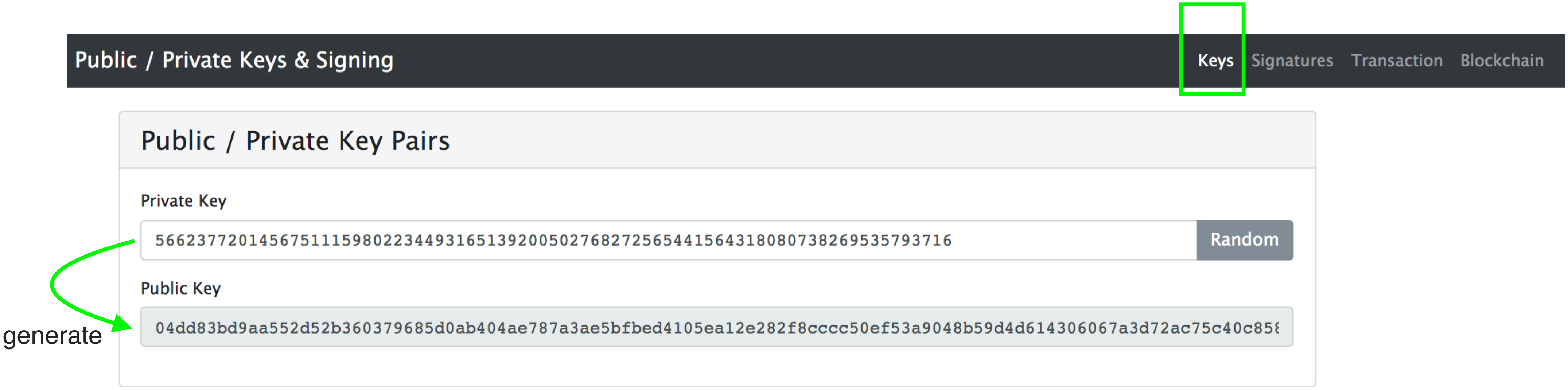
https://anders.com/blockchain/public-private-keys/

Some guy can manipulate by 擅自 sending money from others. To avoid such behavior, use public-private key pair.



Public / Private Key Pairs

Private Key

56623772014567511159802234493165139200502768272565441564318080738269535793716

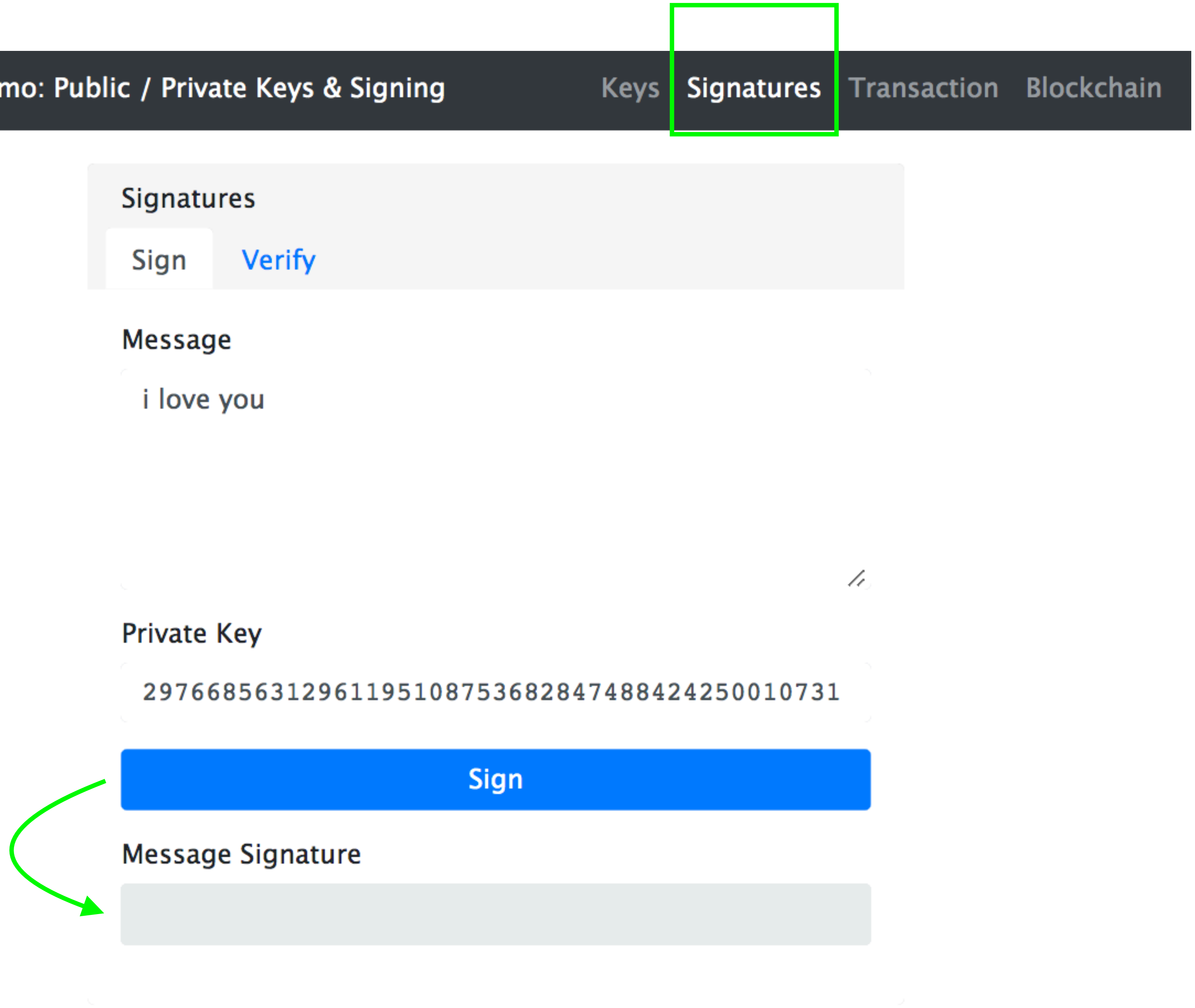
Public Key

04dd83bd9aa552d52b360379685d0ab404ae787a3ae5bfbed4105ea12e282f8cccc50ef53a9048b59d4d614306067a3d72ac75c40c85

generate

Private key: keep it private.
Public key: public version of private key, but the public key doesn't reveal what private key is. Let everyone know public key.

