34ee447 CONTRACT CREATION			
FROM ADDRESS 0x256c8c46c92177b32d9a082026817EF7C6f2B23d	CREATED CONTRACT ADDRESS 0x8666dd71c06201accf43db58bdcEaFC88483Cd9b	GAS USED 1071235	VALUE 0



Ropsten Test Net

Account 1

Ox953a4...

14.982 ETH
9040.48 USD

BUY SEND

SENT TOKENS

6 June 06 2018 00:00
Ox9Df6eCb7...9728 1.0 ETH

5 June 05 2018 23:59
Contract Deployment 0 ETH

June 05 2018 23:58
Contract Deployment (Rejected) 0 ETH


```
user@ByExample-node: ~/Mytestnet
user@ByExample-node:~$ mkdir Mytestnet
user@ByExample-node:~$ cd Mytestnet/
user@ByExample-node:~/Mytestnet$ mkdir nodeA
user@ByExample-node:~/Mytestnet$ mkdir nodeB
user@ByExample-node:~/Mytestnet$ geth account new --datadir nodeA
WARN [06-04|13:40:08] No etherbase set and no accounts found as default
Your new account is locked with a password. Please give a password. Do not forget this password.
Passphrase:
Repeat passphrase:
Address: {0e9fd1369729b91e72c3c9d6287b02ff23e4734a}
user@ByExample-node:~/Mytestnet$ geth account new --datadir nodeB
WARN [06-04|13:40:19] No etherbase set and no accounts found as default
Your new account is locked with a password. Please give a password. Do not forget this password.
Passphrase:
Repeat passphrase:
Address: {1f00d3ff65d0709be473f8798f81498d0ee761f7}
user@ByExample-node:~/Mytestnet$ geth account list --datadir nodeA
Account #0: {0e9fd1369729b91e72c3c9d6287b02ff23e4734a} keystore:///home/user/Mytestnet/nodeA/keystore/UTC--2018-06-04T13-40-12.571747847Z--0e9fd1369729b91e72c3c9d6287b02ff23e4734a
user@ByExample-node:~/Mytestnet$
```

```
user@ByExample-node: ~/Mytestnet
user@ByExample-node:~/Mytestnet$ puppeth
+-----+
| Welcome to puppeth, your Ethereum private network manager |
|
| This tool lets you create a new Ethereum network down to |
| the genesis block, bootnodes, miners and ethstats servers |
| without the hassle that it would normally entail.         |
|
| Puppeth uses SSH to dial in to remote servers, and builds |
| its network components out of Docker containers using the |
| docker-compose toolset.                                   |
+-----+

Please specify a network name to administer (no spaces, please)
> Mytestnet
Sweet, you can set this via --network=Mytestnet next time!

INFO [06-04|13:50:39] Administering Ethereum network           name=Mytestnet
WARN [06-04|13:50:39] No previous configurations found       path=/home/user
peth/Mytestnet

What would you like to do? (default = stats)
 1. Show network stats
 2. Configure new genesis
 3. Track new remote server
 4. Deploy network components
> 2

Which consensus engine to use? (default = clique)
 1. Ethash - proof-of-work
 2. Clique - proof-of-authority
> 1

Which accounts should be pre-funded? (advisable at least one)
> 0x1f00d3ff65d0709be473f8798f81498d0ee761f7
> 0x0e9fd1369729b91e72c3c9d6287b02ff23e4734a
> 0x

Specify your chain/network ID if you want an explicit one (default = random)
> 1234

Anything fun to embed into the genesis block? (max 32 bytes)
>

What would you like to do? (default = stats)
 1. Show network stats
 2. Manage existing genesis
 3. Track new remote server
 4. Deploy network components
> 2

 1. Modify existing fork rules
 2. Export genesis configuration
> 2

Which file to save the genesis into? (default = Mytestnet.json)
> genesis.json
INFO [06-04|13:51:36] Exported existing genesis block

What would you like to do? (default = stats)
 1. Show network stats
 2. Manage existing genesis
 3. Track new remote server
 4. Deploy network components
> █
```

```

user@ByExample-node: ~/Mytestnet
user@ByExample-node:~/Mytestnet$ cat genesis.json
{
  "config": {
    "chainId": 1234,
    "homesteadBlock": 1,
    "eip150Block": 2,
    "eip150Hash": "0x0000000000000000000000000000000000000000000000000000000000000000",
    "eip155Block": 3,
    "eip158Block": 3,
    "byzantiumBlock": 4,
    "ethash": {}
  },
  "nonce": "0x0",
  "timestamp": "0x5b1543b2",
  "extraData": "0x0000000000000000000000000000000000000000000000000000000000000000",
  "gasLimit": "0x47b760",
  "difficulty": "0x100000",
  "mixHash": "0x0000000000000000000000000000000000000000000000000000000000000000",
  "coinbase": "0x0000000000000000000000000000000000",
  "alloc": {
    "0000000000000000000000000000000000": {

```

```

user@ByExample-node:~/Mytestnet$ geth --datadir nodeB --networkid 1234 --rpc --rpcport 9545 --port "9999" --rpcapi db,eth,net,web3,personal,mntr,admin --cache=128 -
-rpcaddr 0.0.0.0 --rpccorsdomain "*" console
INFO [06-04|14:20:12] Starting peer-to-peer node Instance=Geth/v1.7.2-stable-1db4ecd/linu-amd64/go1.9
INFO [06-04|14:20:12] Allocated cache and file handles Database=/home/user/Mytestnet/nodeB/geth/chaindata cache=128 handle=1024
INFO [06-04|14:20:12] Initialised chain configuration Config="{ChainID: 1234 Homestead: 1 DAO: <nil> DAOSupport: false EIP150: 2 EIP150: 3 EIP158: 3 Byzantium
: 4 Engine: ethash}"
INFO [06-04|14:20:12] Disk storage enabled for ethash caches dir=/home/user/Mytestnet/nodeB/geth/ethash count=3
INFO [06-04|14:20:12] Disk storage enabled for ethash DAGs dir=/home/user/.ethash count=2
INFO [06-04|14:20:12] Initialising Ethereum protocol Version="[03 02]" Network="1234"
INFO [06-04|14:20:12] Loaded most recent local header Number=0 hash=347cc2.0973a8 td=1048576
INFO [06-04|14:20:12] Loaded most recent local full block Number=0 hash=347cc2.0973a8 td=1048576
INFO [06-04|14:20:12] Loaded most recent local fast block Number=0 hash=347cc2.0973a8 td=1048576
INFO [06-04|14:20:12] Loaded local transaction journal Transactions=0 dropped=0
INFO [06-04|14:20:12] Regenerated local transaction journal Transactions=0 accounts=0
INFO [06-04|14:20:12] Starting P2P networking self=enode://7649de56ad54a0e6c712bb31db22ad9475bc59d89ecba96a82548c226ef17f10c315bee7e0e8442b11b12069524
INFO [06-04|14:20:14] UDP listener up self=enode://7649de56ad54a0e6c712bb31db22ad9475bc59d89ecba96a82548c226ef17f10c315bee7e0e8442b11b12069524
223306ea5ab894bfc91679fcd32a789b9e[::]:9999
INFO [06-04|14:20:14] RLPX listener up self=enode://7649de56ad54a0e6c712bb31db22ad9475bc59d89ecba96a82548c226ef17f10c315bee7e0e8442b11b12069524
223306ea5ab894bfc91679fcd32a789b9e[::]:9999
INFO [06-04|14:20:14] IPC endpoint opened: /home/user/Mytestnet/nodeB/geth.ipc
INFO [06-04|14:20:14] HTTP endpoint opened: http://0.0.0.0:9545
Welcome to the Geth JavaScript console!

Instance: Geth/v1.7.2-stable-1db4ecd/linu-amd64/go1.9
coinbase: 0x1f0d3ff65d0709be473f8798f81498d0ee761f7
at block: 0 (Mon, 04 Jun 2018 13:50:42 MET)
datadir: /home/user/Mytestnet/nodeB
modules: admin:1.0 debug:1.0 eth:1.0 mntr:1.0 net:1.0 personal:1.0 rpc:1.0 txpool:1.0 web3:1.0

> admn.nodeInfo
{
  enode: "enode://7649de56ad54a0e6c712bb31db22ad9475bc59d89ecba96a82548c226ef17f10c315bee7e0e8442b11b12069524223306ea5ab894bfc91679fcd32a789b9e[::]:9999",
  id: "7649de56ad54a0e6c712bb31db22ad9475bc59d89ecba96a82548c226ef17f10c315bee7e0e8442b11b12069524223306ea5ab894bfc91679fcd32a789b9e",
  ip: ":",
  listenAddr: "[:]:9999",
  name: "Geth/v1.7.2-stable-1db4ecd/linu-amd64/go1.9",
  ports: {
    discovery: 9999,
    listener: 9999
  },
  protocols: {
    eth: {
      difficulty: 1048576,
      genesis: "0x347cc2de7186f480cdee259f224ad464b3308575b22a2e9966f12ce7410973a8",
      head: "0x347cc2de7186f480cdee259f224ad464b3308575b22a2e9966f12ce7410973a8",

```

```

user@ByExample-node: ~/Mytestnet
user@ByExample-node:~/Mytestnet$ puppeth
+-----+
| Welcome to puppeth, your Ethereum private network manager |
|                                                             |
| This tool lets you create a new Ethereum network down to  |
| the genesis block, bootnodes, miners and ethstats servers |
| without the hassle that it would normally entail.          |
|                                                             |
| Puppeth uses SSH to dial in to remote servers, and builds |
| its network components out of Docker containers using the  |
| docker-compose toolset.                                    |
+-----+

Please specify a network name to administer (no spaces, please)
>
> Mytestnet
Sweet, you can set this via --network=Mytestnet next time!

INFO [06-04|14:28:01] Administering Ethereum network          name=Mytestnet
WARN [06-04|14:28:01] No previous configurations found      path=/home/user/.puppeth/Mytestnet

What would you like to do? (default = stats)
1. Show network stats
2. Configure new genesis
3. Track new remote server
4. Deploy network components
> 2

Which consensus engine to use? (default = clique)
1. Ethash - proof-of-work
2. Clique - proof-of-authority
> 2

How many seconds should blocks take? (default = 15)
>

Which accounts are allowed to seal? (mandatory at least one)
> 0x87366ef81db496edd0ea2055ca605e8686eeca1e6
> 0x

```

Car Auction Dapp

Car Details

Brand: BMW

Registration Number: US12M

Bid value

eg. 100

Successful bid, transaction ID: 0xb232680b6e6f2c217527acefb1bc8de4ebef5f11af8c5378348c79b3bab63b21

Auction Operations

Auction Details

- Auction End: 1528321806
- Auction Highest Bid: 1
- My Bid: 1
- Auction Highest Bidder: 0x0e9f1369729b91e72c3c9d6287b02f23e4734a
- Auction Status: 1

Events Logs

0x0e9f1369729b91e72c3c9d6287b02f23e4734a has bidder(30000000000000000 wei)

Functions	Transaction Gas cost estimation
bid()	125350
withdraw()	21008
cancel_auction()	21272
destruct_auction()	14211

▼ [block:72 txIndex:0] from:0x0e9...4734a to:MyAuction.destruct_auction() 0xc2f...b22a1 value:0 wei data:0xbba...fd3d4 logs:0 hash:0x5bc...8e142

status	0x1 Transaction mined and execution succeed
from	0x0e9fd1369729b91e72c3c9d6287b02ff23e4734a
to	MyAuction.destruct_auction() 0xc2f43bd44ab4a621995f51748c41a440e13b22a1
gas	28421 gas
transaction cost	14211 gas
input	0xbba...fd3d4
decoded input	{ }
decoded output	-
logs	[]
value	0 wei

