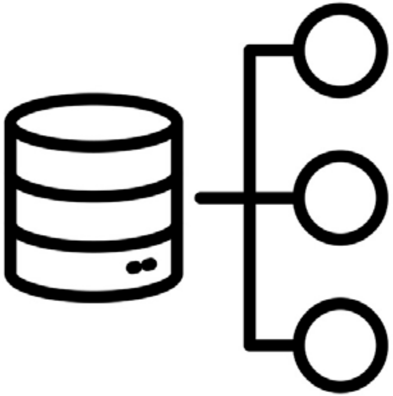
Carnegie Mellon University
Software Engineering Institute

Next Steps with Blockchain Technology

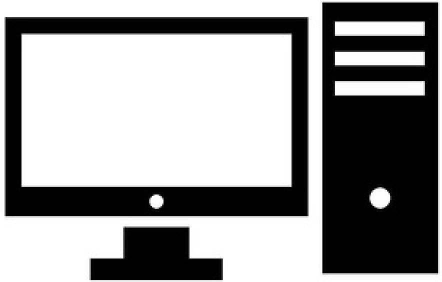
Eliezer Kanal & Gabriel Somlo

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Previous models of computing

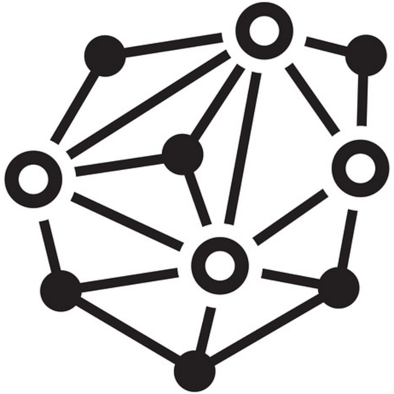


Data Storage:
Database



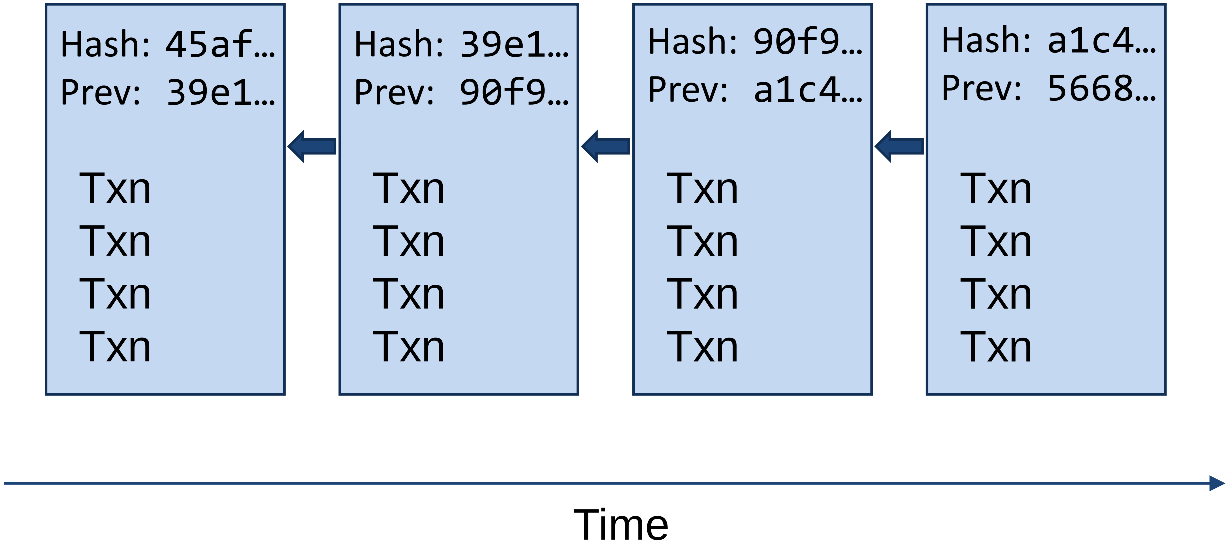
Program Execution:
Local

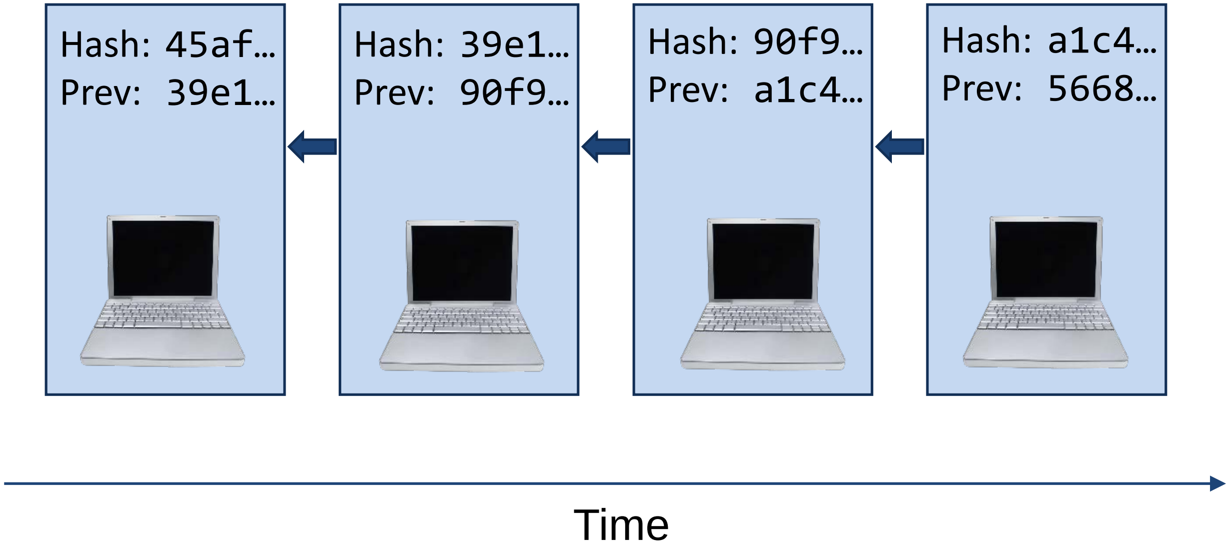
Blockchain



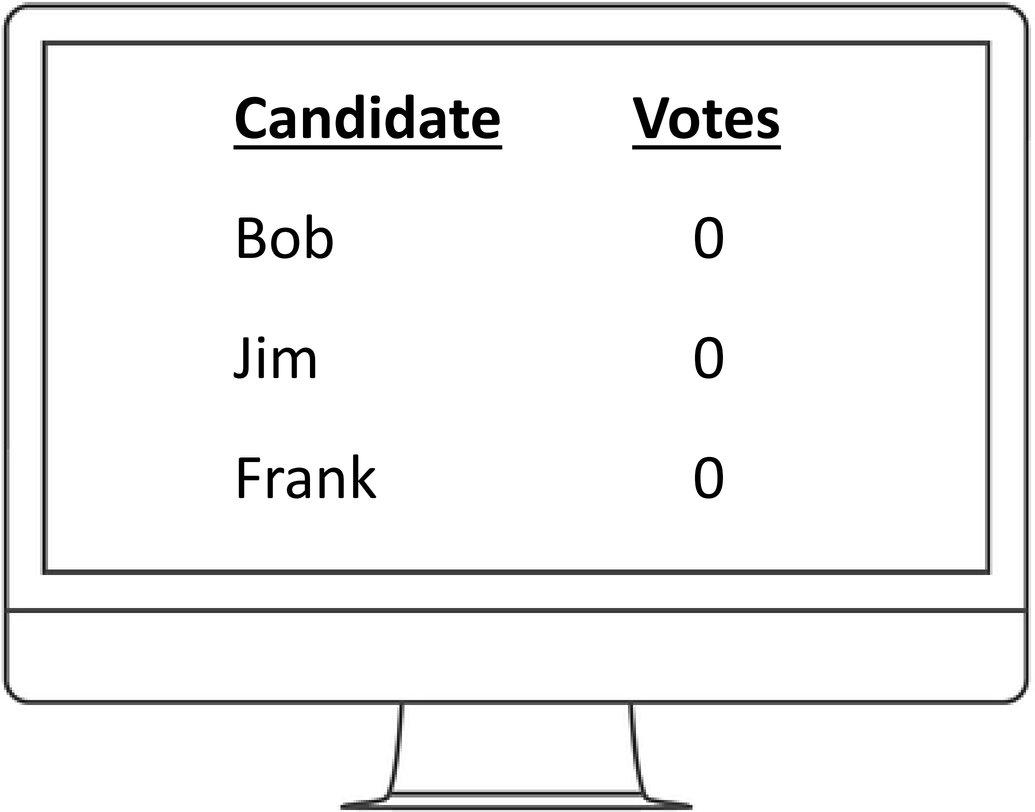
Data Storage:
Blockchain or Network

Program Execution:
Network


Hash: 45af…
Prev: 39e1…
Txn
Txn
Txn
Txn
Hash: 39e1…
Prev: 90f9…
Txn
Txn
Txn
Txn
Hash: 90f9…
Prev: a1c4…
Txn
Txn
Txn
Txn
Hash: a1c4…
Prev: 5668…
Txn
Txn
Txn
Txn
Time

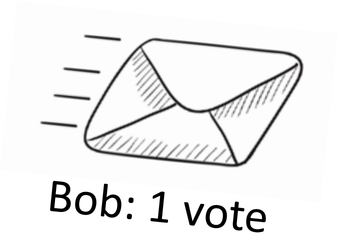

Hash: 45af…
Prev: 39e1…
Hash: 39e1…
Prev: 90f9…
Hash: 90f9…
Prev: a1c4…
Hash: a1c4…
Prev: 5668…
Time

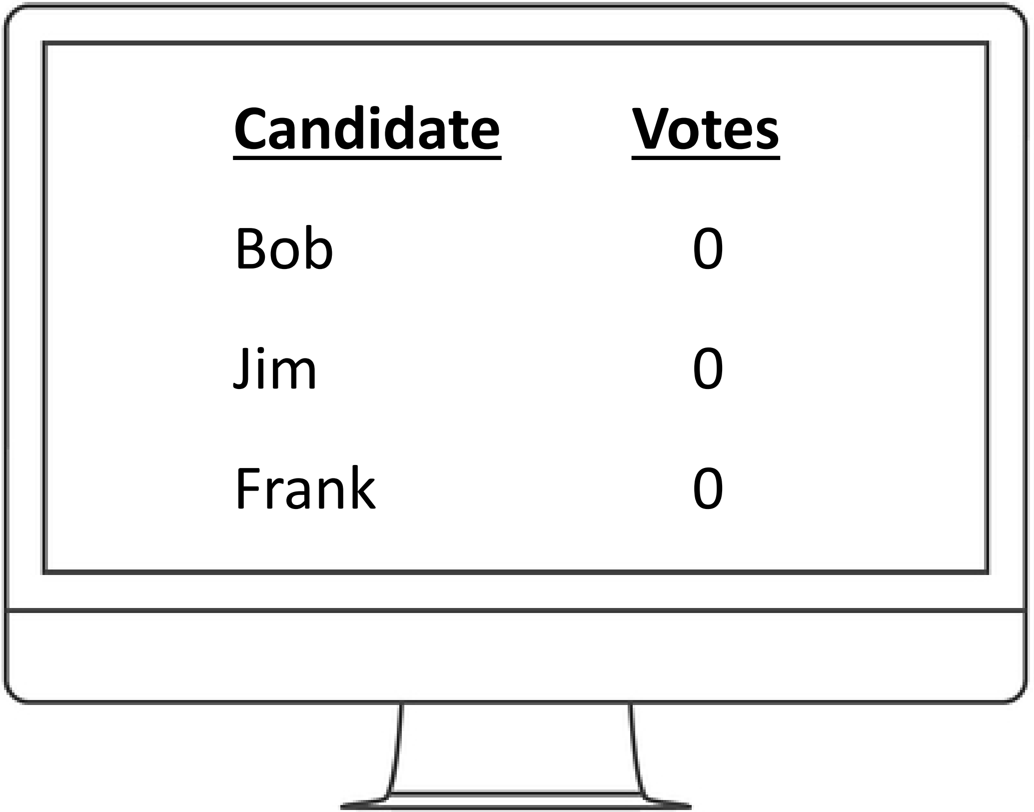
State: 1



Candidate	Votes
Bob	0
Jim	0
Frank	0

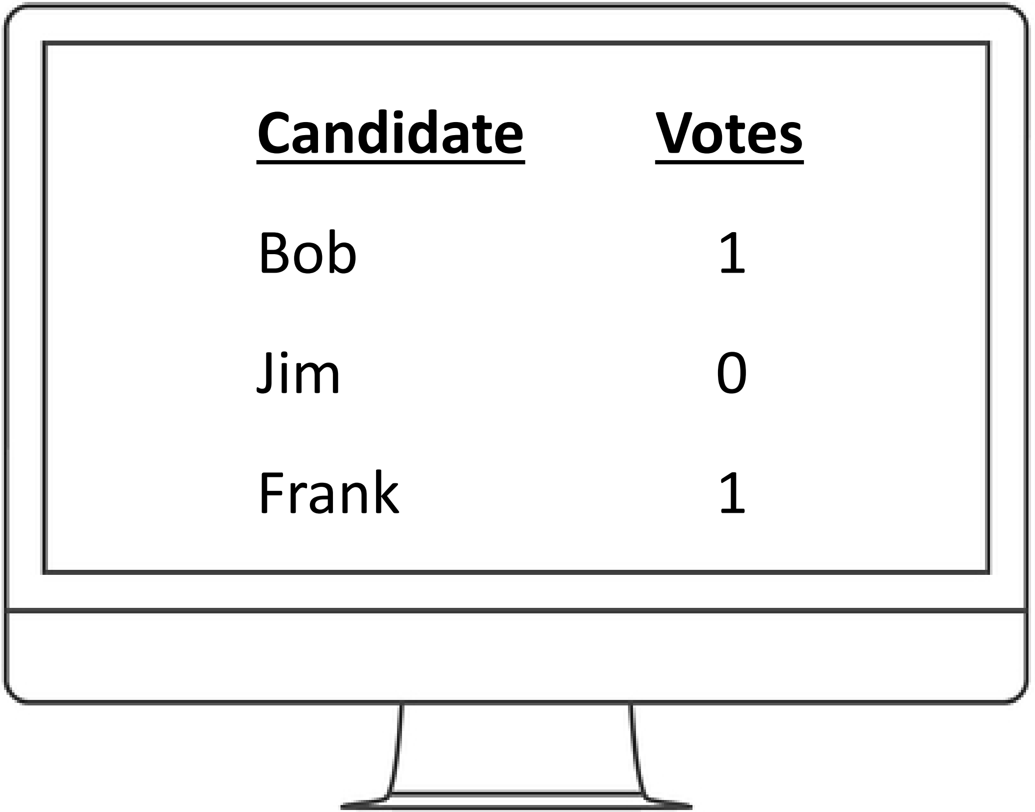
State: 1





Candidate	Votes
Bob	0
Jim	0
Frank	0

State: 2



Candidate	Votes
Bob	1
Jim	0
Frank	1

State: 1

Candidate	Votes
Bob	0
Jim	0
Frank	0

State: 2

Candidate	Votes
Bob	1
Jim	0
Frank	1

Equivalent to:

State: 1

Candidate	**Votes**
Bob	0
Jim	0
Frank	0

State: 2

State 1 plus…

Bob: 1 vote

Frank: 1 vote

Blockchain: Executive Summary

Pros:

Authentication built-in

Easy to audit history

Easy to detect data manipulation

Very difficult to disrupt

Cons:

Proof-of-work very inefficient

State updates are slow

Best for simple computations

Bitcoin: Mining

Input

- Previous block signature
- Bunch of transactions
- Random number

→ 60C89EA…

Signature	Transactions	Random #	Output
482AA…	txn 1, 17, 88, 452	1	854A3…
482AA…	txn 1, 17, 88, 452	2	B4221…
482AA…	txn 1, 17, 88, 452	3	0249F…
⋮			

Block #509169

Summary	
Number Of Transactions	1915
Output Total	10,289.28130284 BTC
Estimated Transaction Volume	1,818.68925455 BTC
Transaction Fees	0.4893378 BTC
Height	509169 (Main Chain)
Timestamp	2018-02-14 15:16:59
Received Time	2018-02-14 15:16:59
Relayed By	58COIN
Difficulty	2,874,674,234,415.94
Bits	392292856
Size	1132.416 kB
Weight	3992.574 kWU
Version	0x20000000
Nonce	1858980081
Block Reward	12.5 BTC

Hashes	
Hash	0000000000000000002c4b94355945eea353bc720c58a73c2b8593f489550cb3
Previous Block	00000000000000000001d620a2e3ad126ec5038bf42343c419eb6fcdf7240a471
Next Block(s)	
Merkle Root	3ad680735c45cc62b1ea6b7efeb34f82a2660c5e8280354c45f7ffa03c9137e2

Transactions

ab0da64ea834fd2acb81eb081d8103c9e31fd14a7d055f2ce2718c59dd4fa5df — 2018-02-14 15:16:59

