



Next Steps with Blockchain Technology

Eliezer Kanal & Gabriel Somlo

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



Copyright 2018 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

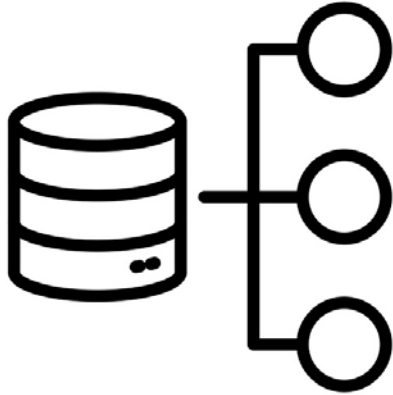
NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University. DM18-1016

Previous models of computing

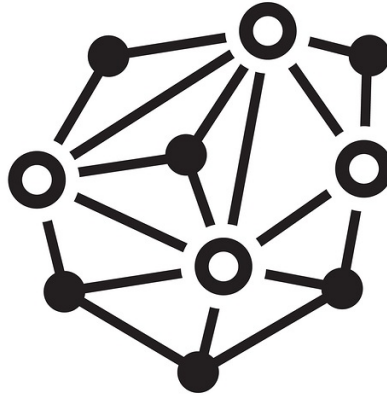


Data Storage:
Database



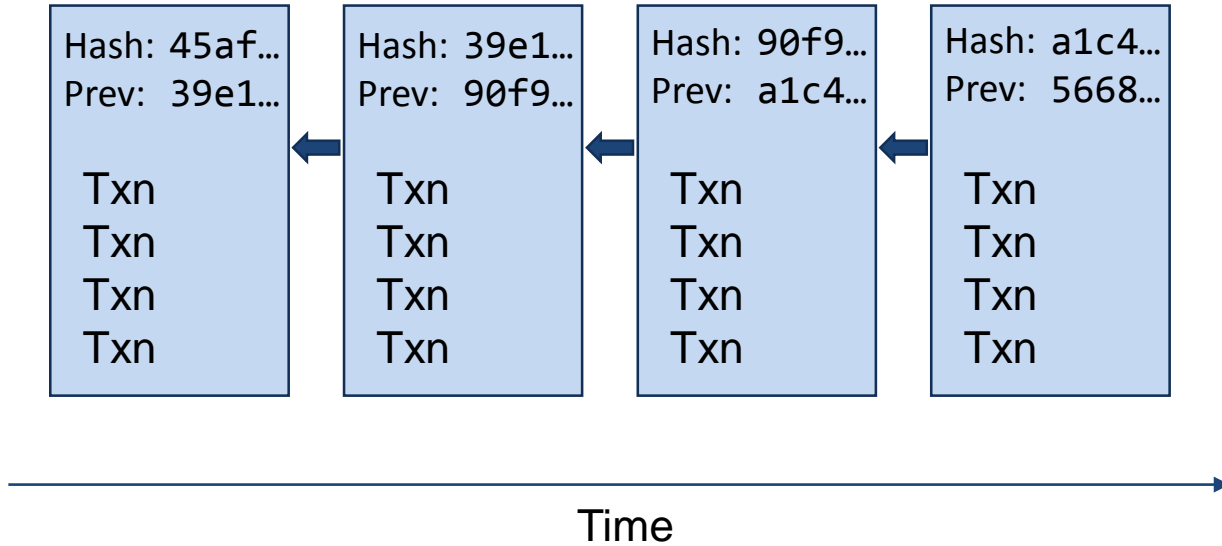
Program Execution:
Local

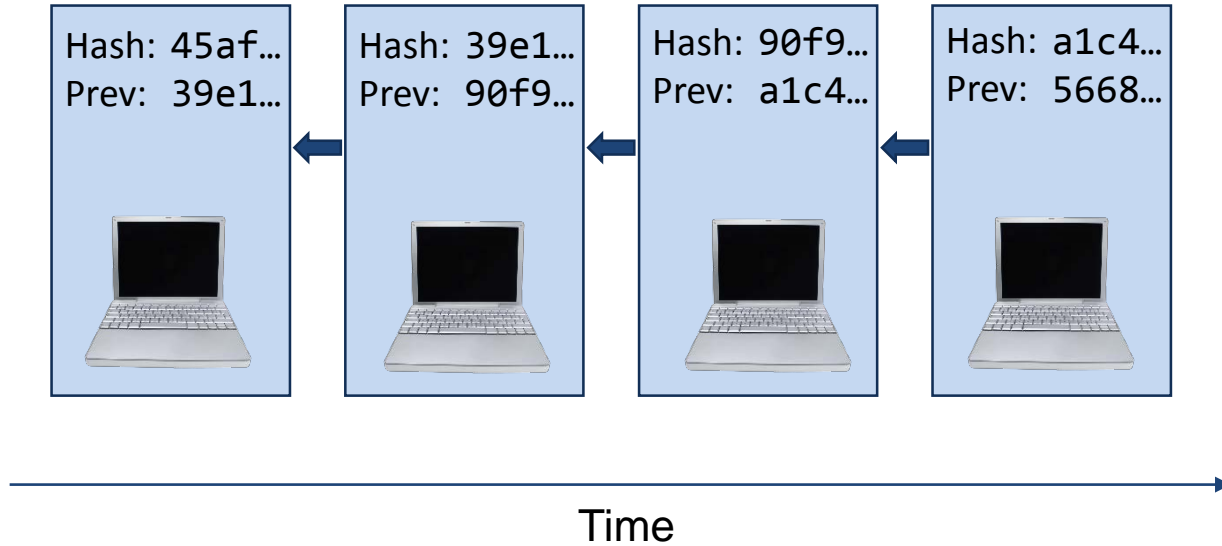
Blockchain

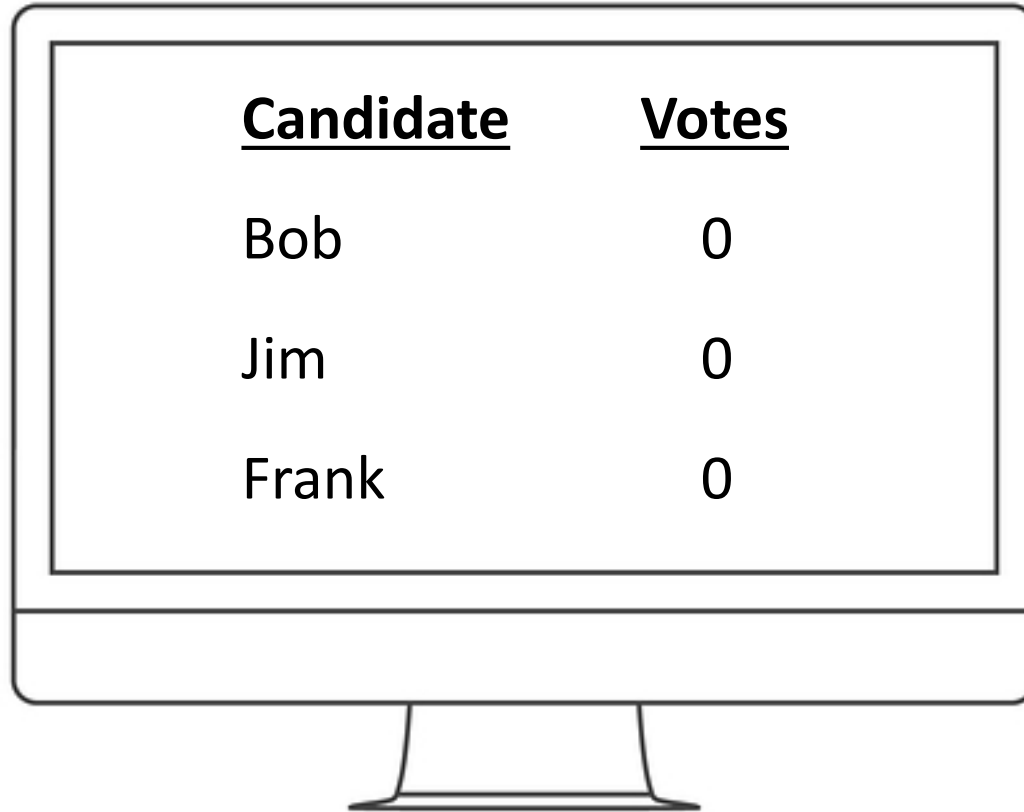


Data Storage:
Blockchain or Network

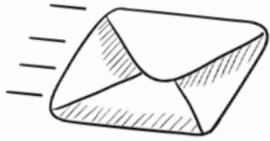
Program Execution:
Network







<u>Candidate</u>	<u>Votes</u>
Bob	0
Jim	0
Frank	0

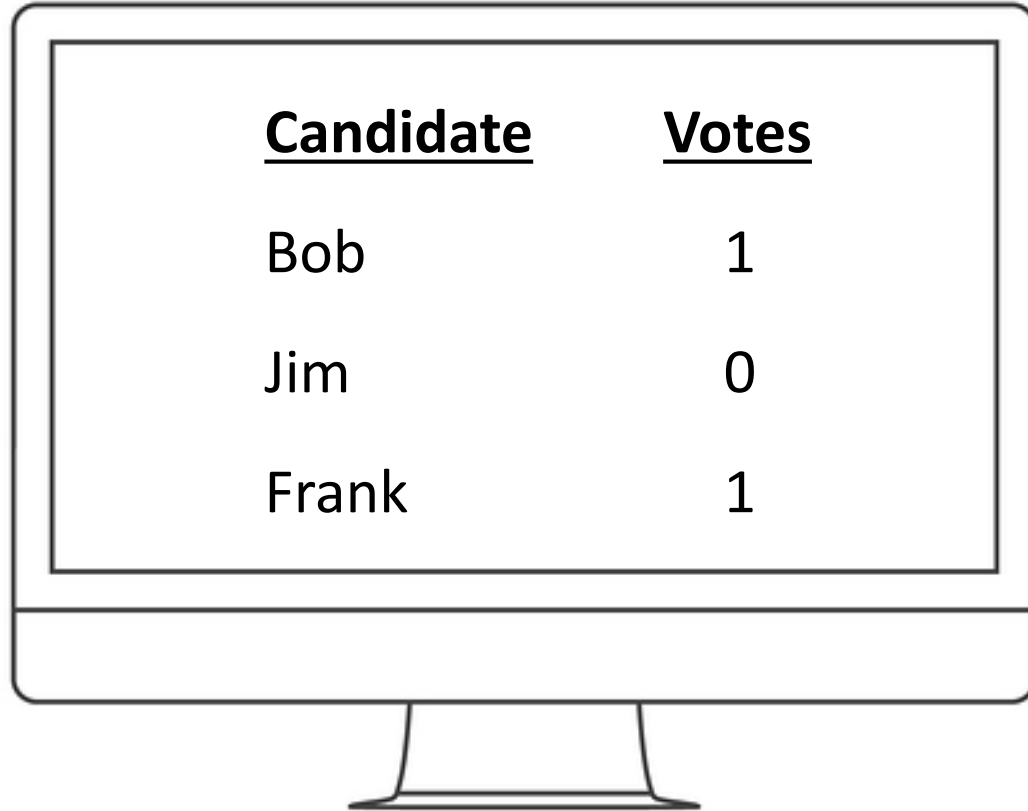


Bob: 1 vote



Frank: 1 vote

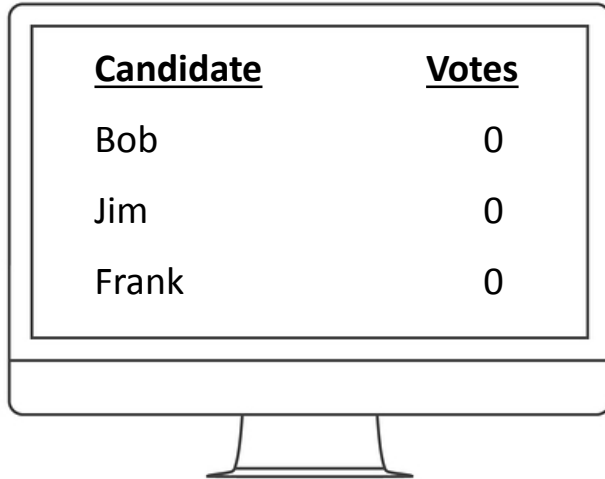
<u>Candidate</u>	<u>Votes</u>
Bob	0
Jim	0
Frank	0



A computer monitor is shown with a table of candidate votes on its screen. The table has two columns: 'Candidate' and 'Votes'. The candidates listed are Bob, Jim, and Frank, with their respective vote counts being 1, 0, and 1.

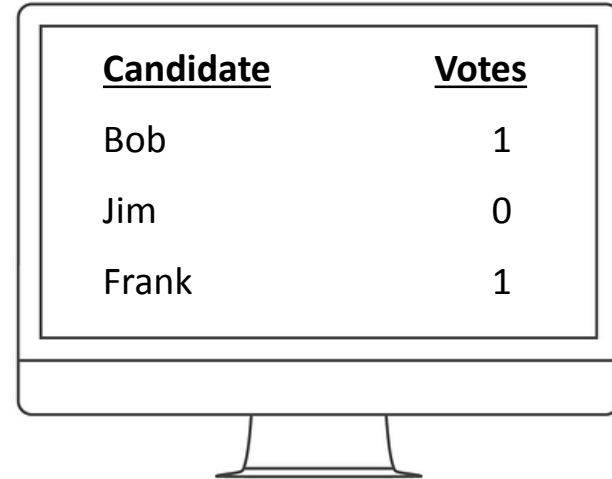
<u>Candidate</u>	<u>Votes</u>
Bob	1
Jim	0
Frank	1

State: 1



<u>Candidate</u>	<u>Votes</u>
Bob	0
Jim	0
Frank	0

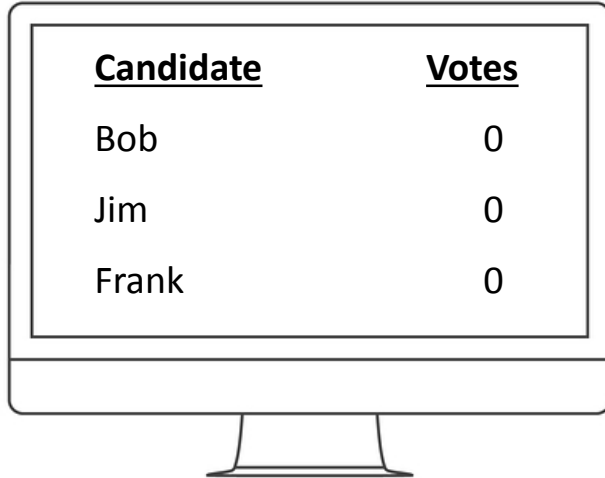
State: 2



<u>Candidate</u>	<u>Votes</u>
Bob	1
Jim	0
Frank	1