remix

Chapter 5: Tontine Game with Truffle and Drizzle

```
user@ByExample-node: ~/tontine
user@ByExample-node:~/tontine$ truffle version
Truffle v4.1.12 (core: 4.1.12)
Solidity v0.4.24 (solc-js)
user@ByExample-node:~/tontine$
```

```
user@ByExample-node: ~/tontine
user@ByExample-node:~/tontine$ truffle init
Downloading...
Unpacking...
Setting up...
Unbox successful. Sweet!

Commands:

  Compile:      truffle compile
  Migrate:     truffle migrate
  Test contracts: truffle test
user@ByExample-node:~/tontine$
```

```
user@ByExample-node:~/tontine$ truffle compile
Compiling ./contracts/hello.sol...
Writing artifacts to ./build/contracts
```



```
user@ByExample-node: ~/tontine
user@ByExample-node:~/tontine$ ganache-cli -p 7545
Ganache CLI v6.1.3 (ganache-core: 2.1.2)

Available Accounts
=====
(0) 0x59646d4b46b4f679ad5b96d360864f6139c13f97
(1) 0x2d65e9e80e63f5711d48f3b82068dffe44d4884b
(2) 0xe3e8c7ea723cef3637f5d99584877b0449eab2ee
(3) 0xcfc5beb66bec69f1d0b2e78598596992dee348c6
(4) 0xd4e8a743705bb31d912c143f50be53599803516d
(5) 0xa0d6960859a0edabcf9937268c6c42c2e695aea4
(6) 0x821854d456f8259e607f5aaea6a3ebd90cdd390e
(7) 0x30967d2018fcdcfab1ba539d4fa03ce9adda0cf43
(8) 0xdbab5349412306fe73baa5995459cfcadf1481b2
(9) 0xed9445f595cd1304d841031c0b14b9b30c5e9719

Private Keys
=====
(0) 8bd589e3571d1b8cb6b95da53570b46822fa31ba2afc9728936487219da42afa
(1) e8250db43131cb83d3d6e4fa8de8d9c9e9d44aaec6a0e30a38ec2334213b8208
(2) 4ab57f6b61c3e241d070d520d5dfb18cb802452be47cf51ed3769023460856e5
(3) 1815d4fd78e159b16e2a307a5241b97a46e66dedfff73650e1a8e5c2c94b3339f
(4) b618b75cb6f144c6634e6bf5584f1c5fef219699f7a9fdecfb876552bbd2afd8
(5) c92c7ab459f13cf939ef6e719462b2a111670c44c4b55340170f331044cbf784
(6) c73fbc5bee30aa8b83d004a55d1071d47f722665c54bd6a6c9132690701fb619
(7) d9b41f9045fc8cf1478fd1811f5d10c91a0c18dbf72d6e8cd380cfc594eb5621
(8) add6754957bed8373e39d823e6b75d678bdb691dd9254e46239baeeb5e1d778f
(9) 5beeca342e3caa4648bf14480c1381c8703c63269e03b1cf23292cfff0771032

HD Wallet
=====
Mnemonic:      ankle banana lady poverty antenna hungry odor plunge tribe park f
labor attract
Base HD Path:  m/44'/60'/0'/0/{account_index}

Gas Price
=====
20000000000

Gas Limit
=====
6721975

Listening on localhost:7545
```

```
user@ByExample-node:~/tontine$ truffle migrate --network my_ganache
Using network 'my_ganache'.

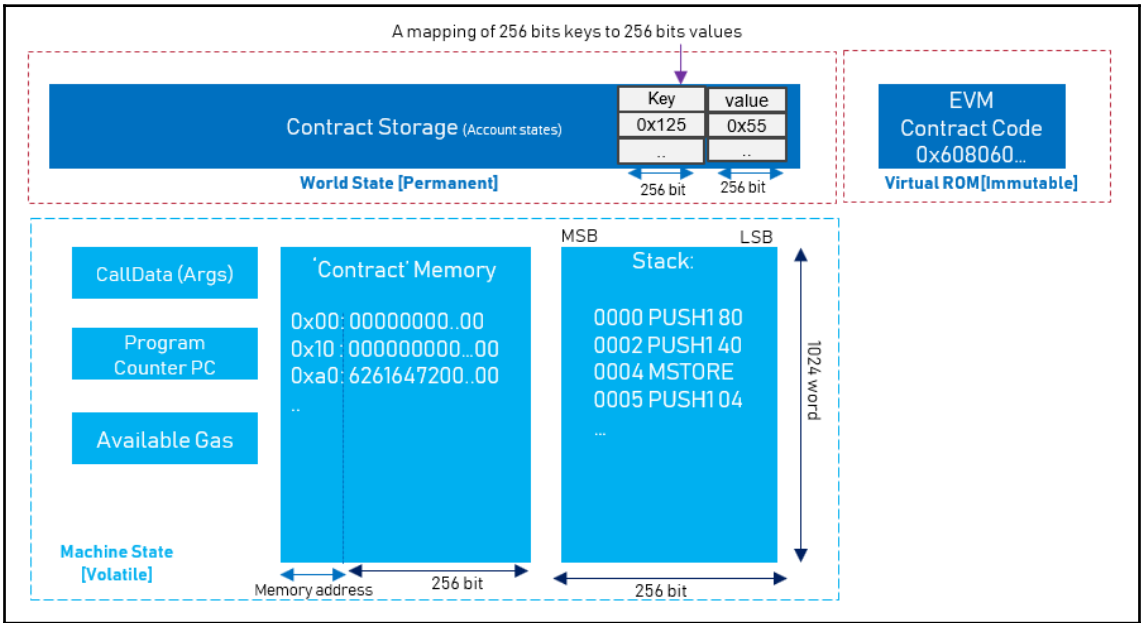
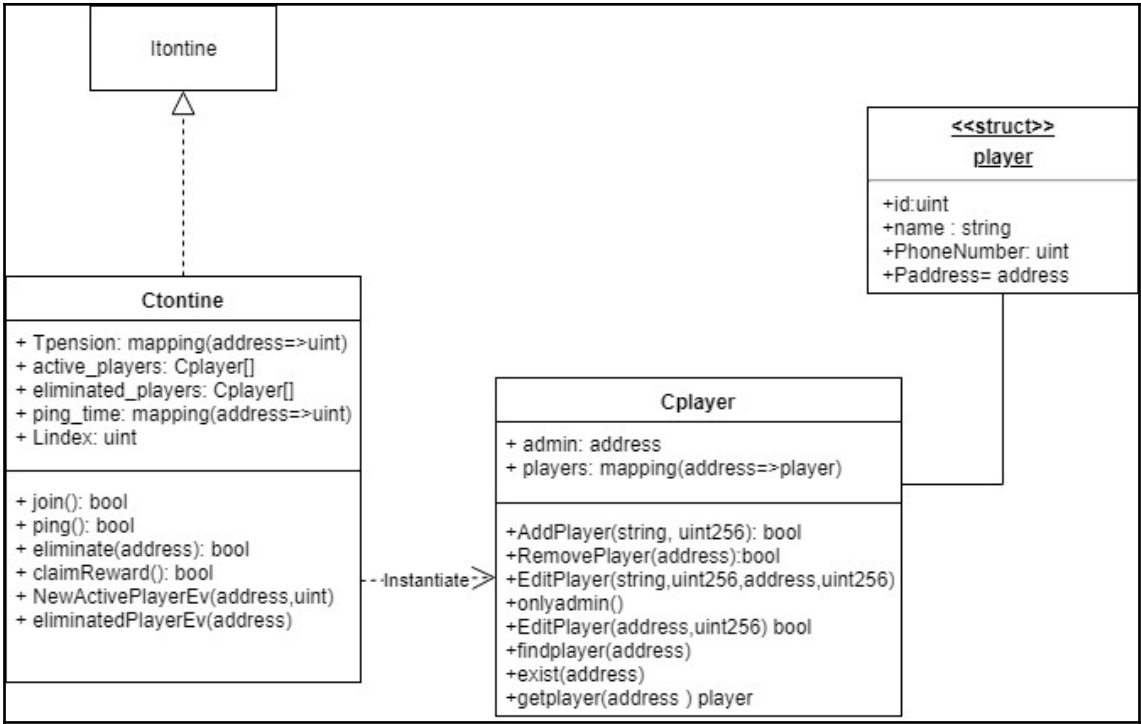
Running migration: 2_initial_migration.js
  Deploying HelloWorld...
    ... 0x65440f0f09fd0c917c9e43214e80ffbaf8c4011a23fe7704ebf909d74b2c6e91
  HelloWorld: 0x279841fcc40a59b161e1a1e5076fb8665820d9c7
Saving successful migration to network...
  ... 0x7dcf44eae29483b2651b3c3a462ce9e873a99e84e1b79442ce46301c2d7f973e
Saving artifacts...
```

```
Transaction: 0x65440f0f09fd0c917c9e43214e80ffbaf8c4011a23fe7704ebf909d74b2c6e9
1
Contract created: 0x279841fcc40a59b161e1a1e5076fb8665820d9c7
Gas usage: 281139
Block Number: 30
Block Time: Wed Jul 25 2018 17:08:56 GMT+0100 (WEST)

eth_newBlockFilter
eth_getFilterChanges
eth_getTransactionReceipt
eth_getCode
eth_uninstallFilter
eth_sendTransaction

Transaction: 0x7dcf44eae29483b2651b3c3a462ce9e873a99e84e1b79442ce46301c2d7f973
e
Gas usage: 27008
Block Number: 31
Block Time: Wed Jul 25 2018 17:08:56 GMT+0100 (WEST)

eth_getTransactionReceipt
```



```

contract Cplayer{
    address admin;
    mapping(address=>string) public players;
    uint[] Array1;

    constructor() public {
        admin=msg.sender;
    }

    function test(string arg1, uint256 arg2, uint[] argArray1, uint[] storage argArray2) public returns (bool arg3){
        address _address=msg.address;
        uint[4] memory adaArr = [1,2,3,4];

        return true;
    }
}

```

Storage
(Permanent states)

Memory

This contract does not implement all functions and thus cannot be created.

OK null

browser/ballot.sol:98:19: TypeError: Member "admin" not found or not visible after argument-dependent lookup in contract Cplayer
address public ad=Tplayer.admin;
^-----^

```

user@ByExample-node: ~/tontine
user@ByExample-node:~/tontine$ truffle compile-all
Compiling ./contracts/Migrations.sol...
Compiling ./contracts/tontine.sol...

Compilation warnings encountered:

/home/user/tontine/contracts/tontine.sol:2:1: Warning: Experimental features are turned on. Do not use experimental features on live deployments.
pragma experimental ABIEncoderV2;
^-----^

Writing artifacts to ./build/contracts
user@ByExample-node:~/tontine$

```

```
user@ByExample-node:~/tontine$ truffle test --network my_ganache
Using network 'my_ganache'.

Contract: Cplayer
  ✓ .. should ADD three Players (496ms)
  ✓ .. should find a player (114ms)
  ✓ .. should authorize Only admin can remove players (221ms)

Contract: Ctontine
  ✓ .. sould enable players to join the game (395ms)
  ✓ .. should emit 'NewActivePlayerEv' event when a player join the game (373
ms)
  ✓ .. should send the reward to the last active player (1437ms)

6 passing (5s)

user@ByExample-node:~/tontine$ █
```

```
user@ByExample-node:~/tontine$ truffle test test/TontineTest.sol --network my_ganache
Using network 'my_ganache'.

Compiling ./contracts/tontine.sol...
Compiling ./test/TontineTest.sol...
Compiling truffle/Assert.sol...
Compiling truffle/DeployedAddresses.sol...

TontineTest
  ✓ testplayer (107ms)
  ✓ testjoingame (189ms)

2 passing (2s)
```

```
user@ByExample-node: ~/tontine

Contract: Cplayer
✓ .. should ADD three Players (455ms)
✓ .. should find a player (160ms)
✓ .. should authorize Only admin can remove players (181ms)

Contract: Ctontine
1) .. sould enable players to join the game
> No events were emitted
2) .. should emit 'NewActivePlayerEv' event when a player join the game
> No events were emitted
3) .. should send the reward to the last active player
> No events were emitted

3 passing (4s)
3 failing

1) Contract: Ctontine
  .. sould enable players to join the game:
    Error: VM Exception while processing transaction: revert
      at Object.InvalidResponse (/home/user/.npm/versions/node/v8.11.2/lib/node_modules/truffle/build/webpack:/~/web3/lib/web3/errors.js:38:1)
      at /home/user/.npm/versions/node/v8.11.2/lib/node_modules/truffle/build/we
```

```
user@ByExample-node: ~
eth_sendTransaction

Transaction: 0x101b45064173614becb9d30322f58f651dc97dbea379ab07339c7d4faa71b1c

Gas usage: 84574
Block Number: 643
Block Time: Thu Aug 02 2018 10:04:30 GMT+0100 (WEST)

th_getTransactionReceipt
th_sendTransaction

Transaction: 0x90e02cc211733cade22bd5ff3b1ea1600781b48a1c792d867cda83190f77331

Gas usage: 24944
Block Number: 644
Block Time: Thu Aug 02 2018 10:04:31 GMT+0100 (WEST)
Runtime Error: revert
```

```
32: function AddPlayer(string _name, uint256 _phonenumber) public returns (bool){
33:   players[msg.sender].name=_name;
34:   players[msg.sender].Address=msg.sender;
                                     ^^^^^^^^^^^
debug(my_ganache:0x81860524...)> v
    _name: 'player1'
  _phonenumber: 123
             : true
    admin: '0x00'
  players: null
debug(my_ganache:0x81860524...)> +:_name
'player1'
```



▶
■

▶
Transaction

↶

↷

↵

↶

⏪

⏩

⏮

⏭

▶
Instructions

▼
Solidity Locals

▼
Solidity State

▶
Step detail

▶
Stack

▶
Storage

▶
Memory

▼
Call Data

0: 0xb688a363

▼
Call Stack

0: 0x791200ad814f6966c55500882c7acf709f52cdeb

▶
Return Value

▼
Full Storages Changes

▼
Storage completely loaded

▼
0x0f4efa3a8f3fb65ade5f38b41770b2e9a01d44b7ddb62981f7fe71d6509f00cd: Object

key: 0xa200d36cac42f24780e7687be1c5b4dc2fd27b8aa5d37853d257e0b44c71a0a2

value: 0x14723a09acff6d2a60dcaf7aa4aff308fddc160c



State changes made during this call will be reverted.

Instructions

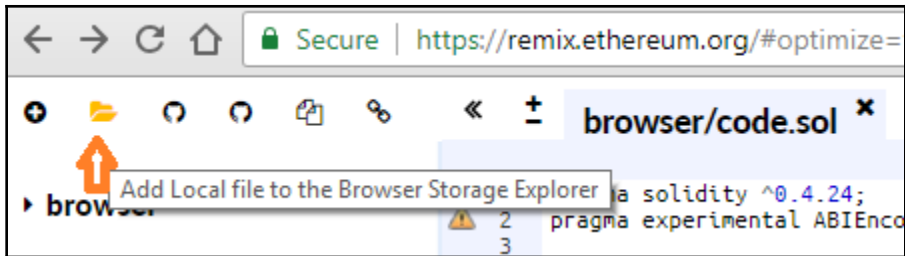
```
1986 REVERT
1987 JUMPDEST
1988 PUSH8 0dc0b6b3a7640000
1997 CALLVALUE
1998 LT
1999 ISZERO
2000 DUP1
2001 ISZERO
2002 PUSH2 07e8
2005 JUMPI
2006 POP
2007 CALLER
2008 PUSH4 00
```

Solidity Locals

<1>: *false* bool

Solidity State

- ▶ *tpension*: *mapping(address => uint256)*
 - ▶ *active_players*: *struct Cplayer.player[]*
 - ▶ *eliminated_players*: *struct Cplayer.player[]*
 - ▶ *ping_time*: *mapping(address => uint256)*
- index*: 0 *uint256*



```
Running migration: 2_initial_migration.js
Deploying Cplayer...
... 0xce5b12c84a4f0fb96f917afc5964be1622eefcb01bceb6534f255b8cfcddccac
Cplayer: 0x7bd9dc68a0d268d9e07e6811d042d2b1bb63608d
Deploying Ctontine...
... 0x5fc630529fd815c5c892f5f8590f3ca086cdc261a97ba7c3092d39f94c7acd61
Ctontine: 0x081cad5cf649e07e8351b4e45a30db3997e0688a
```

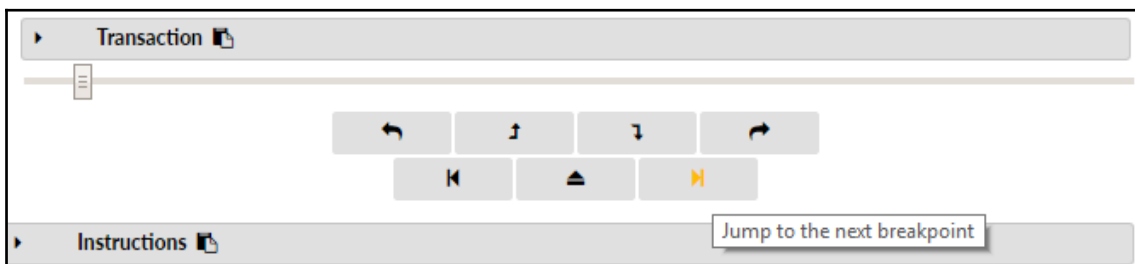
Account	0xca3...a733c (98.99999999999972713 ether)
Gas limit	0xca3...a733c (98.999999999999727137 ether)
Value	0x147...c160c (99.999999999999915855 ether)
	0x4b0...4d2db (98.999999999999742036 ether)
	0x583...40225 (100 ether)
	0xdd8...92148 (100 ether)

Gas limit	<input type="text" value="3000000"/>
Value	<input type="text" value="1"/> ether

```
[vm] from:0xdd8...92148 to:Ctontine.join() 0x1df...bda71 value:0 wei data:0xb68...8a363
logs:0 hash:0x369...ba838
Debug
```

transact to Ctontine.join errored: VM error: revert.
revert The transaction has been reverted to the initial state.
Reason provided by the contract: "send higher pension". Debug the transaction to get more information.


```
261 function join() payable returns(bool){
262
263     require(Tplayer.exist(msg.sender),"player doesn't exist");
264
265     require(msg.value>=1 && Tpension[msg.sender]==0,"send higher pension");
266
267     Tpension[msg.sender]=msg.value;
268
269     Tplayer.EditPlayer(msg.sender,active_players.length);
270
271     active_players.push(Tplayer.getplayer(msg.sender));
272
273     indices +=(active_players.length-1);
274
275     ping_time[msg.sender]=now;
276
277     emit NewActivePlayerEv(msg.sender,now);
278
279     return true;
280
281 }
```



```
user@ByExample-node: ~/deleteme
File Edit View Search Terminal Help
user@ByExample-node:~/deleteme$ truffle unbox drizzle
Downloading...
Unpacking...
Setting up...
Unbox successful. Sweet!
```



Drizzle Examples

Examples of how to get started with Drizzle in various situations.

