Feathercoin's 51% Attack

Double Spending case study

BTC Donations

Corrections, Additions, Technical Revisions or comments are welcome:
max_miner <at> yahoo <dot> com

< If you find the information presented worthy of your support, please donate to these BTC/LTC addresses >

LTC Donations

19VGAnAc6pahc1BUfjaobPZMHNjumDRuK

LRu2pVJu5JGJxKR27gNi9NBYSdCzig8uoC

THE FORKS

Counterfeit Block Generation

Legitimate Blockchain

Difficulty had decreased from 133.065 to 94.087 one week earlier at height 33264 (2013-06-01) Total hashrate available had been increasing

time (UTC) | avgIntervalSinceLast | netHashPerSecond
Generation Address

14:16:08 | 7 | 57.7G
6sdtMFynKZ

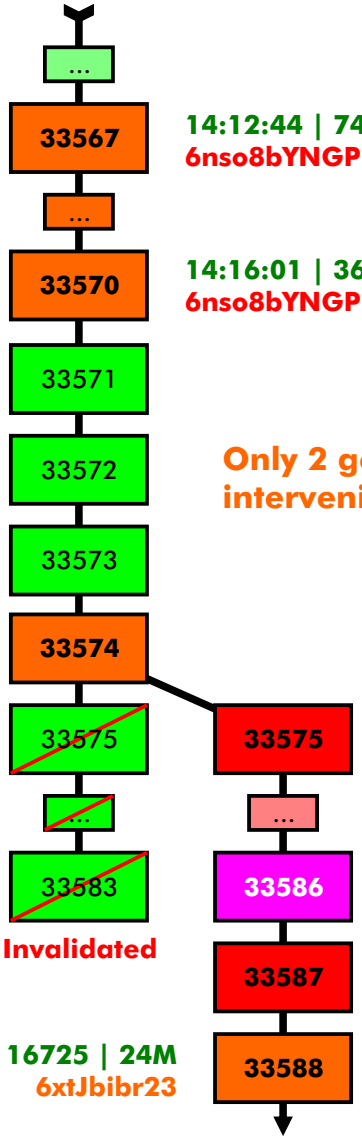
14:21:00 | 292 | 1.4G
6xtJbibr23

14:22:03 | 63 | 6.4G
6xtJbibr23

14:37:42 | 939 | 430M
6xtJbibr23

15:34:19 | ??? | ???
1H7kMSqqit

Several pools/miners affected, the different addresses can still be determined by following this orphaned blockchain



Attack Stage 1 (1st Fork)

14:12:44 | 749 | 539M
6nso8bYNGP

First appearance in the network of Generation address used in the attack (6nso8bYNGP)

14:16:01 | 36 | 11G
6nso8bYNGP

These 4 blocks plus the next 13 would total 17 blocks generated and credited to cited address in this first stage of the attack

Only 2 generation addresses in the intervening time until the fork itself

14:15:29 | -1333 | Infinity
6nso8bYNGP

Notice the timewarp
Next blocks would be logged with similar irregularity

14:15:46 | -48 | Infinity
6nso8bYNGP

33586 is the only block with a registered transaction

14:15:45 | -1 | Infinity
6nso8bYNGP

After 13 blocks Stage 1 ends

18:54:30 | 16725 | 24M
6xtJbibr23

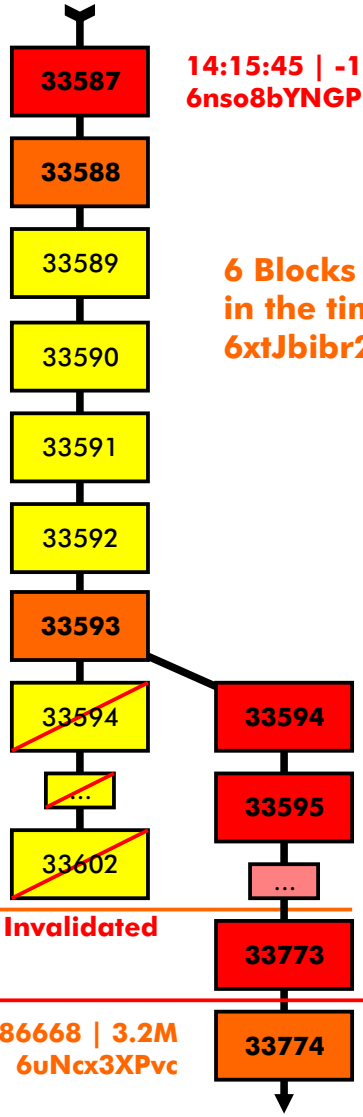
The fork is opened and followed up after the same generating address (6xtJbibr23)