Equivalent to:

State: 1



<u>Candidate</u>	<u>Votes</u>
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

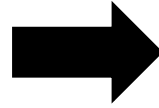
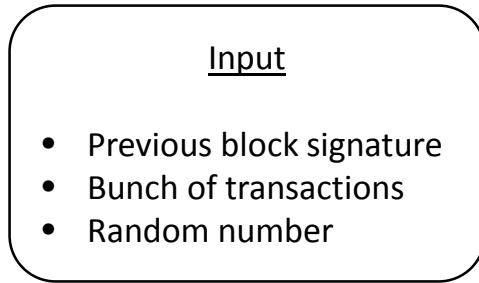
Cons:

Proof-of-work very inefficient

State updates are slow

Best for simple computations

Bitcoin: Mining



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	000000000000000002c4b94355945eea353bc720c58a73c2b8593f489550cb3
Previous Block	00000000000000001d620a2e3ad126ec5038bf42343c419eb6fedf7240a471
Next Block(s)	
Merkle Root	3ad680735c45cc62b1ea6b7efeb34f82a2660c5e8280354c45f7fa03c9137e2

Transactions

ab0da64ea834fd2acb81eb081d8103c9e31fd14a7d055f2ce2718c59dd4fa5df		2018-02-14 15:16:59
No Inputs (Newly Generated Coins)	→ 14DjTuAUh87cwRabU1z6W8hZY6FnEkpFLS Unable to decode output address	12.9893378 BTC 0 BTC
		12.9893378 BTC
4feb8981da942b10a2a384003fba1c1d78c8f192cd2747e43ae552cd2371267d		2018-02-14 15:16:59
1H6ZZpRmMnrw8ytepV3BYwMjYnEkWDqVP	→ 12PaHifRJbmvJYmTpZ32Pswf8eYbKcAE131 1GpgR4vsdvEfgtNylUrDrDLTBjvmsentX 1H6ZZpRmMnrw8ytepV3BYwMjYnEkWDqVP	0.4983 BTC 0.1495 BTC 5.01651602 BTC
		5.66431602 BTC

Block #500100

1H6ZZpRmMnrw8ytepV3BYwMjYnEkWDqVP → 12PaHiRJbmvJYmTpZ32Pswf8eYbKcAE131 0.4983 BTC
 1GpqR4vsdvEfgtNyiUrDrDLTBjvnsentX 0.1495 BTC
 1H6ZZpRmMnrw8ytepV3BYwMjYnEkWDqVP 5.01651602 BTC

5.66431602 BTC

Estimated Transaction Volume 1,818.68925455 BTC Next Block(s)