Active Account

0x9a66ed32D949F5d8fD5Da9D13a3be24Eacf350B5

89.206 Ether

SimpleStorage

This shows a simple ContractData component with no arguments, along with a form to set its value.

Stored Value: 0

TutorialToken

Here we have a form with custom, friendly labels. Also note the token symbol will not display a loading indicator. We've suppressed it with the `hideIndicator` prop because we know this variable is constant.



We can't find any Ethereum accounts! Please check and make sure Metamask or you browser are pointed at the correct network and your account is unlocked.

Active Account

My details:

0xd0B60088575D7dcC2FBcb633813aadFae8677c8A

74.378 Ether

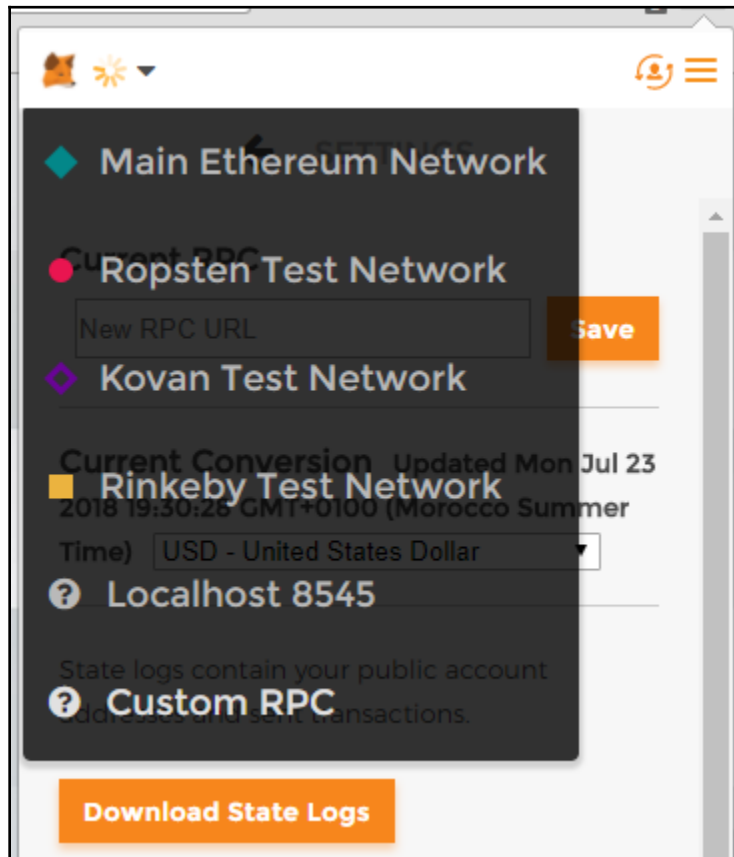
Ctontine

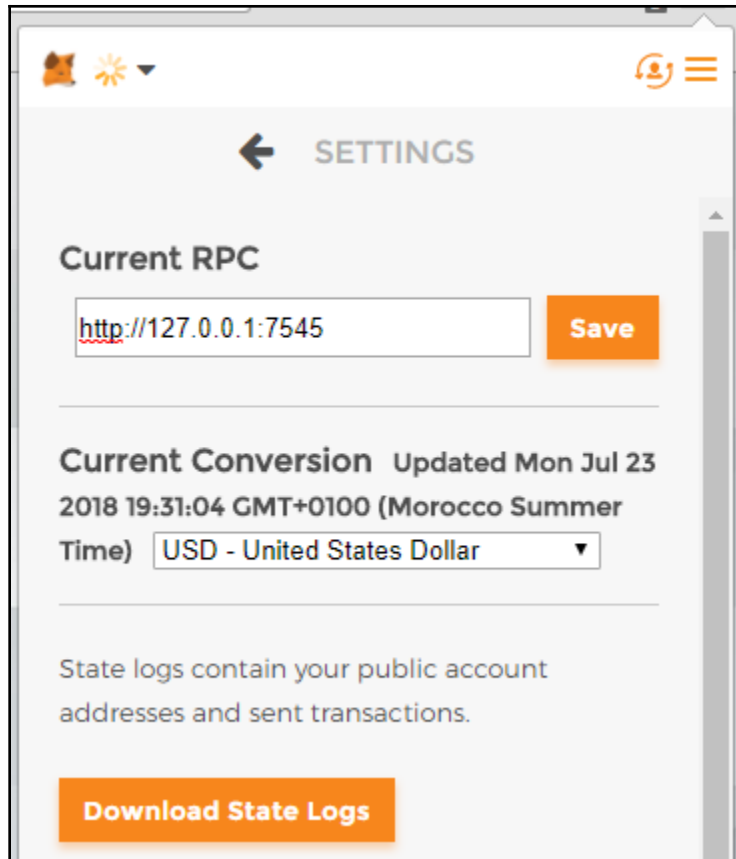
Last Ping: 1533841668

Your Game pension: 20000000000000000000

Eliminate an opponent

use this form to eliminate your opponent

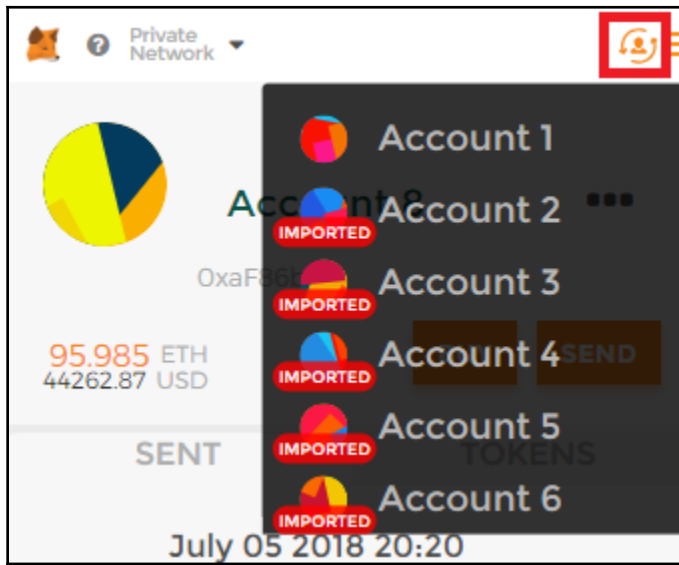
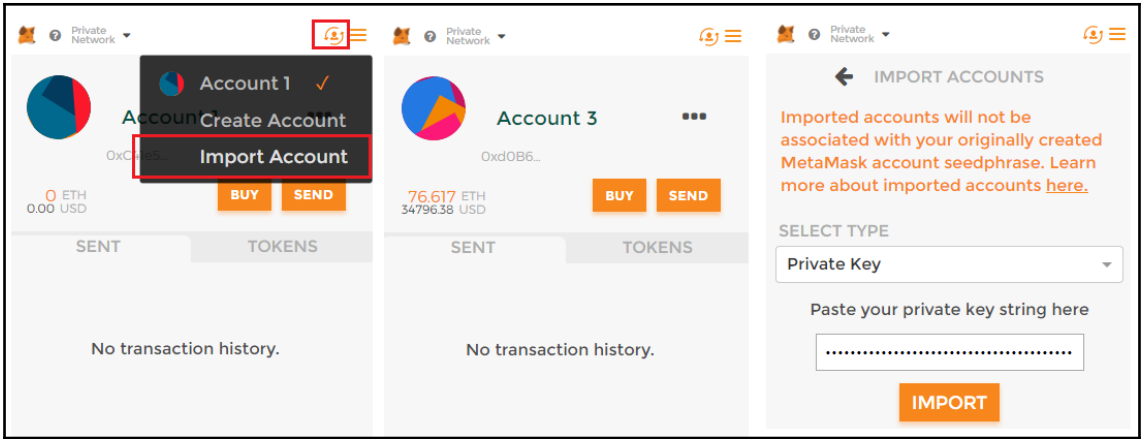




```
user@ByExample-node: ~/deleteme
Ganache CLI v6.1.3 (ganache-core: 2.1.2)

Available Accounts
=====
(0) 0x2de40c5f7c4db7f9015c33136cafcd8d75e929b
(1) 0xfa475e0afe77313fade7fca6ed74a16b5c41f626
(2) 0x929a2dd03f7312883558306a0f9caf88c831c15f

Private Keys
=====
(0) ee30880d0558f63e651d3104f28430547c5c17242256fb8485a227840693b75a
(1) 4a451796272d228d99d64a5d5d251193290adf16e06610c2c92a955260c9091d
(2) 55cdd6245a0b58118baa090b595020b9a8b20c7a9d3939f6e6de501b63391d8c
(3) 0c93944854c0a0402f1004a21ea05a17053019e2170082c1320140a980150904
```





Tontine Game

Examples of how to get started with Drizzle in various situations.

Active Account

My details:

0x6D03B4073651C08d1e4145356beb8Ab3b08B7A2F

9.991 Ether

Cplayer Contract

Register

Before start playing, players should register themselves using AddPlayer from.

Ctontine

Last Ping: 1532560156

Your Game pension: 2000000000000000000

Join game

Press the button below to join the game (only the first time)

Ping game:

Keep pinging the contract to avoid being eliminated (ping interval is 1 day)

Eliminate an opponent

use this form to eliminate your opponent

Claim your reward

0xE1cc319B5A1E06F9e7628cc6F43abB33dE1AF319

100 Ether

Cplayer Contract

Register

Before start playing players register

MetaMask Notification

CONFIRM TRANSACTION

Private Network

Account 13
E1cc31...F319
100.000 ETH
47643.00 USD

>

353142...1a71

Amount	0 ETH 0.00 USD
Gas Limit	<input type="text" value="126409"/> UNITS
Gas Price	<input type="text" value="20"/> GWEI
Max Transaction Fee	0.002528 ETH 1.20 USD
Max Total	0.002528 ETH 1.20 USD

Data included: 132 bytes

join game

Press the button below to join the game (only the first time)

Ping game:

Keep pining the contract to avoid being eliminated (ping interval is 1 day)

The screenshot shows a mobile application interface for a transaction confirmation. At the top, it says "Private Network" with a dropdown arrow and a user profile icon. The main heading is "CONFIRM TRANSACTION" with a back arrow. Below this, it shows "Account 1" with two addresses: "e40B98...9E83" and "066135...E2DC". The first account has a balance of "49.998 ETH" and "23075.72 USD". A right-pointing arrow is between two circular icons representing the accounts. The transaction details are as follows:

Amount	2.000 ETH
	923.06 USD
Gas Limit	<input type="text" value="258502"/> UNITS
Gas Price	<input type="text" value="20"/> GWEI
Max Transaction Fee	0.005170 ETH
	2.39 USD
Max Total	2.005 ETH
	925.45 USD

At the bottom, it says "Data included: 4 bytes" and has three buttons: "RESET" (orange), "SUBMIT" (green), and "REJECT" (red).