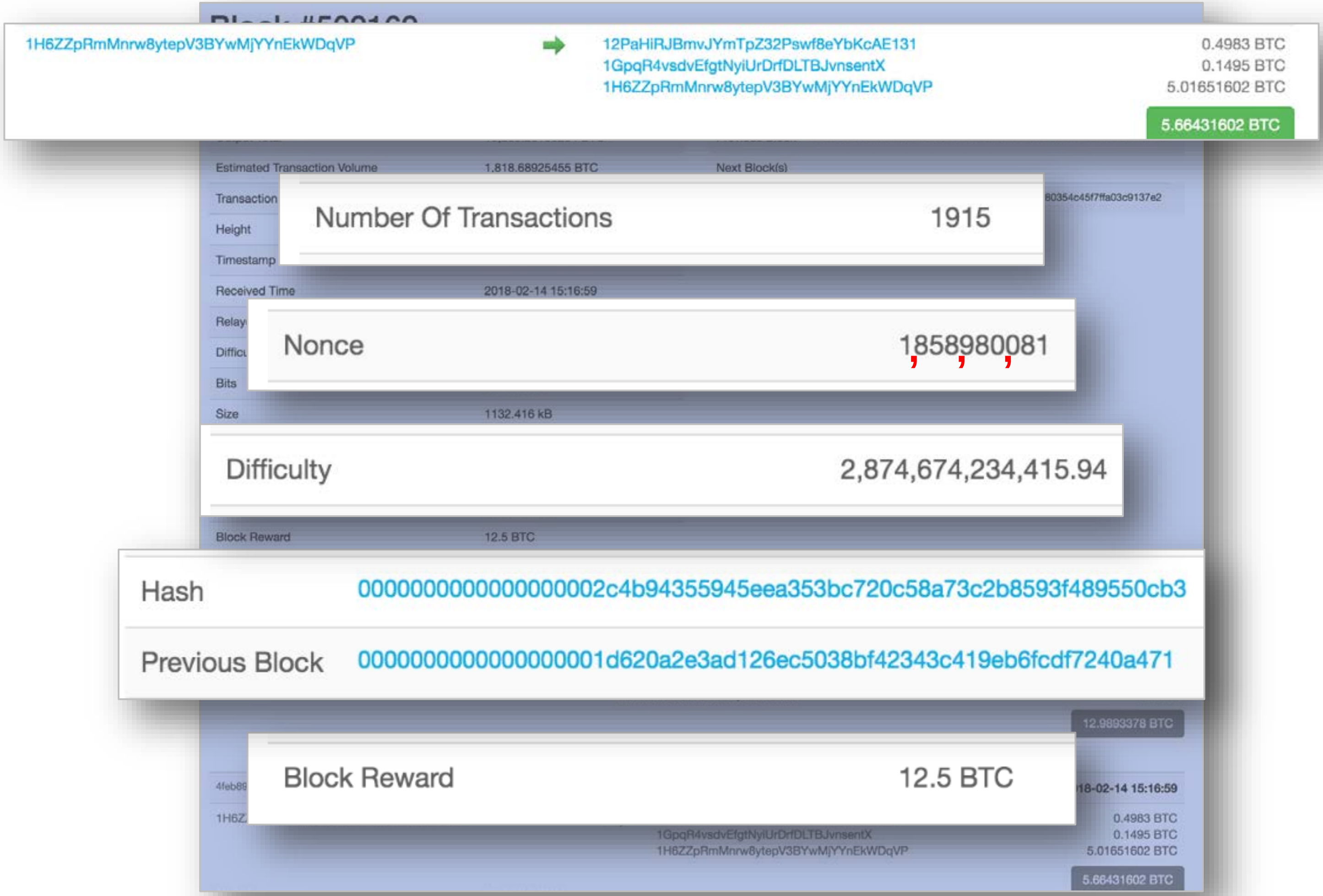
No Inputs (Newly Generated Coins) → 14DjTuAUh87cwRsbU1z6W8hZY6FnEkpfLS 12.9893378 BTC
Unable to decode output address 0 BTC

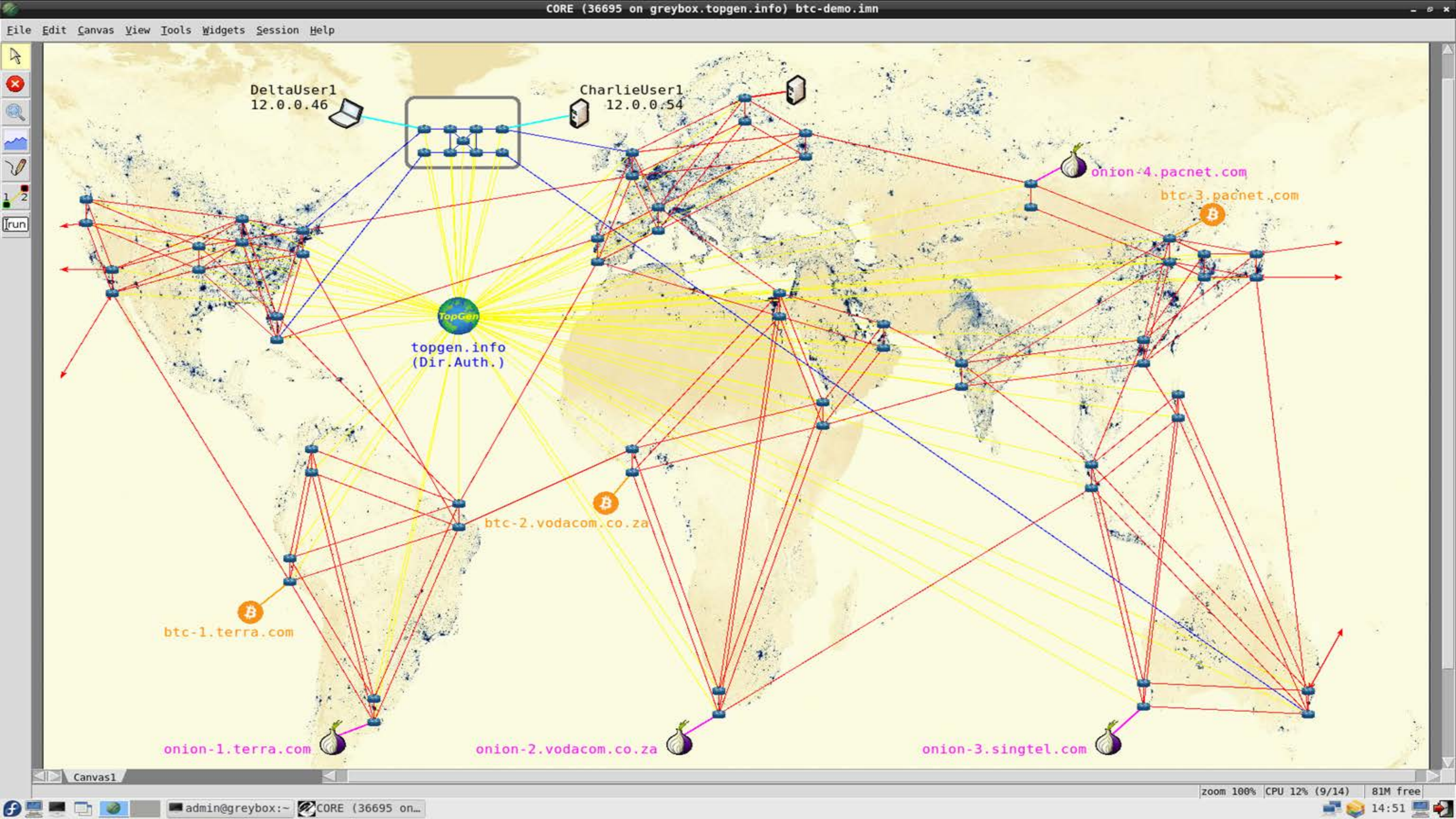
12.9893378 BTC

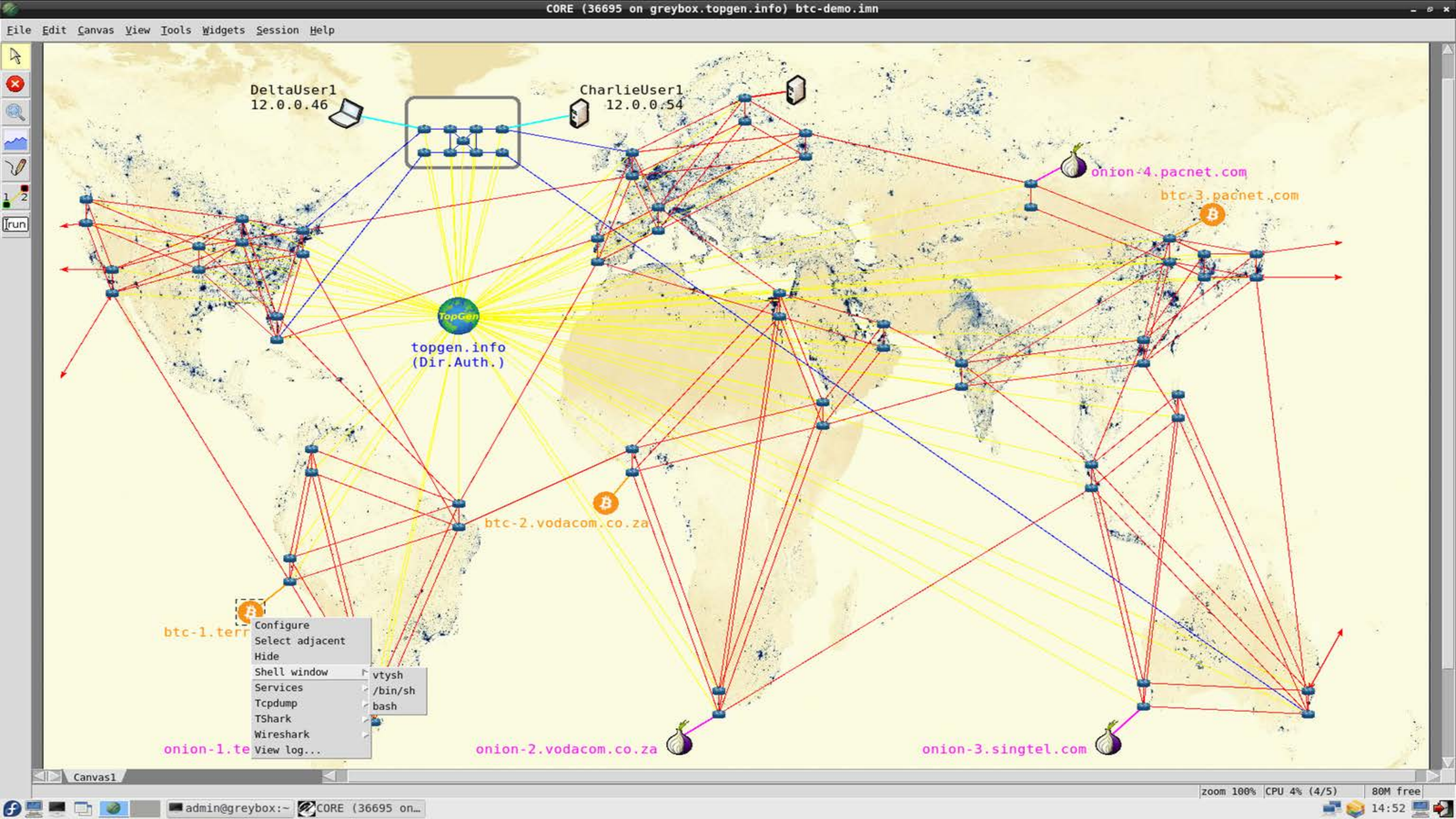
4feb8981da942b10a2a384003fba1c1d78c8f192cd2747e43ae552ed237f267d — 2018-02-14 15:16:59

1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP →
12PaHiRJBmvJYmTpZ32Pswf8eYbKcAE131 0.4983 BTC
1GpqR4vsdvEfgtNyiUrDrfDLTBJvnsentX 0.1495 BTC
1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP 5.01651602 BTC

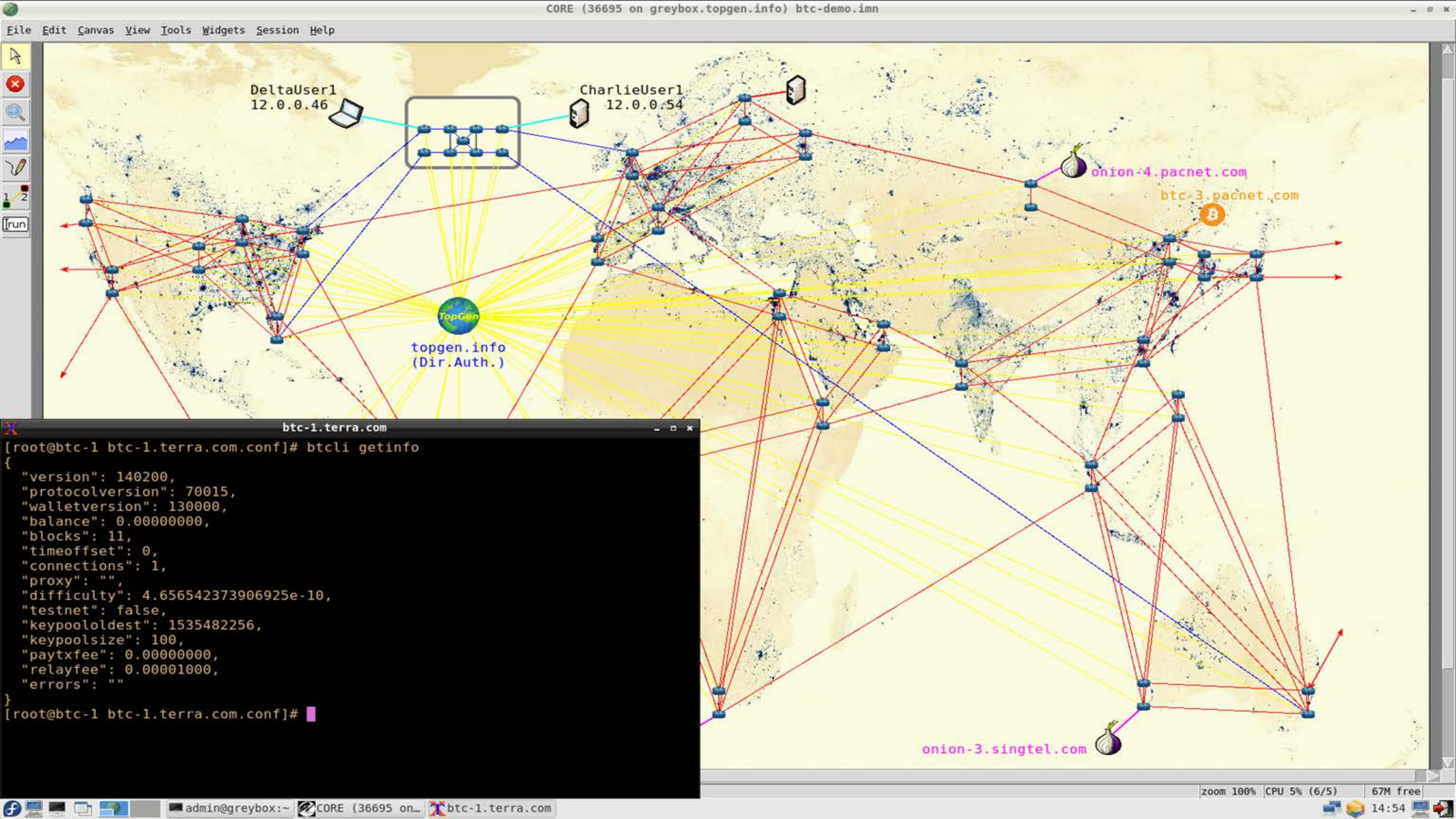
5.66431602 BTC

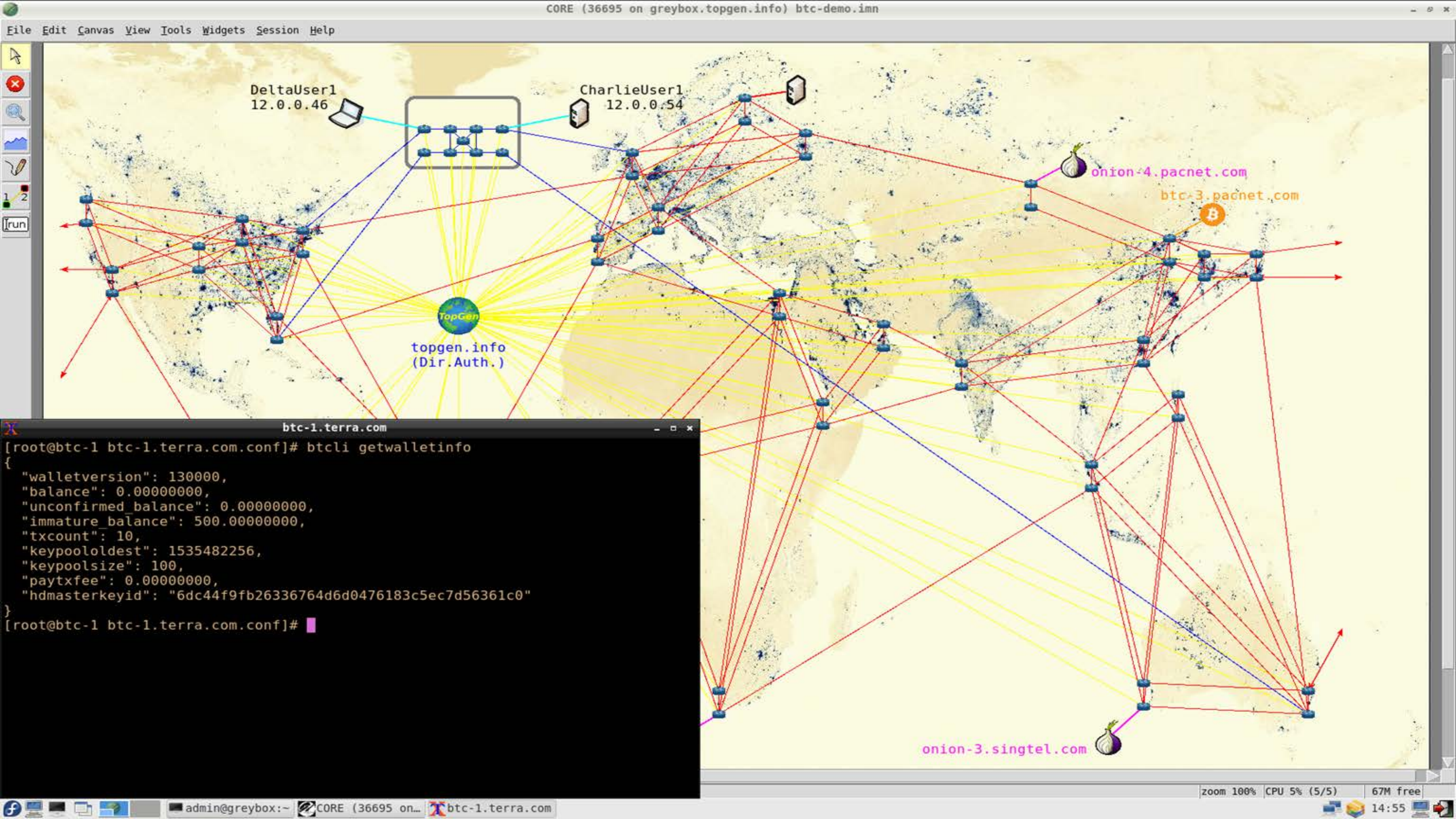

1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP
12PaHiRJBmvJYmTpZ32Pswf8eYbKcAE131 0.4983 BTC
1GpqR4vsdvEfgtNyiUrDrfDLTBJvnsentX 0.1495 BTC
1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP 5.01651602 BTC
5.66431602 BTC
Estimated Transaction Volume 1,818.68925455 BTC
Next Block(s)
Number Of Transactions 1915
Height
Timestamp
Received Time 2018-02-14 15:16:59
Nonce 1,858,980,081
Bits
Size 1132.416 kB
Difficulty 2,874,674,234,415.94
Block Reward 12.5 BTC
Hash 0000000000000000002c4b94355945eea353bc720c58a73c2b8593f489550cb3
Previous Block 0000000000000000001d620a2e3ad126ec5038bf42343c419eb6fcdf7240a471
12.9893378 BTC
Block Reward 12.5 BTC