Public key: 实际是 address，不用去一个 centralized 机构申请，而是自己生成一个 public key，其他人就能付给你钱了。



Message

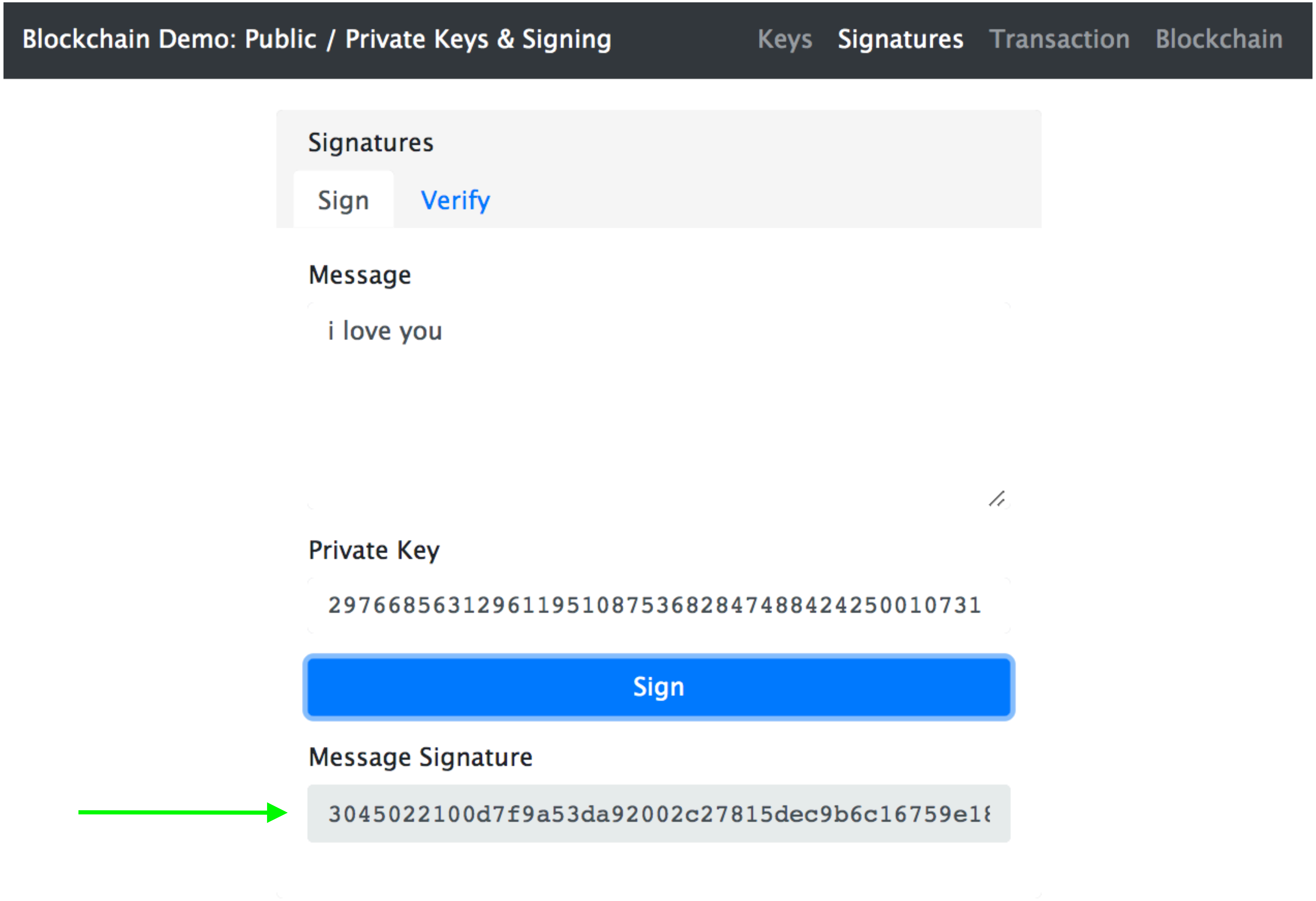
i love you

Private Key

29766856312961195108753682847488424250010731

Message Signature

1) message + private key —> message signature



Message

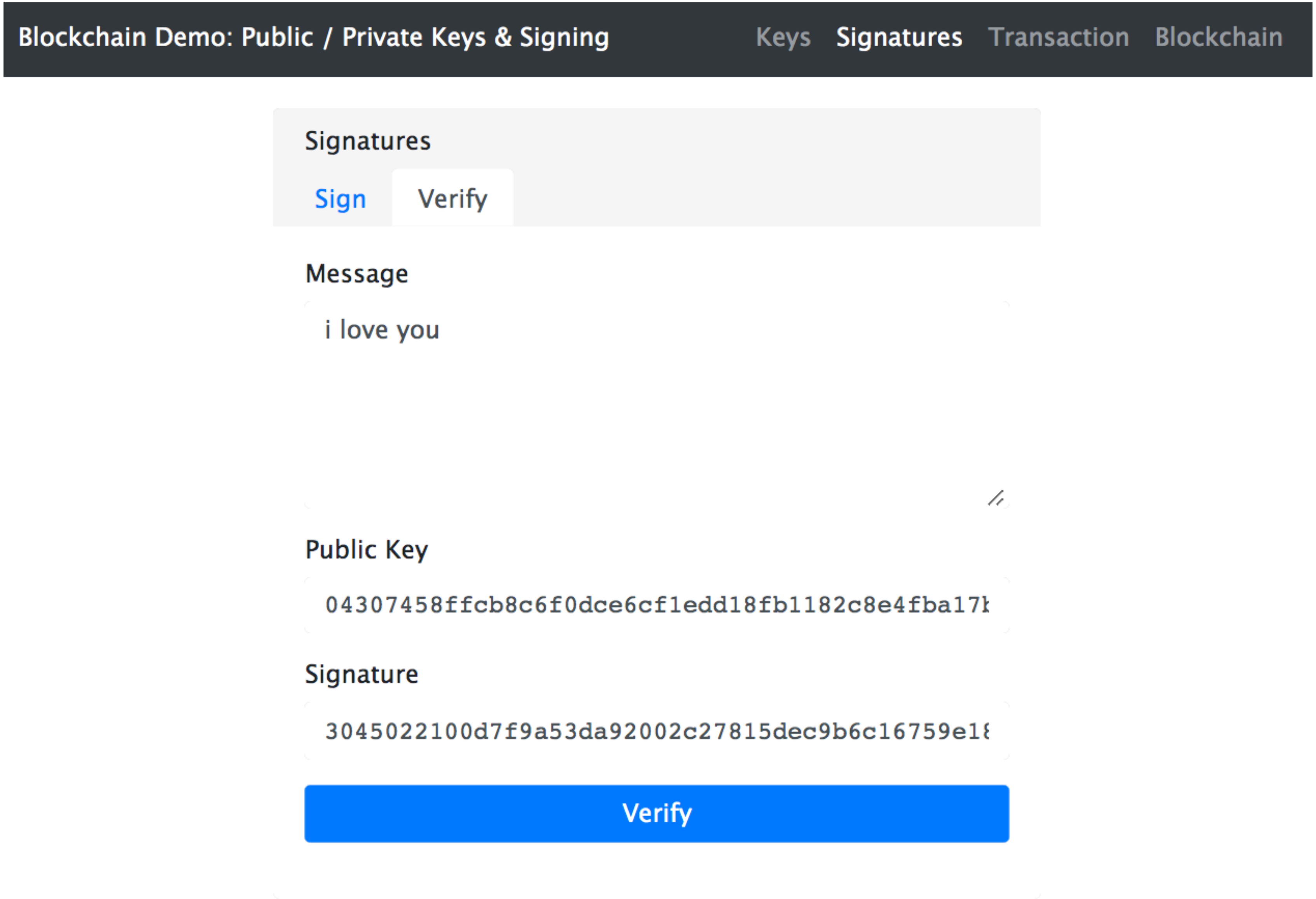
i love you

Private Key

29766856312961195108753682847488424250010731