Ping game:

Keep pining the contract to avoid being eliminated (ping interval is 1 day)

Submit

Eliminate an opponent

use this form to eliminate your opponent

First Eliminated players

name

bellaj

PhoneNumber

2126130384875

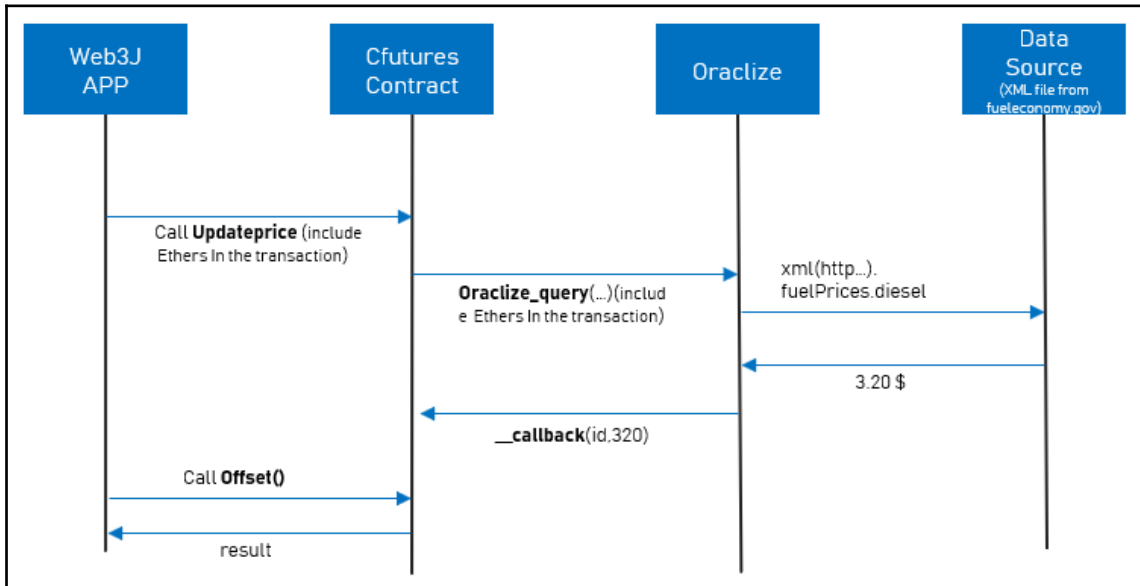
Address

0x953a435b43b605079b42b5e26922d425fDC31c89


id

0

Chapter 6: Blockchain-Based Futures System



New Maven Project

New Maven project 

Specify Archetype parameters

Group Id:

Artifact Id:

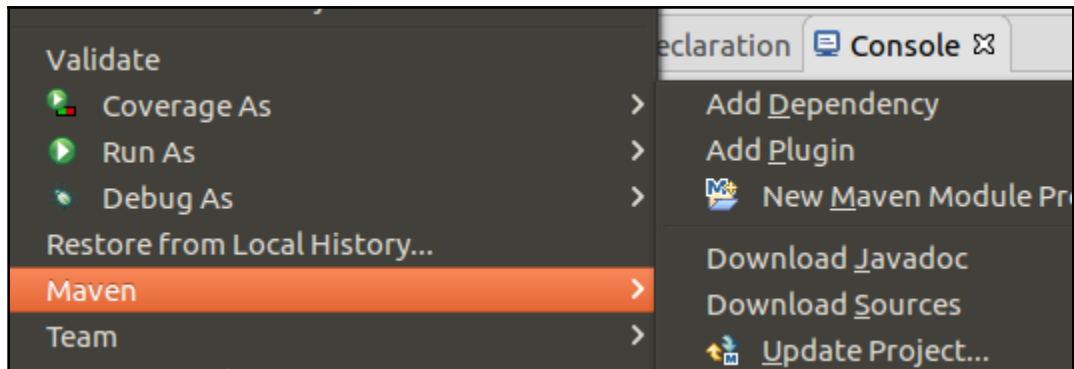
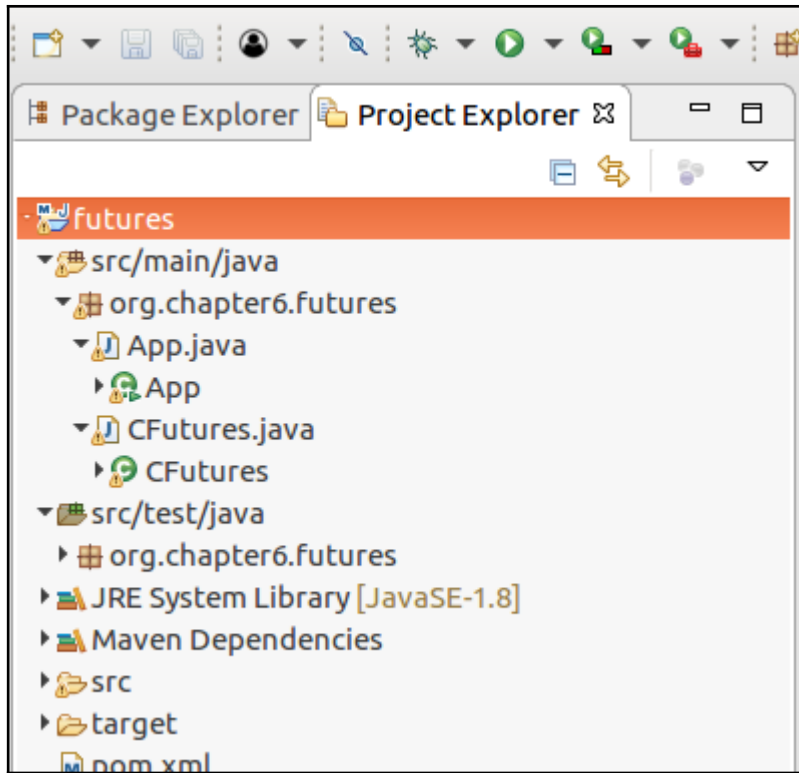
Version:

Package:

Properties available from archetype:

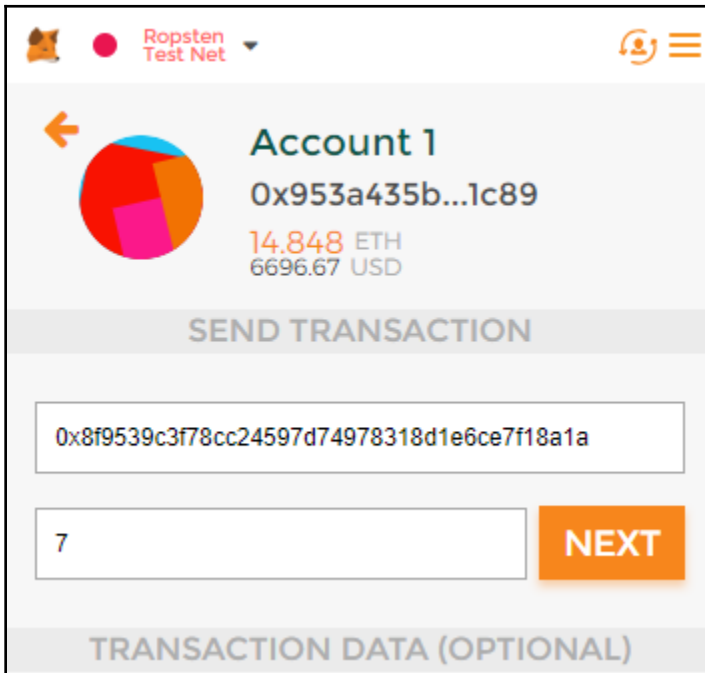
Name	Value
------	-------

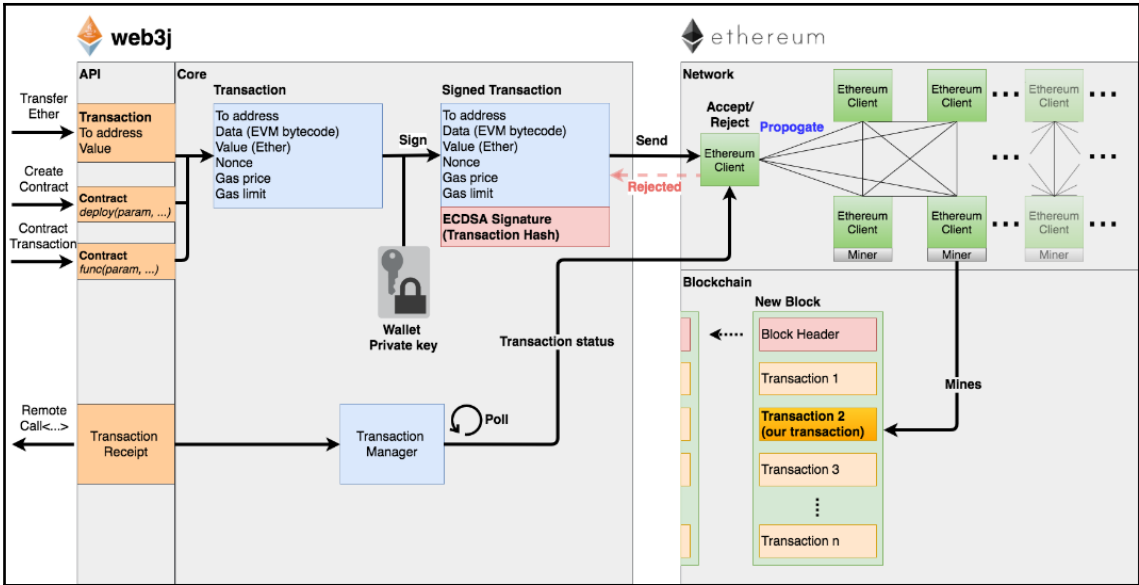
▸ Advanced



```
user@ByExample-node:~/eclipse-workspace/futures/src$ web3j wallet create

Please enter a wallet file password:
Please re-enter the password:
Please enter a destination directory location [/home/user/.ethereum/testnet/keystore]: .
Wallet file UTC--2018-07-15T16-44-45.169000000Z--8f9539c3f78cc24597d74978318d1e6ce7f18a1a.json successfully created in:
user@ByExample-node:~/eclipse-workspace/futures/src$ ls
main test UTC--2018-07-15T16-44-45.169000000Z--8f9539c3f78cc24597d74978318d1e6ce7f18a1a.json
```





```

user@ByExample-node: ~/eclipse-workspace/futures/src/main/java
user@ByExample-node:~/eclipse-workspace/futures/src/main/java$ ~/web3j-3.4.0/bin/web3j truffle generate ~/FuturesWeb3j/build/contracts/CFutures.json -o ~/eclipse-workspace/futures/src/main/java/ -p org.chapter6.futures

Generating org.chapter6.futures.CFutures ... File written to /home/user/eclipse-workspace/futures/src/main/java
user@ByExample-node:~/eclipse-workspace/futures/src/main/java$


```

```

CFutures CFuture2 = CFutures.load(CFuturesAddress, web3j, credentials, CUSTOM_GAS_PRICE, GAS_LIMIT);
CFuture.
// if yo
deposit(BigInteger weiValue) : RemoteCall<Trans
Integer weiValue)
equals(Object obj) : boolean - Object
getClass() : Class<?> - Object
getContractAddress() : String - Contract
getContractBinary() : String - Contract
getDeployedAddress(String networkId) : String -
getfuelPriceUSD() : RemoteCall<BigInteger> - CFu
getGasPrice() : BigInteger - Contract
getpaid() : RemoteCall<TransactionReceipt> - CFu
getSyncThreshold() : long - ManagedTransaction
Optional<TransactionR
Press 'Ctrl+Space' to show Template Proposals

```

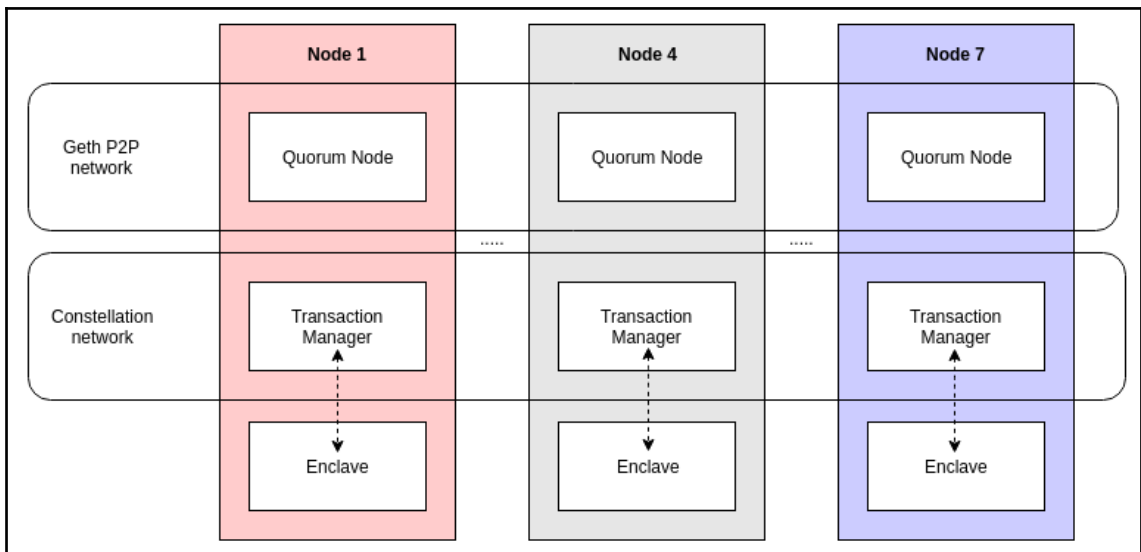
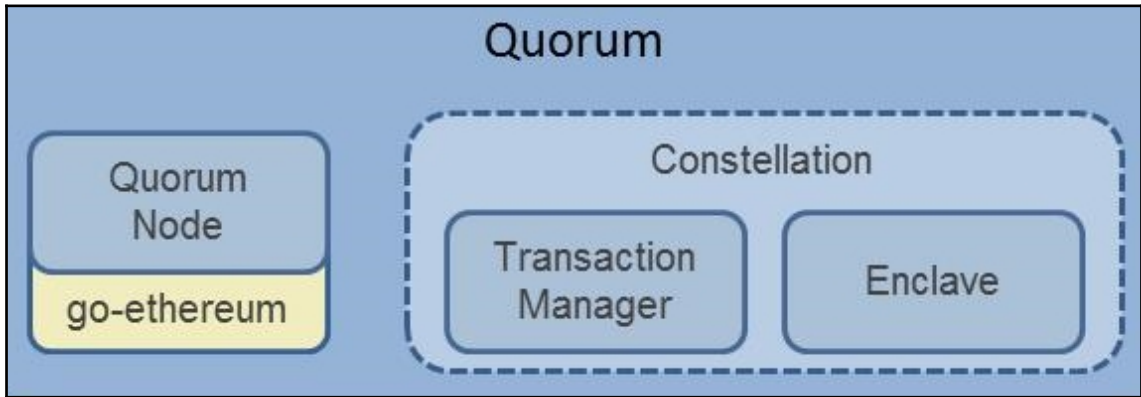
[This is a Ropsten Testnet Transaction Only]

TxHash:	0x4ef437fce1a877c3b155a03b0ba11309695ac4d84d351f6f3aefee1c60202278
TxReceipt Status:	Success
Block Height:	3648112 (1 block confirmation)
TimeStamp:	25 secs ago (Jul-16-2018 09:56:11 AM +UTC)
From:	0x8f9539c3f78cc24597d74978318d1e6ce7f18a1a
To:	Contract 0x7cd884e217c638b04990af8adb5efec6e4aac015 
Value:	360 wei (\$0.00)
Gas Limit:	4700000
Gas Used By Txn:	21998
Gas Price:	0.00000014 Ether (140 Gwei)
Actual Tx Cost/Fee:	0.00307972 Ether (\$0.000000)
Nonce & {Position}:	30 {0}
Input Data:	<div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p>Function: deposit() ***</p> <p>MethodID: 0xd0e30db0</p> </div>