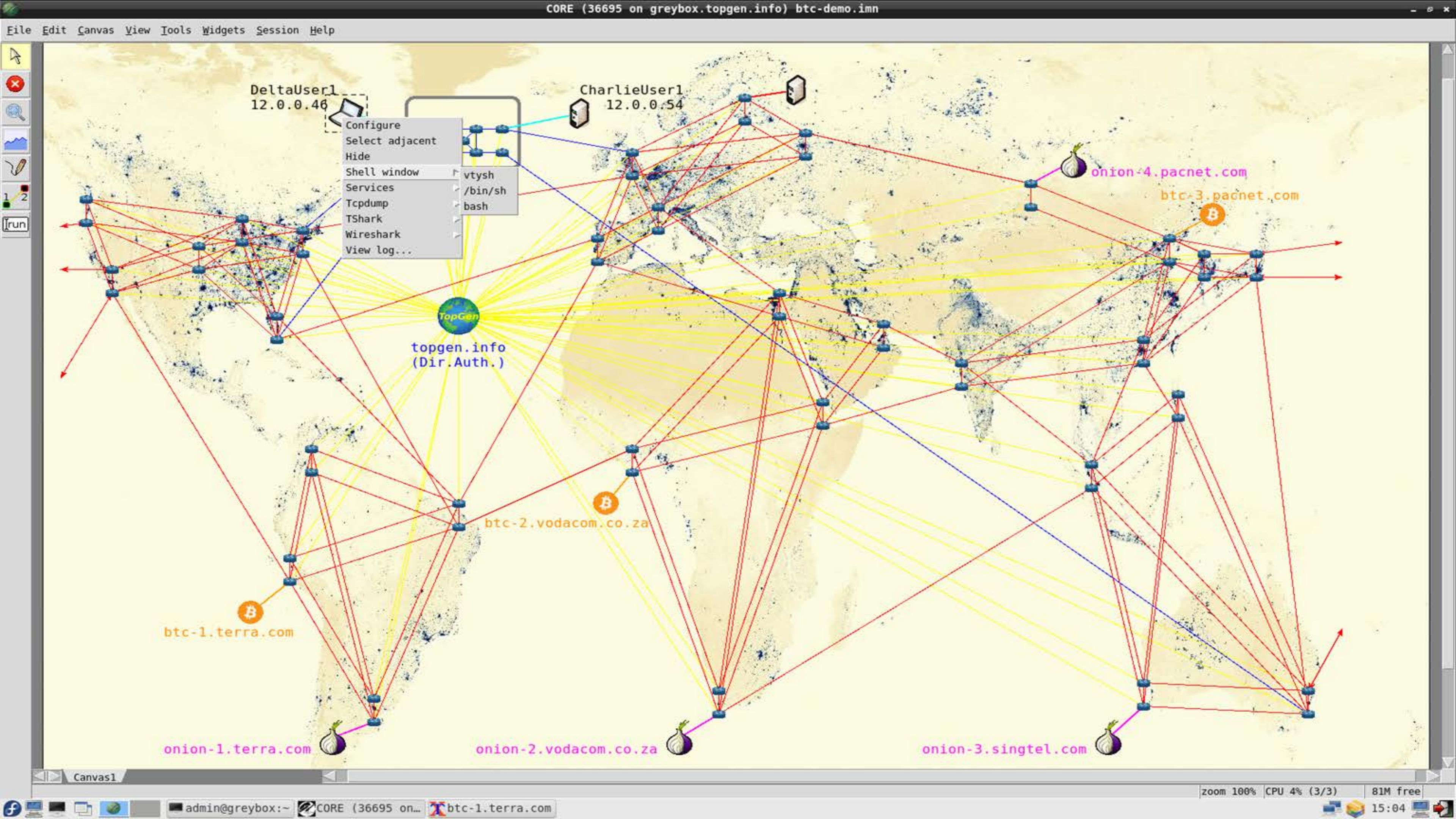

CORE (36695 on greybox.topgen.info) btc-demo.imn
File
Edit
Canvas
View
Tools
Widgets
Session
Help
run
DeltaUser1
12.0.0.46
CharlieUser1
12.0.0.54
onion-4.pacnet.com
btc-3.pacnet.com
topgen.info
(Dir.Auth.)
btc-2.vodacom.co.za
btc-1.terra.com
onion-1.terra.com
onion-2.vodacom.co.za
onion-3.singtel.com
Canvas1
zoom 100%
CPU 12% (9/14)
81M free
admin@greybox:~
CORE (36695 on…
14:51

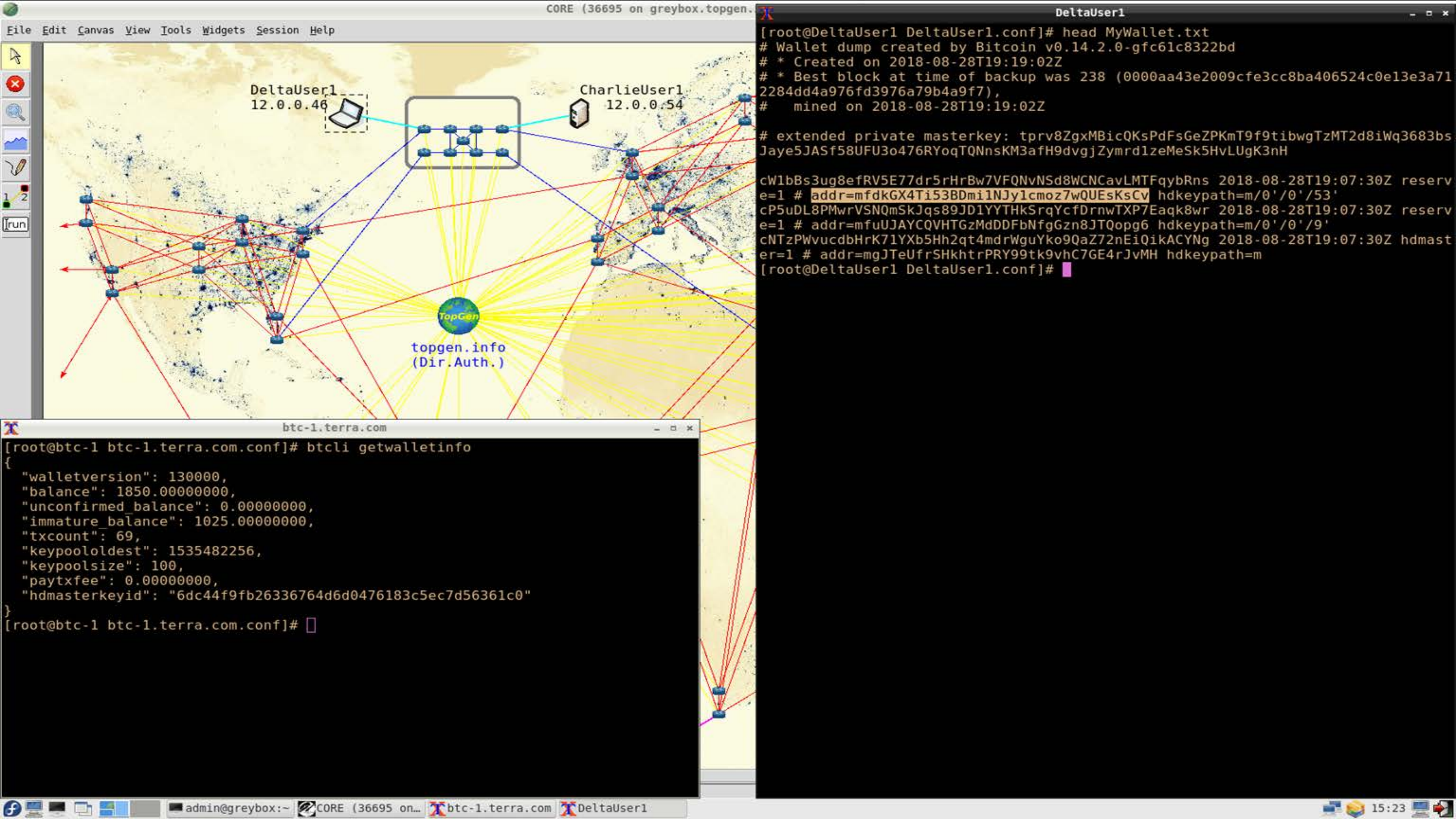


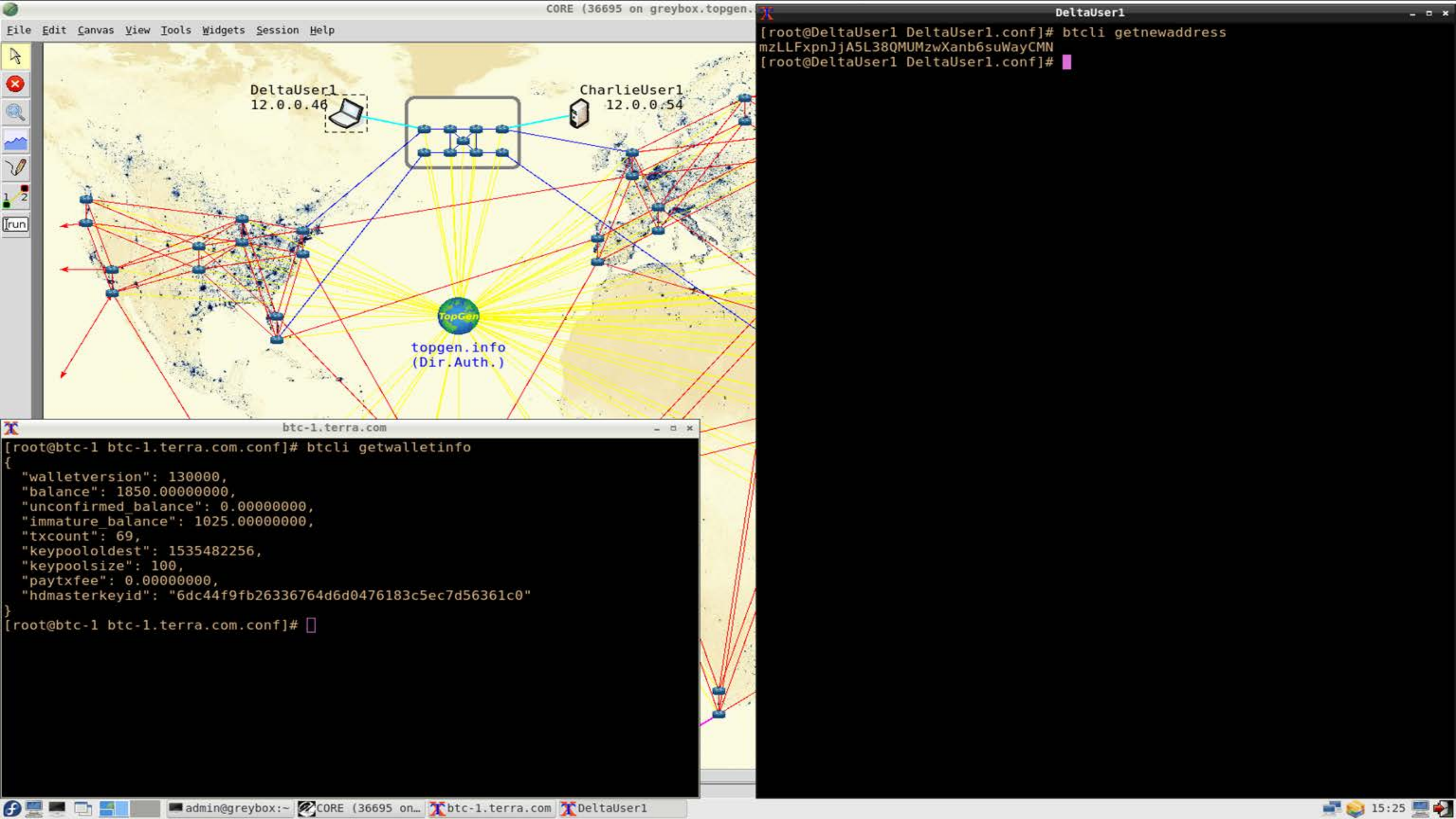
CORE (36695 on greybox.topgen.info) btc-demo.imn
File Edit Canvas View Tools Widgets Session Help
DeltaUser1
12.0.0.46
CharlieUser1
12.0.0.54
onion-4.pacnet.com
btc-3.pacnet.com
topgen.info
(Dir.Auth.)
btc-2.vodacom.co.za
btc-1.terr
Configure
Select adjacent
Hide
Shell window
vtysh
/bin/sh
bash
Services
Tcpdump
TShark
Wireshark
View log...
onion-1.te
onion-2.vodacom.co.za
onion-3.singtel.com
Canvas1
zoom 100%
CPU 4% (4/5)
80M free
admin@greybox:~
CORE (36695 on...
14:52

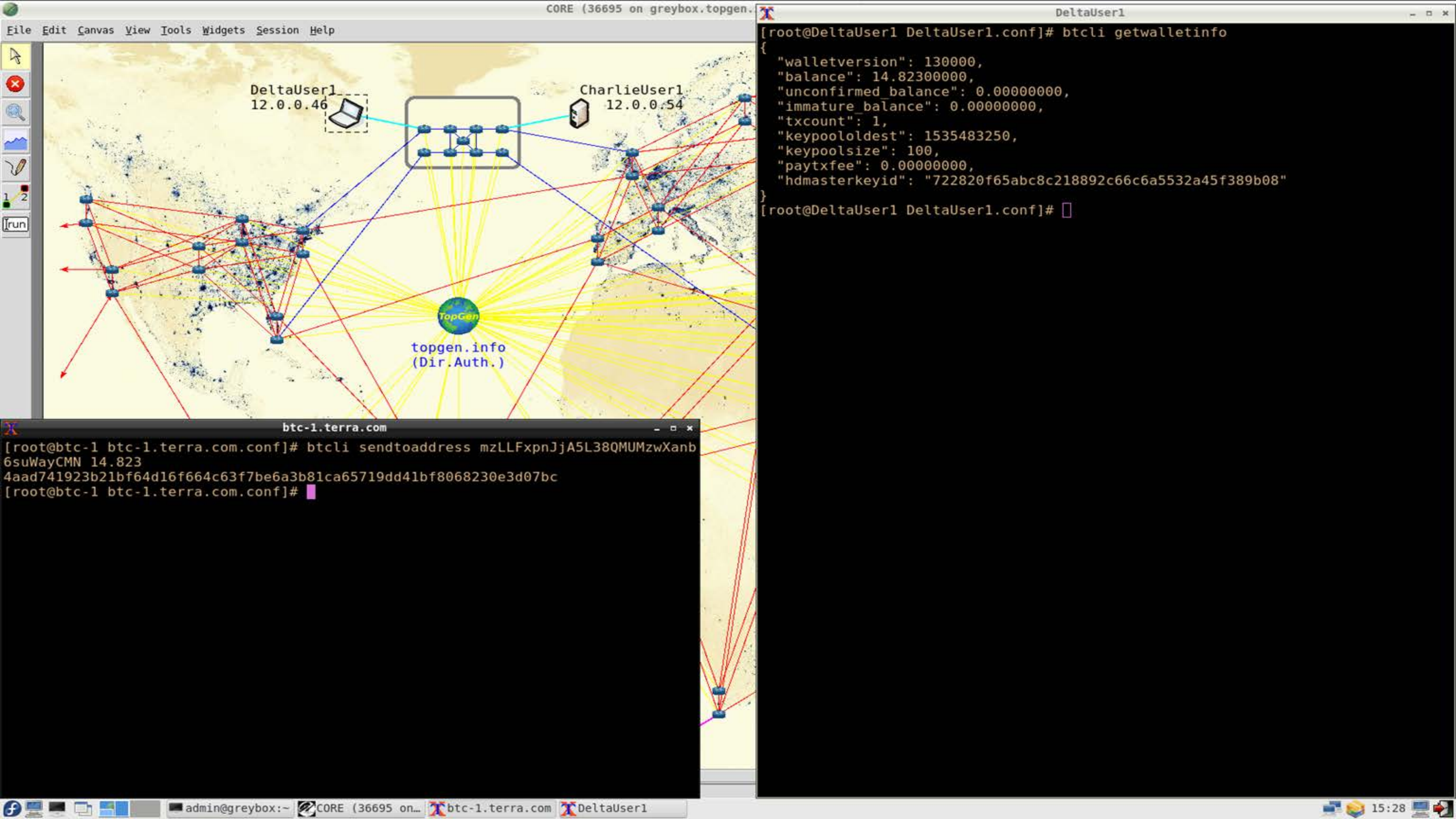

CORE (36695 on greybox.topgen.info) btc-demo.imn
File Edit Canvas View Tools Widgets Session Help
run
DeltaUser1
12.0.0.46
CharlieUser1
12.0.0.54
onion-4.pacnet.com
btc-3.pacnet.com
topgen.info
(Dir.Auth.)
onion-3.singtel.com
btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btcli getinfo
{
"version": 140200,
"protocolversion": 70015,
"walletversion": 130000,
"balance": 0.00000000,
"blocks": 11,
"timeoffset": 0,
"connections": 1,
"proxy": "",
"difficulty": 4.656542373906925e-10,
"testnet": false,
"keypoololdest": 1535482256,
"keypoolsize": 100,
"paytxfee": 0.00000000,
"relayfee": 0.00001000,
"errors": ""
}
[root@btc-1 btc-1.terra.com.conf]#
zoom 100%
CPU 5% (6/5)
67M free
admin@greybox:~
CORE (36695 on...
btc-1.terra.com
14:54


CORE (36695 on greybox.topgen.info) btc-demo.imn
File Edit Canvas View Tools Widgets Session Help
DeltaUser1
12.0.0.46
CharlieUser1
12.0.0.54
onion-4.pacnet.com
btc-3.pacnet.com
TopGen
topgen.info
(Dir.Auth.)
onion-3.singtel.com
btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btcli getwalletinfo
{
"walletversion": 130000,
"balance": 0.00000000,
"unconfirmed_balance": 0.00000000,
"immature_balance": 500.00000000,
"txcount": 10,
"keypoololdest": 1535482256,
"keypoolsize": 100,
"paytxfee": 0.00000000,
"hdmasterkeyid": "6dc44f9fb26336764d6d0476183c5ec7d56361c0"
}
[root@btc-1 btc-1.terra.com.conf]#
zoom 100%
CPU 5% (5/5)
67M free
admin@greybox:~
CORE (36695 on...
btc-1.terra.com
14:55