THE FORKS

Counterfeit Block Generation

Compromised Blockchain

time (UTC) | avgIntervalSinceLast | netHashPerSecond
Generation Address



6 Blocks generated by 2 addresses only
in the timespan of ~66 minutes, up to the 2nd Fork:
6xtJbibr23 and 6uNcx3XPvc

Attack Stage 2 (2nd Fork)

18:54:31 | -3949 | Infinity
6tbxs8oiku

Notice again the timewarp
Address is now 6tbxs8oiku

18:54:36 | 5 | 81G
6tbxs8oiku

Next blocks would be logged
with similar irregularities
at an impossible fast rate

After 180 blocks < 3 minutes
Stage 2 ends

Again (!) the fork is opened and followed up
after the same generating address
(this time by 6uNcx3XPvc)

Block 33767 = Diff. **94.087**

Block 33768 = Diff. **66.526**

Day of the Attack (Feathercoin is 7 weeks old)

Sunday 9 June

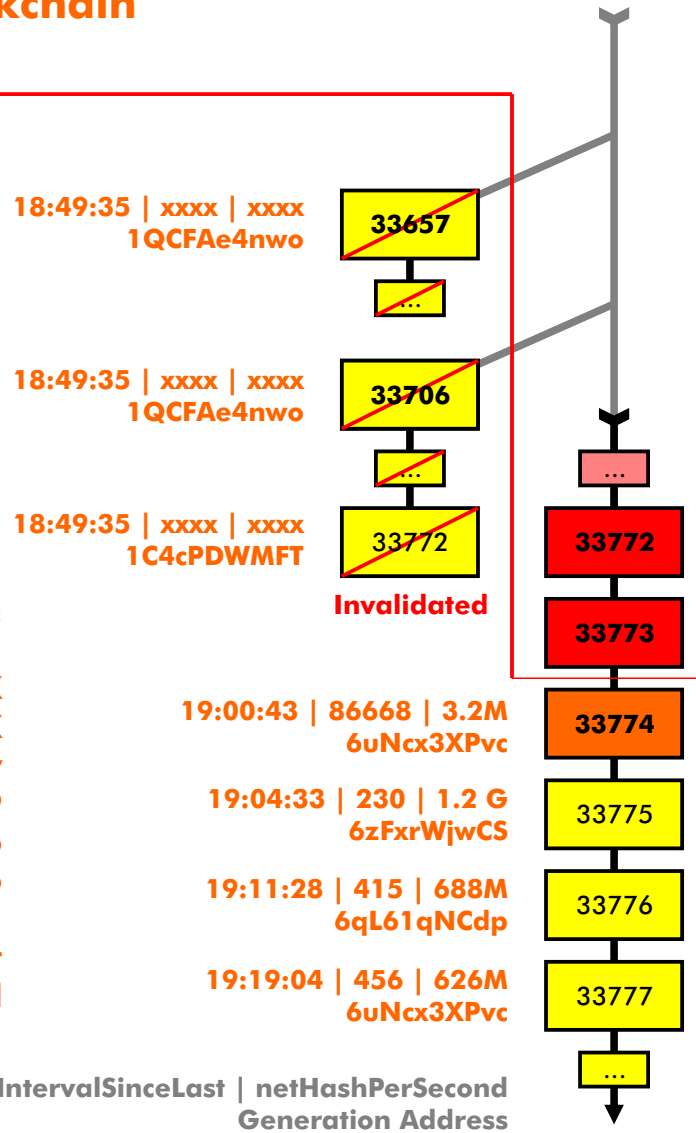
THE FORKS

Counterfeit Block Generation

Compromised Blockchain

Day of the Attack (Feathercoin is 7 weeks old)

Sunday 9 June



Attacker tampered with timestamps
Attacker tampered the computing difficulty
Attacker generated 3'400 FTC + 36'000 FTC

Combined amount = 39'400 FTC
= 0.58% of total coins at height 33773

Attacker's addresses and transaction made in block:

6nso8bYNGP
3'400

6tbxs8oiku
36'000

33586

Total <value out> in transaction = 580K FTC

18:54:36 | 5 | 80G
6tbxs8oiku

18:56:15 | -3 | Infinity
6tbxs8oiku

The whole legitimate network had to wait until 19h on June 9 for blocks to become accepted as valid (~31h since attack begun)

Considerable amounts of FTC were transacted with the first blocks found after the merge
Pending transactions that survived the network splits

Several other forks would occur:

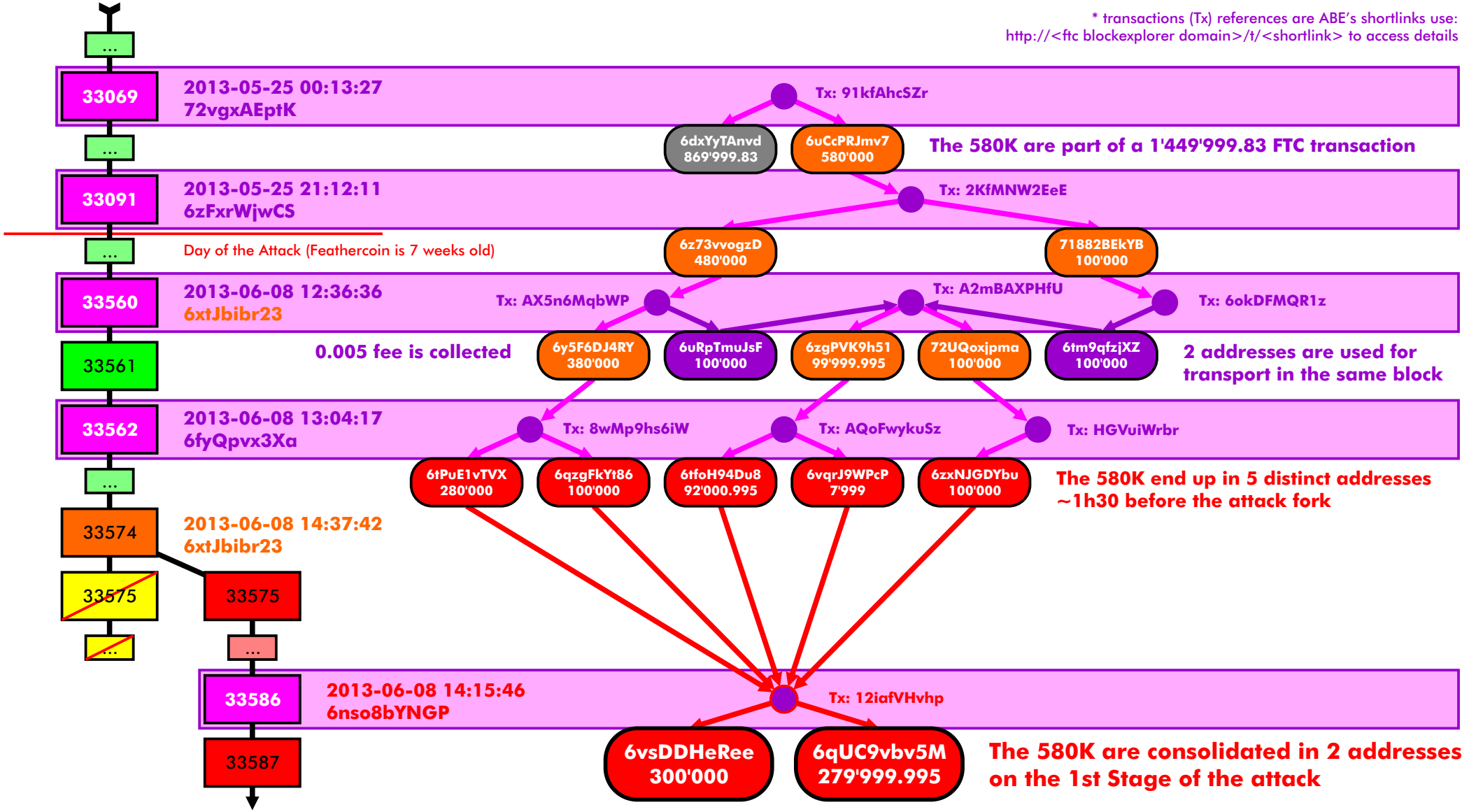
33603 against 1L9rpCRp5X
33616 against 1L9rpCRp5X
33633 against 1MXX4zZuFv
33644 against 15nUxZBmR9
33657 against 1QCFAe4nwo
33706 against 1QCFAe4nwo