View Input As ▾

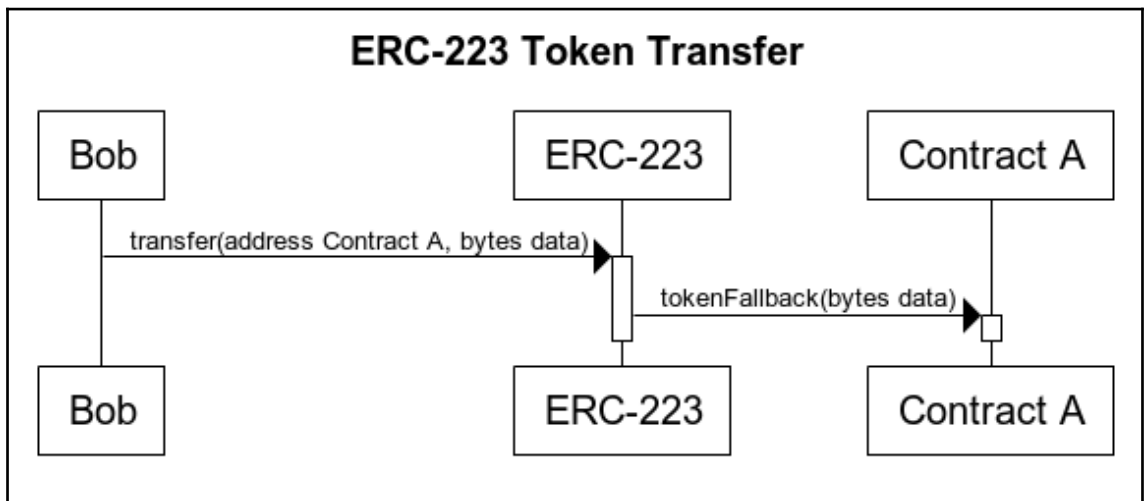
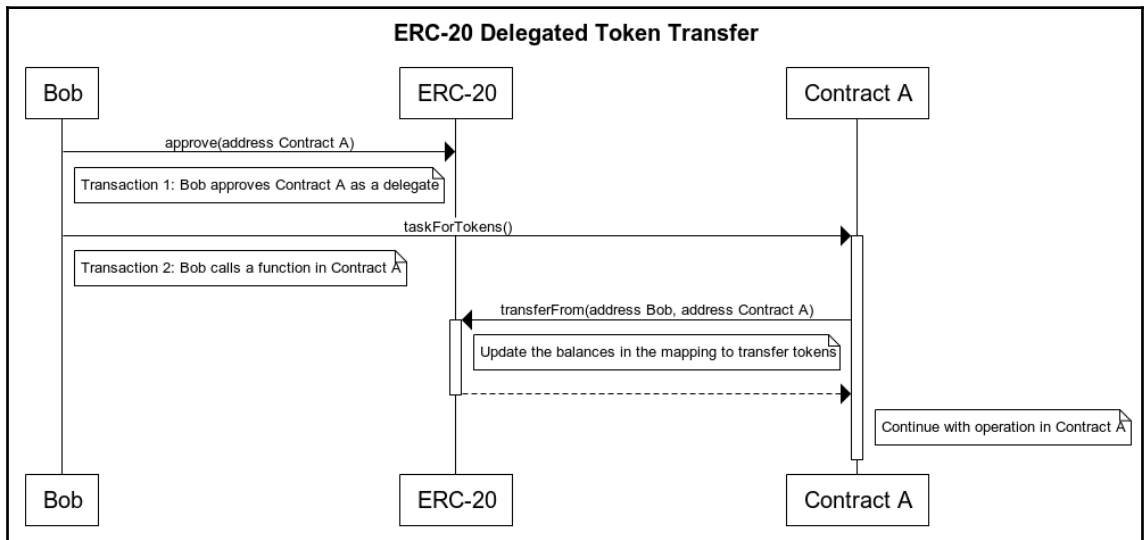
```
Problems @ Javadoc Declaration Console
App (1) [Java Application] /usr/lib/jvm/java-8-openjdk-amd64/bin/java (Jul 19, 2018, 1:17:20 PM)
[main] INFO org.chapter6.futures.App - 0x8f9539c3f78cc24597d74978318d1e6ce7f18a1a Credentials loaded
[main] INFO org.chapter6.futures.App - The accounts balance 326186385999994600 wei
Please make your choice:
1 - Deploy New Cfutures contract.
2 - Load contract
3 - Make deposit
4 - current Fuel price
5 - Update Fuel price
6 - Investment offset
0 - exit
2
Please provide the contract's address to load:
0x4d8e3580f4929c2b4aaf8aaabde0c4e955802a01
[main] INFO org.chapter6.futures.App - Contract loaded: 0x4d8e3580f4929c2b4aaf8aaabde0c4e955802a01
4
[main] INFO org.chapter6.futures.App - Last fuel Price Fuel price According to the Oracle is: 324
5
6
[main] INFO org.chapter6.futures.App - your offset is -2880000
```

Chapter 7: Blockchains in Business



Chapter 8: Creating an ICO

Now that we have the required parts, let's look at the flow of the delegation's functionality:



Packt Token ICO Sale

This is the Packt ERC20 Token sale. The token price is 0.001 ETH.

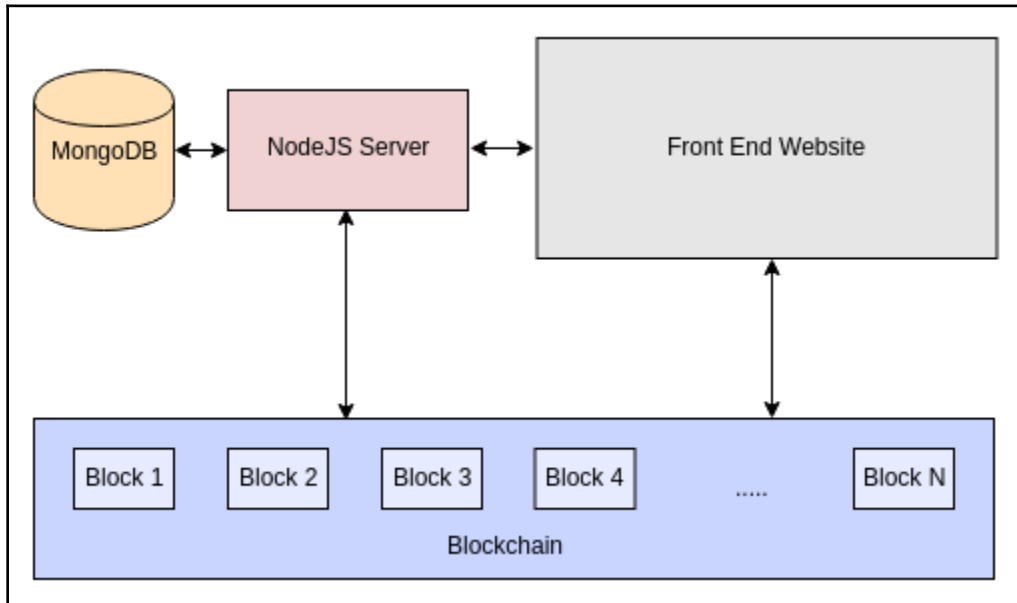
Your token balance is: 0 PET

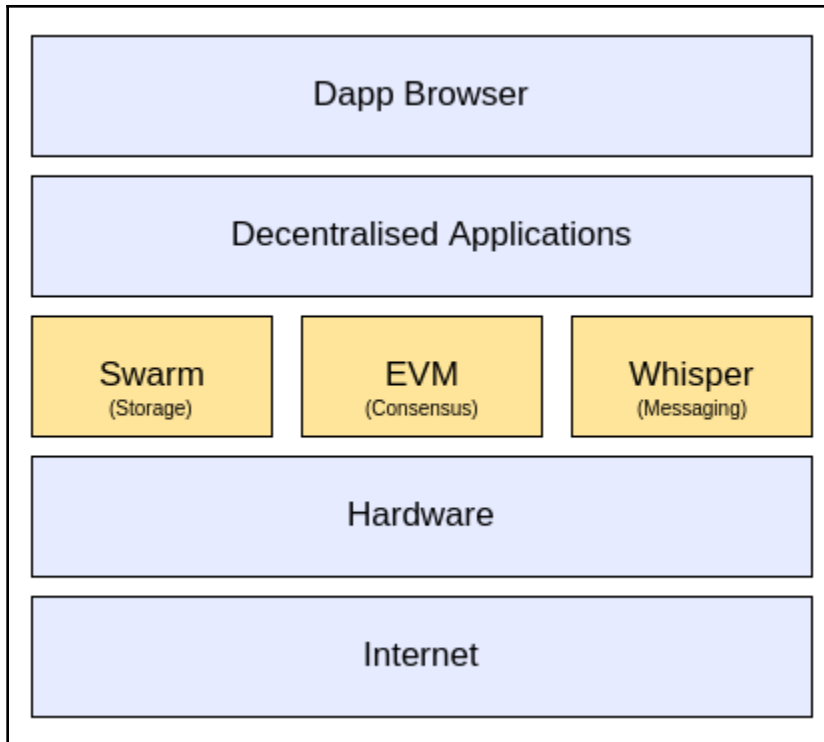
Your active account is:  [0x8ecb6c4e3d7710e2879e6498fa6387e7a33008a7](#)

Buy PET Tokens

0 / 500000

Chapter 9: Distributed Storage IPFS and Swarm





The screenshot shows the IPFS web interface. On the left is a navigation sidebar with options: Home, Connections, Files, DAG, and Config. The main content area is titled "NODE INFO" and displays the following details:

- Peer ID**: `QmZw1zPKuLTbcbaXYCD2JUodw9A2sNffJNeEy8eWk3b6`
- Location**: Leeds, H3, United Kingdom, Earth
- Agent Version**: `go-ipfs/0.4.17/`
- Protocol Version**: `ipfs/0.1.0`
- Public Key**: `CAASpgIwggEiMA9GCSqG5Ib3DQEBQUAA4IBDwAwggEKAoIBAQC5yEMM9snFy2o8dnDTFq6wvmtqr8vgb8I2Q/XBNdPIWu49u47YRPQhr3XFR58835FAdTkrFjGuN/JjOR17eyClqq1nS3am4g3eWRev1QwE:`

Below the node info is a section titled "NETWORK ADDRESSES" containing a list of IPFS addresses:

- `/ip4/127.0.0.1/tcp/4981/ipfs/QmZw1zPKuLTbcbaXYCD2JUodw9A2sNffJNeEy8eWk3b6`
- `/ip4/192.168.1.198/tcp/4981/ipfs/QmZw1zPKuLTbcbaXYCD2JUodw9A2sNffJNeEy8eWk3b6`
- `/ip6:::1/tcp/4981/ipfs/QmZw1zPKuLTbcbaXYCD2JUodw9A2sNffJNeEy8eWk3b6`
- `/ip4/95.150.46.139/tcp/4981/ipfs/QmZw1zPKuLTbcbaXYCD2JUodw9A2sNffJNeEy8eWk3b6`
- `/ip4/95.150.46.139/tcp/12727/ipfs/QmZw1zPKuLTbcbaXYCD2JUodw9A2sNffJNeEy8eWk3b6`

IPFS File Uploader

Web-3.0-Tech-Stack.jpg

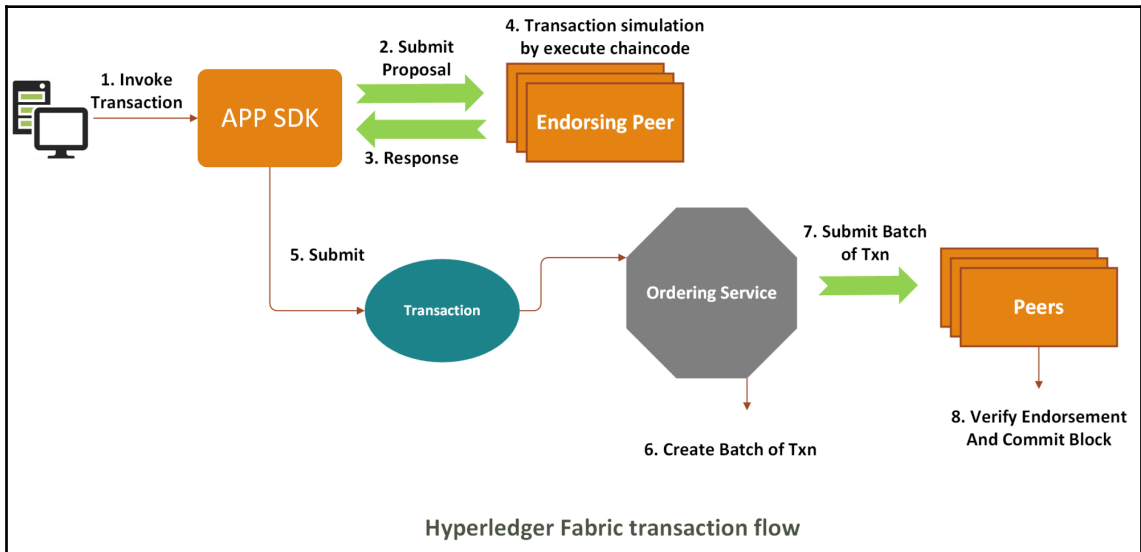
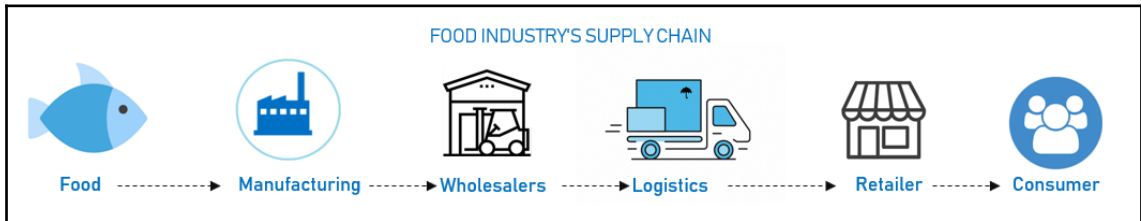
Browse

Upload

File uploaded to:

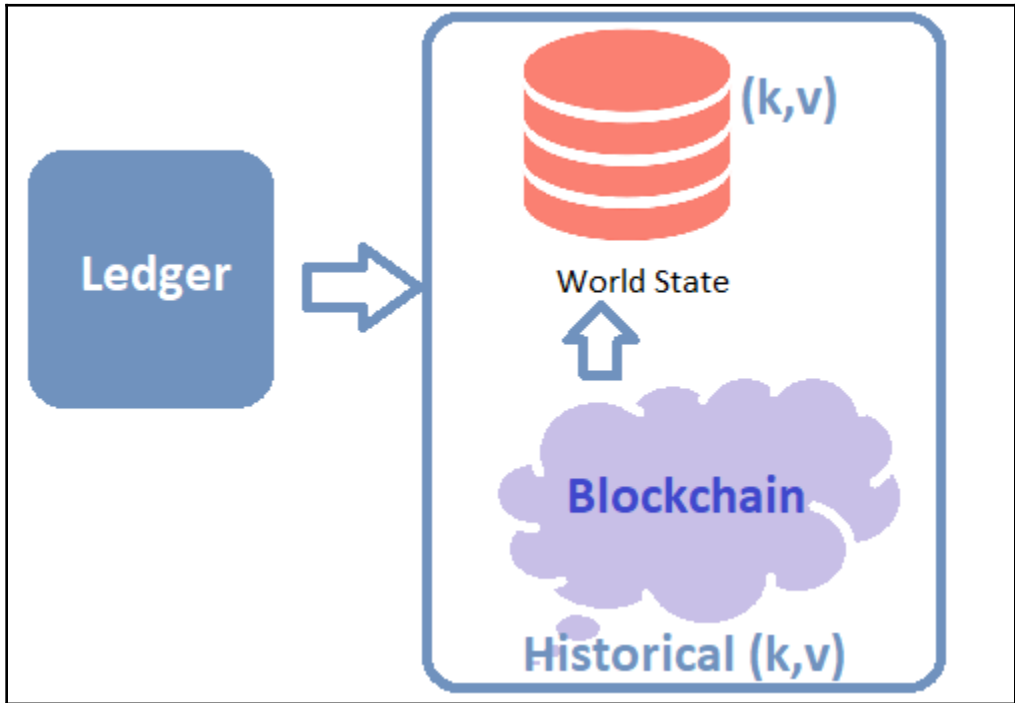
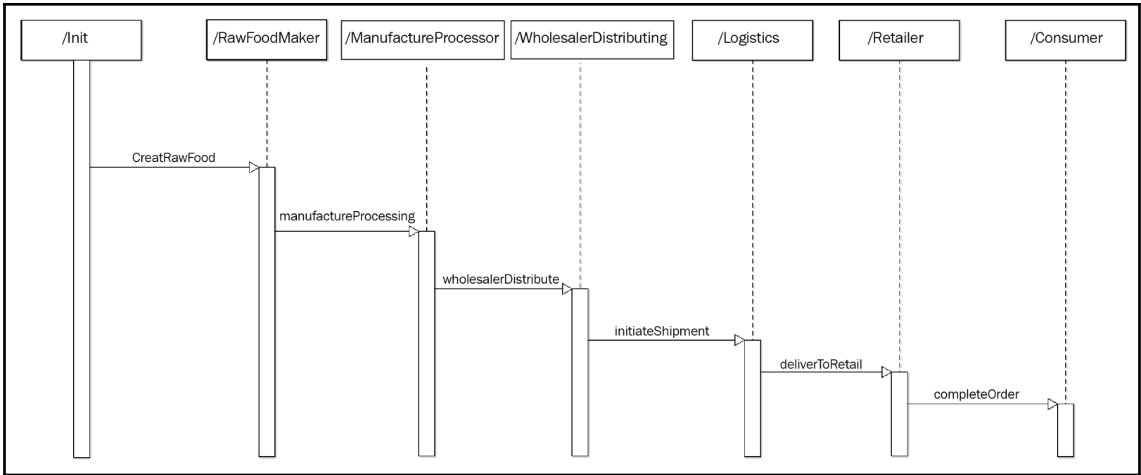
<https://ipfs.io/ipfs/QmcbPuwUJPRSDKo7gajbTtXadbXxYgA5dCdkimKMvfBFV>

Chapter 10: Supply Chain on Hyperledger

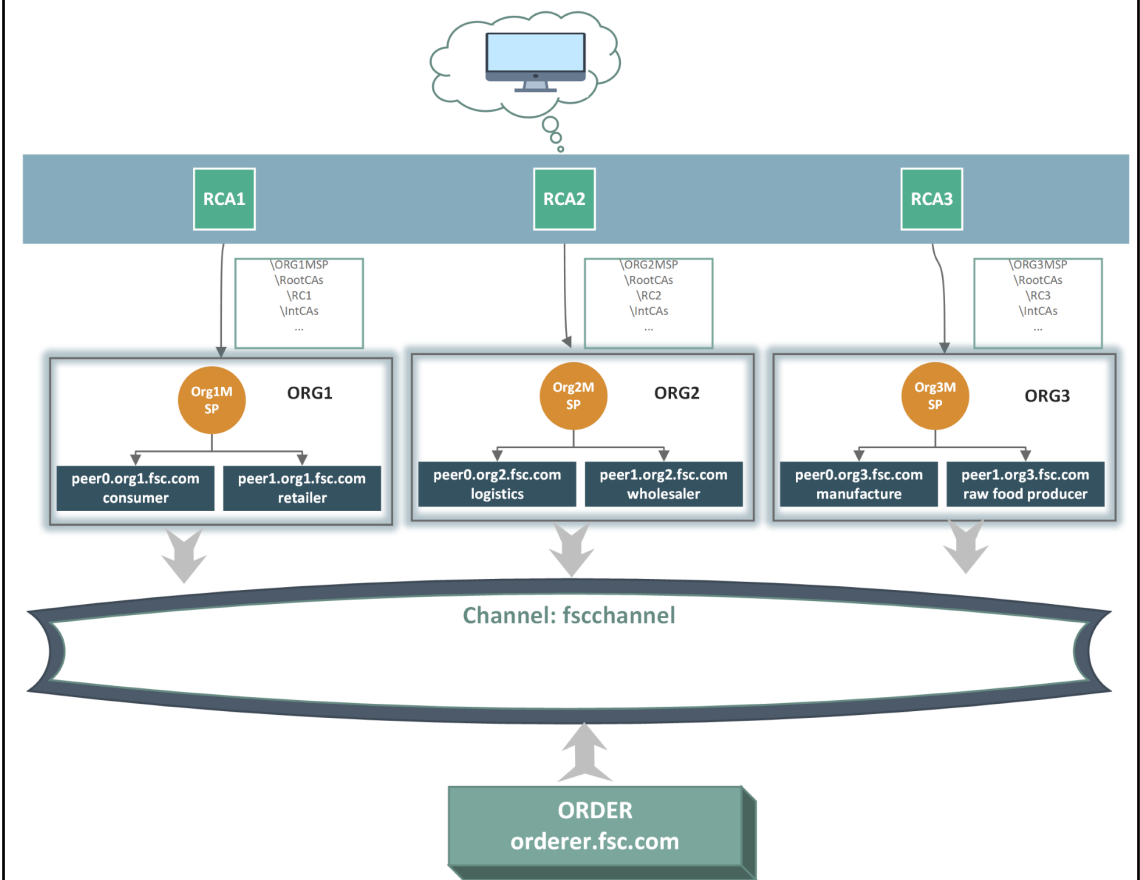


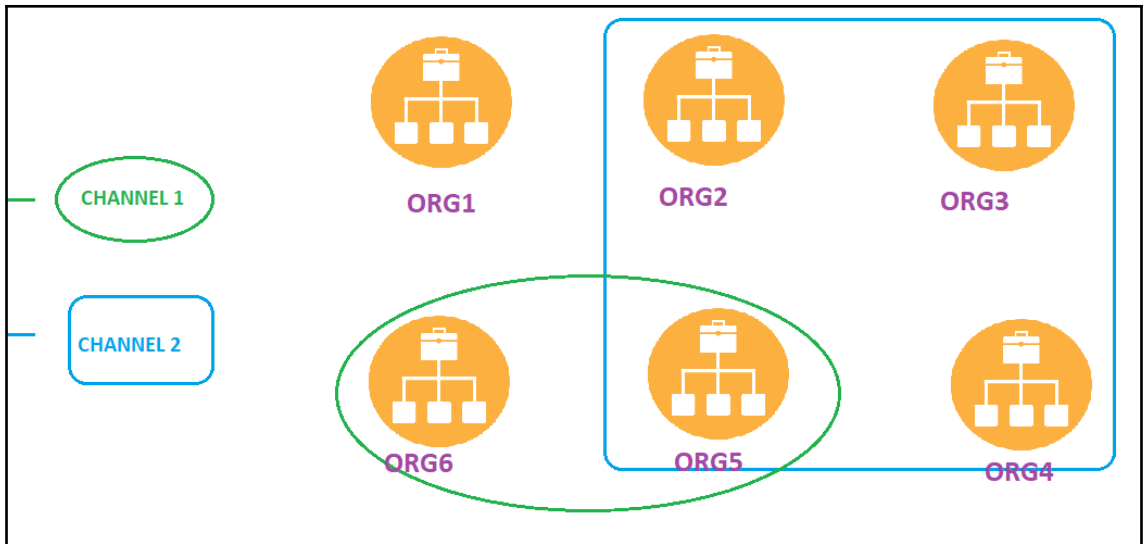
Food

OrderId : String
FoodId : String
ConsumerId: String
ManufactureId: String
WholesalerId: String
RetailerId: String
LogisticsId: String
Status: String
RawFoodProcessDate: String
ManufactureProcessDate: String
WholesaleProcessDate: String
ShippingProcessDate: String
RetailProcessDate: String
DeliveryDate: String
OrderPrice: Int



Blockchain





```

▼ folder food-supply-chain
  ▼ folder base
    /* docker-compose-base.yaml
    /* peer-base.yaml
  ▼ folder chaincode
    ▼ folder foodcontract
      /* foodcontract.go
  ► folder channel-artifacts
  ► folder scripts
    /* configtx.yaml
    /* crypto-config.yaml
    /* docker-compose-cli.yaml
    /* fscn.sh
  <> README.md

```



```

Update Anchor ...
CORE_PEER_TLS_ROOTCERT_FILE=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/peerOrganizations/org1.fsc.com/peers/peer0.org1.fsc.com/tls/ca.crt
CORE_PEER_TLS_KEY_FILE=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/peerOrganizations/org1.fsc.com/peers/peer0.org1.fsc.com/tls/server.key
CORE_PEER_LOCALMSPID=Org1MSP
CORE_VM_ENDPOINT=unix:///host/var/run/docker.sock
CORE_PEER_TLS_CERT_FILE=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/peerOrganizations/org1.fsc.com/peers/peer0.org1.fsc.com/tls/server.crt
CORE_PEER_TLS_ENABLED=true
CORE_PEER MSPCONFIGPATH=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/peerOrganizations/org1.fsc.com/users/Admin@org1.fsc.com/msp
CORE_PEER_ID=cli
CORE_LOGGING_LEVEL=DEBUG
CORE_PEER_ADDRESS=peer0.org1.fsc.com:7051
2018-09-29 23:37:29.688 UTC [msp] GetLocalMSP -> DEBU 001 Returning existing local MSP
2018-09-29 23:37:29.688 UTC [msp] GetDefaultSigningIdentity -> DEBU 002 Obtaining default signing identity
2018-09-29 23:37:29.691 UTC [channelCmd] InitCmdFactory -> INFO 003 Endorser and orderer connections initialized
2018-09-29 23:37:29.691 UTC [msp] GetLocalMSP -> DEBU 004 Returning existing local MSP
2018-09-29 23:37:29.691 UTC [msp] GetDefaultSigningIdentity -> DEBU 005 Obtaining default signing identity
2018-09-29 23:37:29.692 UTC [msp] GetLocalMSP -> DEBU 006 Returning existing local MSP
2018-09-29 23:37:29.692 UTC [msp] GetDefaultSigningIdentity -> DEBU 007 Obtaining default signing identity
2018-09-29 23:37:29.692 UTC [msp/identity] Sign -> DEBU 008 Sign: plaintext: 0A92060A074E7267314D53501286062D...2A0641646D696E732A0641646D696E73
2018-09-29 23:37:29.692 UTC [msp/identity] Sign -> DEBU 009 Sign: digest: F9A28ED47E853FA6D17DF113EFD0DE3398C4E3B96CC660A029A54506A6E35
2018-09-29 23:37:29.692 UTC [msp] GetLocalMSP -> DEBU 00a Returning existing local MSP
2018-09-29 23:37:29.692 UTC [msp] GetDefaultSigningIdentity -> DEBU 00b Obtaining default signing identity
2018-09-29 23:37:29.692 UTC [msp] GetLocalMSP -> DEBU 00c Returning existing local MSP
2018-09-29 23:37:29.692 UTC [msp] GetDefaultSigningIdentity -> DEBU 00d Obtaining default signing identity
2018-09-29 23:37:29.692 UTC [msp/identity] Sign -> DEBU 00e Sign: plaintext: 0ACA60A1608021A0608B999CDD0522...4108FCF83F27D313D77ECD4FFB9D8FE
2018-09-29 23:37:29.692 UTC [msp/identity] Sign -> DEBU 00f Sign: digest: 94451A0C82591021ED7DC1F4ADB7BDDF2E50FF05486DAC46E35C890DFACEF0
2018-09-29 23:37:29.707 UTC [channelCmd] update -> INFO 010 Successfully submitted channel update
2018-09-29 23:37:29.707 UTC [main] main -> INFO 011 Exiting....
*****
Updates Anchor peer1.org1 on the channel "fscchannel" *****

```

```

ubuntu@ip-172-31-15-76:~/apps/blockchain-by-example/food-supply-chain$ sudo bin/cryptogen generate --config=./crypto-config.yaml
org1.fsc.com
org2.fsc.com
org3.fsc.com

```

```

ubuntu@ip-172-31-15-76:~/apps/blockchain-by-example/food-supply-chain$ sudo docker-compose -f docker-compose-cli.yaml up
WARNING: The CHANNEL_NAME variable is not set. Defaulting to a blank string.
WARNING: The DELAY variable is not set. Defaulting to a blank string.
WARNING: The TIMEOUT variable is not set. Defaulting to a blank string.
WARNING: The COMPOSE_PROJECT_NAME variable is not set. Defaulting to a blank string.
Creating peer0.org3.fsc.com ... done
Creating peer0.org2.fsc.com ... done
Creating peer1.org2.fsc.com ... done
Creating peer1.org3.fsc.com ... done
Creating peer0.org1.fsc.com ... done
Creating orderer.fsc.com ... done
Creating peer1.org1.fsc.com ... done
Creating cli ... done
Attaching to peer0.org2.fsc.com, peer0.org1.fsc.com, peer1.org2.fsc.com, peer0.org3.fsc.com, orderer.fsc.com, peer1.org3.fsc.com, peer1.org1.fsc.com, cli
peer0.org2.fsc.com | 2018-09-29 07:30:03.955 UTC [viperutil] getKeysRecursively -> DEBU 001 Found map[string]interface{} value for peer.BCCSP
peer0.org2.fsc.com | 2018-09-29 07:30:03.956 UTC [viperutil] getKeysRecursively -> DEBU 002 Found map[string]interface{} value for peer.BCCSP.PKCS11
peer0.org2.fsc.com | 2018-09-29 07:30:03.956 UTC [viperutil] getKeysRecursively -> DEBU 003 Found map[string]interface{} value for peer.BCCSP