Message Signature

3045022100d7f9a53da92002c27815dec9b6c16759e18



Message

i love you

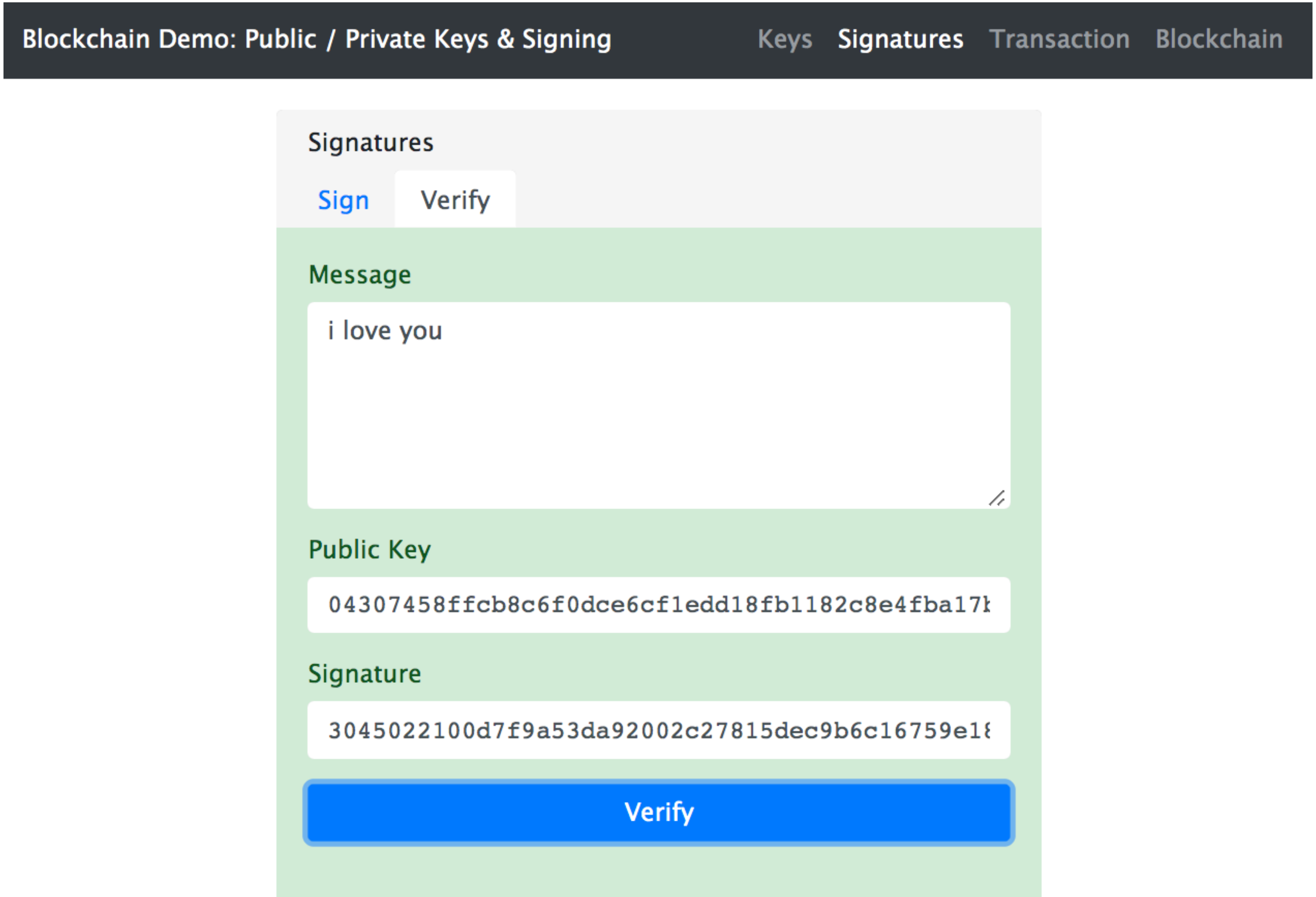
Public Key

04307458ffcb8c6f0dce6cf1edd18fb1182c8e4fba17b

Signature

3045022100d7f9a53da92002c27815dec9b6c16759e18

2) 由 message + signature 来验证：此交易是不是持有private key



Signatures

Message

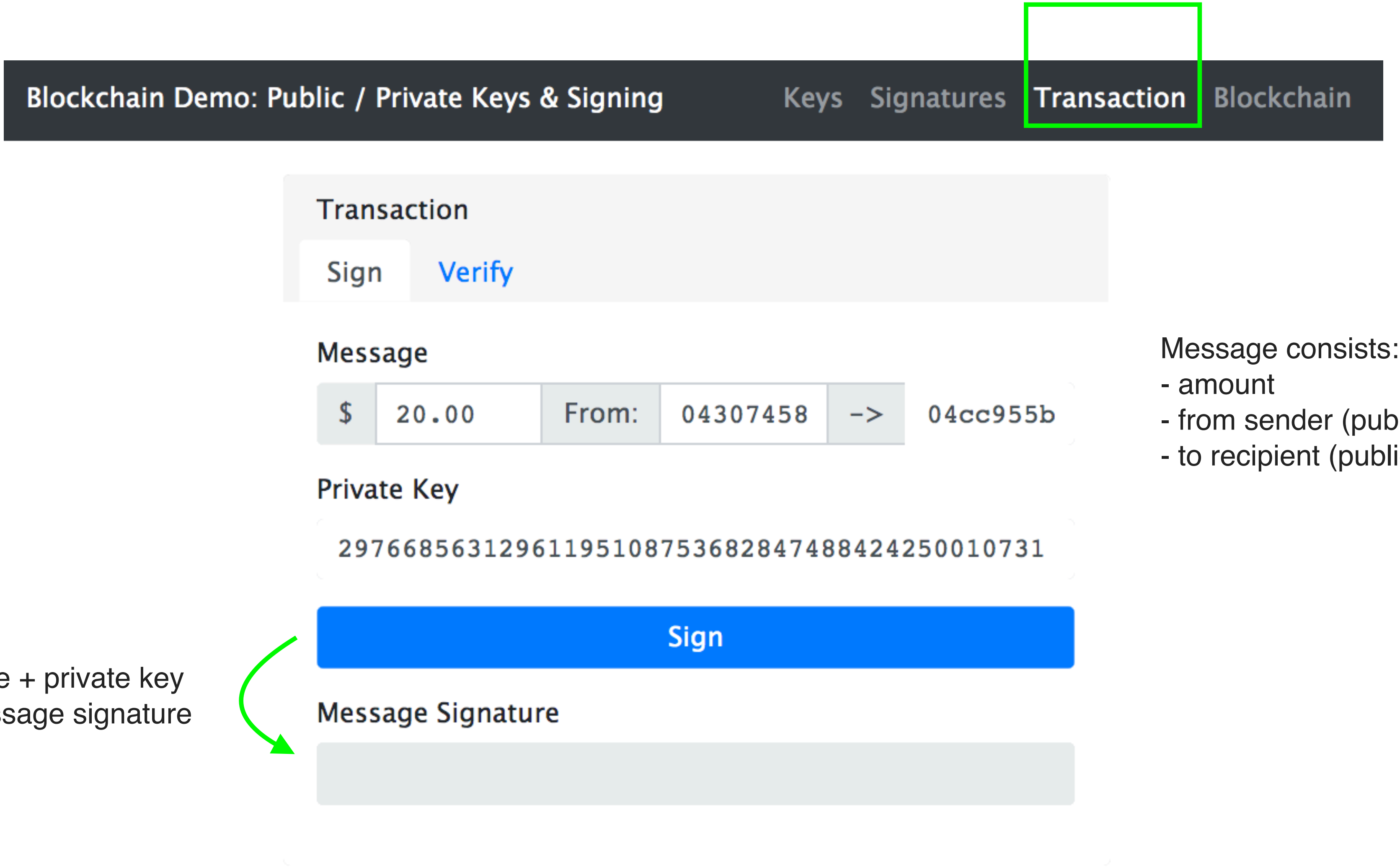
i love you