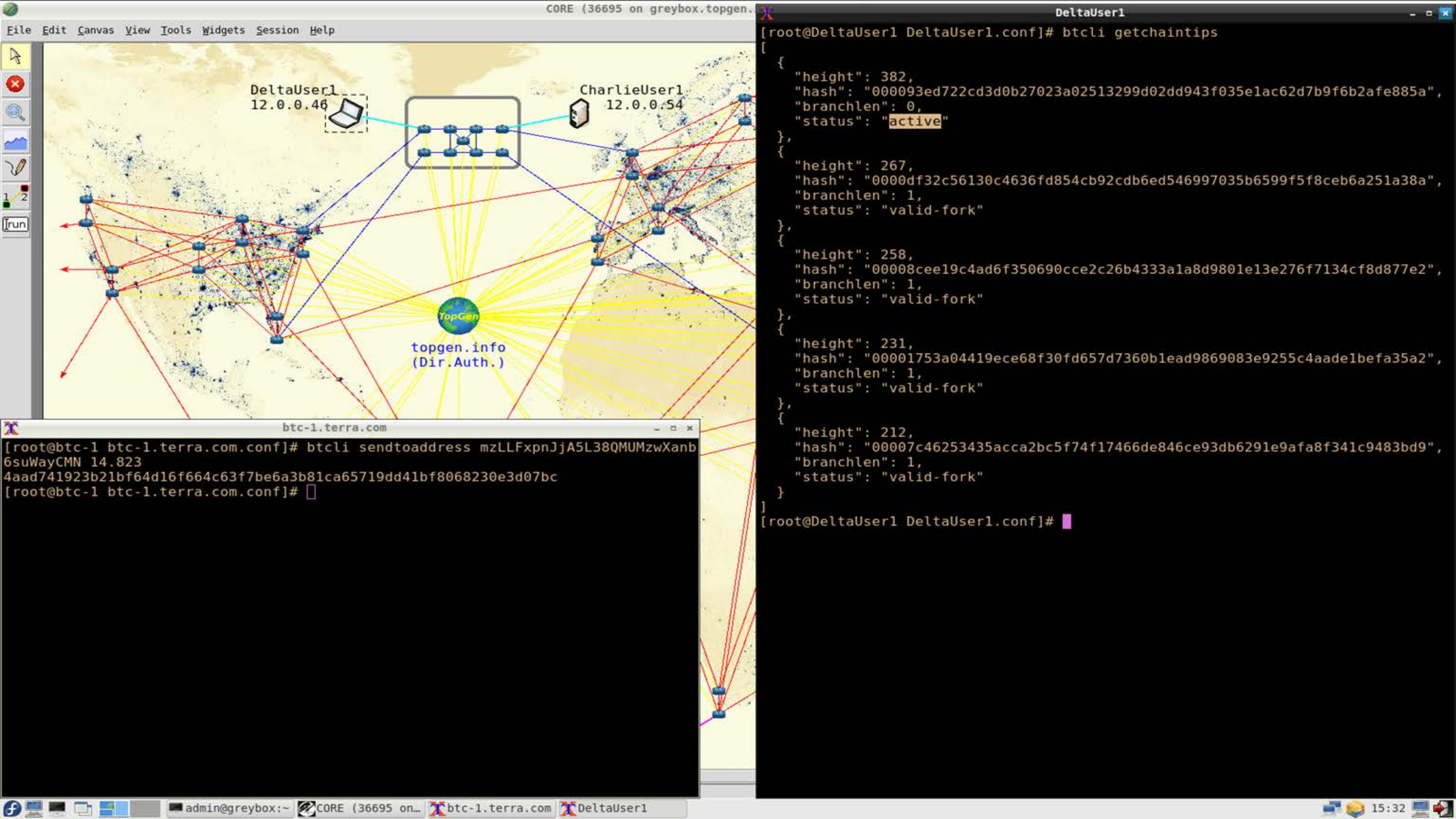

CORE (36695 on greybox.topgen.info) btc-demo.imn
File Edit Canvas View Tools Widgets Session Help
DeltaUser1
12.0.0.46
CharlieUser1
12.0.0.54
Configure
Select adjacent
Hide
Shell window
Services
Tcpdump
TShark
Wireshark
View log...
vtysh
/bin/sh
bash
onion-4.pacnet.com
btc-3.pacnet.com
topgen.info
(Dir.Auth.)
btc-2.vodacom.co.za
btc-1.terra.com
onion-1.terra.com
onion-2.vodacom.co.za
onion-3.singtel.com
Canvas1
zoom 100%
CPU 4% (3/3)
81M free
admin@greybox:~
CORE (36695 on...
btc-1.terra.com
15:04

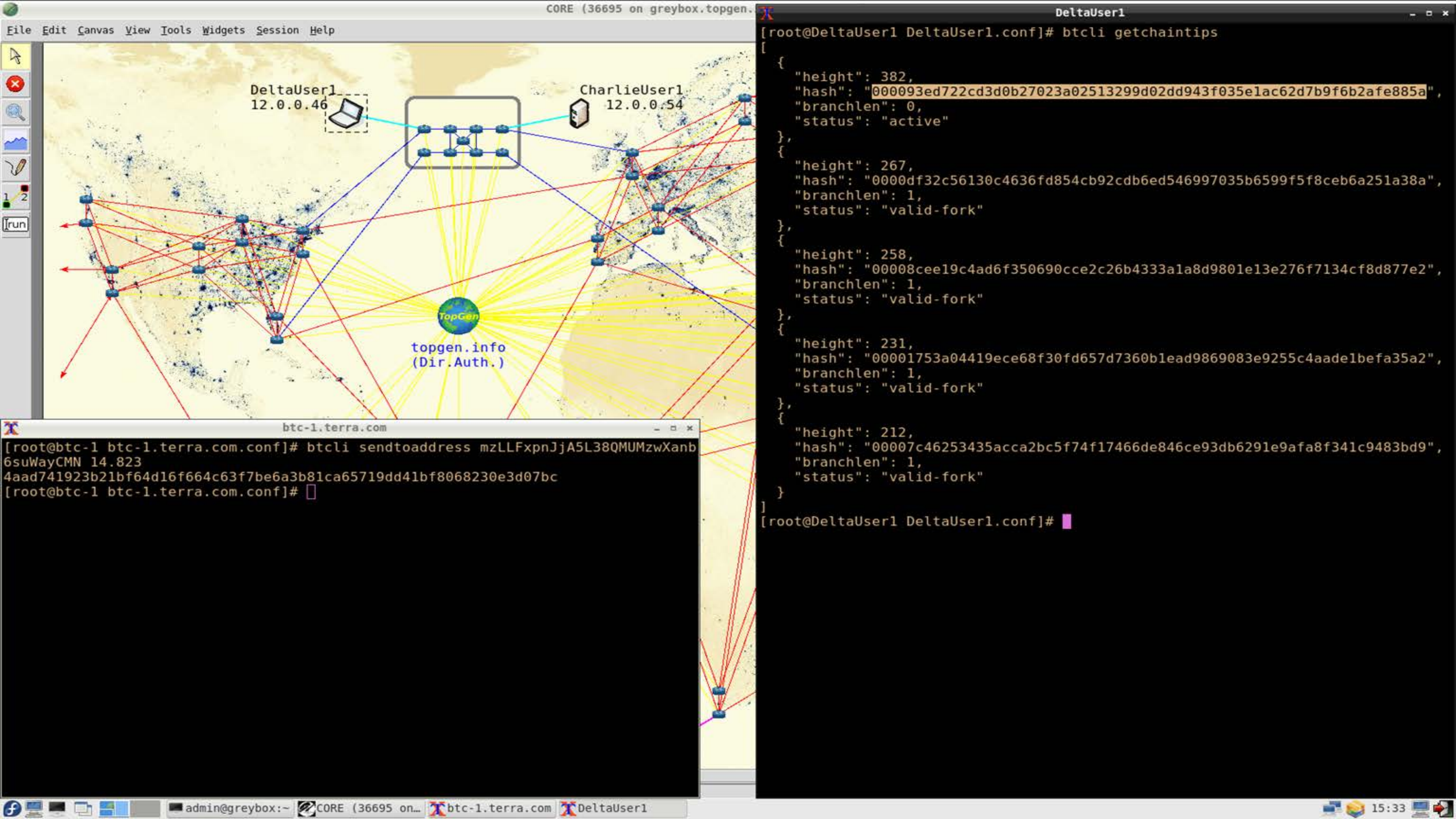

CORE (36695 on greybox.topgen.
File Edit Canvas View Tools Widgets Session Help
DeltaUser1
12.0.0.46
CharlieUser1
12.0.0.54
topgen.info
(Dir.Auth.)
DeltaUser1
[root@DeltaUser1 DeltaUser1.conf]# head MyWallet.txt
Wallet dump created by Bitcoin v0.14.2.0-gfc61c8322bd
* Created on 2018-08-28T19:19:02Z
* Best block at time of backup was 238 (0000aa43e2009cfe3cc8ba406524c0e13e3a712284dd4a976fd3976a79b4a9f7),
mined on 2018-08-28T19:19:02Z
extended private masterkey: tprv8ZgxMBicQKsPdFsGeZPKmT9f9tibwgTzMT2d8iWq3683bsJaye5JASf58UFU3o476RYoqTQNnsKM3afH9dvgjZymrd1zeMeSk5HvLUgK3nH
cW1bBs3ug8efRV5E77dr5rHrBw7VFQNvNSd8WCNCavLMTFqybRns 2018-08-28T19:07:30Z reserve=1 # addr=mfdkGX4Ti53BDmi1NJy1cmoz7wQUEsKsCv hdkeypath=m/0'/0'/53'
cP5uDL8PMwrVSNQmSkJqss89JD1YYTHkSrqYcfDrnwTXP7Eaqk8wr 2018-08-28T19:07:30Z reserve=1 # addr=mfuUJAYCQVHTGzMdDDFbNfgGzn8JTQopg6 hdkeypath=m/0'/0'/9'
cNTzPWvucdbHrK71YXb5Hh2qt4mdrWguYko9QaZ72nEiQikACYNg 2018-08-28T19:07:30Z hdmaster=1 # addr=mgJTeUfrSHkhtrPRY99tk9vhC7GE4rJvMH hdkeypath=m
[root@DeltaUser1 DeltaUser1.conf]#
btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btcli getwalletinfo
{
"walletversion": 130000,
"balance": 1850.00000000,
"unconfirmed_balance": 0.00000000,
"immature_balance": 1025.00000000,
"txcount": 69,
"keypoololdest": 1535482256,
"keypoolsize": 100,
"paytxfee": 0.00000000,
"hdmasterkeyid": "6dc44f9fb26336764d6d0476183c5ec7d56361c0"
}
[root@btc-1 btc-1.terra.com.conf]#
admin@greybox:~
CORE (36695 on...
btc-1.terra.com
DeltaUser1
15:23

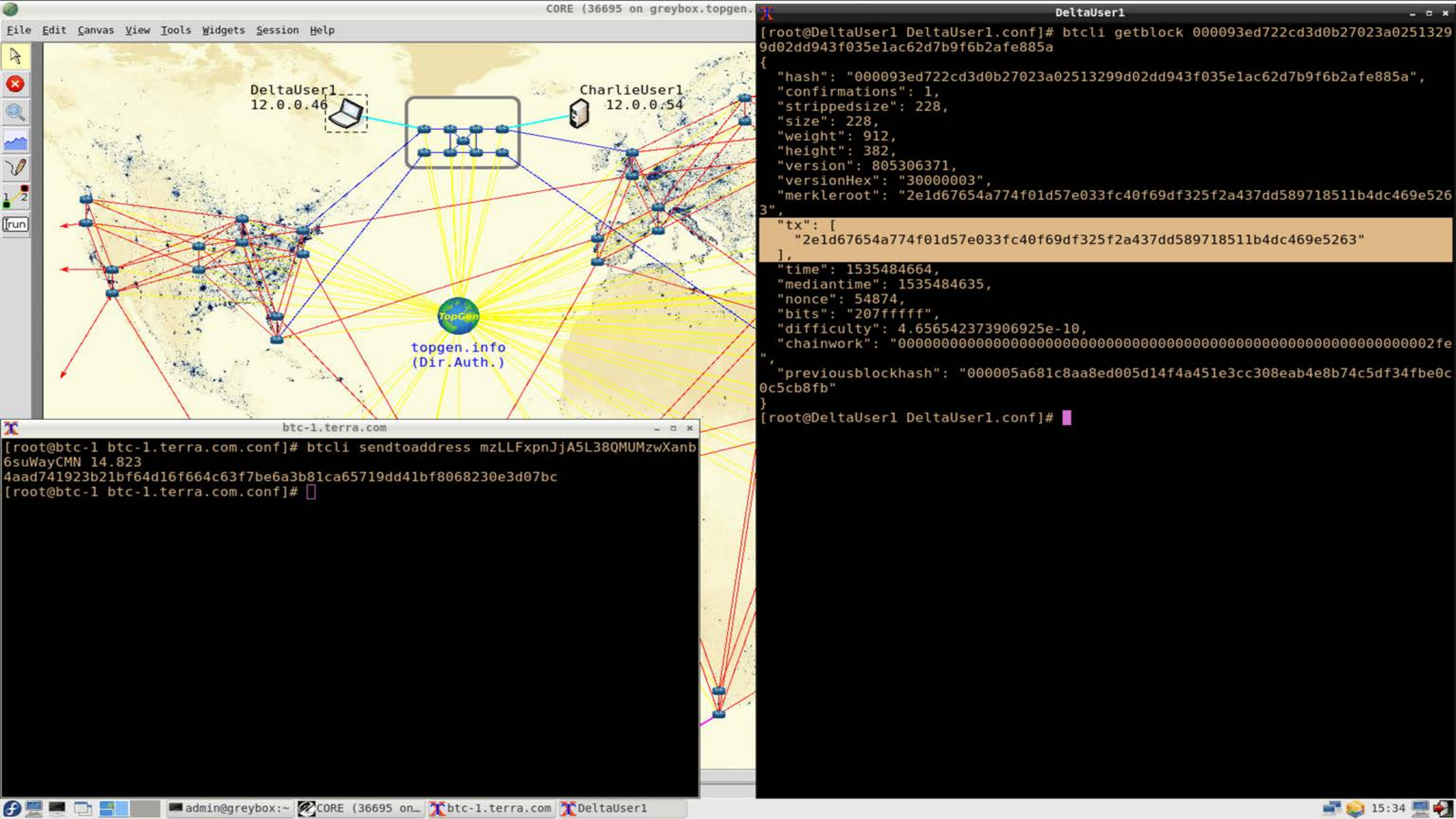

CORE (36695 on greybox.topgen.
File Edit Canvas View Tools Widgets Session Help
DeltaUser1
12.0.0.46
CharlieUser1
12.0.0.54
topgen.info
(Dir.Auth.)
DeltaUser1
[root@DeltaUser1 DeltaUser1.conf]# btcli getnewaddress
mzLLFxpnJjA5L38QMUMzwXanb6suWayCMN
[root@DeltaUser1 DeltaUser1.conf]#
btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btcli getwalletinfo
{
"walletversion": 130000,
"balance": 1850.00000000,
"unconfirmed_balance": 0.00000000,
"immature_balance": 1025.00000000,
"txcount": 69,
"keypoololdest": 1535482256,
"keypoolsize": 100,
"paytxfee": 0.00000000,
"hdmasterkeyid": "6dc44f9fb26336764d6d0476183c5ec7d56361c0"
}
[root@btc-1 btc-1.terra.com.conf]#
admin@greybox:~
CORE (36695 on...
btc-1.terra.com
DeltaUser1
15:25



CORE (36695 on greybox.topgen.
File Edit Canvas View Tools Widgets Session Help
DeltaUser1
12.0.0.46
CharlieUser1
12.0.0.54
topgen.info
(Dir.Auth.)
DeltaUser1
[root@DeltaUser1 DeltaUser1.conf]# btcli getwalletinfo
{
"walletversion": 130000,
"balance": 14.82300000,
"unconfirmed_balance": 0.00000000,
"immature_balance": 0.00000000,
"txcount": 1,
"keypoololdest": 1535483250,
"keypoolsize": 100,
"paytxfee": 0.00000000,
"hdmasterkeyid": "722820f65abc8c218892c66c6a5532a45f389b08"
}
[root@DeltaUser1 DeltaUser1.conf]#
btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btcli sendtoaddress mzLLFxpnJjA5L38QMUMzwXanb
6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#
admin@greybox:~
CORE (36695 on...
btc-1.terra.com
DeltaUser1
15:28

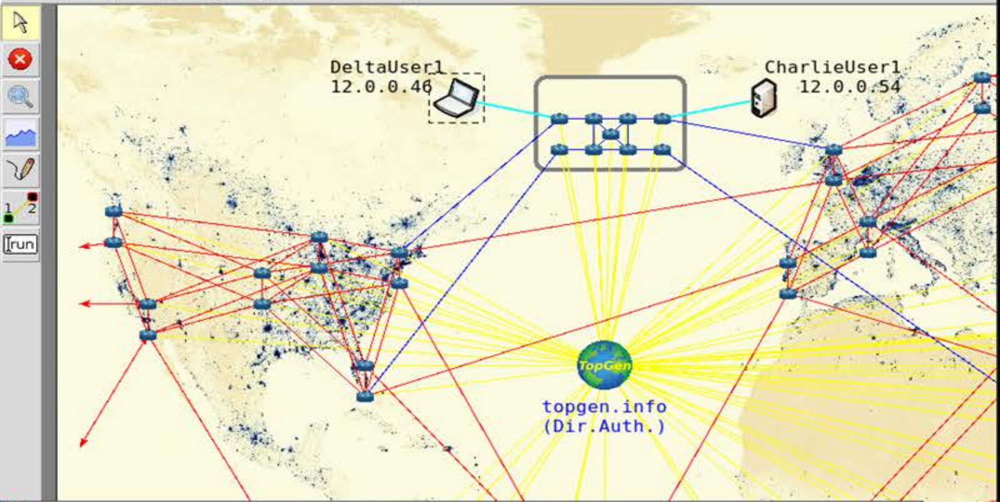

CORE (36695 on greybox.topgen.
File Edit Canvas View Tools Widgets Session Help
DeltaUser1
12.0.0.46
CharlieUser1
12.0.0.54
topgen.info
(Dir.Auth.)
TopGen
run
btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btcli sendtoaddress mzLLFxpnJjA5L38QMUMzwXanb
6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#
DeltaUser1
[root@DeltaUser1 DeltaUser1.conf]# btcli getchaintips
[
{
"height": 382,
"hash": "000093ed722cd3d0b27023a02513299d02dd943f035e1ac62d7b9f6b2afe885a",
"branchlen": 0,
"status": "active"
},
{
"height": 267,
"hash": "0000df32c56130c4636fd854cb92cdb6ed546997035b6599f5f8ceb6a251a38a",
"branchlen": 1,
"status": "valid-fork"
},
{
"height": 258,
"hash": "00008cee19c4ad6f350690cce2c26b4333a1a8d9801e13e276f7134cf8d877e2",
"branchlen": 1,
"status": "valid-fork"
},
{
"height": 231,
"hash": "00001753a04419ece68f30fd657d7360b1ead9869083e9255c4aade1befa35a2",
"branchlen": 1,
"status": "valid-fork"
},
{
"height": 212,
"hash": "00007c46253435acca2bc5f74f17466de846ce93db6291e9afa8f341c9483bd9",
"branchlen": 1,
"status": "valid-fork"
}
]
[root@DeltaUser1 DeltaUser1.conf]#
admin@greybox:~
CORE (36695 on...
btc-1.terra.com
DeltaUser1
15:32