```



```
Querying chaincode on CompletedOrder/PEER0.peer0.org1...
CORE_PEER_TLS_ROOTCERT_FILE=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/peerOrganizations/org1.fsc.com/peers/peer0.org1.fsc.com/tls/ca.crt
CORE_PEER_TLS_KEY_FILE=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/peerOrganizations/org1.fsc.com/peers/peer0.org1.fsc.com/tls/server.key
CORE_PEER_LOCALMSPID=Org1MSP
CORE_VM_ENDPOINT=unix:///host/var/run/docker.sock
CORE_PEER_TLS_CERT_FILE=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/peerOrganizations/org1.fsc.com/peers/peer0.org1.fsc.com/tls/server.crt
CORE_PEER_TLS_ENABLED=true
CORE_PEER_MSPCONFIGPATH=/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/peerOrganizations/org1.fsc.com/users/Admin/org1.fsc.com/msp
CORE_PEER_ID=cli
CORE_LOGGING_LEVEL=DEBUG
CORE_PEER_ADDRESS=peer0.org1.fsc.com:7051
===== Querying on peerPEER0.org1 on channel 'fscchannel'... =====
Attempting to Query peerPEER0.org1 ...3 secs
Attempting to Query peerPEER0.org1 ...6 secs
Attempting to Query peerPEER0.org1 ...9 secs
Attempting to Query peerPEER0.org1 ...12 secs
Attempting to Query peerPEER0.org1 ...15 secs
Attempting to Query peerPEER0.org1 ...18 secs
Attempting to Query peerPEER0.org1 ...21 secs

2018-06-08 19:13:01.008 UTC [msp] GetLocalMSP -> DEBU 001 Returning existing local MSP
2018-06-08 19:13:01.008 UTC [msp] GetDefaultSigningIdentity -> DEBU 002 Obtaining default signing identity
2018-06-08 19:13:01.008 UTC [chaincodeCmd] checkChaincodeCmdParams -> INFO 003 Using default escc
2018-06-08 19:13:01.008 UTC [chaincodeCmd] checkChaincodeCmdParams -> INFO 004 Using default vsc
2018-06-08 19:13:01.008 UTC [chaincodeCmd] getChaincodeSpec -> DEBU 005 java chaincode disabled
2018-06-08 19:13:01.008 UTC [msp/identity] Sign -> DEBU 006 Sign: plaintext: 0A5CD70A6808031A808080DAE6B08510...71756572798A096F726465725F303031
2018-06-08 19:13:01.008 UTC [msp/identity] Sign -> DEBU 007 Sign: digest: F0B0602CF92E9615E049D33E70AA96222EF8A5393E9CD489830BA0D2E51DF48
Query Result: {"OrderId":"order_001","FoodId":"FISH_1","ConsumerId":"John_1","ManufactureId":"Manufacture_1","WholesalerId":"Wholesaler_1","RetailerId":"Retailer_1","LogisticsId":"LogisticsId_1","Status":"Consumer received order","RawFoodProcessDate":"2018-06-08 19:10:01","ManufactureProcessDate":"2018-06-08 19:10:39","WholesaleProcessDate":"2018-06-08 19:11:17","ShippingProcessDate":"2018-06-08 19:11:55","RetailProcessDate":"2018-06-08 19:12:17","OrderPrice":100,"ShippingPrice":5,"DeliveryDate":"2018-06-08 19:12:39"}
2018-06-08 19:13:01.023 UTC [main] main -> INFO 008 Exiting....

===== All GOOD, FSCN execution completed =====

END
```

← → ↻ 🏠 18.188.241.128:3000

Register Admin

Register User

OrderId	<input type="text"/>	Status	<input type="text"/>
ConsumerId	<input type="text"/>	ShippingPrice	<input type="text"/>
OrderPrice	<input type="text"/>	RawFoodProcessDate	<input type="text"/>
ManufactureId	<input type="text"/>	ManufactureProcessDate	<input type="text"/>
WholesalerId	<input type="text"/>	WholesaleProcessDate	<input type="text"/>
LogisticsId	<input type="text"/>	ShippingProcessDate	<input type="text"/>
RetailerId	<input type="text"/>	RetailProcessDate	<input type="text"/>
DeliveryDate	<input type="text"/>		

Query Chaincode

Register Admin

Register User

18.188.241.128:3000 says
Assigned the admin user to the fabric client

OK

OrderId

Status

ConsumerId

ShippingPrice

Register Admin

Register User

18.188.241.128:3000 says
User1 was successfully registered and enrolled and is ready to interact with the fabric network

OK

OrderId

Status

Register Admin

Register User

OrderId

order_001

Status

raw food created

ConsumerId

ShippingPrice

5

OrderPrice

100

RawFoodProcessDate

2018-06-10 04:30:04

ManufactureId

ManufactureProcessDate

WholesalerId

WholesaleProcessDate

LogisticsId

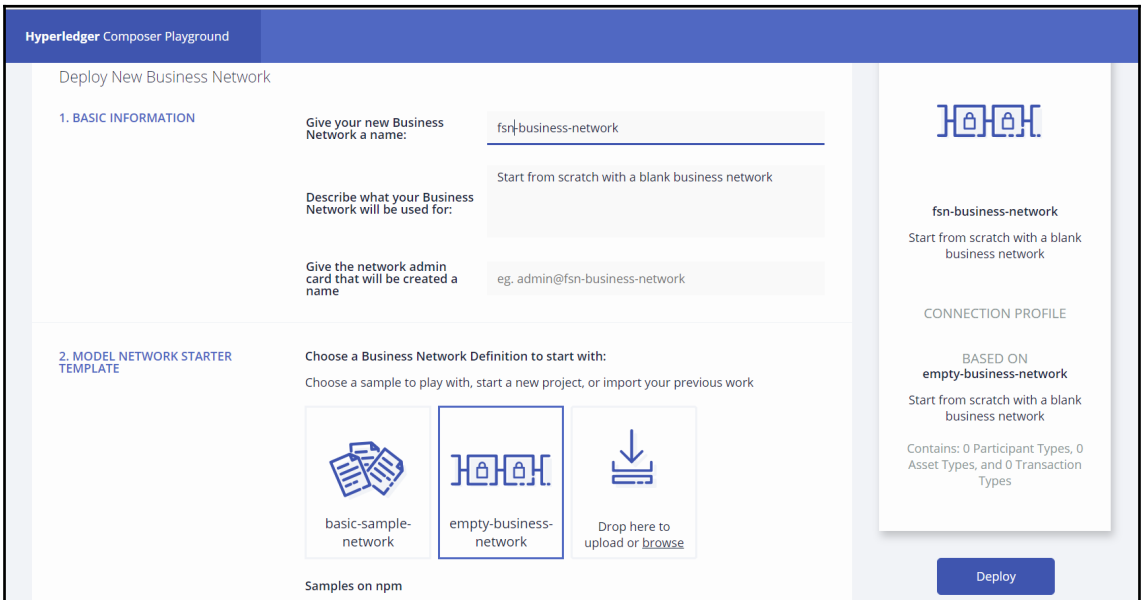
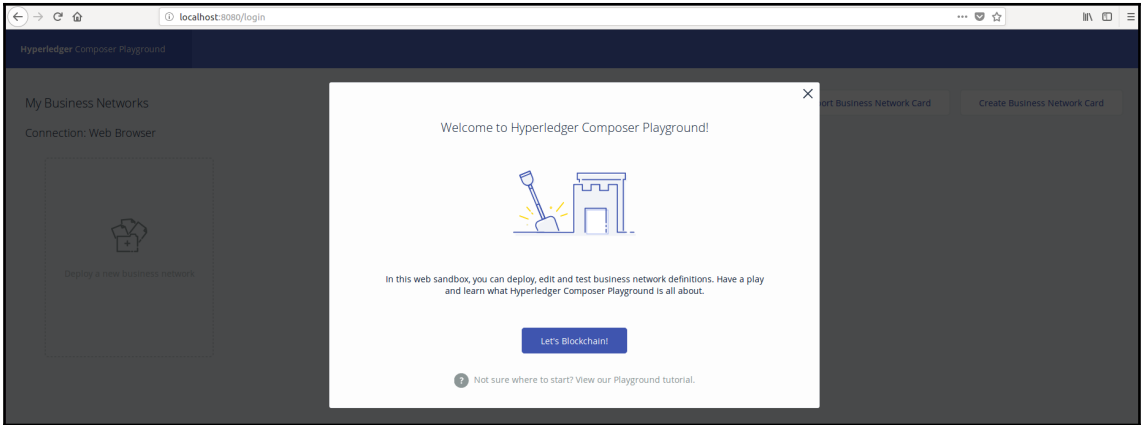
ShippingProcessDate

RetailerId

RetailProcessDate

DeliveryDate


Query Chaincode



Hyperledger Composer Playground

My Business Networks
[Import Business Network Card](#)
[Create Business Network Card](#)

Connection: Web Browser



admin@fsn-business-network


USER ID

admin

BUSINESS NETWORK

fsn-business-network

Connect now →




Deploy a new business network

Web fsn-network Define Test

FILES

- About**
README.md, package.json
- Model File**
models/model.cto
- Script File**
lib/script.js
- Access Control**
permissions.acl

Model File *models/model.cto* 

```

1
2 namespace org.fsn.testnetwork
3 asset Food identified by orderId {
4   o String orderId
5   o String status
6   o String date
7   o String orderPrice
8   o String shippingPrice
9   o String foodId
10  --> Consumer consumer
11
12 }
13 participant Consumer identified by consumerId {
14   o String consumerId
15   o String firstName
16   o String lastName
17 }
18 transaction Order {
19   --> Food food
20   --> Consumer newConsumer
21 }
```


FILES

About
README.md, package.json

Model File
models/model.cto

Script File
lib/script.js

Access Control
permissions.acl

Script File lib/script.js

```

1  /**
2  * @param {org.fsn.testnetwork.Order} order - order food product
3  * @transaction
4  */
5  function orderFoodProduct(order) {
6      order.food.consumer= order.newConsumer;
7      return getAssetRegistry('org.fsn.testnetwork.Food')
8          .then(function (assetRegistry) {
9          return assetRegistry.update(order.food);
10     });
11     }
```

Web fsn-business-network

Define Test

FILES

About
README.md, package.json

Model File
models/model.cto

Script File
lib/script.js

Access Control
permissions.acl

Add a file... Export

UPDATE NETWORK

From: 0.0.1

To: 0.0.2-deploy.0

Deploy changes

ACL File permissions.acl

```

1  /**
2  * Licensed under the Apache License, Version 2.0 (the "License");
3  * you may not use this file except in compliance with the License.
4  * You may obtain a copy of the License at
5  *
6  * http://www.apache.org/licenses/LICENSE-2.0
7  *
8  * Unless required by applicable law or agreed to in writing, software
9  * distributed under the License is distributed on an "AS IS" BASIS,
10 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
11 * See the License for the specific language governing permissions and
12 * limitations under the License.
13 */
14
15 rule NetworkAdminUser {
16     description: "Grant business network administrators full access to user resources"
17     participant: "org.hyperledger.composer.system.NetworkAdmin"
18     operation: ALL
19     resource: "*"
20     action: ALLOW
21 }
22
23 rule NetworkAdminSystem {
24     description: "Grant business network administrators full access to system resources"
25     participant: "org.hyperledger.composer.system.NetworkAdmin"
26     operation: ALL
27     resource: "org.hyperledger.composer.system.*"
28     action: ALLOW
29 }
```

Everything looks good!
Any problems detected in your code would be reported here

In registry: **org.fsn.testnetwork.Consumer**

JSON Data Preview

```
1  {
2    "$class": "org.fsn.testnetwork.Consumer",
3    "consumerId": "Brian",
4    "firstName": "Brian",
5    "lastName": "Wu"
6  }
```

The screenshot shows a web application interface for 'Web fsn-network'. The top navigation bar includes 'Define', 'Test', and 'admin' tabs. The left sidebar contains a menu with sections: PARTICIPANTS (Consumer), ASSETS (Food), and TRANSACTIONS (All Transactions). A 'Submit Transaction' button is located at the bottom left. The main content area displays 'Asset registry for org.fsn.testnetwork.Food' with a table showing one asset entry. The table has columns for 'ID' and 'Data'. The data for ID '001' is a JSON object: { "\$class": "org.fsn.testnetwork.Food", "orderId": "001", "status": "New", "date": "2018-06-10 10:22:01", "orderPrice": "100", "shippingPrice": "5", "foodId": "Food001", "consumer": "resource:org.fsn.testnetwork.Consumer#0531" }. A 'Collapse' button is located below the data field.