Transaction **Number Of Transactions** 1915

Height

Timestamp

Received Time 2018-02-14 15:16:59

Relay

Difficulty **Nonce** 1858980081

Bits

Size 1132.416 kB

Difficulty 2,874,674,234,415.94

Block Reward 12.5 BTC

Hash 000000000000000002c4b94355945eea353bc720c58a73c2b8593f489550cb3

Previous Block 000000000000000001d620a2e3ad126ec5038bf42343c419eb6fcdf7240a471

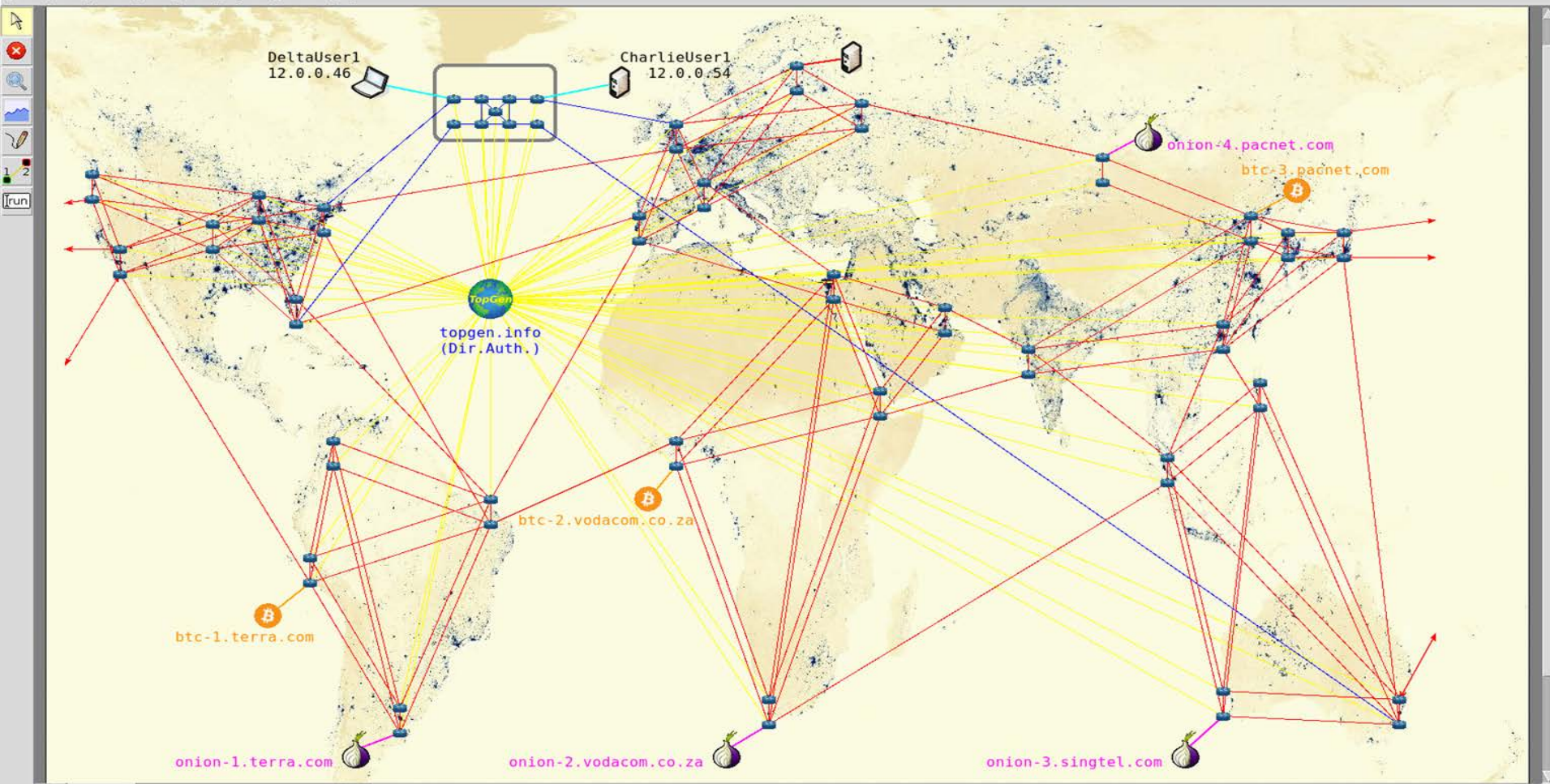
Block Reward 12.5 BTC

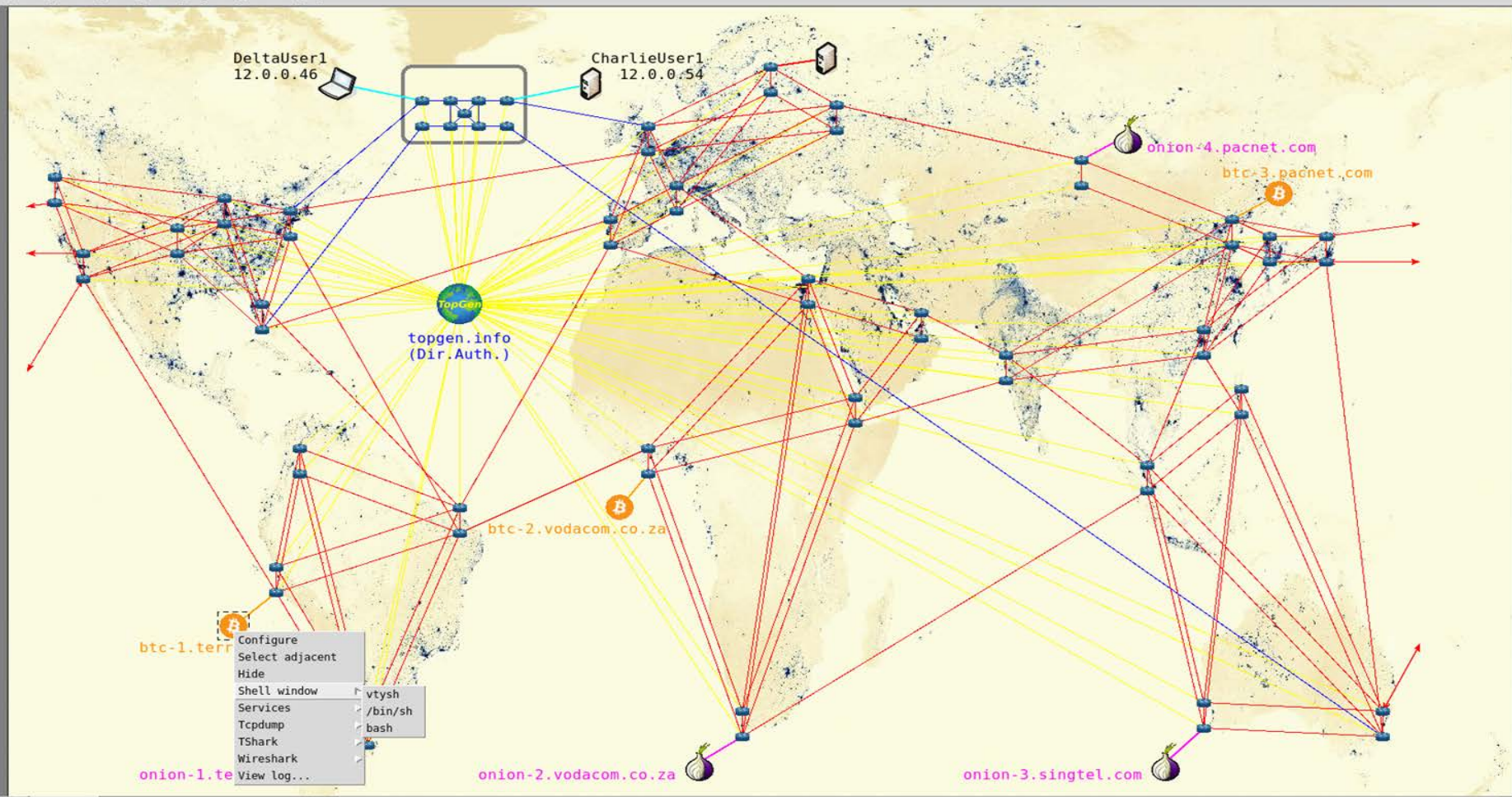
12.9893378 BTC

18-02-14 15:16:59

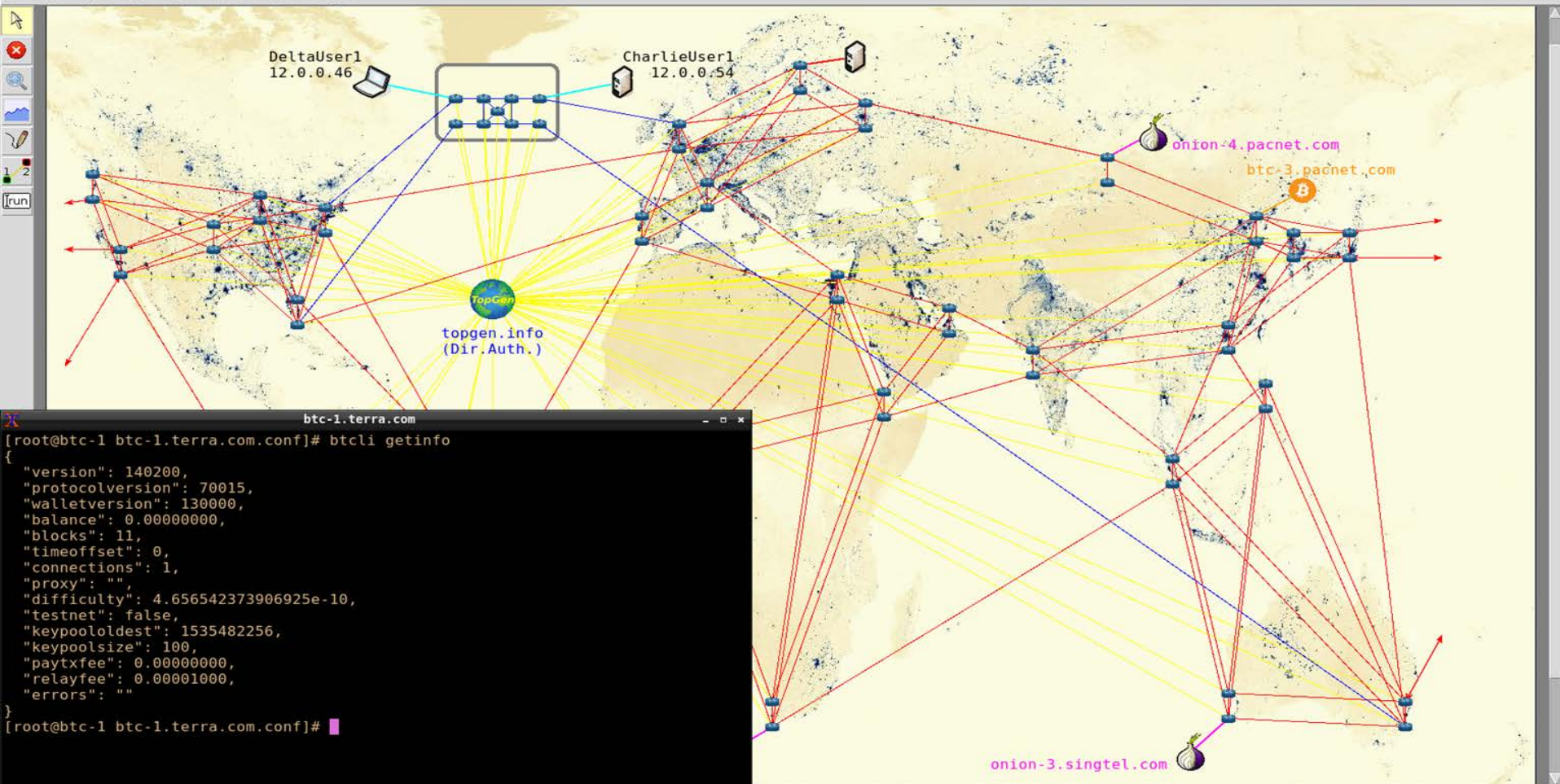
0.4983 BTC
 0.1495 BTC
 5.01651602 BTC

5.66431602 BTC





- Configure
- Select adjacent
- Hide
- Shell window vtysh
- Services /bin/sh
- Tcpdump bash
- TShark
- Wireshark
- View log...