Public Key

04307458ffcb8c6f0dce6cf1edd18fb1182c8e4fba17

Signature

3045022100d7f9a53da92002c27815dec9b6c16759e1



Transaction

Message

$ 20.00 From: 04307458 -> 04cc955b

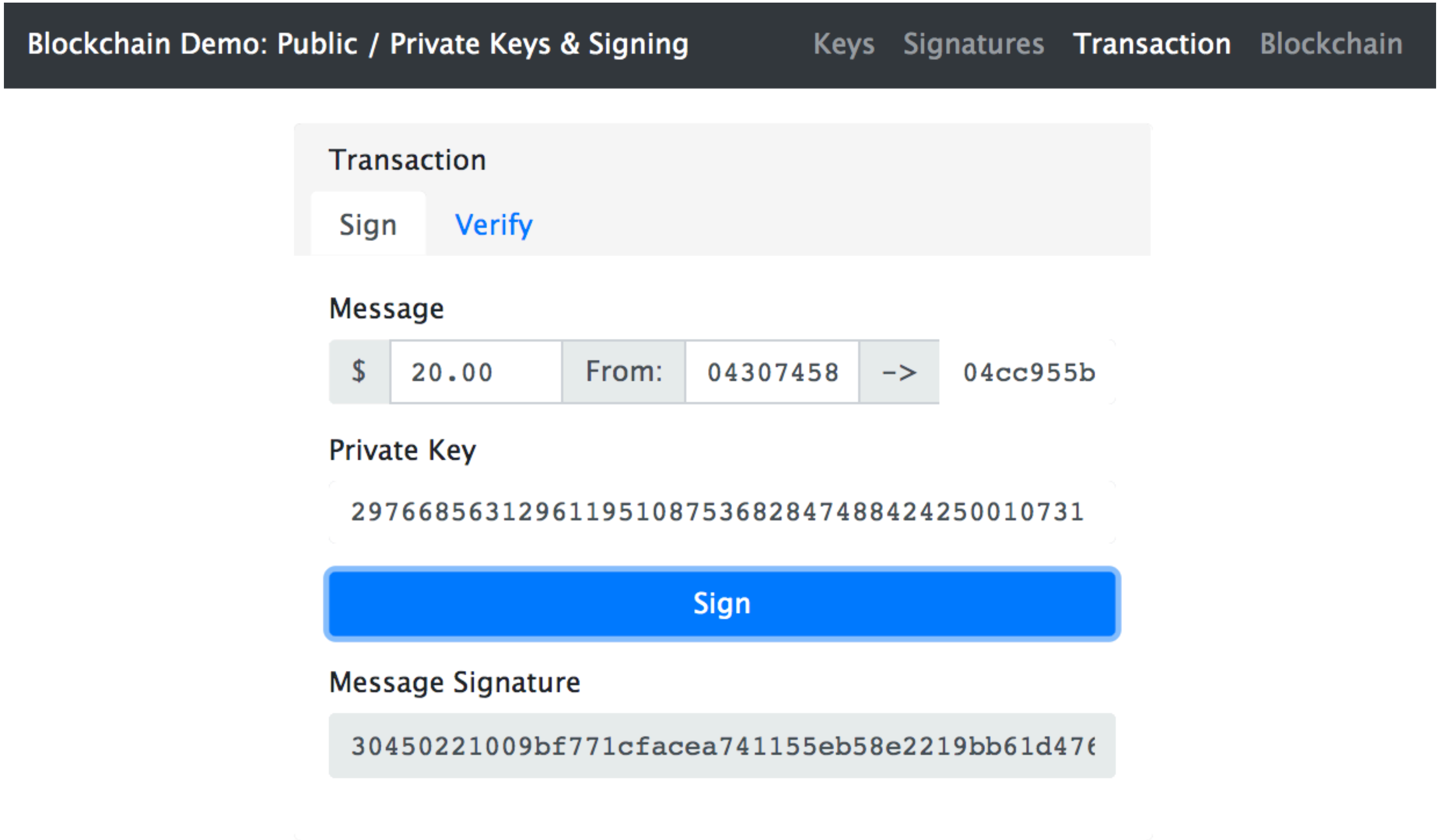
Private Key

29766856312961195108753682847488424250010731

Message Signature

Message consists:
- amount
- from sender (public key)
- to recipient (public key)