CORE (36695 on greybox.topgen.
File Edit Canvas View Tools Widgets Session Help
DeltaUser1
12.0.0.46
CharlieUser1
12.0.0.54
topgen.info
(Dir.Auth.)
btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btcli sendtoaddress mzLLFxpnJjA5L38QMUMzwXanb6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#
DeltaUser1
[root@DeltaUser1 DeltaUser1.conf]# btcli getchaintips
[
{
"height": 382,
"hash": "000093ed722cd3d0b27023a02513299d02dd943f035e1ac62d7b9f6b2afe885a",
"branchlen": 0,
"status": "active"
},
{
"height": 267,
"hash": "0000df32c56130c4636fd854cb92cdb6ed546997035b6599f5f8ceb6a251a38a",
"branchlen": 1,
"status": "valid-fork"
},
{
"height": 258,
"hash": "00008cee19c4ad6f350690cce2c26b4333a1a8d9801e13e276f7134cf8d877e2",
"branchlen": 1,
"status": "valid-fork"
},
{
"height": 231,
"hash": "00001753a04419ece68f30fd657d7360b1ead9869083e9255c4aade1befa35a2",
"branchlen": 1,
"status": "valid-fork"
},
{
"height": 212,
"hash": "00007c46253435acca2bc5f74f17466de846ce93db6291e9afa8f341c9483bd9",
"branchlen": 1,
"status": "valid-fork"
}
]
[root@DeltaUser1 DeltaUser1.conf]#
admin@greybox:~
CORE (36695 on...
btc-1.terra.com
DeltaUser1
15:33


CORE (36695 on greybox.topgen.
File Edit Canvas View Tools Widgets Session Help
run
DeltaUser1
12.0.0.46
CharlieUser1
12.0.0.54
topgen.info
(Dir.Auth.)
TopGen
btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btcli sendtoaddress mzLLFxpnJjA5L38QMUMzwXanb
6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#
DeltaUser1
[root@DeltaUser1 DeltaUser1.conf]# btcli getblock 000093ed722cd3d0b27023a0251329
9d02dd943f035e1ac62d7b9f6b2afe885a
{
"hash": "000093ed722cd3d0b27023a02513299d02dd943f035e1ac62d7b9f6b2afe885a",
"confirmations": 1,
"strippedsize": 228,
"size": 228,
"weight": 912,
"height": 382,
"version": 805306371,
"versionHex": "30000003",
"merkleroot": "2e1d67654a774f01d57e033fc40f69df325f2a437dd589718511b4dc469e526
3",
"tx": [
"2e1d67654a774f01d57e033fc40f69df325f2a437dd589718511b4dc469e5263"
],
"time": 1535484664,
"mediantime": 1535484635,
"nonce": 54874,
"bits": "207fffff",
"difficulty": 4.656542373906925e-10,
"chainwork": "00000000000000000000000000000000000000000000000000000000000002fe
",
"previousblockhash": "000005a681c8aa8ed005d14f4a451e3cc308eab4e8b74c5df34fbe0c
0c5cb8fb"
}
[root@DeltaUser1 DeltaUser1.conf]#
admin@greybox:~
CORE (36695 on...
btc-1.terra.com
DeltaUser1
15:34

CORE (36695 on greybox.topgen.

File Edit Canvas View Tools Widgets Session Help



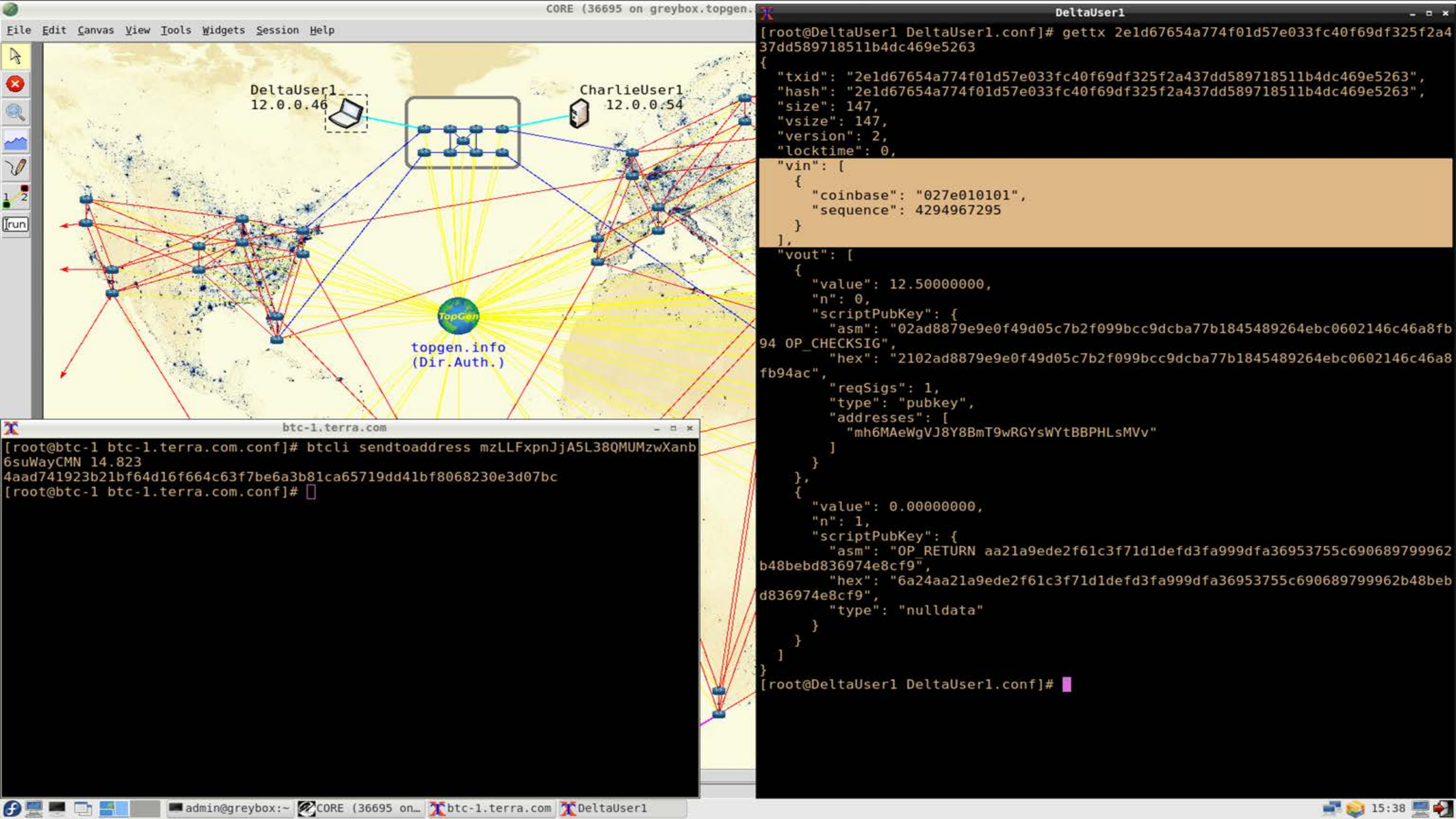
DeltaUser1

```
[root@DeltaUser1 DeltaUser1.conf]# gettx () {
> local TXID=${1}
> btcli decoderawtransaction $(btcli getrawtransaction ${TXID})
> }
[root@DeltaUser1 DeltaUser1.conf]#
```

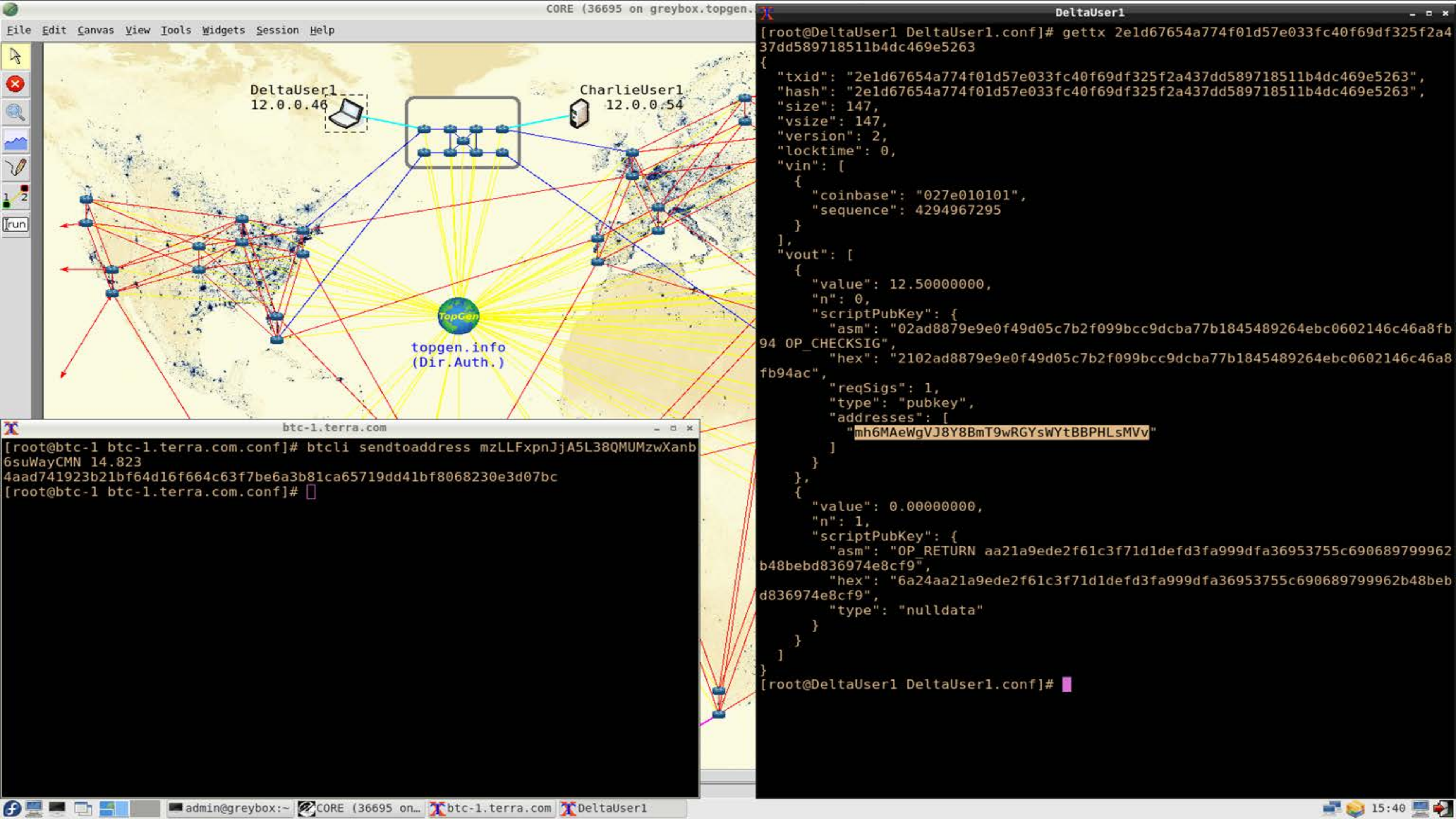
btc-1.terra.com

```
[root@btc-1 btc-1.terra.com.conf]# btcli sendtoaddress mzLLFxpnJjA5L38QMUMzwXanb
6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#
```

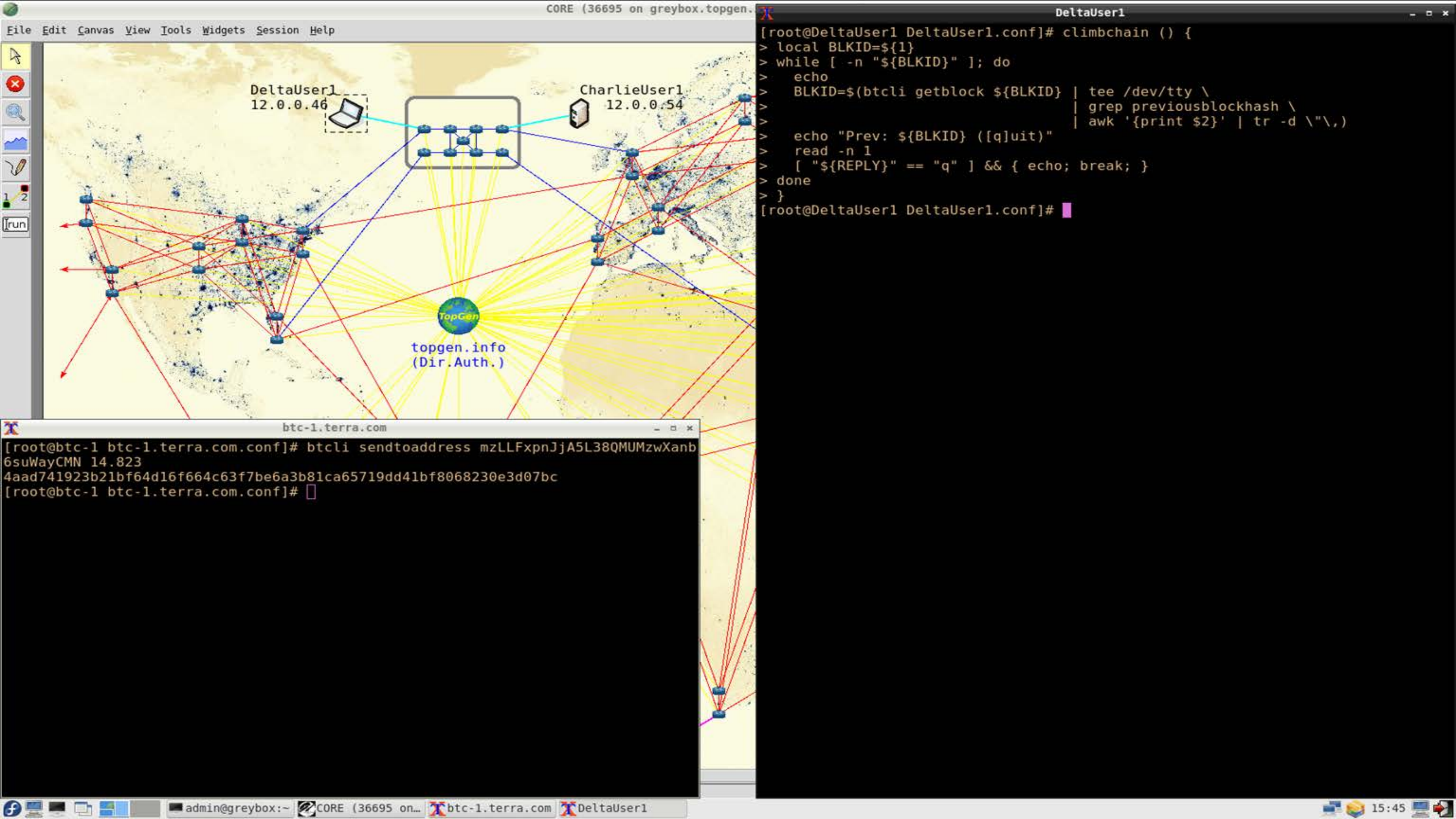
admin@greybox:~ CORE (36695 on... btc-1.terra.com DeltaUser1 15:36

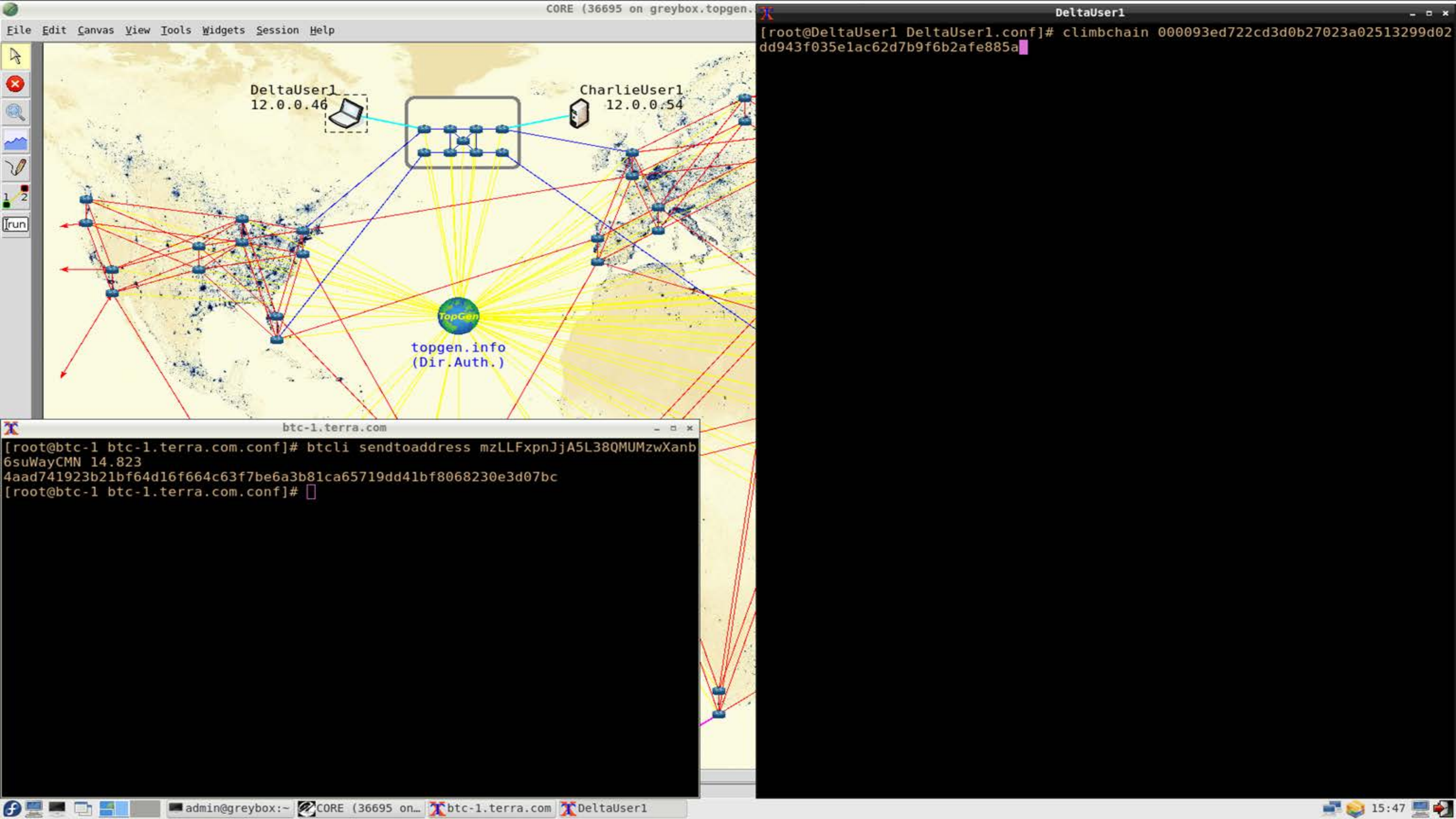


CORE (36695 on greybox.topgen.
File Edit Canvas View Tools Widgets Session Help
DeltaUser1
12.0.0.46
CharlieUser1
12.0.0.54
topgen.info
(Dir.Auth.)
btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btcli sendtoaddress mzLLFxpnJjA5L38QMUMzwXanb
6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#
DeltaUser1
[root@DeltaUser1 DeltaUser1.conf]# gettx 2e1d67654a774f01d57e033fc40f69df325f2a4
37dd589718511b4dc469e5263
{
"txid": "2e1d67654a774f01d57e033fc40f69df325f2a437dd589718511b4dc469e5263",
"hash": "2e1d67654a774f01d57e033fc40f69df325f2a437dd589718511b4dc469e5263",
"size": 147,
"vsize": 147,
"version": 2,
"locktime": 0,
"vin": [
{
"coinbase": "027e010101",
"sequence": 4294967295
}
],
"vout": [
{
"value": 12.50000000,
"n": 0,
"scriptPubKey": {
"asm": "02ad8879e9e0f49d05c7b2f099bcc9dcba77b1845489264ebc0602146c46a8fb
94 OP_CHECKSIG",
"hex": "2102ad8879e9e0f49d05c7b2f099bcc9dcba77b1845489264ebc0602146c46a8
fb94ac",
"reqSigs": 1,
"type": "pubkey",
"addresses": [
"mh6MAeWgVJ8Y8BmT9wRGYsWYtBBPHLsMVv"
]
}
},
{
"value": 0.00000000,
"n": 1,
"scriptPubKey": {
"asm": "OP_RETURN aa21a9ede2f61c3f71d1defd3fa999dfa36953755c690689799962
b48bebd836974e8cf9",
"hex": "6a24aa21a9ede2f61c3f71d1defd3fa999dfa36953755c690689799962b48beb
d836974e8cf9",
"type": "nulldata"
}
}
]
}
[root@DeltaUser1 DeltaUser1.conf]#
admin@greybox:~
CORE (36695 on...
btc-1.terra.com
DeltaUser1
15:38