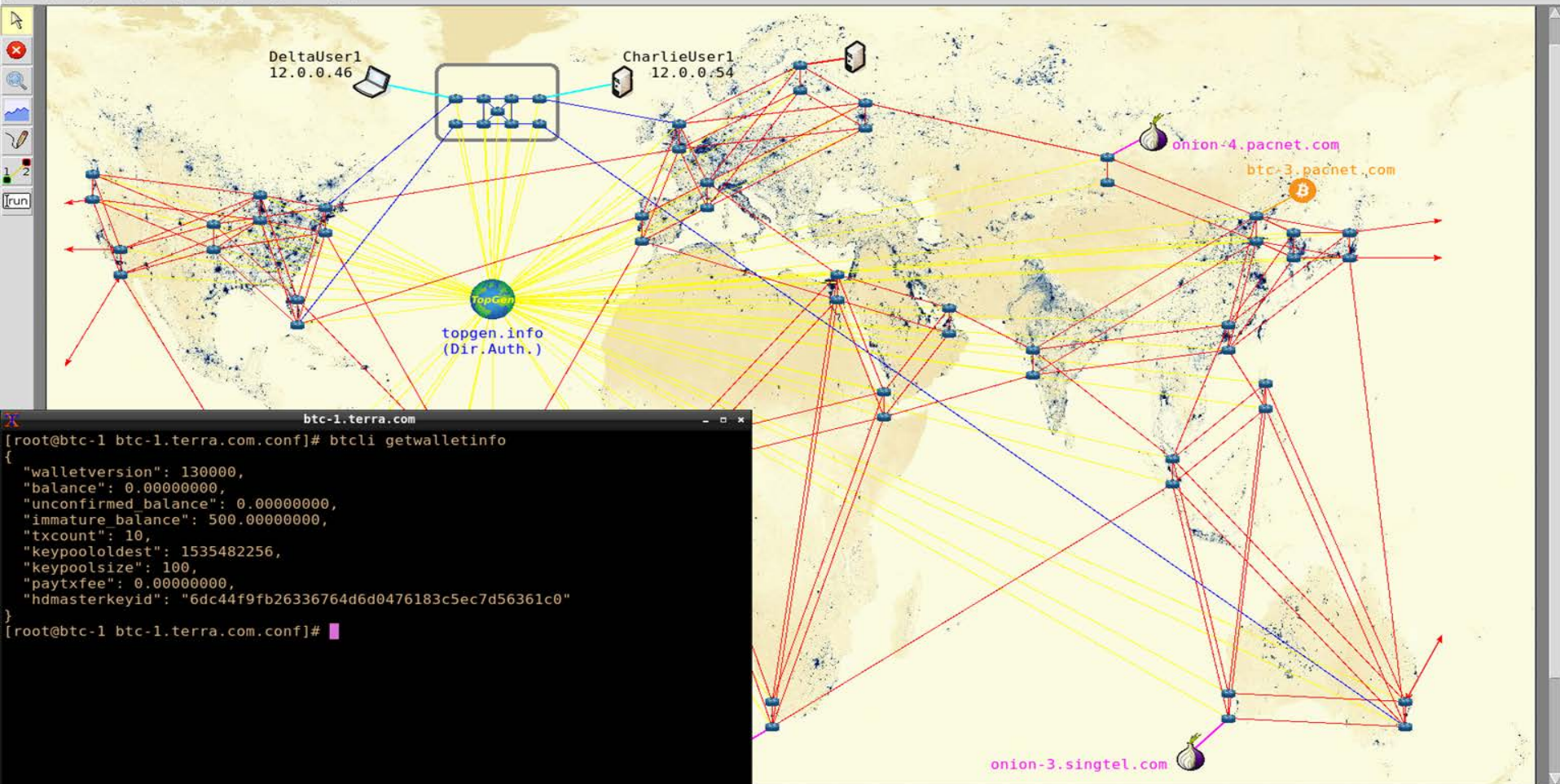


btc-1.terra.com

```
[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": ""  
}
```

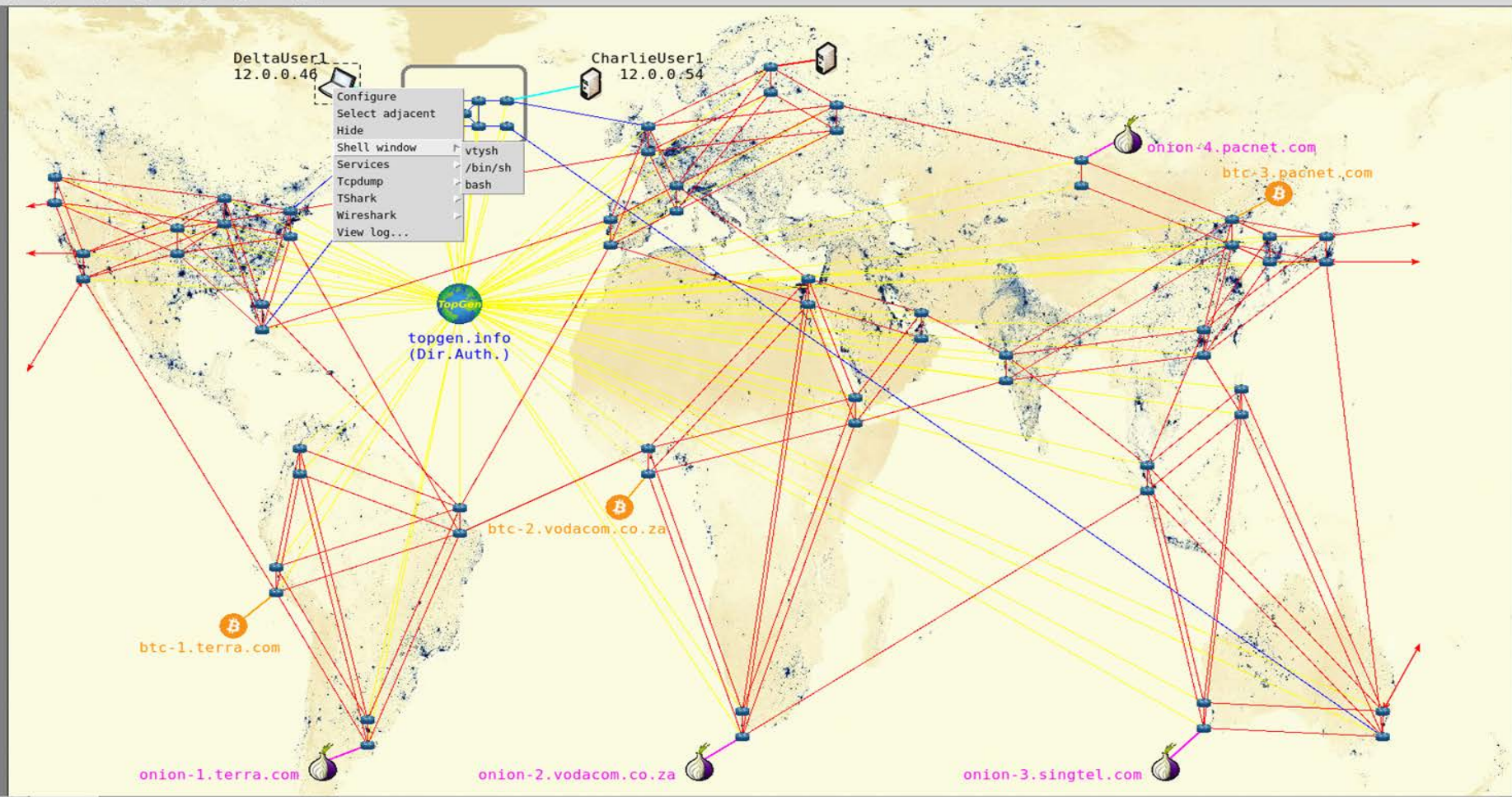
```
[root@btc-1 btc-1.terra.com.conf]#
```



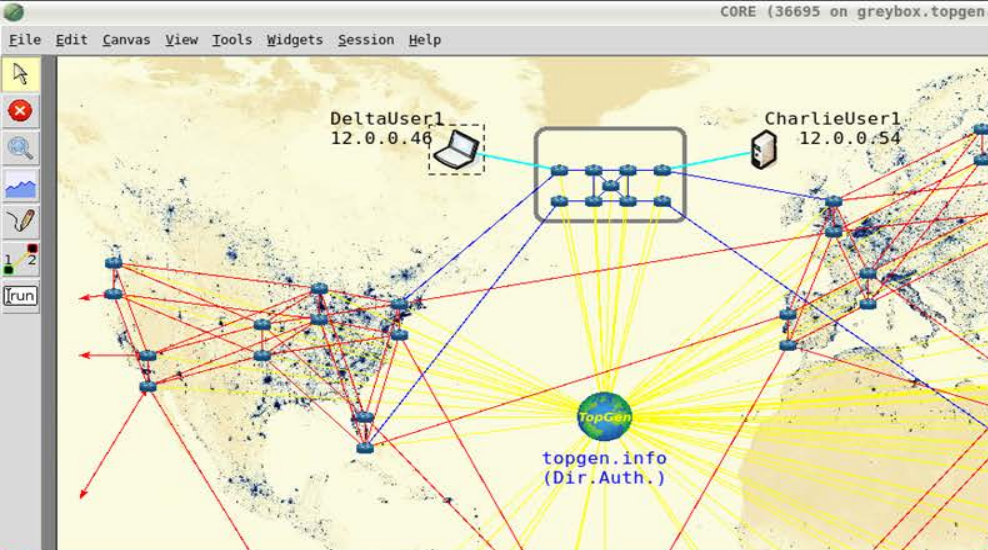
```

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]#

```



- Configure
- Select adjacent
- Hide
- Shell window
- Services
 - vttysh
 - /bin/sh
 - bash
- Tcpdump
- TShark
- Wireshark
- View log...



```

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 (0000aa43e2009cfe3cc8ba406524c0e13e3a71
2284dd4a976fd3976a79b4a9f7),
#   mined on 2018-08-28T19:19:02Z

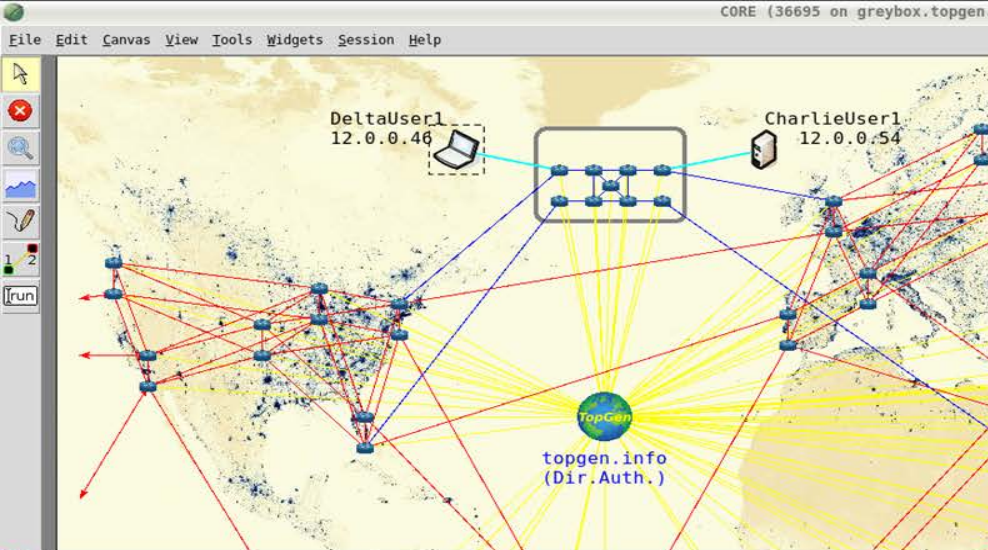
# extended private masterkey: tprv8ZgxMBic0KsPdFsGeZPKmT9f9tibwgTzMT2d8iWq3683bs
Jaye5JASf58UFU3o476RYoqTQNnsKM3afH9dvgjZymrd1zeMeSk5HvLUgK3nH

cw1bBs3ug8efRV5E77dr5rHrBw7VFQNVnsd8WCNCavLMTFqybRns 2018-08-28T19:07:30Z reserv
e=1 # addr=mfdkGX4T153Bdm1NjYlcmoz7wQUeSkScv hdkeypath=m/0'/0'/53'
cP5uDL8PMwrVSNQmSkJqs89JD1YYTHkSrQYcfDrnwTXP7Eaqk8wr 2018-08-28T19:07:30Z reserv
e=1 # addr=mfuUJAYCQVHTGzMddDFbNfgGzn8JTQopp6 hdkeypath=m/0'/0'/9'
cNTzPWvucdbHrK71YXb5Hh2qt4mdrWguYko90aZ72nEi0ikACYNg 2018-08-28T19:07:30Z hdmast
er=1 # addr=mgJTeUfrSHkhtPRY99tk9vhC7GE4rJvMH hdkeypath=m
[root@DeltaUser1 DeltaUser1.conf]#
  