message + private key
—> message signature



Transaction

Message

$ 20.00 From: 04307458 -> 04cc955b

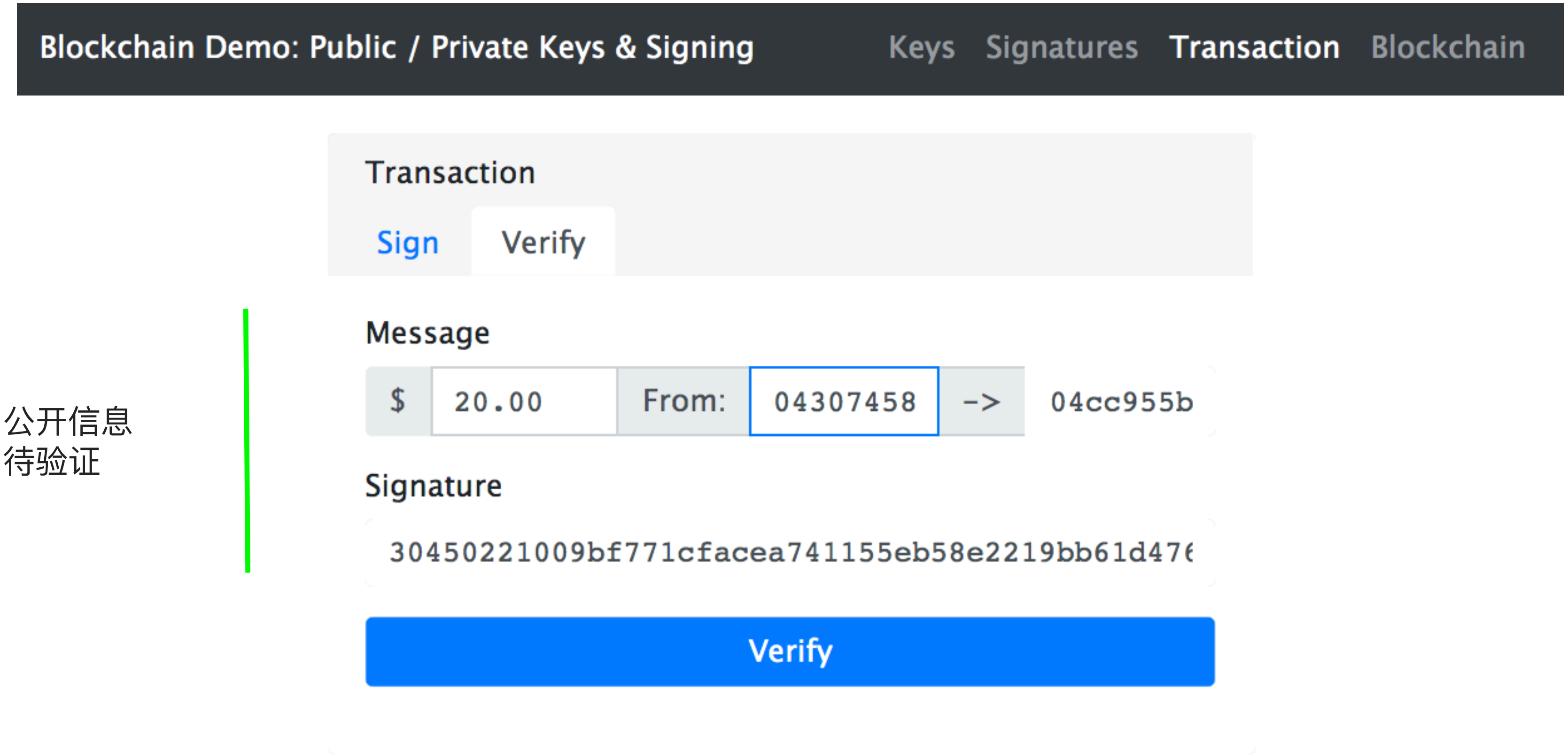
Private Key

29766856312961195108753682847488424250010731

Message Signature

30450221009bf771cfacea741155eb58e2219bb61d47

公开信息
待验证



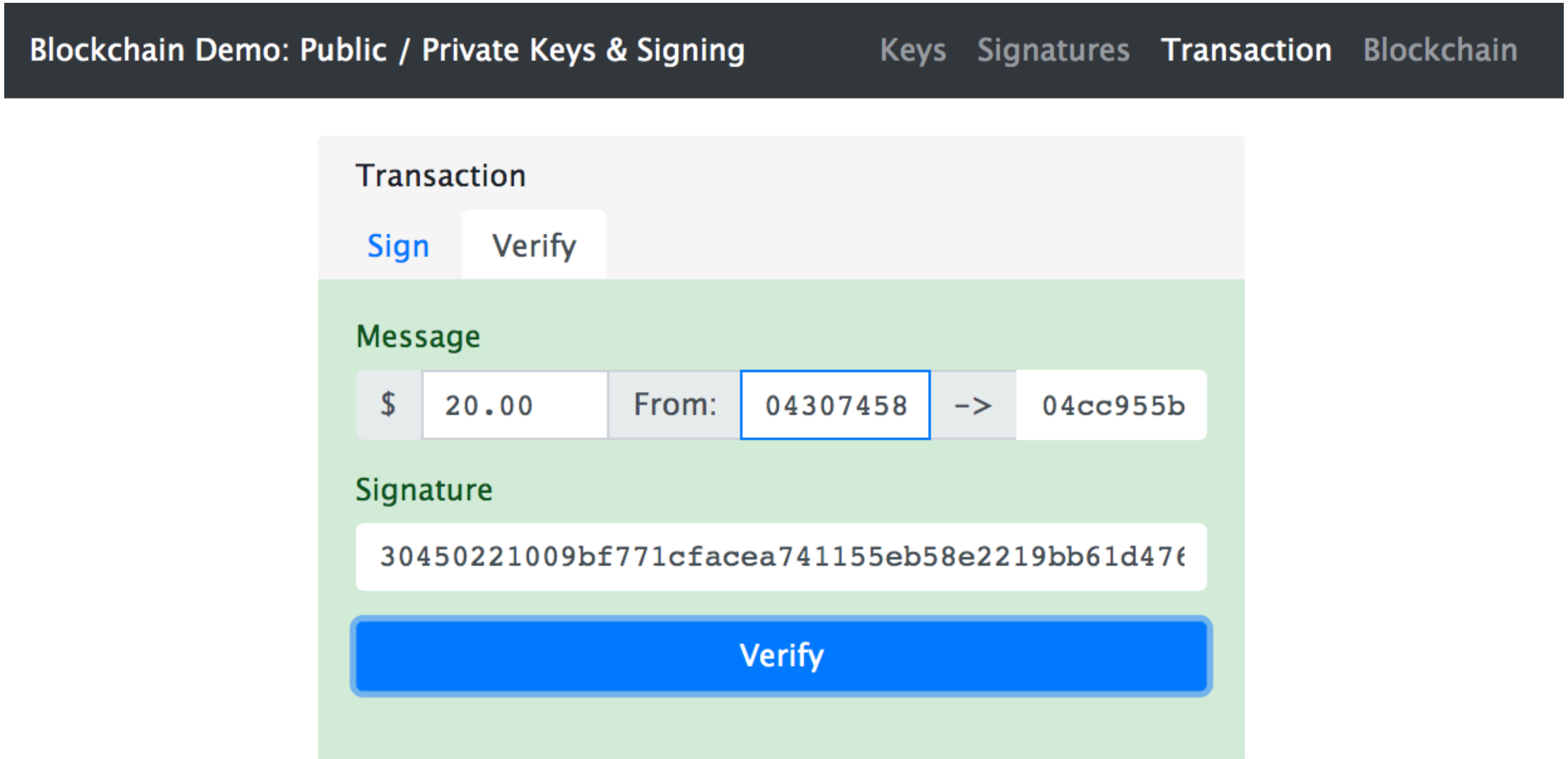
Transaction

Message

$ 20.00 From: 04307458 -> 04cc955b

Signature

30450221009bf771cfacea741155eb58e2219bb61d47



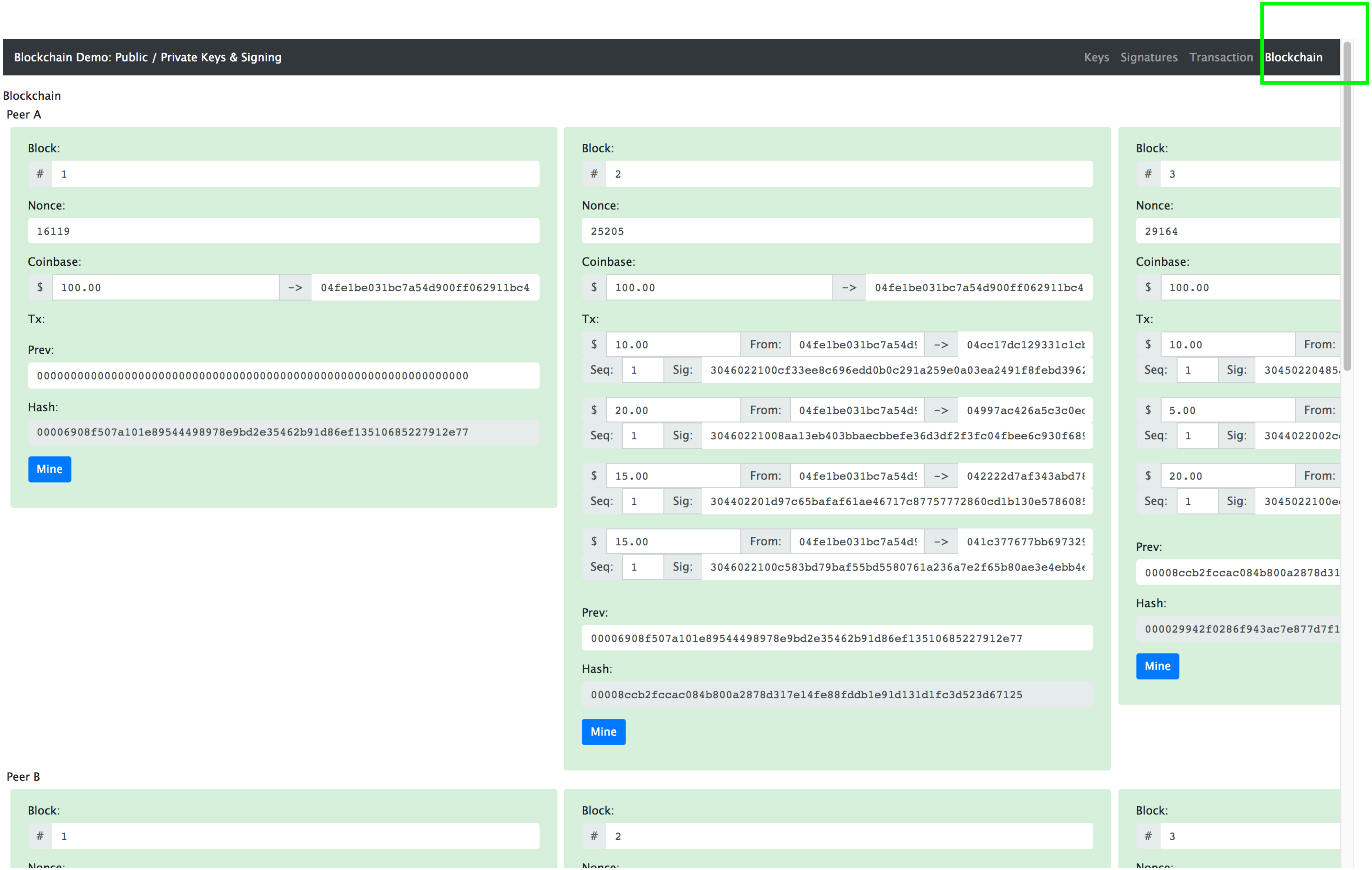
Message

$ 20.00 From: 04307458 -> 04cc955b

Signature

30450221009bf771cfacea741155eb58e2219bb61d47

验证成功：只有持有private key的人send money，这个交易才能被验证。
而不是别的想manipulate的人。



Blockchain

Peer A

Block:
# 1

Nonce:
16119

Coinbase:
$ 100.00 -> 04fe1be031bc7a54d900ff062911bc4

Tx:

Prev:
0000000000000000000000000000000000000000000000000000000000000000

Hash:
00006908f507a101e89544498978e9bd2e35462b91d86ef13510685227912e77

Mine

Block:
# 2

Nonce:
25205

Coinbase:
$ 100.00 -> 04fe1be031bc7a54d900ff062911bc4

Tx:
$ 10.00 From: 04fe1be031bc7a54d -> 04cc17dc129331c1c
Seq: 1 Sig: 3046022100cf33ee8c696edd0b0c291a259e0a03ea2491f8febd396