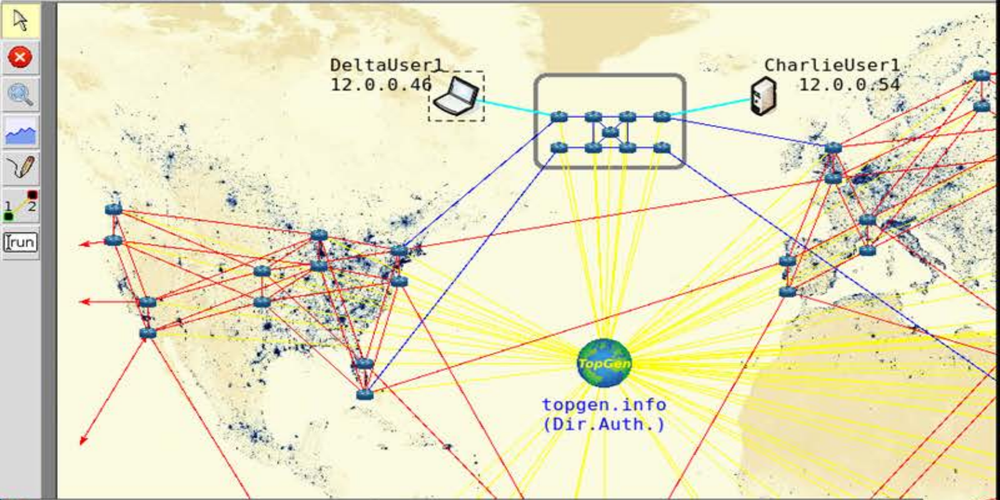
CORE (36695 on greybox.topgen.
File Edit Canvas View Tools Widgets Session Help
run
DeltaUser1
12.0.0.46
CharlieUser1
12.0.0.54
topgen.info
(Dir.Auth.)
btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btcli sendtoaddress mzLLFxpnJjA5L38QMUMzwXanb6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#
DeltaUser1
[root@DeltaUser1 DeltaUser1.conf]# gettx 2e1d67654a774f01d57e033fc40f69df325f2a437dd589718511b4dc469e5263
{
"txid": "2e1d67654a774f01d57e033fc40f69df325f2a437dd589718511b4dc469e5263",
"hash": "2e1d67654a774f01d57e033fc40f69df325f2a437dd589718511b4dc469e5263",
"size": 147,
"vsize": 147,
"version": 2,
"locktime": 0,
"vin": [
{
"coinbase": "027e010101",
"sequence": 4294967295
}
],
"vout": [
{
"value": 12.50000000,
"n": 0,
"scriptPubKey": {
"asm": "02ad8879e9e0f49d05c7b2f099bcc9dcba77b1845489264ebc0602146c46a8fb94 OP_CHECKSIG",
"hex": "2102ad8879e9e0f49d05c7b2f099bcc9dcba77b1845489264ebc0602146c46a8fb94ac",
"reqSigs": 1,
"type": "pubkey",
"addresses": [
"mh6MAeWgVJ8Y8BmT9wRGYsWYtBBPHLsMVv"
]
}
},
{
"value": 0.00000000,
"n": 1,
"scriptPubKey": {
"asm": "OP_RETURN aa21a9ede2f61c3f71d1defd3fa999dfa36953755c690689799962b48bebd836974e8cf9",
"hex": "6a24aa21a9ede2f61c3f71d1defd3fa999dfa36953755c690689799962b48bebd836974e8cf9",
"type": "nulldata"
}
}
]
}
[root@DeltaUser1 DeltaUser1.conf]#
admin@greybox:~
CORE (36695 on...
btc-1.terra.com
DeltaUser1
15:40


CORE (36695 on greybox.topgen.
File Edit Canvas View Tools Widgets Session Help
DeltaUser1
12.0.0.46
CharlieUser1
12.0.0.54
topgen.info
(Dir.Auth.)
DeltaUser1
[root@DeltaUser1 DeltaUser1.conf]# climbchain () {
> local BLKID=${1}
> while [-n "${BLKID}"]; do
>   echo
>   BLKID=$(btcli getblock ${BLKID} | tee /dev/tty \
> | grep previousblockhash \
> | awk '{print $2}' | tr -d \"\,)
>   echo "Prev: ${BLKID} ([q]uit)"
>   read -n 1
>   ["${REPLY}" == "q"] && { echo; break; }
> done
> }
[root@DeltaUser1 DeltaUser1.conf]#
btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btcli sendtoaddress mzLLFxpnJjA5L38QMUMzwXanb
6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#
admin@greybox:~
CORE (36695 on...
btc-1.terra.com
DeltaUser1
15:45


CORE (36695 on greybox.topgen.
File Edit Canvas View Tools Widgets Session Help
DeltaUser1
12.0.0.46
CharlieUser1
12.0.0.54
TopGen
topgen.info
(Dir.Auth.)
DeltaUser1
[root@DeltaUser1 DeltaUser1.conf]# climbchain 000093ed722cd3d0b27023a02513299d02
dd943f035e1ac62d7b9f6b2afe885a
btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btcli sendtoaddress mzLLFxpnJjA5L38QMUMzwXanb
6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#
admin@greybox:~
CORE (36695 on...
btc-1.terra.com
DeltaUser1
15:47

CORE (36695 on greybox.topgen.

File Edit Canvas View Tools Widgets Session Help



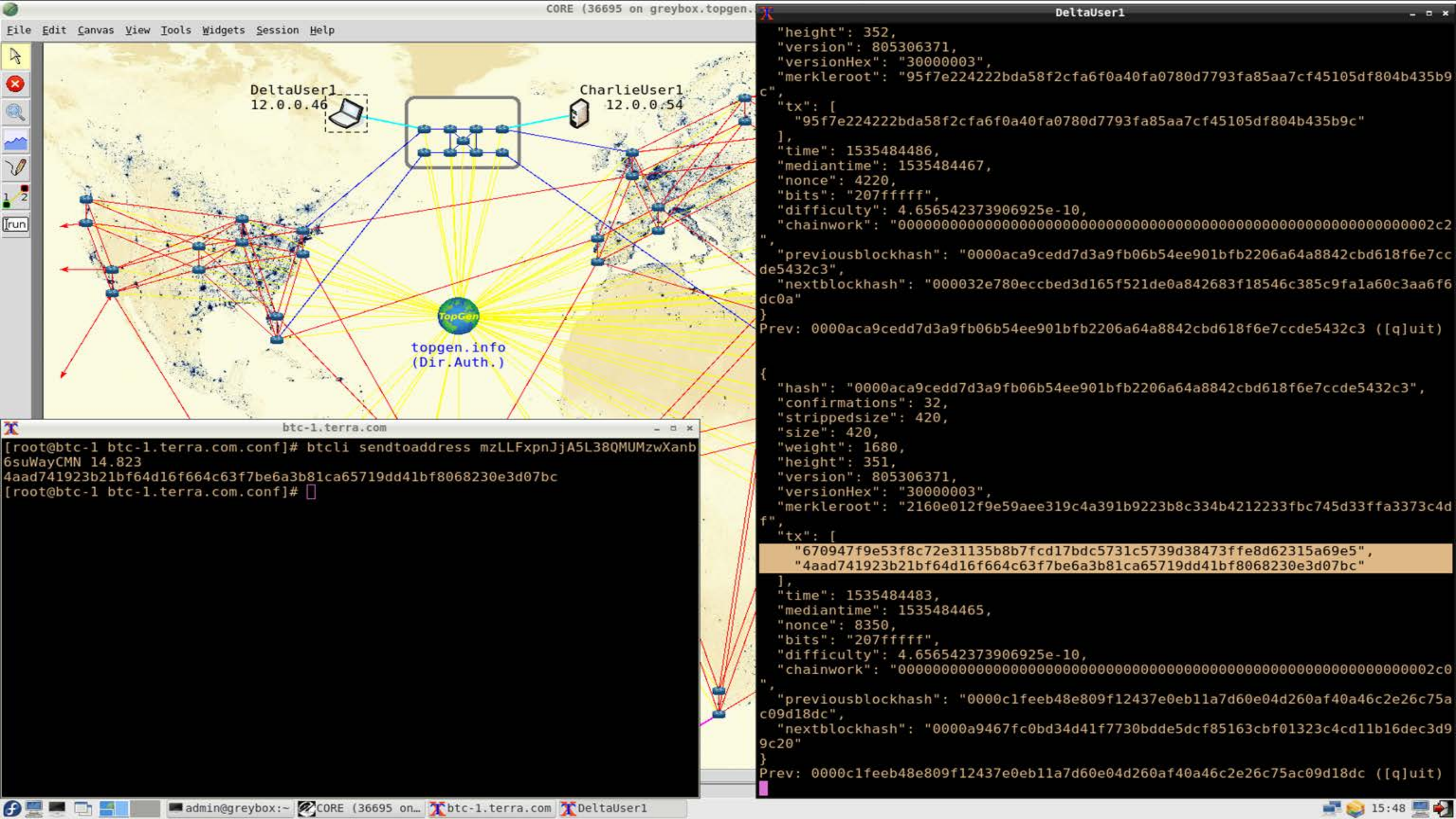
btc-1.terra.com

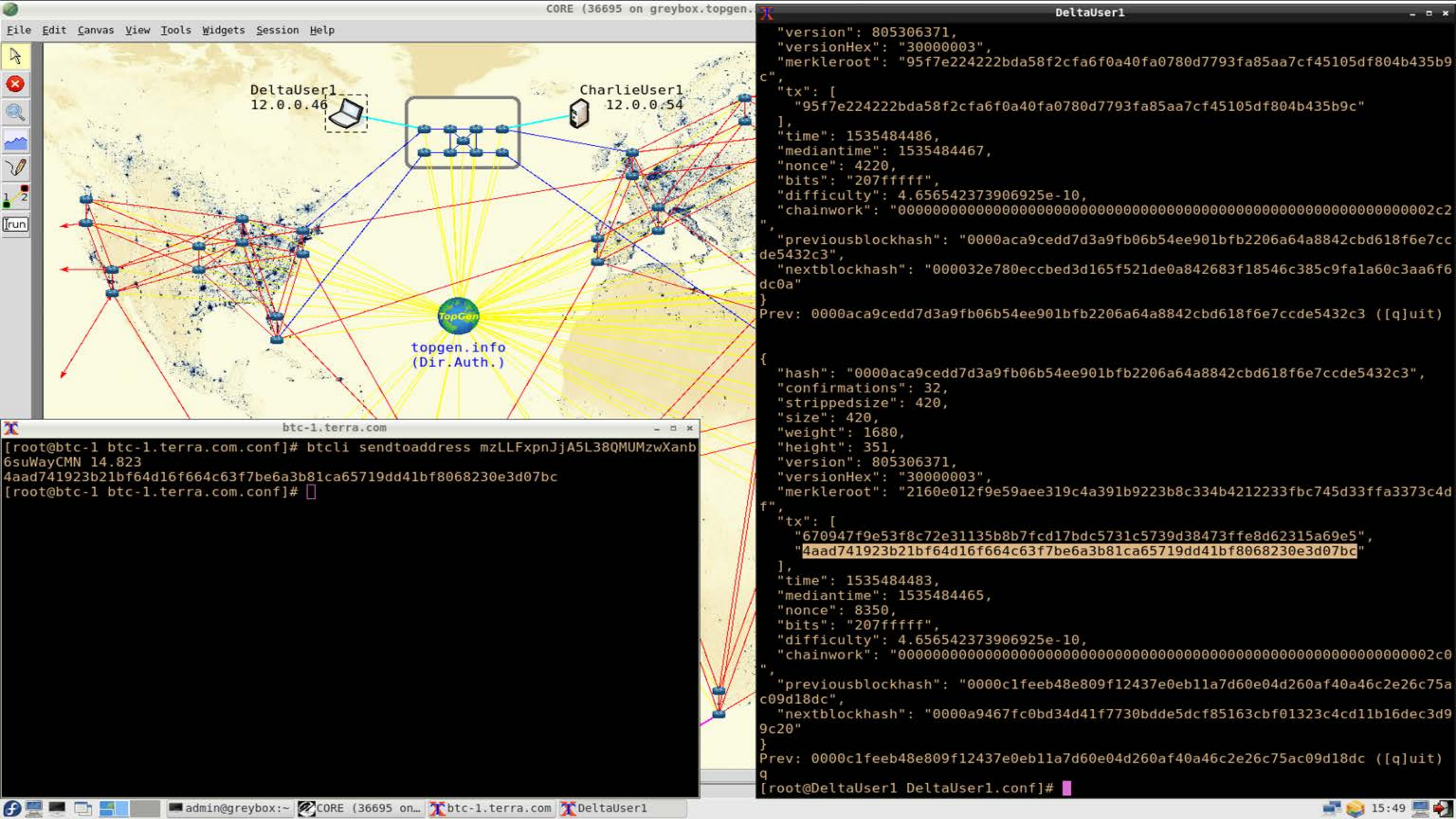
```
[root@btc-1 btc-1.terra.com.conf]# btcli sendtoaddress mzLLFxpnJjA5L38QMUMzwXanb
6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#
```

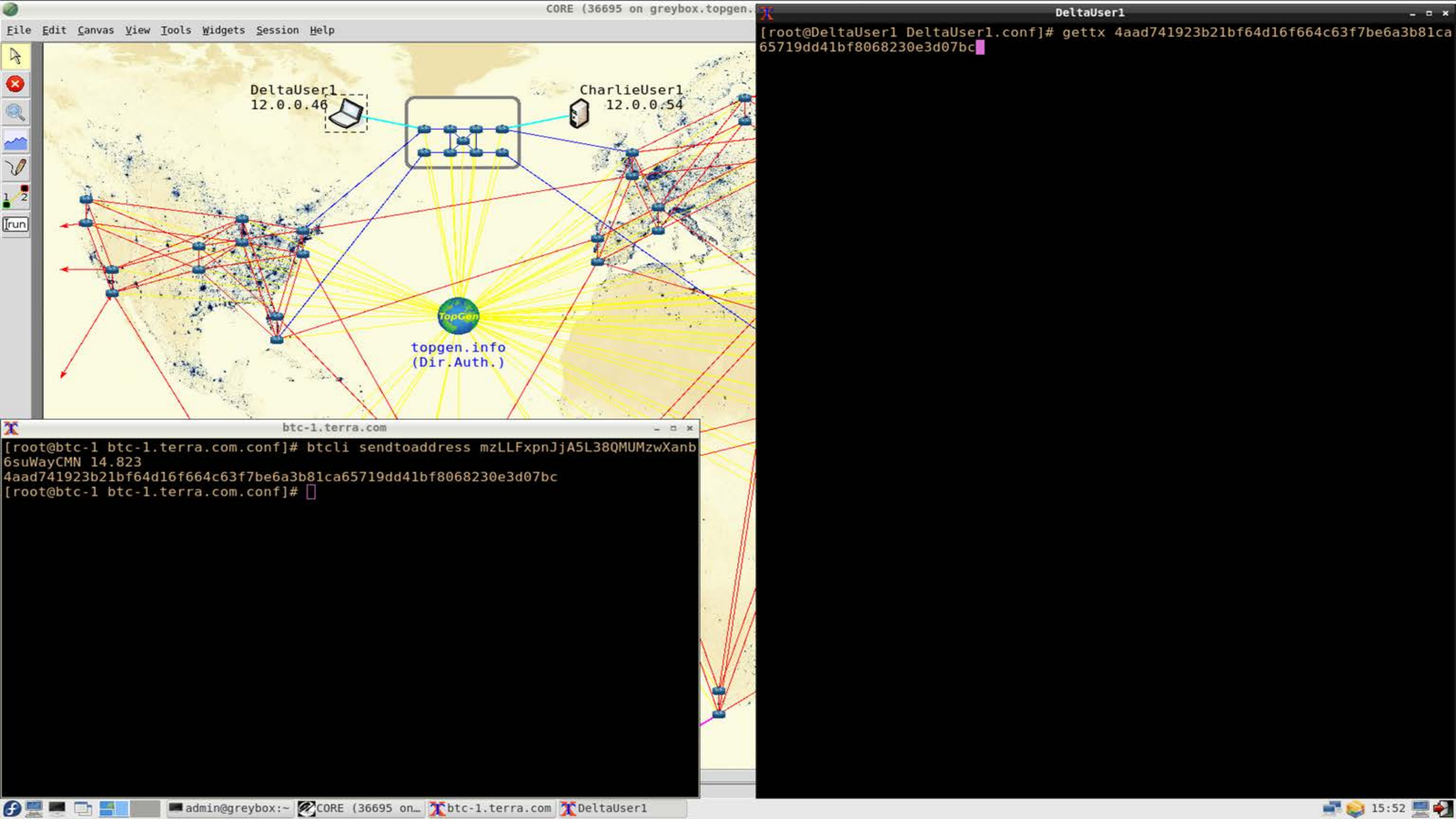
DeltaUser1

```
[root@DeltaUser1 DeltaUser1.conf]# climbchain 000093ed722cd3d0b27023a02513299d02
dd943f035e1ac62d7b9f6b2afe885a

{
  "hash": "000093ed722cd3d0b27023a02513299d02dd943f035e1ac62d7b9f6b2afe885a",
  "confirmations": 1,
  "strippedsize": 228,
  "size": 228,
  "weight": 912,
  "height": 382,
  "version": 805306371,
  "versionHex": "30000003",
  "merkleroot": "2e1d67654a774f01d57e033fc40f69df325f2a437dd589718511b4dc469e526
3",
  "tx": [
    "2e1d67654a774f01d57e033fc40f69df325f2a437dd589718511b4dc469e5263"
  ],
  "time": 1535484664,
  "mediantime": 1535484635,
  "nonce": 54874,
  "bits": "207fffff",
  "difficulty": 4.656542373906925e-10,
  "chainwork": "00000000000000000000000000000000000000000000000000000000000002fe
",
  "previousblockhash": "000005a681c8aa8ed005d14f4a451e3cc308eab4e8b74c5df34fbe0c
0c5cb8fb"
}
Prev: 000005a681c8aa8ed005d14f4a451e3cc308eab4e8b74c5df34fbe0c0c5cb8fb ([q]uit)
```