```

btc-1.terra.com

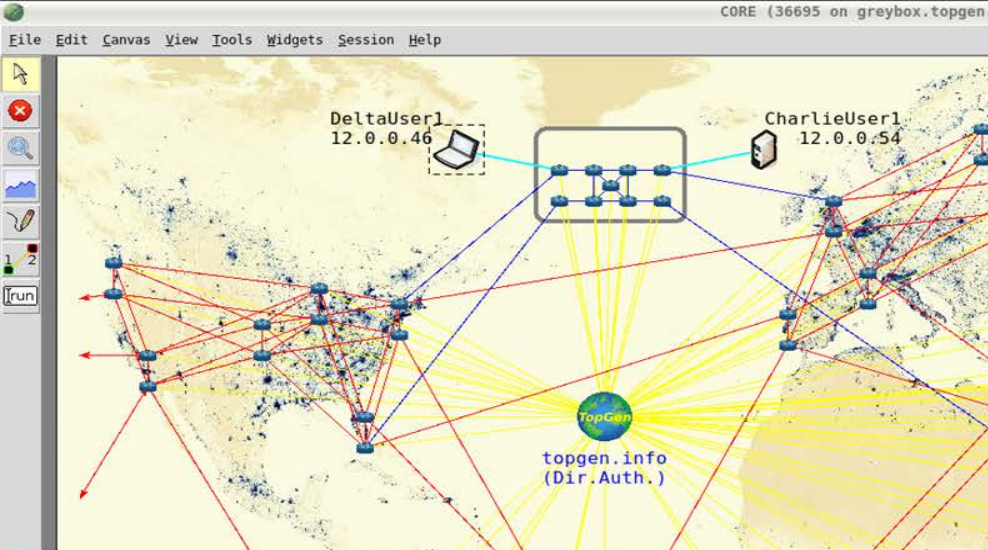
```

[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]#
  
```



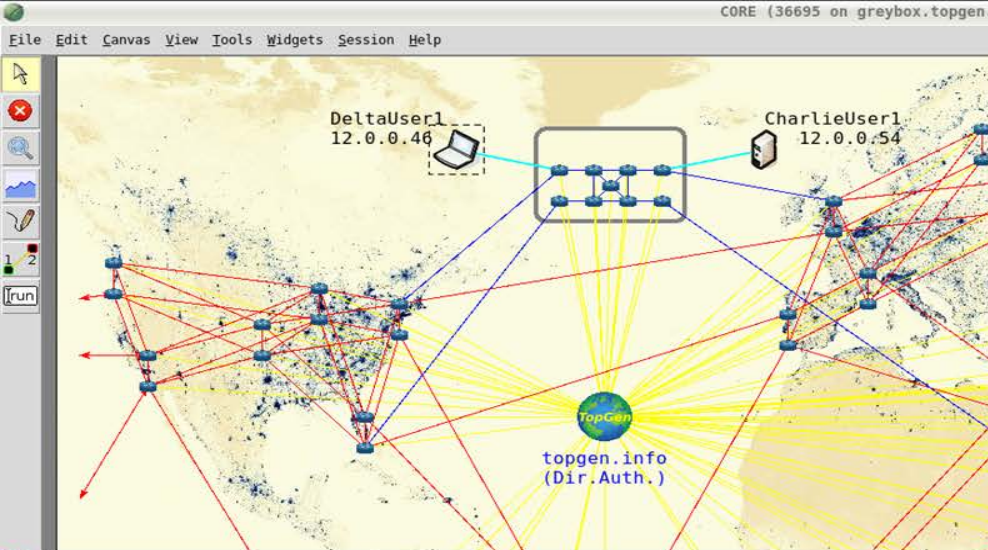
```
DeltaUser1
[root@DeltaUser1 DeltaUser1.conf]# btcli getnewaddress
mzLLFxpjJjA5L380MUMzwXanb6suWayCMN
[root@DeltaUser1 DeltaUser1.conf]#
```

```
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]#
```



```
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]#
```

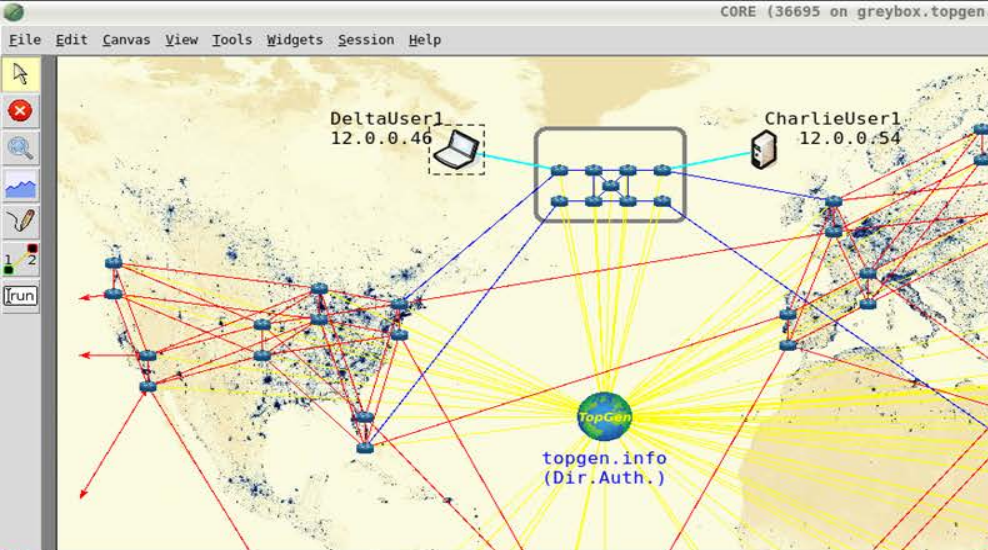


```

[root@btc-1 btc-1.terra.com]# btcli sendtoaddress mZLLFxpNjJA5L38QMUMzwXanB
6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com]#
  
```

```

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": "00001753a04419ece68f30fd657d7360blead9869083e9255c4aad1befa35a2",
  "branchlen": 1,
  "status": "valid-fork"
},
{
  "height": 212,
  "hash": "00007c46253435acca2bc5f74f17466de846ce93db6291e9afa8f341c9483bd9",
  "branchlen": 1,
  "status": "valid-fork"
}
]
[root@DeltaUser1 DeltaUser1.conf]#
  
```

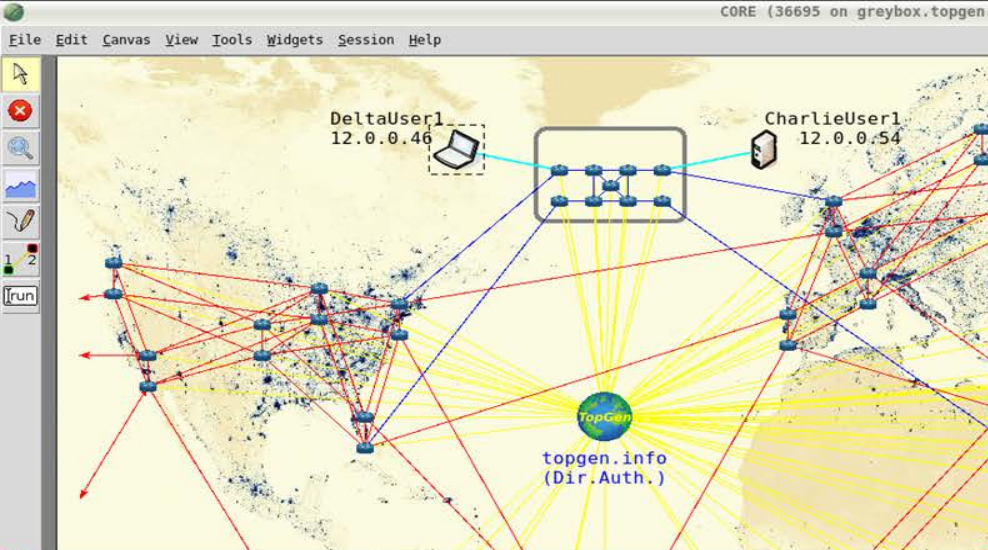



```

[root@btc-1 btc-1.terra.com]# btcli sendtoaddress mzLLFxpNjJA5L38QMUMzwXanb
6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com]#
  
```

```

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": "00001753a04419ece68f30fd657d7360blead9869083e9255c4aad1befa35a2",
  "branchlen": 1,
  "status": "valid-fork"
},
{
  "height": 212,
  "hash": "00007c46253435acca2bc5f74f17466de846ce93db6291e9afa8f341c9483bd9",
  "branchlen": 1,
  "status": "valid-fork"
}
]
[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]#

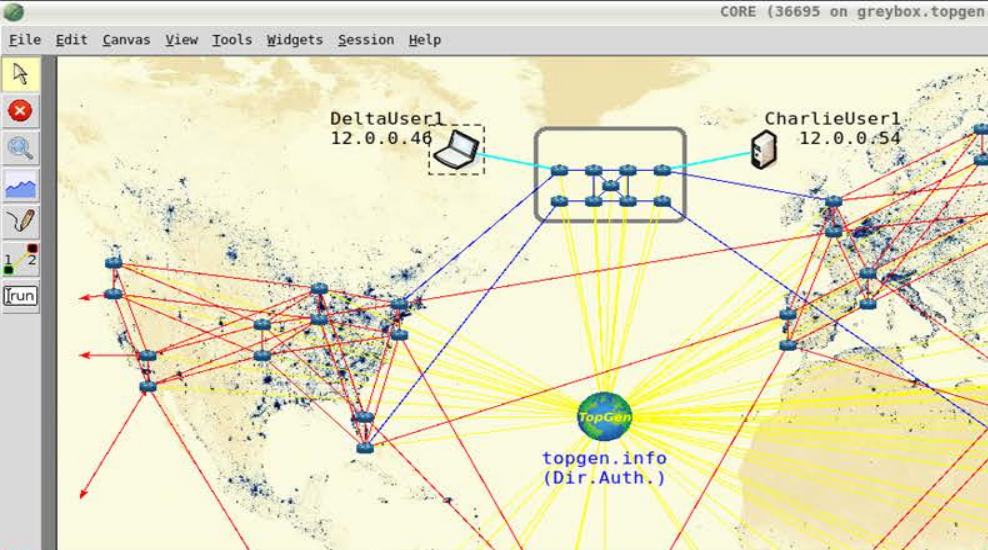
```