It was on some of these forks that double spending was attempted

Compromised Blockchain

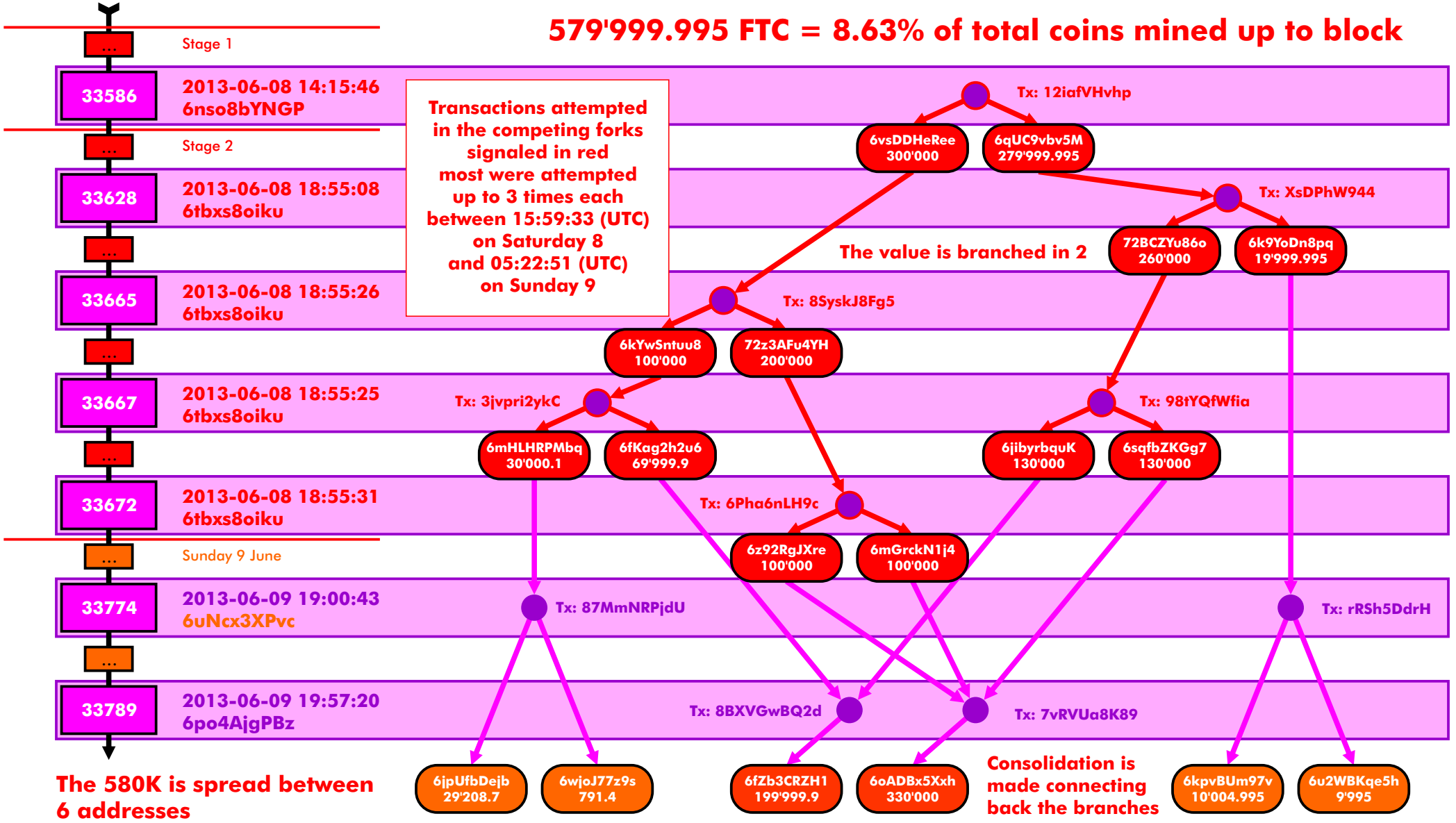
ASSOCIATED FTC MOVEMENTS

580K Origin addresses



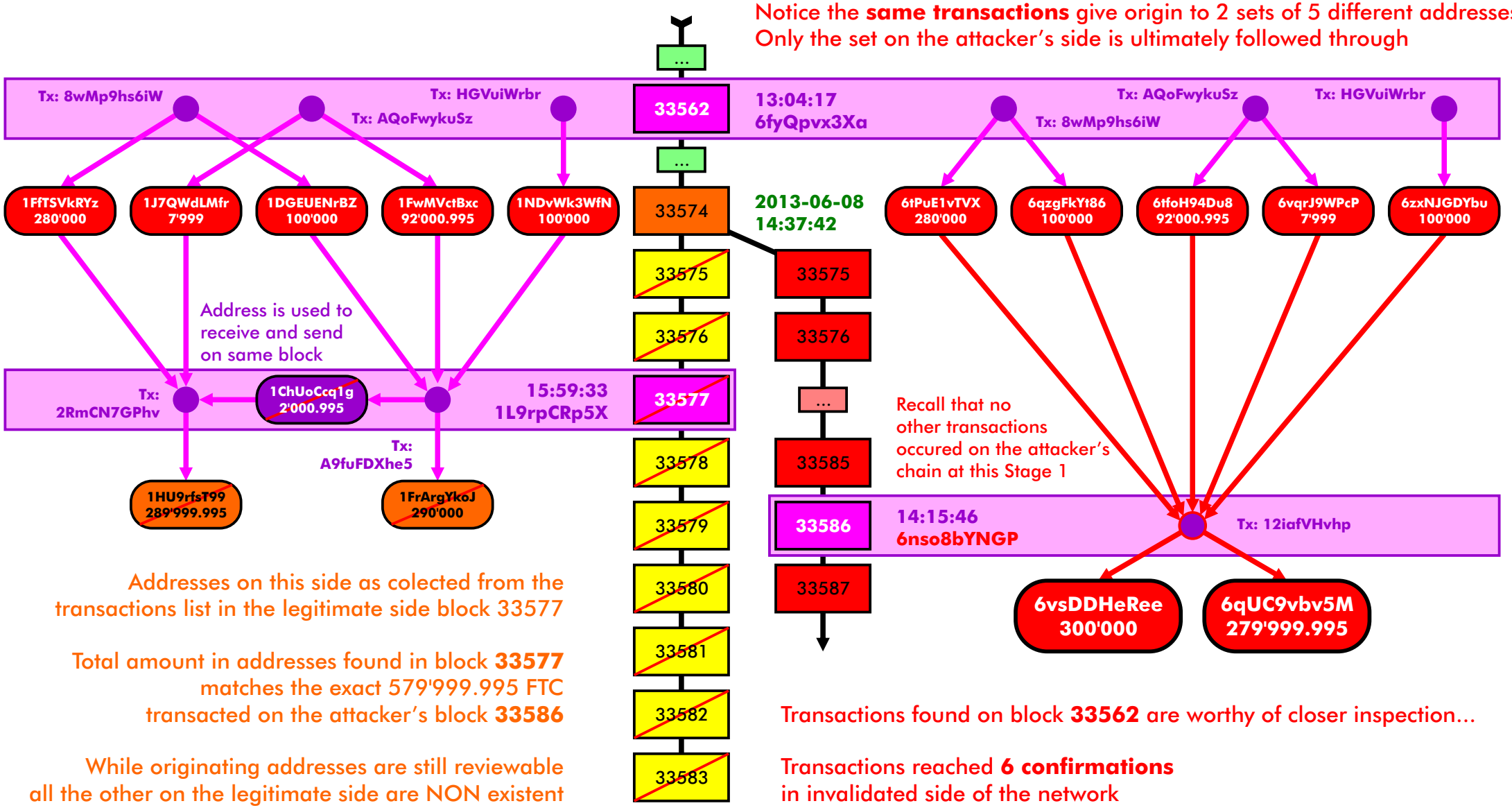