admin@greybox:~ CORE (36695 on... btc-1.terra.com DeltaUser1 15:47

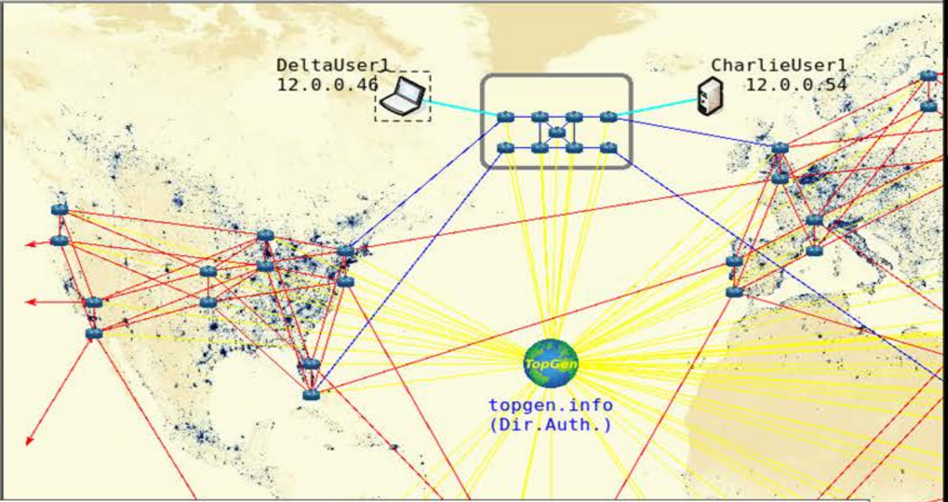

CORE (36695 on greybox.topgen.
File Edit Canvas View Tools Widgets Session Help
DeltaUser1
12.0.0.46
CharlieUser1
12.0.0.54
topgen.info
(Dir.Auth.)
btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btcli sendtoaddress mzLLFxpnJjA5L38QMUMzwXanb6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#
DeltaUser1
"height": 352,
"version": 805306371,
"versionHex": "30000003",
"merkleroot": "95f7e224222bda58f2cfa6f0a40fa0780d7793fa85aa7cf45105df804b435b9c",
"tx": [
"95f7e224222bda58f2cfa6f0a40fa0780d7793fa85aa7cf45105df804b435b9c"
],
"time": 1535484486,
"mediantime": 1535484467,
"nonce": 4220,
"bits": "207fffff",
"difficulty": 4.656542373906925e-10,
"chainwork": "00000000000000000000000000000000000000000000000000000000000002c2",
"previousblockhash": "0000aca9cedd7d3a9fb06b54ee901bfb2206a64a8842cbd618f6e7ccde5432c3",
"nextblockhash": "000032e780eccbed3d165f521de0a842683f18546c385c9fa1a60c3aa6f6dc0a"
}
Prev: 0000aca9cedd7d3a9fb06b54ee901bfb2206a64a8842cbd618f6e7ccde5432c3 ([q]uit)
{
"hash": "0000aca9cedd7d3a9fb06b54ee901bfb2206a64a8842cbd618f6e7ccde5432c3",
"confirmations": 32,
"strippedsize": 420,
"size": 420,
"weight": 1680,
"height": 351,
"version": 805306371,
"versionHex": "30000003",
"merkleroot": "2160e012f9e59aee319c4a391b9223b8c334b4212233fbc745d33ffa3373c4df",
"tx": [
"670947f9e53f8c72e31135b8b7fcd17bdc5731c5739d38473ffe8d62315a69e5",
"4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc"
],
"time": 1535484483,
"mediantime": 1535484465,
"nonce": 8350,
"bits": "207fffff",
"difficulty": 4.656542373906925e-10,
"chainwork": "00000000000000000000000000000000000000000000000000000000000002c0",
"previousblockhash": "0000c1feeb48e809f12437e0eb11a7d60e04d260af40a46c2e26c75ac09d18dc",
"nextblockhash": "0000a9467fc0bd34d41f7730bdde5dcf85163cbf01323c4cd11b16dec3d99c20"
}
Prev: 0000c1feeb48e809f12437e0eb11a7d60e04d260af40a46c2e26c75ac09d18dc ([q]uit)
admin@greybox:~
CORE (36695 on...
btc-1.terra.com
DeltaUser1
15:48


CORE (36695 on greybox.topgen.
File Edit Canvas View Tools Widgets Session Help
DeltaUser1
12.0.0.46
CharlieUser1
12.0.0.54
topgen.info
(Dir.Auth.)
btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btcli sendtoaddress mzLLFxpnJjA5L38QMUMzwXanb6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#
DeltaUser1
"version": 805306371,
"versionHex": "30000003",
"merkleroot": "95f7e224222bda58f2cfa6f0a40fa0780d7793fa85aa7cf45105df804b435b9c",
"tx": [
"95f7e224222bda58f2cfa6f0a40fa0780d7793fa85aa7cf45105df804b435b9c"
],
"time": 1535484486,
"mediantime": 1535484467,
"nonce": 4220,
"bits": "207fffff",
"difficulty": 4.656542373906925e-10,
"chainwork": "00000000000000000000000000000000000000000000000000000000000002c2",
"previousblockhash": "0000aca9cedd7d3a9fb06b54ee901bfb2206a64a8842cbd618f6e7ccde5432c3",
"nextblockhash": "000032e780eccbed3d165f521de0a842683f18546c385c9fa1a60c3aa6f6dc0a"
}
Prev: 0000aca9cedd7d3a9fb06b54ee901bfb2206a64a8842cbd618f6e7ccde5432c3 ([q]uit)
{
"hash": "0000aca9cedd7d3a9fb06b54ee901bfb2206a64a8842cbd618f6e7ccde5432c3",
"confirmations": 32,
"strippedsize": 420,
"size": 420,
"weight": 1680,
"height": 351,
"version": 805306371,
"versionHex": "30000003",
"merkleroot": "2160e012f9e59aee319c4a391b9223b8c334b4212233fbc745d33ffa3373c4df",
"tx": [
"670947f9e53f8c72e31135b8b7fcd17bdc5731c5739d38473ffe8d62315a69e5",
"4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc"
],
"time": 1535484483,
"mediantime": 1535484465,
"nonce": 8350,
"bits": "207fffff",
"difficulty": 4.656542373906925e-10,
"chainwork": "00000000000000000000000000000000000000000000000000000000000002c0",
"previousblockhash": "0000c1feeb48e809f12437e0eb11a7d60e04d260af40a46c2e26c75ac09d18dc",
"nextblockhash": "0000a9467fc0bd34d41f7730bdde5dcf85163cbf01323c4cd11b16dec3d99c20"
}
Prev: 0000c1feeb48e809f12437e0eb11a7d60e04d260af40a46c2e26c75ac09d18dc ([q]uit)
q
[root@DeltaUser1 DeltaUser1.conf]#
admin@greybox:~
CORE (36695 on...
btc-1.terra.com
DeltaUser1
15:49


CORE (36695 on greybox.topgen.
File Edit Canvas View Tools Widgets Session Help
DeltaUser1
12.0.0.46
CharlieUser1
12.0.0.54
topgen.info
(Dir.Auth.)
btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btcli sendtoaddress mzLLFxpnJjA5L38QMUMzwXanb
6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#
DeltaUser1
[root@DeltaUser1 DeltaUser1.conf]# gettx 4aad741923b21bf64d16f664c63f7be6a3b81ca
65719dd41bf8068230e3d07bc
admin@greybox:~
CORE (36695 on...
btc-1.terra.com
DeltaUser1
15:52

CORE (36695 on greybox.topgen.

File Edit Canvas View Tools Widgets Session Help



btc-1.terra.com

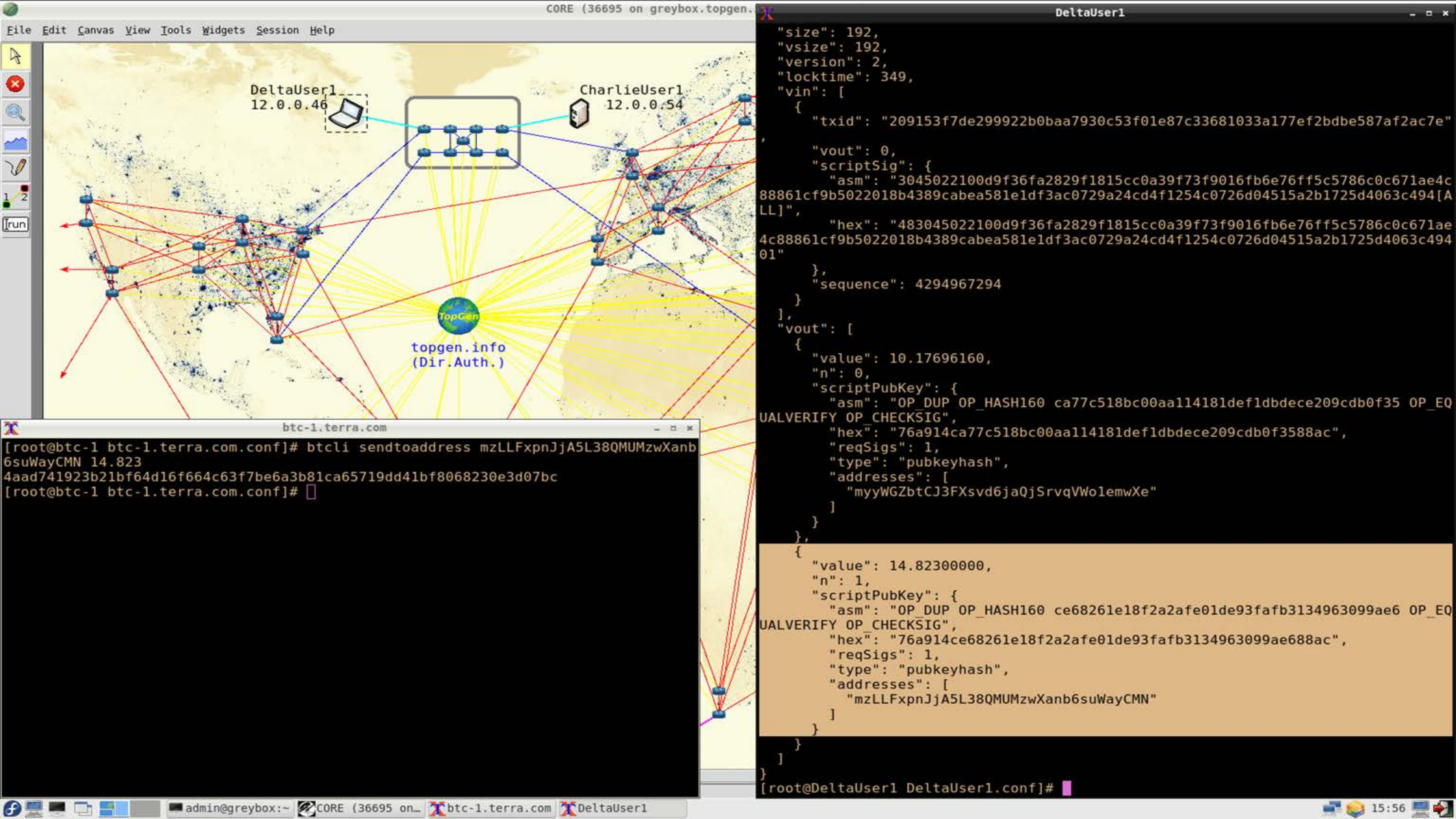
```
[root@btc-1 btc-1.terra.com.conf]# btcli sendtoaddress mzLLFxpnJjA5L38QMUMzwXanb
6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#
```

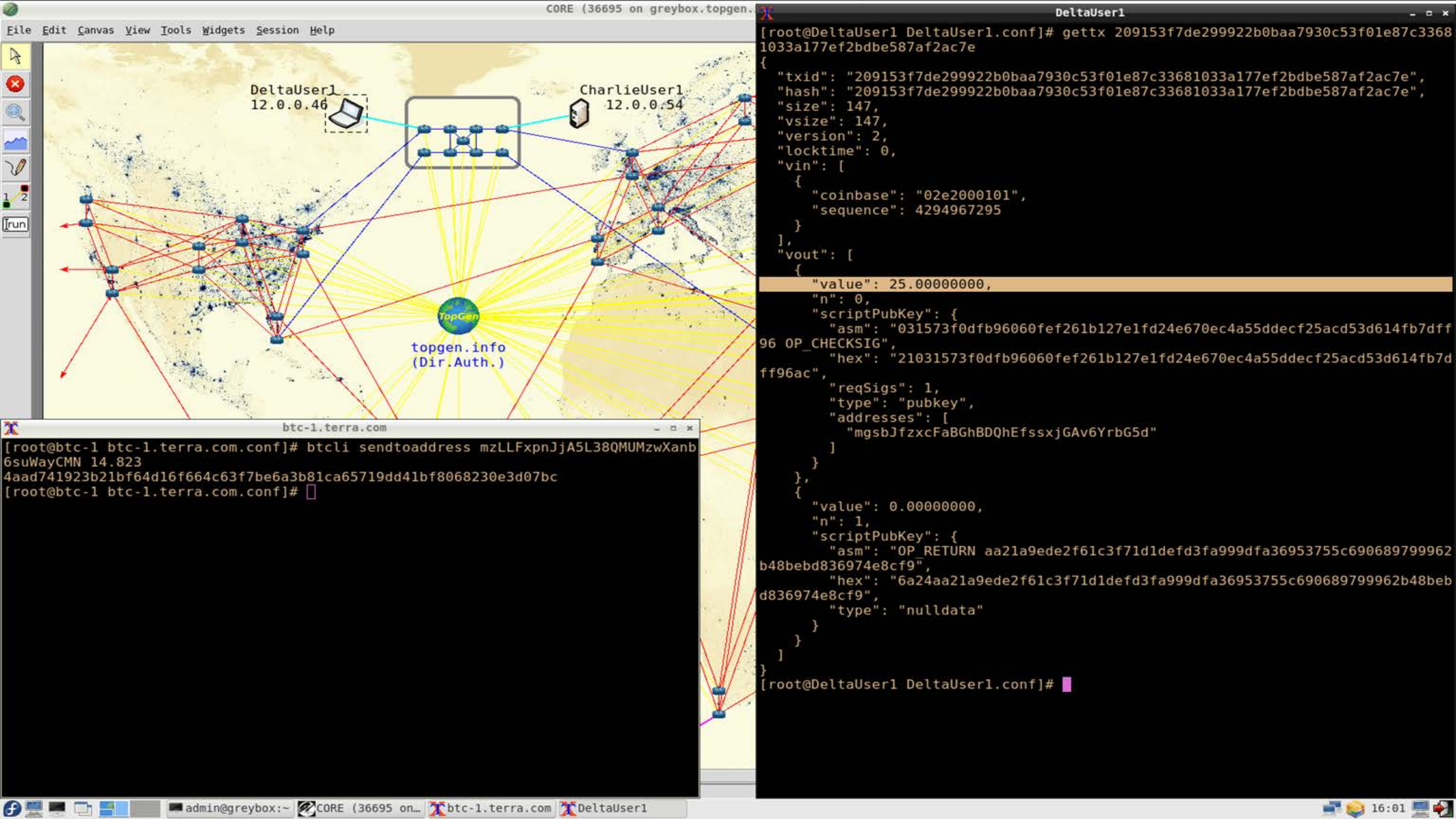
DeltaUser1


```
  "size": 192,
  "vsize": 192,
  "version": 2,
  "locktime": 349,
  "vin": [
    {
      "txid": "209153f7de299922b0baa7930c53f01e87c33681033a177ef2bdbe587af2ac7e"
,
      "vout": 0,
      "scriptSig": {
        "asm": "3045022100d9f36fa2829f1815cc0a39f73f9016fb6e76ff5c5786c0c671ae4c
88861cf9b5022018b4389cabea581e1df3ac0729a24cd4f1254c0726d04515a2b1725d4063c494[A
LL]",
        "hex": "483045022100d9f36fa2829f1815cc0a39f73f9016fb6e76ff5c5786c0c671ae
4c88861cf9b5022018b4389cabea581e1df3ac0729a24cd4f1254c0726d04515a2b1725d4063c494
01"
      },
      "sequence": 4294967294
    }
  ],
  "vout": [
    {
      "value": 10.17696160,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 ca77c518bc00aa114181def1dbdece209cdb0f35 OP_EQ
UALVERIFY OP_CHECKSIG",
        "hex": "76a914ca77c518bc00aa114181def1dbdece209cdb0f3588ac",
        "reqSigs": 1,
        "type": "pubkeyhash",
        "addresses": [
          "myyWGZbtCJ3FXsvd6jaQjSrvqVWolemwXe"
        ]
      }
    },
    {
      "value": 14.82300000,
      "n": 1,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 ce68261e18f2a2afe01de93fafb3134963099ae6 OP_EQ
UALVERIFY OP_CHECKSIG",
        "hex": "76a914ce68261e18f2a2afe01de93fafb3134963099ae688ac",
        "reqSigs": 1,
        "type": "pubkeyhash",
        "addresses": [
          "mzLLFxpnJjA5L38QMUMzwXanb6suWayCMN"
        ]
      }
    }
  ]
}
```


```
[root@DeltaUser1 DeltaUser1.conf]#
```

admin@greybox:~ CORE (36695 on... btc-1.terra.com DeltaUser1 15:54


CORE (36695 on greybox.topgen.
File Edit Canvas View Tools Widgets Session Help
DeltaUser1
12.0.0.46
CharlieUser1
12.0.0.54
topgen.info
(Dir.Auth.)
btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btcli sendtoaddress mzLLFxpnJjA5L38QMUMzwXanb
6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#
DeltaUser1
"size": 192,
"vsize": 192,
"version": 2,
"locktime": 349,
"vin": [
{
"txid": "209153f7de299922b0baa7930c53f01e87c33681033a177ef2bdbe587af2ac7e"
,
"vout": 0,
"scriptSig": {
"asm": "3045022100d9f36fa2829f1815cc0a39f73f9016fb6e76ff5c5786c0c671ae4c
88861cf9b5022018b4389cabea581e1df3ac0729a24cd4f1254c0726d04515a2b1725d4063c494[A
LL]",
"hex": "483045022100d9f36fa2829f1815cc0a39f73f9016fb6e76ff5c5786c0c671ae
4c88861cf9b5022018b4389cabea581e1df3ac0729a24cd4f1254c0726d04515a2b1725d4063c494
01"
},
"sequence": 4294967294
}
],
"vout": [
{
"value": 10.17696160,
"n": 0,
"scriptPubKey": {
"asm": "OP_DUP OP_HASH160 ca77c518bc00aa114181def1dbdece209cdb0f35 OP_EQ
UALVERIFY OP_CHECKSIG",
"hex": "76a914ca77c518bc00aa114181def1dbdece209cdb0f3588ac",
"reqSigs": 1,
"type": "pubkeyhash",
"addresses": [
"myyWGZbtCJ3FXsvd6jaQjSrvqVWo1emwXe"
]
}
},
{
"value": 14.82300000,
"n": 1,
"scriptPubKey": {
"asm": "OP_DUP OP_HASH160 ce68261e18f2a2afe01de93fafb3134963099ae6 OP_EQ
UALVERIFY OP_CHECKSIG",
"hex": "76a914ce68261e18f2a2afe01de93fafb3134963099ae688ac",
"reqSigs": 1,
"type": "pubkeyhash",
"addresses": [
"mzLLFxpnJjA5L38QMUMzwXanb6suWayCMN"
]
}
}
]
}
[root@DeltaUser1 DeltaUser1.conf]#
admin@greybox:~
CORE (36695 on...
btc-1.terra.com
DeltaUser1
15:56