DeltaUser1

```

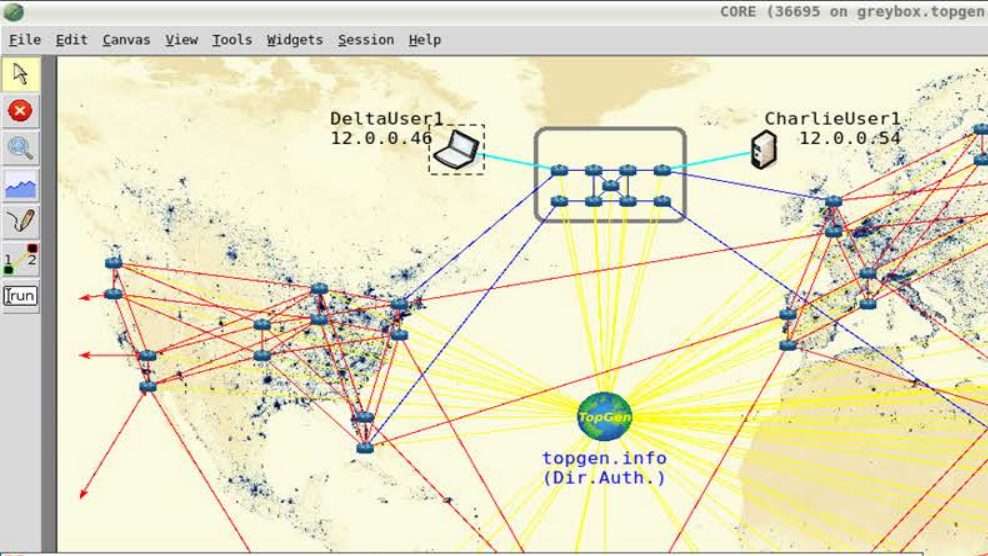
[root@DeltaUser1 DeltaUser1.conf]# btcli getblock 000093ed722cd3d0b27023a0251329
9d02dd943f035e1ac62d7b9f6b2afe885a
{
  "hash": "000093ed722cd3d0b27023a02513299d02dd943f035e1ac62d7b9f6b2afe885a",
  "confirmations": 1,
  "strippedsize": 228,
  "size": 228,
  "weight": 912,
  "height": 382,
  "version": 805306371,
  "versionHex": "30000003",
  "merkleroot": "2e1d67654a774f01d57e033fc40f69df325f2a437dd589718511b4dc469e526
3",
  "tx": [
    {
      "txid": "2e1d67654a774f01d57e033fc40f69df325f2a437dd589718511b4dc469e5263"
    }
  ],
  "time": 1535484664,
  "mediantime": 1535484635,
  "nonce": 54874,
  "bits": "207fffff",
  "difficulty": 4.656542373906925e-10,
  "chainwork": "00000000000000000000000000000000000000000000000000000000000002fe",
  "previousblockhash": "000005a681c8aa8ed005d14f4a451e3cc308eab4e8b74c5df34fbe0c
0c5cb8fb"
}
[root@DeltaUser1 DeltaUser1.conf]#

```



```
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 mzLLFxpjA5L38QMUMzwXanb
6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#
```

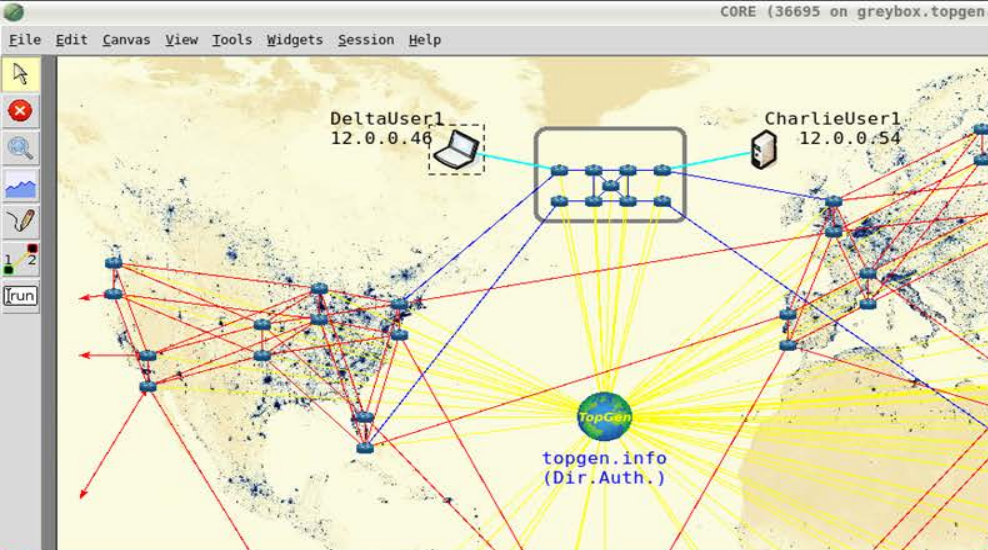


```

[root@btc-1 btc-1.terra.com]# btcli sendtoaddress mzLLFxpNjJA5L38QMUMzwXanb
6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com]#
  
```

```

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]#
  
```

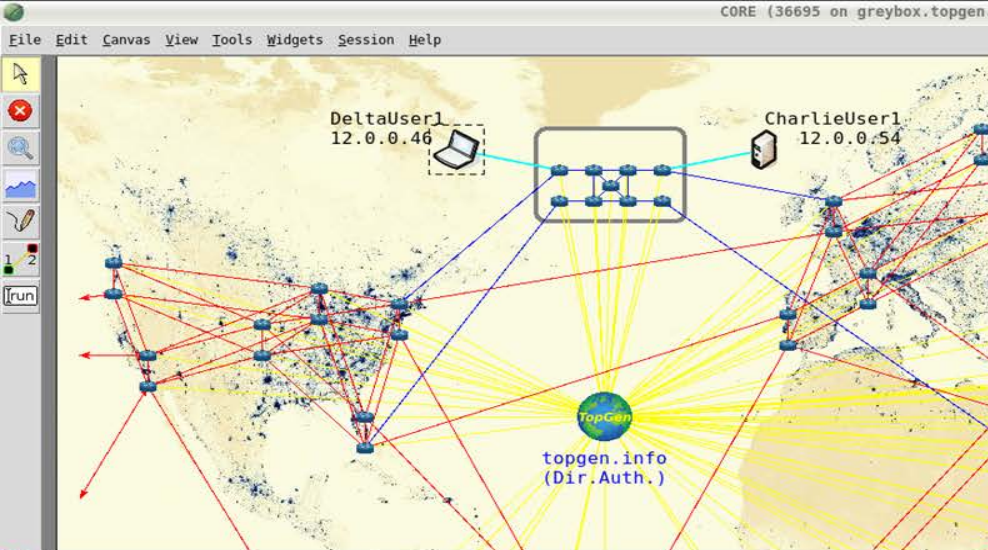


```

[root@btc-1 btc-1.terra.com]# btcli sendtoaddress mzLLFxpjA5L38QMUMzwXanb
6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com]#
  
```

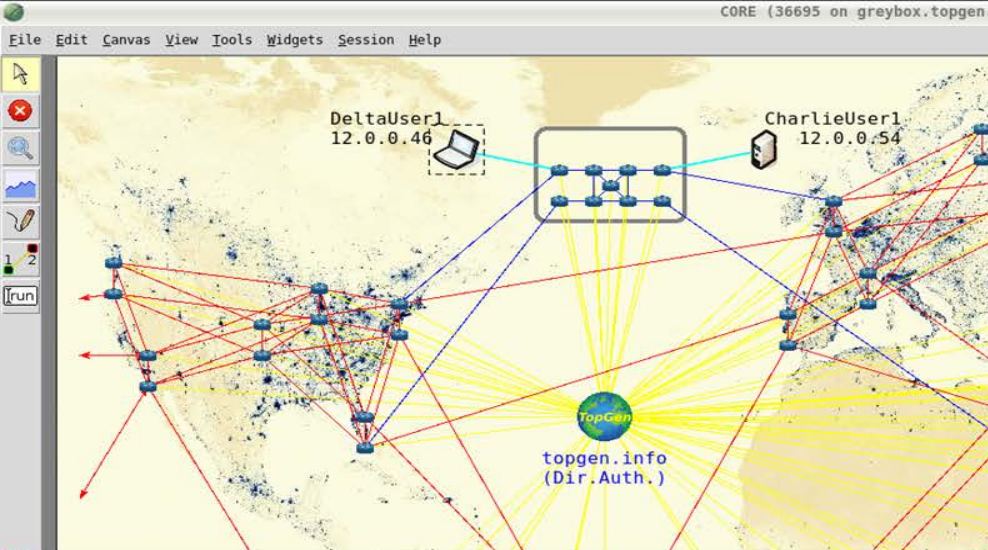
```

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]#
  