ASSOCIATED FTC MOVEMENTS

580K Destination addresses



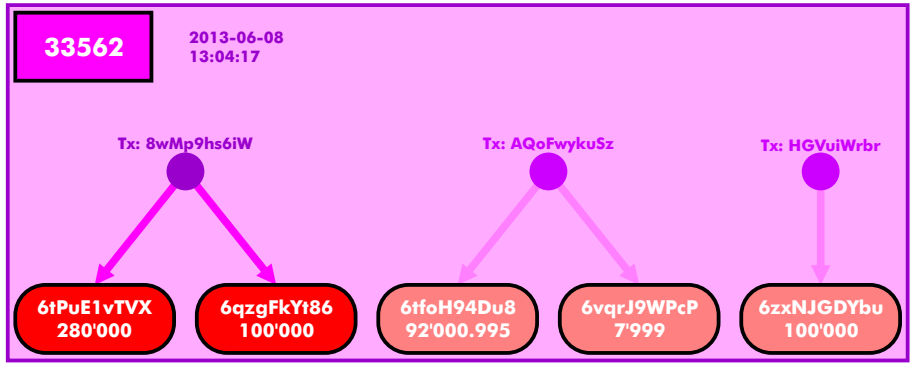
ASSOCIATED FTC TRANSACTIONS

580K 1st Double-Spend Attempt



ASSOCIATED FTC TRANSACTIONS

580K PRE-Fork Ambiguity



8wMp9hs6iW:

1. Block 33562
2. Input = 380K
3. Output = 760K | 2x Input !
4. Fee = -380K | Negative value !
5. Input value split into 2 output transactions twice to each address
5.1 Prevailing transactions which are executed at **33586** (attacker's side)
5.2 Transactions attempted at **33577** (legitimate side), notice the addresses as registered under this transaction are the same in both sides

Must be noted that inspecting the Outputs via «Raw Transaction», **the duplication is NOT visible**

Remaining transactions **AQoFwykuSz** and **HGVuiWrbr** yield similar characteristics as above

Transaction 8wMp9hs6iW

Short Link: http://explorer.feathercoin.com/t/8wMp9hs6iW

Information

Hash:	d1733c20a5822bf228f561b25910c59a7aed9fe6b756b1342401e999f8f04678
Appeared in:	Feathercoin 33562 (2013-06-08 13:04:17) 1
Number of inputs:	1 (Jump to inputs)
Total in:	380000 2
Number of outputs:	4 (Jump to outputs)
Total out:	760000 3
Size:	226 bytes
Fee:	-380000 4

Raw transaction

Inputs

Index	Previous output	Amount	From address	ScriptSig
0	fb2e856758...:0	380000	6y5F6DJ4RYUucqgD5gqR1DMxphvFtJt76f	72:3045...bc01 33:03ed...dd68

Outputs

Index	Redeemed at input	Amount	To address	ScriptPubKey
0	00c7f8ee24...:0	280000	6tPuE1vTVXGQ5nxH7NHHWp1n2ZxdQ58cZ3	DUP HASH160 20:a0d7...bc7c EQUALVERIFY CHECKSIG
.01	25a783530d...:1	280000	6tPuE1vTVXGQ5nxH7NHHWp1n2ZxdQ58cZ3	DUP HASH160 20:a0d7...bc7c EQUALVERIFY CHECKSIG
.2	00c7f8ee24...:1	100000	6qzgFkYt86DLbMaRNqshNR261NhB73R38z	DUP HASH160 20:8682...bc8b EQUALVERIFY CHECKSIG
1	f170e58642...:1	100000	6qzgFkYt86DLbMaRNqshNR261NhB73R38z	DUP HASH160 20:8682...bc8b EQUALVERIFY CHECKSIG

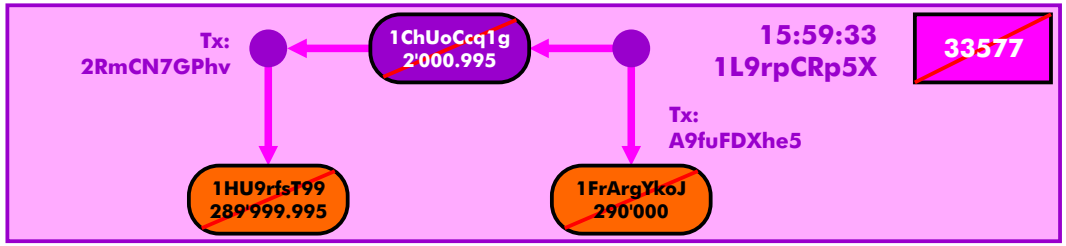
5

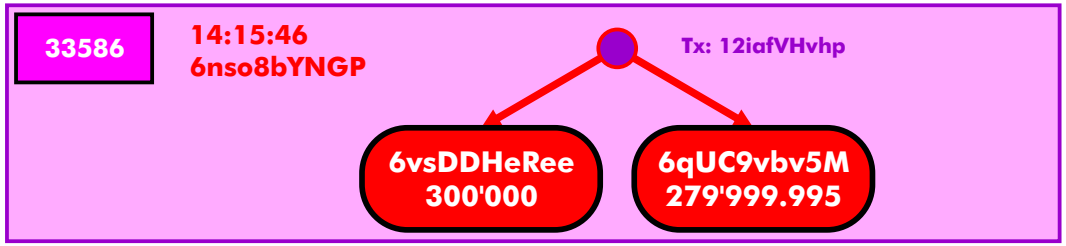
API (machine-readable pages)

