1.1 Bitcoin Structure - Double Spending

Feathercoin’s 51% Attack
Double Spending case study

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 >

BTC Donations
19VGAnAc6pahc1BUfjaobPZMHNjumDRuK

LTC Donations
LRu2pVJJu5JGJxKR27gNi9NBYSdCzig8uoC

Feathercoin’s 51% Attack
MaxMiner - June 2013
**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.

- **Attack Stage 1 (1st Fork)**
  - First appearance in the network of Generation address used in the attack (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.
  - Notice the timewarp. Next blocks would be logged with similar irregularity.
  - 33586 is the only block with a registered transaction.
  - After 13 blocks Stage 1 ends.

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

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

**Feathercoin’s 51% Attack**

BTC 19VGAnAc6pahc1BUfaoobPZMHNjumDRuK
LTC LRu2pVJu5JGJxKR27gNi9NBYSdCzig8uoC

MaxMiner - June 2013
THE FORKS
Counterfeit Block Generation

Compromised Blockchain

<table>
<thead>
<tr>
<th>time (UTC)</th>
<th>avgIntervalSinceLast</th>
<th>netHashPerSecond</th>
<th>Generation Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>18:54:30</td>
<td>16725</td>
<td>24M</td>
<td>6xtJbibr23</td>
</tr>
<tr>
<td>19:24:09</td>
<td>1779</td>
<td>227M</td>
<td>6xtJbibr23</td>
</tr>
<tr>
<td>19:27:18</td>
<td>189</td>
<td>2.1G</td>
<td>6xtJbibr23</td>
</tr>
<tr>
<td>19:27:55</td>
<td>37</td>
<td>11G</td>
<td>6uNcx3XPvc</td>
</tr>
<tr>
<td>19:50:04</td>
<td>1329</td>
<td>3G</td>
<td>6xtJbibr23</td>
</tr>
<tr>
<td>20:00:20</td>
<td>616</td>
<td>656M</td>
<td>6uNcx3XPvc</td>
</tr>
<tr>
<td>20:35:26</td>
<td>xxxx</td>
<td>xxxx</td>
<td>1L9rpCRp5X</td>
</tr>
<tr>
<td>21:28:37</td>
<td>xxxx</td>
<td>xxxx</td>
<td>1L9rpCRp5X</td>
</tr>
</tbody>
</table>

Day of the Attack (Feathercoin is 7 weeks old)

Sunday 9 June

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 6tbs8oiku
Notice again the timewarp Address is now 6tbs8oiku
Next blocks would be logged with similar irregularities at an impossible fast rate

18:54:36 | 5 | 81G 6tbs8oiku

18:56:15 | -3 | Infinity 6tbs8oiku
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)

Feathercoin’s 51% Attack

MaxMiner - June 2013
Compromised Blockchain

Day of the Attack (Feathercoin is 7 weeks old)

Sunday 9 June

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

Compromised Blockchain

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

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

BTC 19VGAnAc6pahc1BUjaoBPZMHJumDRuK
LTC LRu2pVJu5JGJxKR27gNi9NBYSdCzig8uoC

MaxMiner - June 2013

Feathercoin’s 51% Attack
ASSOCIATED FTC MOVEMENTS
580K Origin addresses

The 580K are part of a 1'449'999.83 FTC transaction

Day of the Attack (Feathercoin is 7 weeks old)

2 addresses are used for transport in the same block

The 580K end up in 5 distinct addresses
~1h30 before the attack fork

The 580K are consolidated in 2 addresses
on the 1st Stage of the attack

* transactions (Tx) references are ABE’s shortlinks use:
http://<ftc blockexplorer domain>/t/<shortlink> to access details

maxminer - June 2013
ASSOCIATED FTC MOVEMENTS
580K Destination addresses

579,999,995 FTC = 8.63% of total coins mined up to block

Stage 1
2013-06-08 14:15:46
6nso8bYNGF

Stage 2
2013-06-08 18:55:08
6tbxs8oiuku

Stage 1
2013-06-08 18:55:26
6tbxs8oiuku

Stage 9 June
2013-06-09 19:00:43
6uNcx3XPvc

The 580K is spread between 6 addresses

Transactions attempted in the competing forks signaled in red most were attempted up to 3 times each between 15:59:33 (UTC) on Saturday 8 and 05:22:51 (UTC) on Sunday 9

The value is branched in 2

Consolidation is made connecting back the branches

Feathercoin’s 51% Attack

BTC 19VGArAc6pahc1BUfaoaPZMHNjumDRuK
LTC LRu2pVJu5jGJxXK27gN9NBYSdCzr8uoC

MaxMiner - June 2013
ASSOCIATED FTC TRANSACTIONS
580K 1st Double-Spend Attempt

Notice the **same transactions** give origin to 2 sets of 5 different addresses
Only the set on the attacker’s side is ultimately followed through

Addresses on this side as colected from the transactions list in the legitimate side block 33577

While originating addresses are still reviewable all the other on the legitimate side are NON existent

Transactions found on block **33562** are worthy of closer inspection...

Transactions reached **6 confirmations** in invalidated side of the network

MaxMiner - June 2013

Feathercoin’s 51% Attack

BTC 19VGArAc6pahc1BUjaoobPZMHNjumDRuK
LTC LRu2pVJu5JGjXR27gN9i9NBYSadCzg8uoC
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

Feathercoin’s 51% Attack

BTC 19VGAnAc6pohc1BUfaoBpZMHNjumDRuK
LTC LRu2pVju5JGjxKR27gNi9NBYsdCzvig8uoC
MaxMiner - June 2013
1. The attempted transactions 2. The destination addresses

3. Prevailing transaction 4. Prevailing addresses

---

**Feathercoin’s 51% Attack**

BTC 19VGAnAc6pahc1BUjaoobPZMHNjmMDKuK
LTC LRu2pVju5JGxK27gN9NYSdCzjgBuC

MaxMiner - June 2013
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.
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.

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 >

BTC Donations
19VGAnAc6pahc1BUfjaobPZMHNjumDRuK

LTC Donations
LRu2pVJu5JGJxKR27gNi9NBYSdCzig8uoC

Feathercoin’s 51% Attack

MaxMiner - June 2013