$ 20.00 From: 04fe1be031bc7a54d -> 04997ac426a5c3c0e
Seq: 1 Sig: 30460221008aa13eb403bbaecbbefe36d3df2f3fc04fbee6c930f68

$ 15.00 From: 04fe1be031bc7a54d -> 042222d7af343abd7
Seq: 1 Sig: 304402201d97c65bafaf61ae46717c87757772860cd1b130e578608

$ 15.00 From: 04fe1be031bc7a54d -> 041c377677bb69732
Seq: 1 Sig: 3046022100c583bd79baf55bd5580761a236a7e2f65b80ae3e4ebb4

Prev:
00006908f507a101e89544498978e9bd2e35462b91d86ef13510685227912e77

Hash:
00008ccb2fccac084b800a2878d317e14fe88fddb1e91d131d1fc3d523d67125

Mine

Block:
# 3

Nonce:
29164

Coinbase:
$ 100.00

Tx:
$ 10.00 From:
Seq: 1 Sig: 30450220485

$ 5.00 From:
Seq: 1 Sig: 3044022002c

$ 20.00 From:
Seq: 1 Sig: 3045022100e

Prev:
00008ccb2fccac084b800a2878d31

Hash:
000029942f0286f943ac7e877d7f1

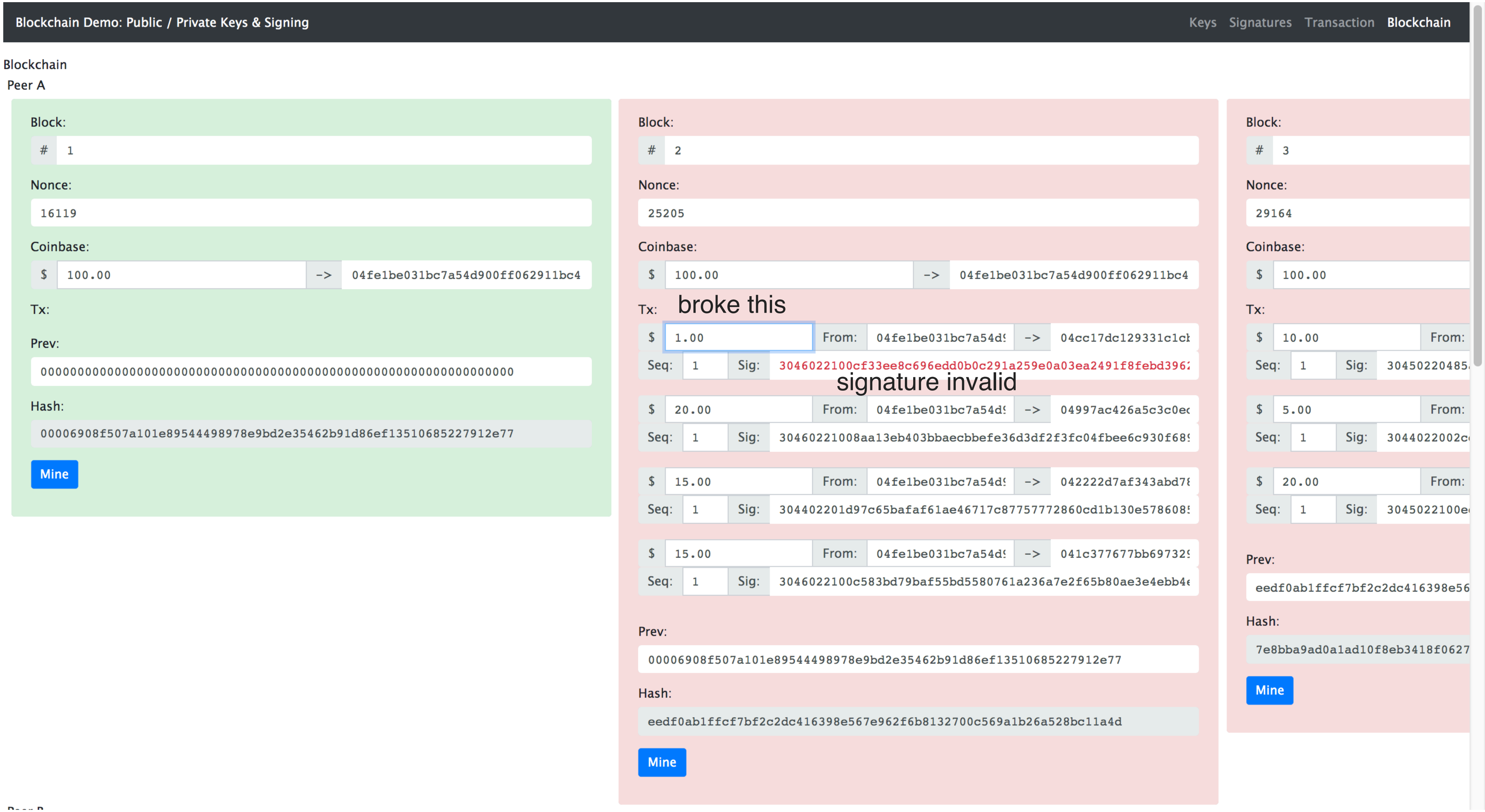
Mine

Peer B

Block:
# 1

Block:
# 2

Block:
# 3



Blockchain

Peer A

Block:
# 1

Nonce:
16119

Coinbase:
$ 100.00 -> 04fe1be031bc7a54d900ff062911bc4

Tx:

Prev:
0000000000000000000000000000000000000000000000000000000000000000

Hash:
00006908f507a101e89544498978e9bd2e35462b91d86ef13510685227912e77

Block:
# 2

Nonce:
25205

Coinbase:
$ 100.00 -> 04fe1be031bc7a54d900ff062911bc4

Tx: broke this

$ 1.00 From: 04fe1be031bc7a54d -> 04cc17dc129331c1c
Seq: 1 Sig: 3046022100cf33ee8c696edd0b0c291a259e0a03ea2491f8febd396

signature invalid

$ 20.00 From: 04fe1be031bc7a54d -> 04997ac426a5c3c0e
Seq: 1 Sig: 30460221008aa13eb403bbaecbbefe36d3df2f3fc04fbee6c930f68

$ 15.00 From: 04fe1be031bc7a54d -> 042222d7af343abd7
Seq: 1 Sig: 304402201d97c65bafaf61ae46717c87757772860cd1b130e578608

$ 15.00 From: 04fe1be031bc7a54d -> 041c377677bb69732
Seq: 1 Sig: 3046022100c583bd79baf55bd5580761a236a7e2f65b80ae3e4ebb4