ID	Data
001	{ "\$class": "org.fsn.testnetwork.Food", "orderId": "001", "status": "New", "date": "2018-06-10 10:22:01", "orderPrice": "100", "shippingPrice": "5", "foodId": "Food001", "consumer": "resource:org.fsn.testnetwork.Consumer#0531" }

Submit Transaction

Transaction Type

Order



JSON Data Preview

```
1 {
2   "$class": "org.fsn.testnetwork.Order",
3   "food": "resource:org.fsn.testnetwork.Food#001",
4   "newConsumer": "resource:org.fsn.testnetwork.Consumer#Brian"
5 }
```

Define Test

admin



Date, Time	Entry Type	Participant	
2018-06-10, 02:59:00	Order	admin (NetworkAdmin)	view record
2018-06-10, 02:53:42	AddAsset	admin (NetworkAdmin)	view record
2018-06-10, 02:52:00	AddParticipant	admin (NetworkAdmin)	view record

Web fsn-network Define Test admin

PARTICIPANTS

Consumer

ASSETS

Food

TRANSACTIONS

All Transactions

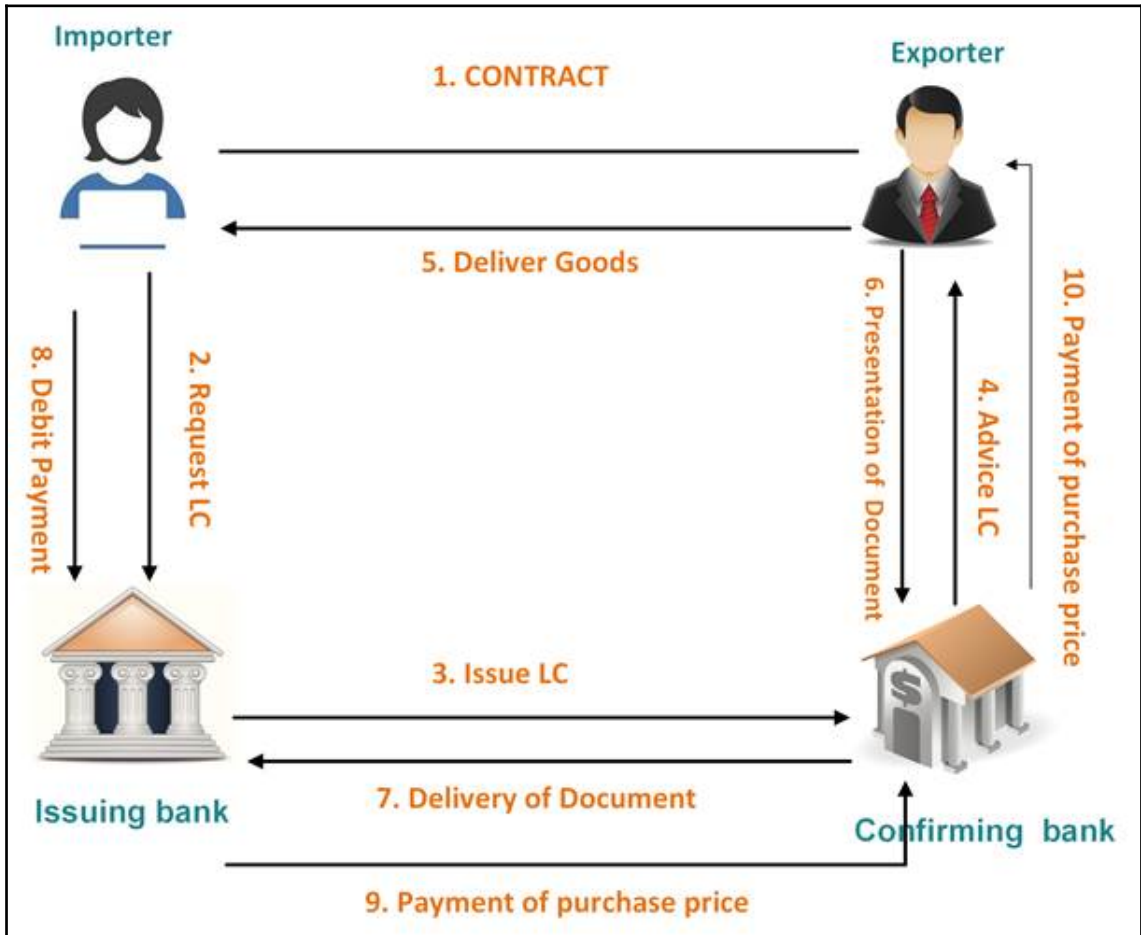
Asset registry for org.fsn.testnetwork.Food

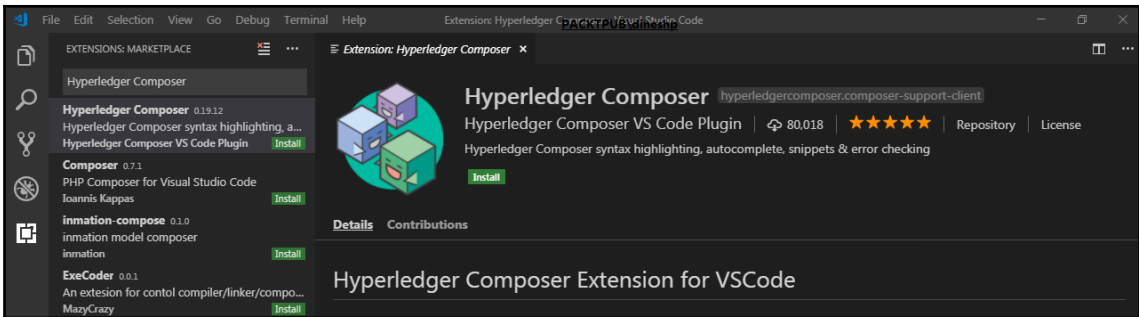
+ Create New Asset

ID	Data
001	<pre>{ "\$class": "org.fsn.testnetwork.Food", "orderId": "001", "status": "New", "date": "2018-06-10 10:22:01", "orderPrice": "100", "shippingPrice": "5", "foodId": "Food001" "consumer": "resource:org.fsn.testnetwork.Consumer#Brian" }</pre>

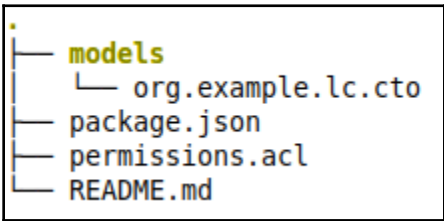
Collapse

Chapter 11: Letter of Credit (LC) Hyperledger





```
Welcome to the business network generator
? Business network name: lc-network
? Description: LC Business network
? Author name: your name
? Author email: your Email
? License: Apache-2.0
? Namespace: org.example.lc
? Do you want to generate an empty template network? Yes: generate an empty template network
create package.json
create README.md
create models/org.example.lc.cto
create permissions.acl
create .eslintrc.vml
```



```

ubuntu@ip-172-31-15-76:~/fabric-dev-servers$ ls
createComposerProfile.sh  DevServer  connection.json  fabric-dev-servers.tar.gz  loader.sh  startFabric.sh  teardownAllDocker.sh
createPeerAdminCard.sh  downloadFabric.sh  fabric-scripts  package.json  stopFabric.sh  teardownFabric.sh
ubuntu@ip-172-31-15-76:~/fabric-dev-servers$ ./createPeerAdminCard.sh
Development only script for Hyperledger Fabric control
Running 'createPeerAdminCard.sh'
FABRIC_VERSION is unset, assuming hlfv1
FABRIC_START_TIMEOUT is unset, assuming 15 (seconds)

Using composer-cli at v0.19.5

Successfully created business network card file to
  Output file: /tmp/PeerAdmin@hlfv1.card

Command succeeded

Successfully imported business network card
  Card file: /tmp/PeerAdmin@hlfv1.card
  Card name: PeerAdmin@hlfv1

Command succeeded

The following Business Network Cards are available:

Connection Profile: hlfv1

```

Card Name	UserId	Business Network
PeerAdmin@hlfv1	PeerAdmin	

```

Issue composer card list --card <Card Name> to get details a specific card

Command succeeded

Hyperledger Composer PeerAdmin card has been imported, host of fabric specified as 'localhost'

```

```

ubuntu@ip-172-31-15-76:~/apps/blockchain-by-example/letterofcredit/lc-network$ composer-rest-server
? Enter the name of the business network card to use: admin@lc-network
? Specify if you want namespaces in the generated REST API: never use namespaces
? Specify if you want to use an API key to secure the REST API: No
? Specify if you want to enable authentication for the REST API using Passport: No
? Specify if you want to enable event publication over WebSockets: Yes
? Specify if you want to enable TLS security for the REST API: No

To restart the REST server using the same options, issue the following command:
  composer-rest-server -c admin@lc-network -n never -w true

Discovering types from business network definition ...
Discovered types from business network definition
Generating schemas for all types in business network definition ...
Generated schemas for all types in business network definition
Adding schemas for all types to Loopback ...
Added schemas for all types to Loopback
Web server listening at: http://localhost:3000
Browse your REST API at http://localhost:3000/explorer

```

Hyperledger Composer REST server	
Bank	: A participant named Bank
BanksTransferPayment	: A transaction named BanksTransferPayment
BuyerDepositPayment	: A transaction named BuyerDepositPayment
BuyerRequestLC	: A transaction named BuyerRequestLC
Close	: A transaction named Close
ConfirmingBankAdviceLC	: A transaction named ConfirmingBankAdviceLC
ConfirmingBankDeliverDocument	: A transaction named ConfirmingBankDeliverDocument
CreateDemoParticipants	: A transaction named CreateDemoParticipants
InitialApplication	: A transaction named InitialApplication
IssuingBankApproveLC	: A transaction named IssuingBankApproveLC
LetterOfCredit	: An asset named LetterOfCredit
SellerDeliverGoods	: A transaction named SellerDeliverGoods
SellerPresentDocument	: A transaction named SellerPresentDocument
SellerReceivedPayment	: A transaction named SellerReceivedPayment
System	: General business network methods
User	: A participant named User
[BASE URL: /api , API VERSION: 0.0.1]	

POST /CreateDemoParticipants

Response Class (Status 200)
Request was successful

Model | Example Value

```
{
  "$class": "org.example.lc.CreateDemoParticipants",
  "transactionId": "string",
  "timestamp": "2018-06-27T00:43:56.330Z"
}
```

Response Content Type

Parameters

Parameter	Value
data	<pre>{ "\$class": "org.example.lc.CreateDemoParticipants", "timestamp": "2018-06-27T00:43:56.330Z" }</pre>

Parameter content type:

[Try it out!](#) [Hide Response](#)

Curl

```
curl -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' -d '{ \
  "$class": "org.example.lc.CreateDemoParticipants", \
  "timestamp": "2018-06-27T00:43:56.330Z" \
}' 'http://18.220.135.130:3000/api/CreateDemoParticipants'
```

Request URL

```
http://18.220.135.130:3000/api/CreateDemoParticipants
```

Response Body

```
{
  "$class": "org.example.lc.CreateDemoParticipants",
  "transactionId": "1313100c75122992600360b135da3dce6bfd7cbc91a2257e364d6afdcf7b76ec",
  "timestamp": "2018-06-27T00:43:56.330Z"
}
```

Response Code

```
200
```

Curl

```
curl -X GET --header 'Accept: application/json' 'http://18.220.135.130:3000/api/User'
```

Request URL

```
http://18.220.135.130:3000/api/User
```

Response Body

```
[
  {
    "$class": "org.example.lc.User",
    "userId": "david",
    "name": "David",
    "lastName": "Wilson",
    "companyName": "Toy Mart Inc",
    "type": "BUYER",
    "bank": "resource:org.example.lc.Bank#BI"
  },
  {
    "$class": "org.example.lc.User",
    "userId": "jason",
    "name": "Jason",
    "lastName": "Jones",
    "companyName": "Valley Toys Manufacturing",
    "type": "SELLER",
    "bank": "resource:org.example.lc.Bank#EB"
  }
]
```

Curl

```
curl -X GET --header 'Accept: application/json' 'http://18.220.135.130:3000/api/Bank'
```

Request URL

```
http://18.220.135.130:3000/api/Bank
```

Response Body

```
[
  {
    "$class": "org.example.lc.Bank",
    "bankID": "BE",
    "name": "Bank of Eastern Export",
    "type": "CONFIRMING_BANK"
  },
  {
    "$class": "org.example.lc.Bank",
    "bankID": "BI",
    "name": "First Consumer Bank",
    "type": "ISSUING_BANK"
  }
]
```

Response Code

```
200
```

IBM Cloud Catalog Docs Support Manage Search for resource...


Catalog

blockchain

All Categories (1) >

- Compute
- Containers
- Networking
- Storage
- AI
- Analytics
- Databases (1)
- Developer Tools
- Integration
- Internet of Things

Databases



Blockchain
IBM

IBM Blockchain Platform is a flexible software-as-a-service offering that simplifies the blockchain journey of developing, governing, and operating a blockchain network.

Pricing Plans

Monthly prices shown are for country or region: United States

PLAN	FEATURES	PRICING
Try out Blockchain with your credits.		
✓ Starter Membership Plan	<p>Get \$500 towards your first Starter Plan network - sign up today*</p> <p>This plan entitles a member of the Blockchain Platform to:</p> <ul style="list-style-type: none"> - With a single click, setup and a fully functional kick starter network that is configured with 2 organizations and 1 peer per organization. - This easily deployed development environment, includes all components of the blockchain network, quickly install and instantiate chaincode or import your business network archive 	<p>\$250.00 USD/Membership Fee</p> <p>\$125.00 USD/Small Peer</p>

Create

IBM Cloud Catalog Docs Support Manage Search for resource... Pack

Create toolchain: Marbles sample for IBM Blockchain

This toolchain will deploy a Marbles sample application against a IBM Blockchain Platform network.

The toolchain starts by creating your own repository of the Marbles code. This repo is connected to a Delivery Pipeline which means if you update the code in your GitHub repo, the Deployment Pipeline will detect it and deploy your changes. The toolchain also creates a **new Blockchain Platform service instance**, which is your blockchain network.

You do not need to change any of the options on the right, though you may tweak configurations if you need to.

You may need to authorize IBM Cloud with your GitHub account before you can create the toolchain.

TEMPLATE INFO
GIT URL <https://github.com/IBM...>
GIT BRANCH [master](#)

This toolchain will...

Clone the GitHub repo → Setup deployment pipeline → Run code in IBM Blockchain

Run web apps in IBM Cloud

Toolchain Name: marbles-tc-20181129090611065

Select Region: Washington DC

Select a resource group: Default

Create

IBM Cloud Catalog Docs Support Manage Search for resource... Packt

Washington DC Default

Tool Integrations

Marbles GitHub Delivery Pipeline **Required**

The Delivery Pipeline powers your continuous integration. It will update/deploy Marbles whenever you push Git commits to your fork and branch.

Marbles: ⓘ
marbles-20181129090611065

IBM Cloud API Key: ⓘ
..... **Create** +

Pipeline Location

Region	Organization	Space
Washington DC (f)	Loading...	Loading...

The value is required. **The value is not valid.**

Create

marbles-20181129142336291 | Delivery Pipeline

Deploy Marbles Application



Add Stage +

STAGE RUNNING...

LAST INPUT

[Git URL](#)



Last commit by Shunji Makino 31d ago
[Update README-ja.md \(#272\)](#)

JOBS

[View logs and history](#)



deploy-marbles-... Running




LAST EXECUTION RESULT

No results

IBM Cloud Catalog Docs Support Manage Search for resource... Packt


Toolchains / marbles-tc-20181129142336291


 marbles-tc-20181129142336291 View app


Resource Group: Default Location: London

✔ Your Toolchain is ready! Click the "Delivery Pipeline" tile below to see Marble's build status.

CODE DELIVER RUN


 GitHub
marbles-2018112914...
✔ Configured

 Delivery Pipeline
marbles-2018112914...
✔ Configured

 Marbles
Node.js Application
✔ Configured

Add a Tool

Secure https://marbles-20180630194905968.mybluemix.net/login

 Company A Admin




WELCOME TO THE MARBLES DEMO APP
Hello again **Company A** admin !

This application allows you to simulate a simple asset transaction over a Hyperledger Fabric blockchain. You can connect multiple peers to trade with a larger marble user base. In this application, you can:

Trade
Transfer assets (marbles) across the marbles user base

Create
Create new assets (marbles)

Verify
Verify marble transactions

For more information, please visit our [GitHub](#)

Enter
admin Login