```



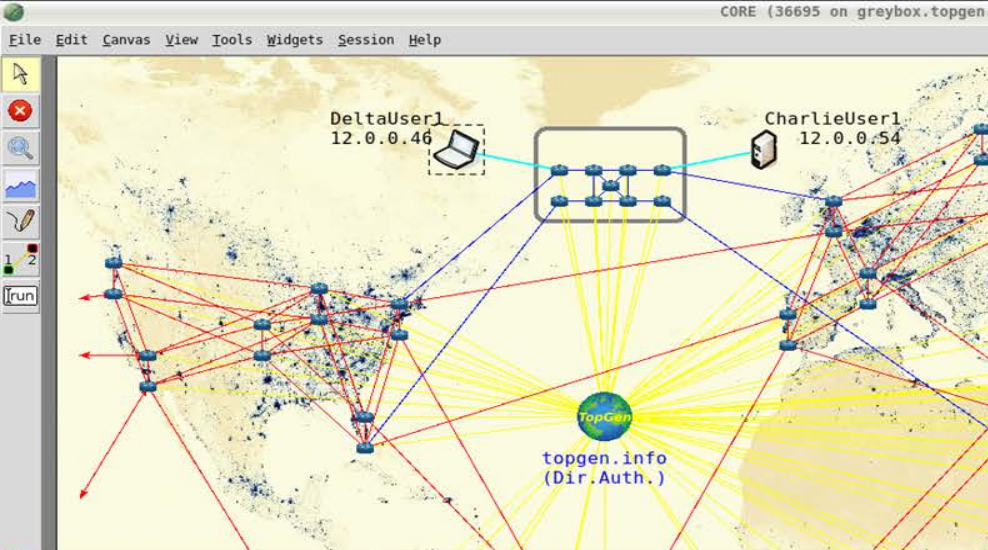
```
DeltaUser1
[root@DeltaUser1 DeltaUser1.conf]# climbchain () {
> local BLKID=${1}
> while [ -n "${BLKID}" ]; do
>   echo
>   BLKID=$(btcli getblock ${BLKID} | tee /dev/tty \
>     | grep previousblockhash \
>     | awk '{print $2}' | tr -d "\,")
>   echo "Prev: ${BLKID} ([q]uit)"
>   read -n 1
>   [ "${REPLY}" == "q" ] && { echo; break; }
> done
> }
[root@DeltaUser1 DeltaUser1.conf]#
```

```
btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btcli sendtoaddress mzLLFxpjA5L38QMUMzwXanb
6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#
```



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

```
btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btccli sendtoaddress mZLLFxpNjJA5L38QMUMzwXanb
6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#
```



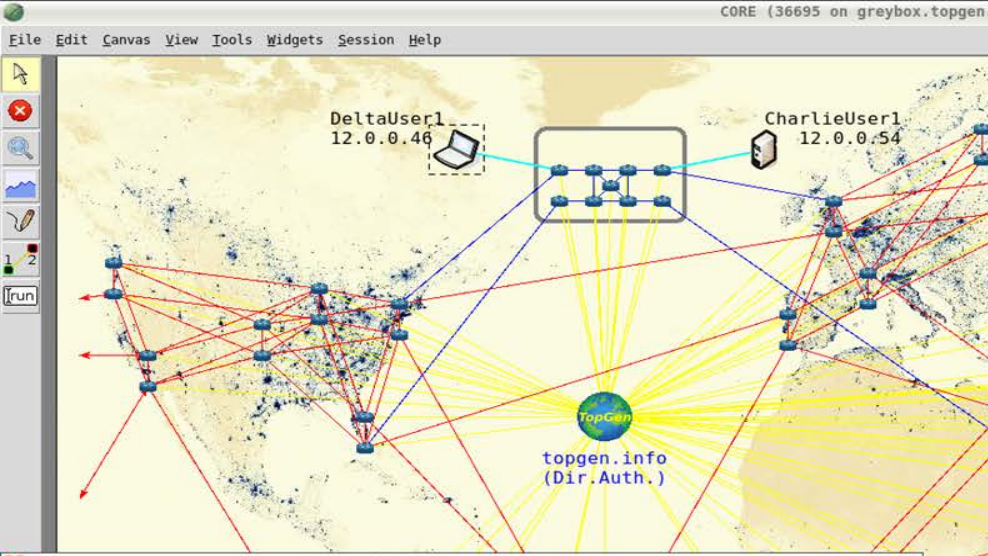
```

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]#
  
```

```

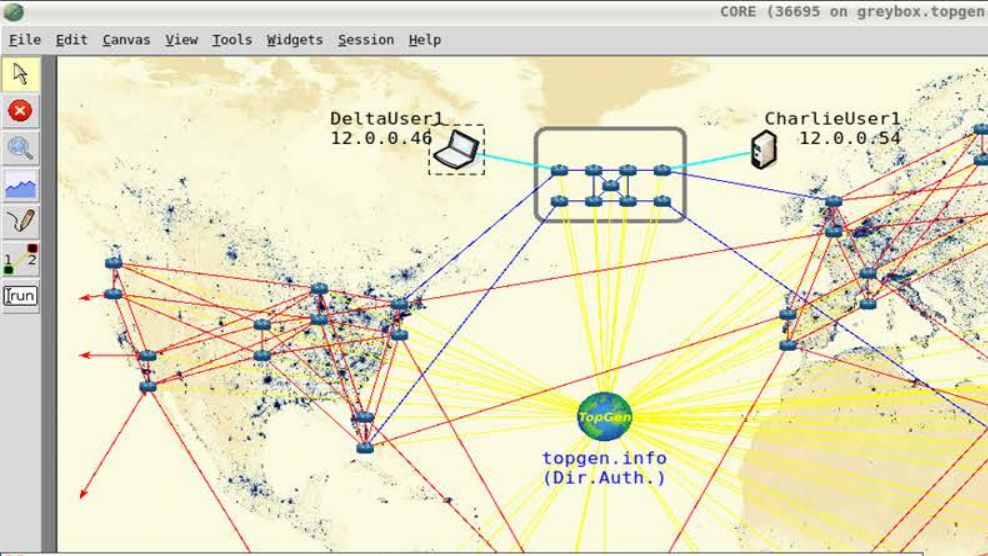
DeltaUser1
[root@DeltaUser1 DeltaUser1.conf]# climbchain 000093ed722cd3d0b27023a02513299d02
dd943f035elac62d7b9f6b2afe885a

{
  "hash": "000093ed722cd3d0b27023a02513299d02dd943f035elac62d7b9f6b2afe885a",
  "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": "000000000000000000000000000000000000000000000000000000000002fe
0c5cb8fb"
}
Prev: 000005a681c8aa8ed005d14f4a451e3cc308eab4e8b74c5df34fbe0c0c5cb8fb ([q]uit)
  
```

```
DeltaUser1
[root@DeltaUser1 DeltaUser1.conf]# gettx 4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
```

```
btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btccli sendtoaddress mZLLFxpNjJA5L38QMUMzwXanb6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#
```

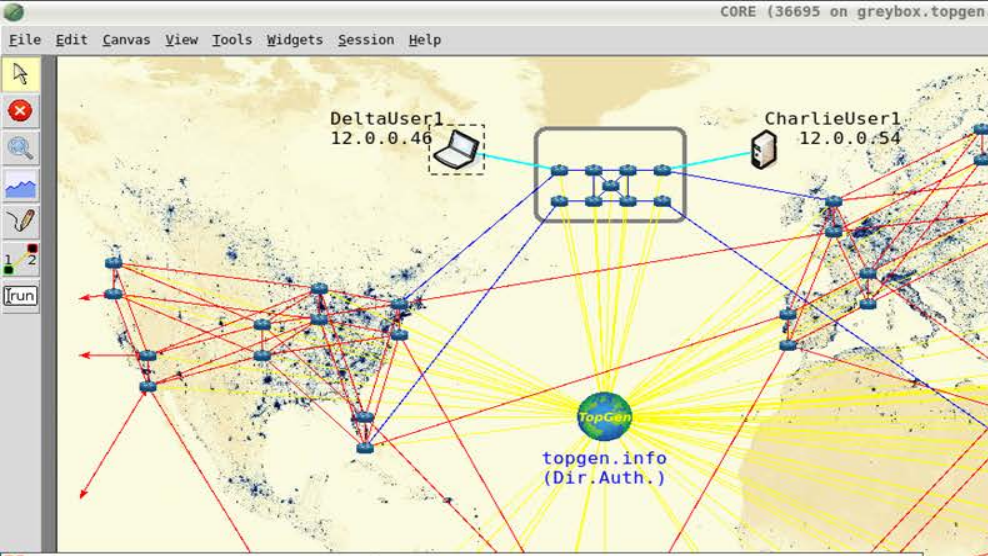


```

btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btcli sendtoaddress mzLLFxpjJjA5L38QMUMzwXanb
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_EO
UALVERIFY OP_CHECKSIG",
      "hex": "76a914ca77c518bc00aa114181def1dbdece209cdb0f3588ac",
      "reqSigs": 1,
      "type": "pubkeyhash",
      "addresses": [
        "myyWGZbtCJ3FXsvd6jaQjSrvqVWo1emwXe"
      ]
    }
  },
  {
    "value": 14.82300000,
    "n": 1,
    "scriptPubKey": {
      "asm": "OP_DUP OP_HASH160 ce68261e18f2a2afe01de93fafb3134963099ae6 OP_EO
UALVERIFY OP_CHECKSIG",
      "hex": "76a914ce68261e18f2a2afe01de93fafb3134963099ae688ac",
      "reqSigs": 1,
      "type": "pubkeyhash",
      "addresses": [
        "mzLLFxpjJjA5L38QMUMzwXanb6suWayCMN"
      ]
    }
  }
]
}
}
}
[root@DeltaUser1 DeltaUser1.conf]#
  
```



```

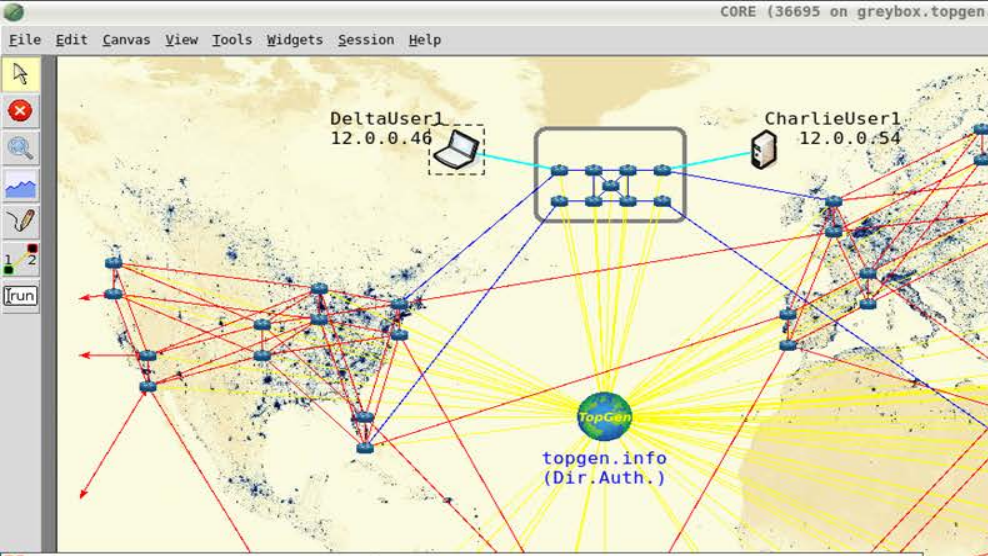
btc-1.terra.com
[root@btc-1 btc-1.terra.com.conf]# btcli sendtoaddress mZLLFxpNJjA5L38QMUMzwXanB
6suWayCMN 14.823
4aad741923b21bf64d16f664c63f7be6a3b81ca65719dd41bf8068230e3d07bc
[root@btc-1 btc-1.terra.com.conf]#