CORE (36695 on greybox.topgen.
File Edit Canvas View Tools Widgets Session Help
DeltaUser1
12.0.0.46
CharlieUser1
12.0.0.54
topgen.info
(Dir.Auth.)
btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btcli sendtoaddress mzLLFxpnJjA5L38QMUMzwXanb
6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#
DeltaUser1
[root@DeltaUser1 DeltaUser1.conf]# gettx 209153f7de299922b0baa7930c53f01e87c3368
1033a177ef2bdbe587af2ac7e
{
"txid": "209153f7de299922b0baa7930c53f01e87c33681033a177ef2bdbe587af2ac7e",
"hash": "209153f7de299922b0baa7930c53f01e87c33681033a177ef2bdbe587af2ac7e",
"size": 147,
"vsize": 147,
"version": 2,
"locktime": 0,
"vin": [
{
"coinbase": "02e2000101",
"sequence": 4294967295
}
],
"vout": [
{
"value": 25.00000000,
"n": 0,
"scriptPubKey": {
"asm": "031573f0dfb96060fef261b127e1fd24e670ec4a55ddecf25acd53d614fb7dff
96 OP_CHECKSIG",
"hex": "21031573f0dfb96060fef261b127e1fd24e670ec4a55ddecf25acd53d614fb7d
ff96ac",
"reqSigs": 1,
"type": "pubkey",
"addresses": [
"mgsbJfzxcFaBGhBDQhEfssxjGAv6YrbG5d"
]
}
},
{
"value": 0.00000000,
"n": 1,
"scriptPubKey": {
"asm": "OP_RETURN aa21a9ede2f61c3f71d1defd3fa999dfa36953755c690689799962
b48bebd836974e8cf9",
"hex": "6a24aa21a9ede2f61c3f71d1defd3fa999dfa36953755c690689799962b48beb
d836974e8cf9",
"type": "nulldata"
}
}
]
}
[root@DeltaUser1 DeltaUser1.conf]#
admin@greybox:~
CORE (36695 on...
btc-1.terra.com
DeltaUser1
16:01

Koinbase, Inc is a financial institution registered in the U.S. One of the services it offers is to exchange customers' Bitcoin for U.S. Dollars. Customers send BTC to Koinbase's public address:

```
Koinbase "mtDqnengHstY1grsnoDscdnurbX598Nzfh"
```

In return, Koinbase deposits an amount of USD matching the current exchange rate into the each customer's Koinbase checking account.

Four customers sent approximately BTC 50.00 each to Koinbase's public address today (name and BTC address listed below):

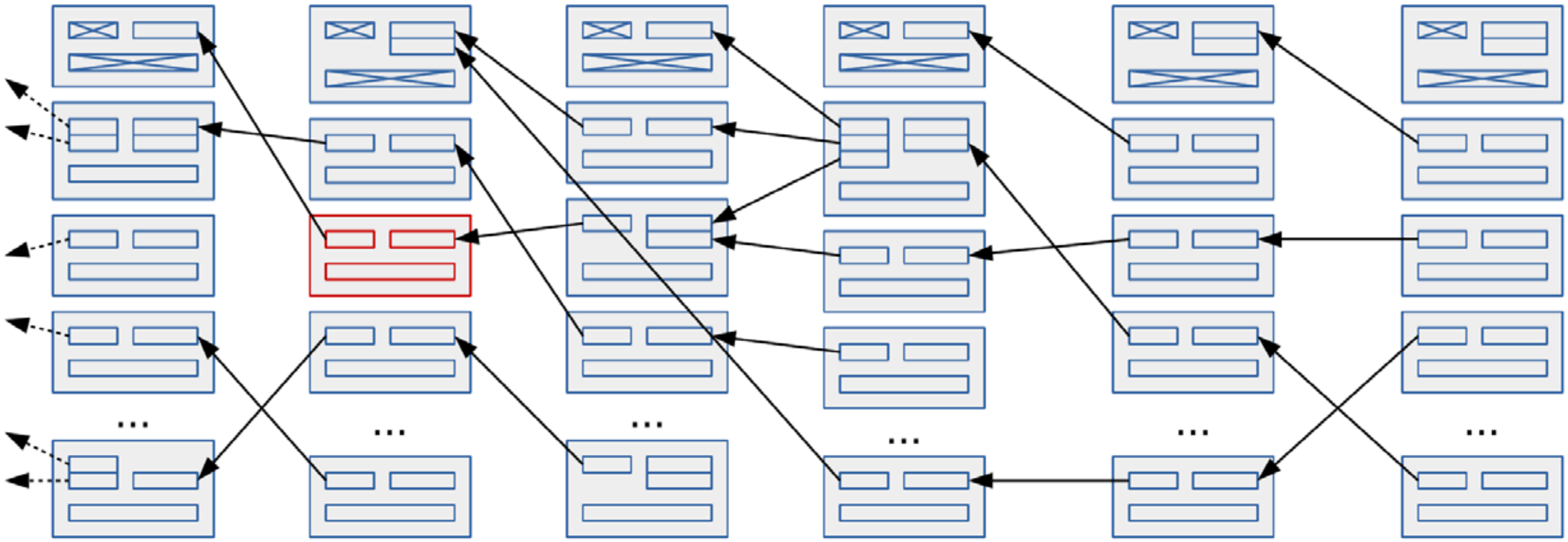
```
Alice   "mk8PhnCTpq5Nk3C7bMg65Dg4GCY2XJNp6Z"
Bob     "mrd57X428oHkm3ca1LPvS6uiyqLtjEVU61"
Charlie "mxmhKxHrXmZTDUPY58Ydantp7oZX7VYrwN"
Diane   "mne3hNXYhtetpzqbh6CJzvjx5TsJawtmpV"
```

Koinbase monitors a blacklist of reported illegal transactions, and is required to flag and refer suspicious transactions to law enforcement for further investigation. The list of known illegal transactions currently contains one instance of a ransomware attack being paid off, in the amount of BTC 100.00. That transaction's TxID (hash) is:

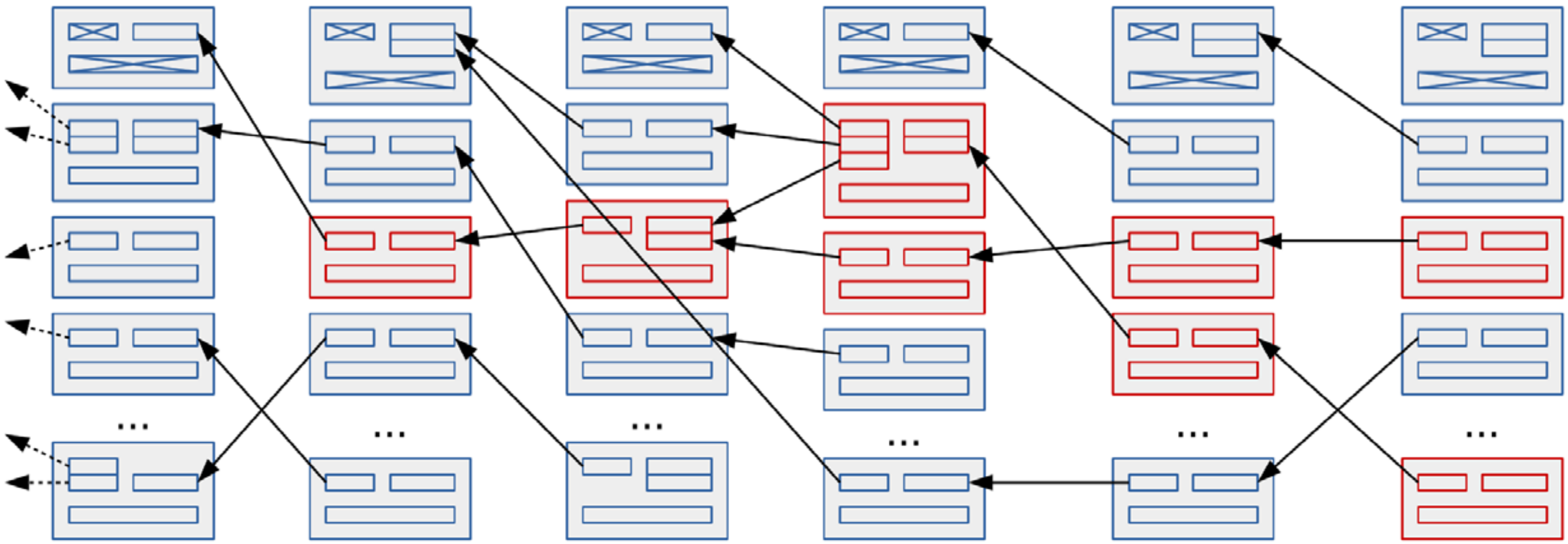
```
014dd5ff639fbaed2e23f94d6d73e5bb4bc0cc45bafc0f88bf6b25a5023122c8
```

As Koinbase's security analyst, you are tasked with determining which, if any, of these four customers' transactions to flag as potentially suspicious.

Tracing Transaction History



Tracing Transaction History



Blockchain programming is hard!

- Over **$40M** were stolen from TheDAO due to a bug in the implementation (June 2016)
- **$32M** were stolen due to a bug
  in a commonly used contract (June 2017)
- Bugs in smart contracts cannot be fixed after deployment

We want to build correct software, but current approaches have been shown to have security vulnerabilities

Obsidian: a new programming language

- Obsidian is a blockchain-based language with the goal of minimizing the risk of common security vulnerabilities

- Obsidian contains core features to allow users to write safe programs easily and effectively

- Obsidian programs consist of **contracts,** which contain fields, states, and **transactions**

Obsidian: a new programming language

Goals

- Make certain vulnerabilities impossible
- Make it easier to write correct programs
- Show effectiveness and correctness

Components

1. Typestate-oriented programming
2. Resource types

Typestate

- Blockchain programs commonly state-oriented
- Obsidian makes state first-class
    - An object in Obsidian has a **state** that restricts which **transactions** can be invoked on it.
- **State transitions** can change the state of an object

Typestate

```
contract LibraryPatron {
  state NoCard {
    transaction getCard(){
      …
      ->HasCard;
    }
  }

  state HasCard {
    transaction getBook(){
      …
    }
  }
}
```

- A `LibraryPatron` is always in either the `NoCard` or `HasCard` state

Typestate

```
contract LibraryPatron {
  state NoCard {
    transaction getCard(){
      …
      ->HasCard;
    }
  }

  state HasCard {
    transaction getBook(){
      …
    }
  }
}
```

- A `LibraryPatron` is always in either the `NoCard` or `HasCard` state
- `getBook` can only be called in `HasCard`; calling from `NoCard` state results in compile-time error

Typestate

```
contract LibraryPatron {
  state NoCard {
    transaction getCard(){
      …
      ->HasCard;
    }
  }

  state HasCard {
    transaction getBook(){
      …
    }
  }
}
```

- A `LibraryPatron` is always in either the `NoCard` or `HasCard` state.
- `getBook` can only be called in `HasCard`; calling from `NoCard` state results in compile-time error
- `->HasCard` is a state transition

Typestate – Other common applications

Voting

- Not Eligible
- Eligible, not voted
- Eligible, voted

Typestate – Other common applications

Supply chain

- Browsing
- Purchasing
- Order in processing
- Shipping
- Delivering to customer
- Return requested
- Delivering to business
- Returned

Typestate – Other common applications

Supply chain

- Browsing
- Purchasing
- Order in processing
- Shipping
- Delivering to customer
- Return requested
- Delivering to business
- Returned

Customer management

Manufacturing

Add steps for wholesale distributor

Linear Types

- Blockchain programs often manage some kind of resource
  - e.g., cryptocurrency, votes, items in supply chain
- **Linear types** allow the compiler to enforce “resource safety”:
  - Resources cannot be used more than once
  - Resources must be used before leaving the current scope (i.e., don’t lose it)

Linear Types

```
resource contract Money {…};

contract Account {
  Money balance;

  transaction closeAccount(Account a) {
    a.withdraw(balance);
    balance = new Money(0);
  }

  transaction withdraw(Money m) {…}
}
```

- Financial application example
- `balance` is a type of `Money`, which is a *linear type*

Linear Types

```
resource contract Money {…};

contract Account {
  Money balance;

  transaction closeAccount(Account a) {
    a.withdraw(balance);
    balance = new Money(0);
  }

  transaction withdraw(Money m) {…}
}
```

- When `balance` is moved out of scope, we need to create a new `Money` object to replace it
- The new `Money` is created with a value of 0
- Note that we're not referring to the actual amount of money, we're referring to the code used to track the money
  - Code security, not accounting

Linear Types

```
resource contract Money {…};

contract Account {
  Money balance;

  transaction closeAccount(Account a) {
    a.withdraw(balance);
    a.withdraw(balance);
    balance = new Money(0);
  }

  transaction withdraw(Money m) {…}
}
```

- Introducing bug… spending more `Money` than available
- Program would fail when trying to compile, rather than when the user tried to run the program

Usability

Programmers should be able to write correct Obsidian code easily and effectively.

Creating an intuitive language is hard! Many difficult design choices exist

Usability

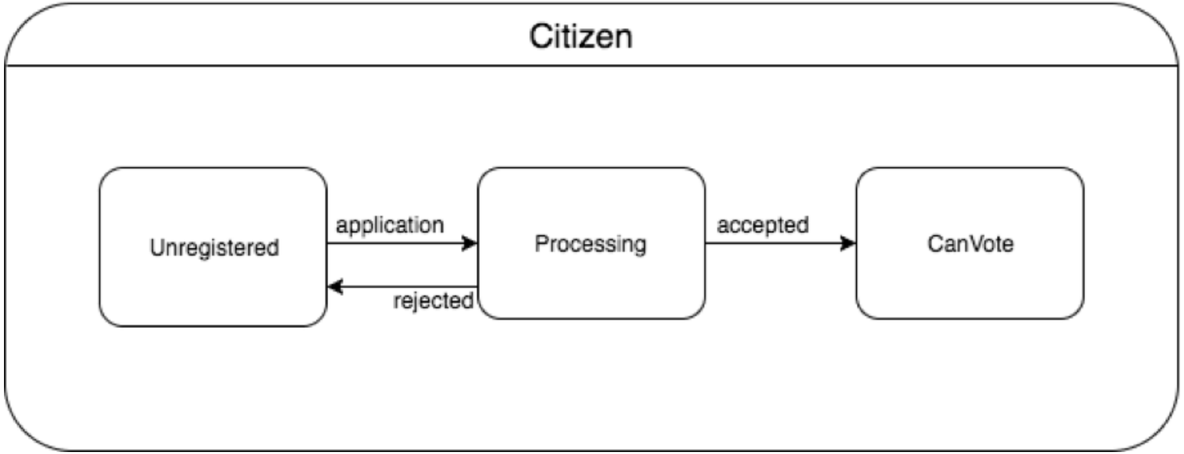
```
contract C {
   state S1 {
      transaction t(int x) {
         ->S2(x);
      }
   }

   state S2 {
      int x1;
      S2(int x) {
         x1 = x;
         ->S3(x1);
      }
   }

   state S3 {
      ...
   }
}
```

```
contract C {
   state S1 {
      transaction t(int x) {
         ->S2{x1 = x};
         toS3();
      }
   }

   state S2 {
      int x1;
      transaction toS3() {
         ->S3{x2 = x1};
      }
   }

   state S3{
      ...
   }
}
```

Which is “correct”?

Usability study

Participants were given a description of a voter registration system for a hypothetical democratic nation.



Usability study

1. Write pseudocode to implement program.
2. Given a state diagram modeling the voter registration system, modify pseudocode.
3. Given Obsidian tutorial (with no information on state transitions) invent syntax for state transitions and complete an Obsidian contract.
4. Shown three options for state transitions, complete a brief contract for each option.
5. Choose one of the three options and use it to complete the Obsidian program from part 3.

Usability study – Findings

- Programmers do not naturally consider state-based design when architecting code
- Most intuitive design: include all possible state actions explicitly within the state

Summary

Bitcoin simulator

- Virtual implementation of Bitcoin network
- Useful for forensic analysis

Obsidian

- Secure-by-design language for blockchain development
- Typestate and linear resources help users write safe programs easily and effectively
- Usable programming language design requires iteration and user testing

Contact Information

Presenters

Elli Kanal

Technical Manager

Email: ekanal@cert.org

Gabe Somlo

Cybersecurity Researcher

Email: glsomlo@cert.org