BTC 19VGAnAc6pahc1BUfjaobPZMHNjumDRuK
LTC LRu2pVJu5JGJxKR27gNi9NBYSdCzig8uoC

ASSOCIATED FTC TRANSACTIONS

580K Competing Blocks





1. The attempted transactions **2.** The destination addresses

3. Prevailing transaction **4.** Prevailing addresses

Block 33577

Information

Hash:	9199d4f6043dc633ac64c5260d440780b56a712ef7667a4f1a23f0aae6265d20
Previous Block:	5b829c3484575b47671f1f96584d09f3d7b11a650aecbfb5437abcb08b8c9b60
Next Block:	af8d0abbea49a9059996c5a34a56b00643b2697e3ef85b50cc3a54874786552c
Transaction Merkle Root:	faa2491aa216a551f3625bec27f83312e993c67f611aa4f4a626838f5f81f9cb
Time:	1370707173 (2013-06-08 15:59:33)
Difficulty:	94.000000087 (Bits: 1c02b88b)
Nonce:	319330048
Transactions:	6
Value out:	583149.1930341
Average Coin Age:	22.0303 days
Coin-days Destroyed:	79300.46929379
Cumulative Coin-days Destroyed:	52.464%

Transactions

Transaction	Fee	Size (kB)	From (amount)	To (amount)
8b06100ed8...	0	0.12	Generation: 200 + 0.015 total fees	1L9rpCRp5X3nw9SmgsZvB8BGZDNTrqHS1K: 200.015
f170a58642...	0	0.522	1FwMVctBxc7z65TrBXeFGyQgE1CvQBYzV2: 92000.995 1DGEUENrBZj59HdD2yDEafD5CK5y4tKTSx: 100000 1NDvWk3WfNYLUhNs2JU3S4Rx8PB8LkrWHq: 100000	1ChUoCcq1g5rp1keSwTDfPPHR55uUPsRf5: 2000.995 1FrArgYkoJddhgstj6JULgtkQ1HqKaUqVZ: 290000
25a783530d...	0	0.489	1J7QWdLMfrbnRbF8SoMhxAo9t2yKfa7fMi: 7999 1FfTSVkRYzn8dj14mVcpj4CmDWMRMdj1YV: 280000 1ChUoCcq1g5rp1keSwTDfPPHR55uUPsRf5: 2000.995	1HU9rfaT99fpM1NzLyr9fSuwFAhZc8ZZtT: 289999.995

1 2

Block 33586

Information

Hash:	01381913866c2d92b73c398fa59f6ff00dee451bbcf1d78cb6fe50898257d5b8
Previous Block:	ad4d61681ff961735475e9ed6aa55748365abf00986e89da33563bf8db4ddda5
Next Block:	0e8c2edc6211f7a1ca70e160da36d19ad1da798f66b85a04f85258af5b7b070b
Transaction Merkle Root:	31995c3cdb8c0a59ec92ca26b69215e93322f9e029b223d903d5508ac800d67f
Time:	1370700946 (2013-06-08 14:15:46)
Difficulty:	94.000000087 (Bits: 1c02b88b)
Nonce:	716782080
Transactions:	2
Value out:	580199.995
Average Coin Age:	22.0085 days
Coin-days Destroyed:	28791.89789994
Cumulative Coin-days Destroyed:	52.4243%

Transactions

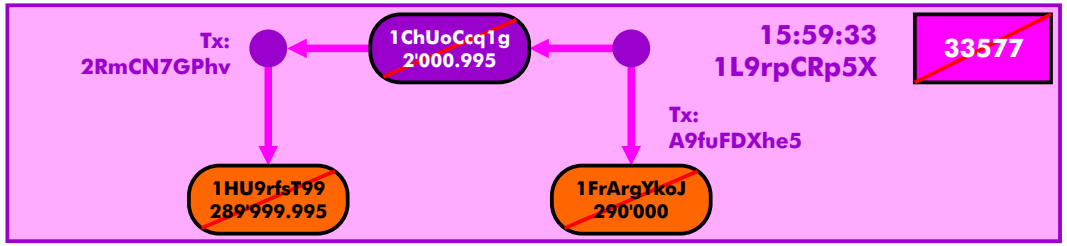
Transaction	Fee	Size (kB)	From (amount)	To (amount)
40c97fef35...	0	0.106	Generation: 200 + 0 total fees	6nso8bYNGPG25x3Bjvy4ihTuQa5qXb1UaF: 200
00c7f8ee24...	0	0.819	6tPuE1vTVXGQ5nxH7NHHWp1n2ZxtQ58cZ3: 280000 6qzgFkYt86DLbMaRNqshNR261NhB73R38z: 100000 6tfoH94Du8cFY9R4XQJi4jDh34p8L6mfrX: 92000.995 6vqrJ9WPcP63sfCLng2AjvcAh6aXanMsMS: 7999 6zxNJGDYbu2bvmL5NB8WDpExwSnLHMnexG: 100000	6vsDDHeReeEcwxp5kYN5g7ZC3Vh8bjc2y9: 300000 6qUC9vbv5MUkCkUQ5tDnnSqRi5mJdeoyqf: 279999.995