Prev:
00006908f507a101e89544498978e9bd2e35462b91d86ef13510685227912e77

Hash:
eedf0ab1ffcf7bf2c2dc416398e567e962f6b8132700c569a1b26a528bc11a4d

Block:
# 3

Nonce:
29164

Coinbase:
$ 100.00

Tx:

$ 10.00 From:
Seq: 1 Sig: 3045022048

$ 5.00 From:
Seq: 1 Sig: 3044022002c

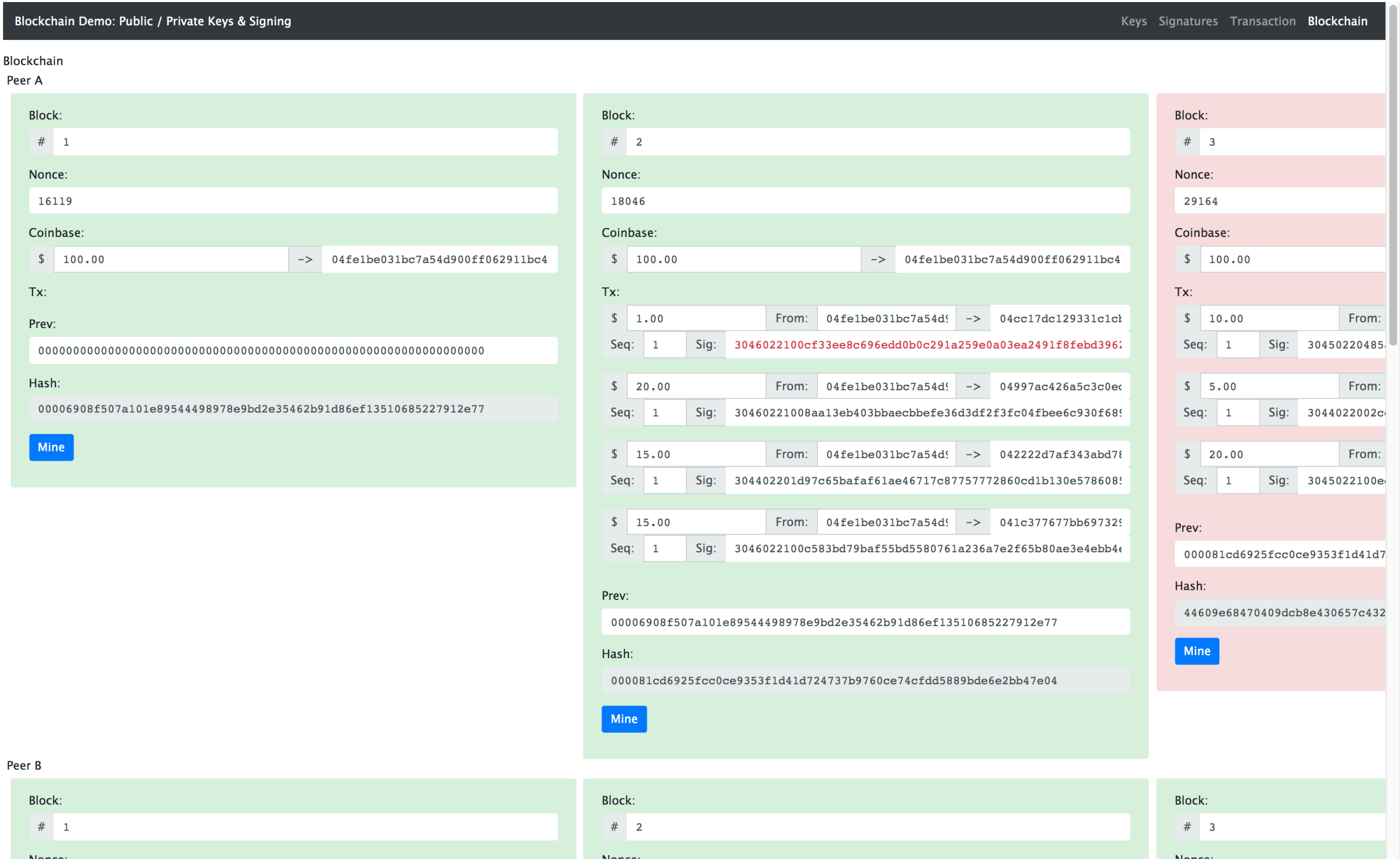
$ 20.00 From:
Seq: 1 Sig: 3045022100e

Prev:
eedf0ab1ffcf7bf2c2dc416398e56

Hash:
7e8bba9ad0a1ad10f8eb3418f0627

Peer B

re-mine the block, but the signature still invalid
because the miners don't have my private key, they only have public keys



Blockchain Demo: Public / Private Keys & Signing

Blockchain

Peer A

Block:
1

Nonce:
16119

Coinbase:
$ 100.00 -> 04fe1be031bc7a54d900ff062911bc4

Tx:

Prev:
0000000000000000000000000000000000000000000000000000000000000000

Hash:
00006908f507a101e89544498978e9bd2e35462b91d86ef13510685227912e77

Block:
2

Nonce:
18046

Coinbase:
$ 100.00 -> 04fe1be031bc7a54d900ff062911bc4

Tx:
$ 1.00 From: 04fe1be031bc7a54d -> 04cc17dc129331c1c
Seq: 1 Sig: 3046022100cf33ee8c696edd0b0c291a259e0a03ea2491f8febd396

$ 20.00 From: 04fe1be031bc7a54d -> 04997ac426a5c3c0e
Seq: 1 Sig: 3046022100 8aa13eb403bbaecbbefe36d3df2f3fc04fbee6c930f68

$ 15.00 From: 04fe1be031bc7a54d -> 042222d7af343abd7
Seq: 1 Sig: 304402201d97c65bafaf61ae46717c87757772860cd1b130e578608

$ 15.00 From: 04fe1be031bc7a54d -> 041c377677bb69732
Seq: 1 Sig: 3046022100c583bd79baf55bd5580761a236a7e2f65b80ae3e4ebb4

Prev:
00006908f507a101e89544498978e9bd2e35462b91d86ef13510685227912e77

Hash:
000081cd6925fcc0ce9353f1d41d724737b9760ce74cfdd5889bde6e2bb47e04

Block:
3

Nonce:
29164

Coinbase:
$ 100.00

Tx:
$ 10.00 From:
Seq: 1 Sig: 30450220485

$ 5.00 From:
Seq: 1 Sig: 3044022002c

$ 20.00 From:
Seq: 1 Sig: 3045022100e

Prev:
000081cd6925fcc0ce9353f1d41d7

Hash:
44609e68470409dcb8e430657c432

Peer B

Block:
1

Nonce:

Block:
2

Nonce:

Block:
3

Nonce:

In that way, we can ensure the transaction is post by the person who really have the money and only that person.