```

```

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_EO
UALVERIFY OP_CHECKSIG",
      "hex": "76a914ca77c518bc00aa114181def1dbdece209cdb0f3588ac",
      "reqSigs": 1,
      "type": "pubkeyhash",
      "addresses": [
        "myyWGZbtCJ3FXsvd6jaQjSrvqVWo1emwXe"
      ]
    }
  },
  {
    "value": 14.82300000,
    "n": 1,
    "scriptPubKey": {
      "asm": "OP_DUP OP_HASH160 ce68261e18f2a2afe01de93fafb3134963099ae6 OP_EO
UALVERIFY OP_CHECKSIG",
      "hex": "76a914ce68261e18f2a2afe01de93fafb3134963099ae688ac",
      "reqSigs": 1,
      "type": "pubkeyhash",
      "addresses": [
        "mZLLFxpNJjA5L38QMUMzwXanB6suWayCMN"
      ]
    }
  }
]
}
}
[root@DeltaUser1 DeltaUser1.conf]#

```



```
DeltaUser1
[root@DeltaUser1 DeltaUser1.conf]# gettx 209153f7de299922b0baa7930c53f01e87c33681033a177ef2bdbe587af2ac7e
{
  "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": "031573f0dfb96060fef261b127e1fd24e670ec4a55ddecf25acd53d614fb7df
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]#
```

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.

```
299922b0baa7930c53f01e87c33681033a177ef2bdbe587af2ac7e",
299922b0baa7930c53f01e87c33681033a177ef2bdbe587af2ac7e",
```

```
2000101",
967295
```

```
0000,
```

```
{
f0dfb96060fef261b127e1fd24e670ec4a55ddecf25acd53d614fb7dff
```

```
73f0dfb96060fef261b127e1fd24e670ec4a55ddecf25acd53d614fb7d
```

```
ey",
```

```
BGhBDQhEfsxjGAv6YrbG5d"
```

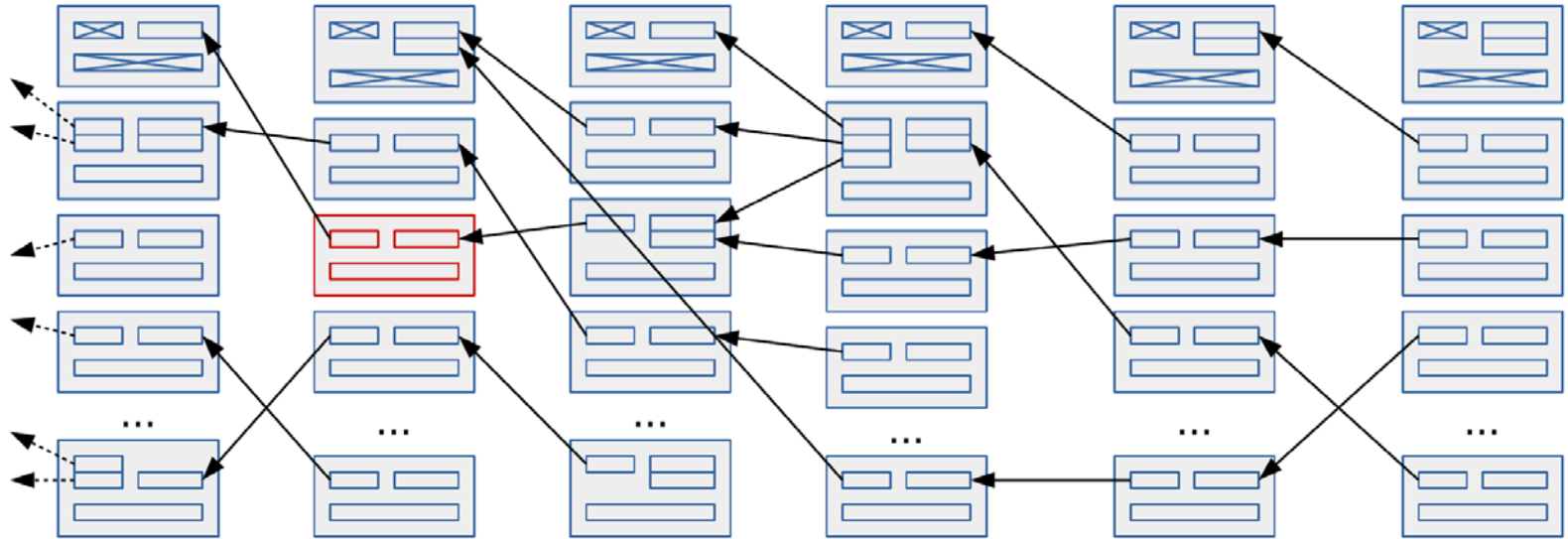
```
0000,
```

```
{
URN aa21a9ede2f61c3f71d1defd3fa999dfa36953755c690689799962
```

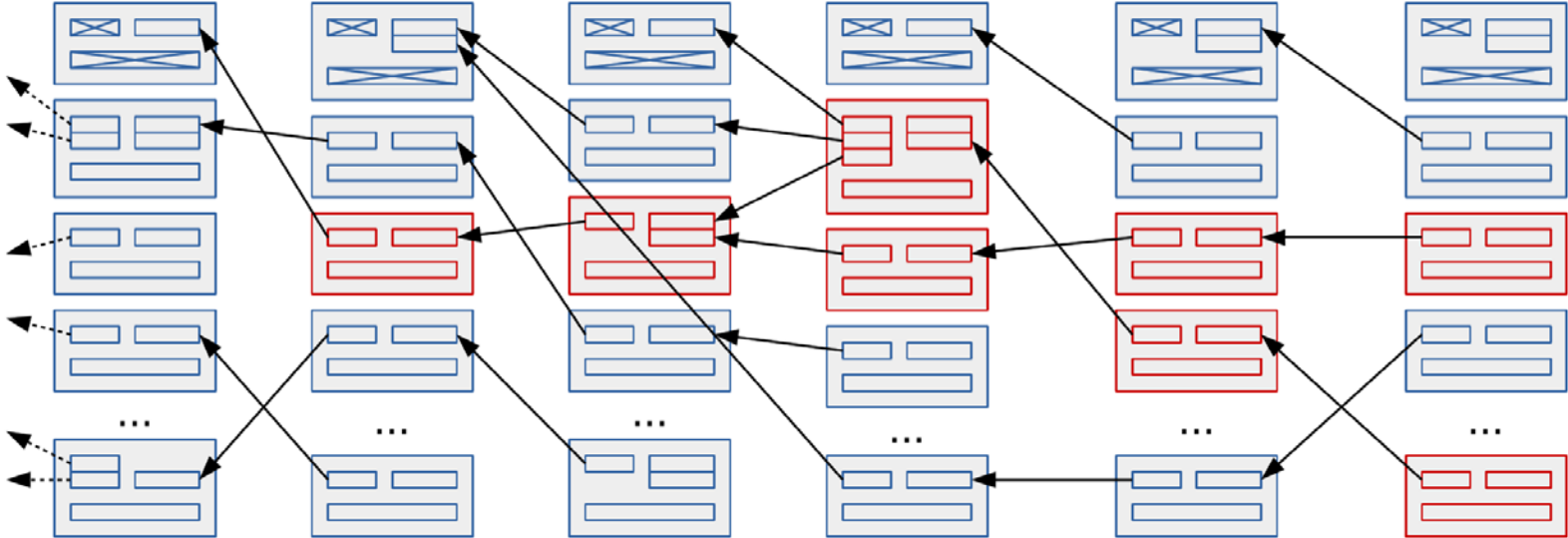
```
21a9ede2f61c3f71d1defd3fa999dfa36953755c690689799962b48beb
```

```
ata"
```

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

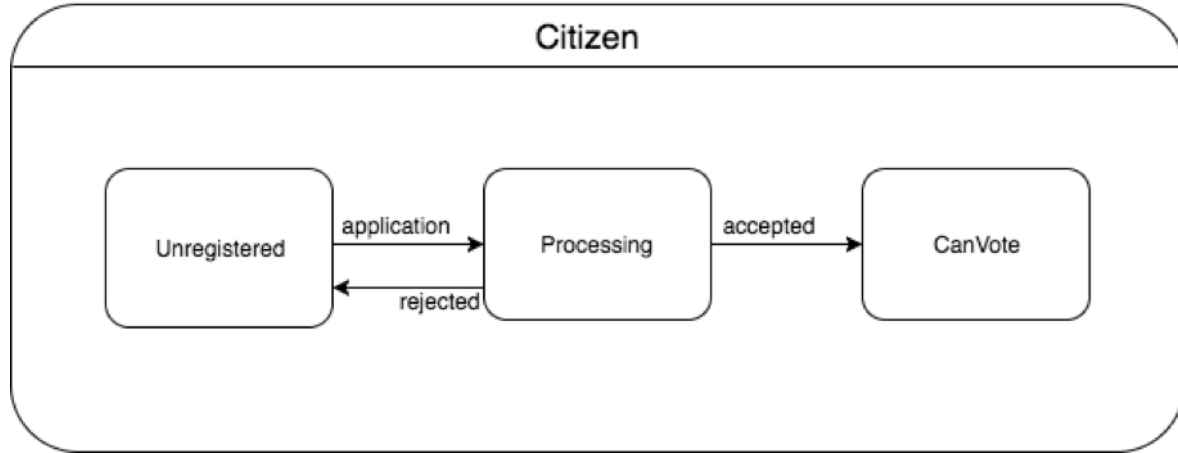
```
contract C {  
  state S1 {  
    transaction t(int x) {  
      ->S2(x);  
    }  
  }  
  
  state S2 {  
    int x1;  
    S2(int x) {  
      x1 = x;  
      ->S3(x1);  
    }  
  }  
  
  state S3 {  
    ...  
  }  
}
```

```
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