4 3

API (machine-readable pages)

ASSOCIATED FTC TRANSACTIONS

580K Ambiguity Traces



Inspecting the transactions yields yet **additional concurrent** destination addresses, these addresses are **also inexistent** (as far as block explorer allows us to check)
Originating addresses are, on the other hand, **consistent with the addresses on the attacker's chain**

Transaction 2RmCN7GPhv

Short Link: http://explorer.feathercoin.com/t/2RmCN7GPhv

Information

Hash:	25a783530dcbf575655f367eb3c36fb4e7e0975986b6515074964ea353fe66dd
Appeared in:	Feathercoin 9199d4f604...5d20 (2013-06-08 15:59:33)
Number of inputs:	3 (Jump to inputs)
Total in:	289999.995
Number of outputs:	1 (Jump to outputs)
Total out:	289999.995
Size:	489 bytes
Fee:	0

Raw transaction

Inputs

Index	Previous output	Amount	From address	ScriptSig
0	f85282c697...:1	7999	6vqrJ9WPcP63afCLng2AjvcAh6aXanMsMS	72:3045...0e01 33:02ce...67d1
1	d1733c20a5...:0	280000	6tPuE1vTVXGQ5nxH7NHHWp1n2ZxdQ58cZ3	72:3045...fa01 33:0298...7afd
2	f170a58642...:0	2000.995	6qRvainrxCa8G5hrnp7gT9CJE8h7PLUNpS	73:3046...9401 33:0348...992f

Outputs

Index	Redeemed at input	Amount	To address	ScriptPubKey
0	Not yet redeemed	289999.995	6vCbeC3V5gA5o5LCgrWcTCix4EJmYVkRYh	DUP HASH160 20:b4a4...3995 EQUALVERIFY CHECKSIG

API (machine-readable pages)

Transaction A9fuFDXhe5

Short Link: http://explorer.feathercoin.com/t/A9fuFDXhe5

Information

Hash:	f170a58642d836714d63b92f495dcbdde6d7d3631bda9030220c9ce47fb52543
Appeared in:	Feathercoin 9199d4f604...5d20 (2013-06-08 15:59:33)
Number of inputs:	3 (Jump to inputs)
Total in:	292000.995
Number of outputs:	2 (Jump to outputs)
Total out:	292000.995
Size:	522 bytes
Fee:	0

Raw transaction

Inputs

Index	Previous output	Amount	From address	ScriptSig
0	f85282c697...:0	92000.995	6tfoH94Du8cFY9R4XQJi4jDh34p8L6mfrX	72:3045...e201 33:02fc...34e2
1	d1733c20a5...:1	100000	6qzgFkYt86DLbMaRNqshNR261NhB73R38z	72:3045...9601 33:03ef...1b42
2	0766afefeb...:0	100000	6zxNJGDYbu2bvmL5NB8WDpExwSnLHMnexG	72:3045...c301 33:03f4...8d0b

Outputs

Index	Redeemed at input	Amount	To address	ScriptPubKey
0	25a783530d...:2	2000.995	6qRvainrxCa8G5hrnp7gT9CJE8h7PLUNpS	DUP HASH160 20:8051...5e9e EQUALVERIFY CHECKSIG
1	Not yet redeemed	290000	6taceCinjq7u9kq74xxw8ShmD4u3DHCEvt	DUP HASH160 20:a2de...1ef7 EQUALVERIFY CHECKSIG

API (machine-readable pages)

BTC 19VGAnAc6pahc1BUfjaobPZMHNjumDRuK
LTC LRu2pVJu5JGJxKR27gNi9NBYSdCzig8uoC

These are the facts as collected from publicly accessible and official block explorer
http://explorer.feathercoin.com/

Additional facts crosschecking made at
http://ftc.cryptocoinexplorer.com/

General Context and Interpretation of these facts are left to the audience with the exception of the following comments:

There exists a Feathercoin user holding about a fifth of all coins with the intent and capability to execute a highly damaging attack to the network and its users.

Recipients of Feathercoin when the network shows signs of being under attack should increase their confirmation requirements before accepting any payments.

BTC Donations

19VGAnAc6pahc1BUfjaobPZMHNjumDRuK

Corrections, Additions, Technical Revisions or comments are welcome:
max_miner <at> yahoo <dot> com

< If you find the information presented worthy of your support, please donate to these BTC/LTC addresses >

LTC Donations

LRu2pVJu5JGJxKR27gNi9NBYSdCzig8uoC