**FACTOM**

**COMMUNITY**

**Cancellation**

**of**

**Coinbase Outputs**

**DOC 203**

|  |  |  |  |
| --- | --- | --- | --- |
| VERSION | DATE | CHANGED BY | CHANGES |
| 0.1 | 2019-06-09 | The 42ND Factoid LTD | First version |
| 0.2 | 2019-06-12 | The 42ND Factoid LTD | Amended instructions to use Factom Open Node system. |
| 0.3 | 2019-06-14 | Paul Bernier | Reworked document. |
| 1.0 | 2019-06-17 | The 42ND Factoid LTD | Changed version number to 1.0 |
| 1.1 | 2019-07-07 | Brian Deery | Updated technical details |
|  |  |  |  |
|  |  |  |  |

1. Introduction
   1. In the Factom ecosystem there are two uses of coinbase transactions on the protocol level, and both resulting in new FCT (“Factoids”) being minted:
      1. Authority Node Remuneration

*Note: See* [*Factom Governance Document*](https://factomize.com/forums/documents/doc-001-factom-governance.9/)*, Chapter 5.1.*

* + 1. Factom Grant Payments

Note: in accordance with the [Factom Grant Process](https://factomize.com/forums/documents/doc-107-factom-grant-process.76/).

* 1. As a security measure against potential attacks or errors these coinbase transactions have a payout delay of 1000 blocks (approx. 7 days), and may be cancelled during this “waiting period” if a majority of the **Authority servers** signs and broadcasts a **coinbase cancellation message.**
     1. This is formalized in[*Factom Governance Document*](https://factomize.com/forums/documents/doc-001-factom-governance.9/)*, Chapter 5.4.*
  2. The **coinbase descriptor** is an entry recorded in an Admin block that describes the outputs of the coinbase transaction that will happen in 1000 blocks. [Here](https://explorer.factom.com/ablocks/6ecb783bd051f33724465754a332320151d344a0acb4a8efd4cfec9bf308e231?page=2) is an example visualized in the Factom explorer:



* + 1. For Authority Node Remuneration Coinbase descriptors, they are populated into Admin blocks at heights divisible by 25. For example 196850, 196875, 196900, 196925, etc.
    2. For Grant Payment Coinbase descriptors, they are populated into Admin blocks at heights divisible by 25+1. For example, grants have activated at blocks 152751, 155501, 168576, 181001, etc.
  1. This document describes the necessary steps an Authority Node Operator (“ANO”) should take if they want to issue a coinbase cancellation message.
  2. Each Authority server identity can emit a coinbase cancellation message. In particular it means that if an ANO controls 2 Authority servers it should emit a cancellation message for each server identity.
  3. Note that the ANOs are independent actors in this regard, and have the authority to issue any coinbase cancellation messages they see fit.
  4. The final section in [this GitHub document](https://github.com/FactomProject/FactomDocs/blob/master/Identity.md#coinbase-cancel) provides a more thorough explanation of the concept of Coinbase Cancellation and should be read by **everyone** before attempting to issue a cancellation message.

1. Coinbase cancellation procedure

To perform the process we will be using the open-source CLI tool [factom-identity-cli](https://github.com/PaulBernier/factom-identity-cli)

Note: The same tool is used for updating efficiency and Authority Node coinbase addresses.

* 1. **Prerequisite**
     1. The coinbase cancellation message has to be submitted **after** the coinbase descriptor has been recorded in an Admin block.
        1. For example, if a grantee loses the private key to their FCT payout address, the grant can be canceled and the FCT retained by the grant pool. If the loss is discovered after the factomd release is installed by ANOs, instead of attempting a new release, the specific grant can be canceled. The grant cannot be canceled until after it is activated and shows up in a coinbase descriptor.
     2. The coinbase cancellation message has to be submitted **before** the actualcoinbase transaction. If the coinbase transaction has already happened there is no mechanism to roll it back.
  2. **Necessary information to prepare**
     1. A mainnet **factomd endpoint**. You can use your own node or an open endpoint such as [Factom Open Node](https://factomd.net/).
     2. A **funded EC address** to pay for the entry containing the cancellation message. You need the private part (starting with Es…).
     3. **Root chain ID** of the Authority Server Identity (starts with 888888).
     4. The **Server Management Subchain ID** associated with the Authority Server Identity (starts with 888888).
     5. The **SK1 secret key** of the Authority Server Identity.
     6. The **block height** of the coinbase descriptor to cancel.
     7. The **index** in the coinbase descriptor of the output to cancel.
  3. **Command line to write coinbase cancellation message**  
       
     Please refer to the latest version of the documentation (README) of factom-identity-cli. [Here is an example of the command to execute](https://github.com/PaulBernier/factom-identity-cli#to-generate-a-script-to-add-a-coinbase-cancel-message).  
       
     In order to guarantee the safety for the SK1 key it is strongly recommended to follow an offline procedure similar to [the one described here](https://github.com/PaulBernier/factom-identity-cli/blob/master/offline-process-proposal.md).
  4. **Verification**
     1. To verify that the cancellation message has been registered, navigate to the Server Management Subchain(same as 2.2.4) in a Factom block explorer ([1](https://explorer.factom.com/dblocks), [2](https://explorer.factoid.org)) and observe that the entry has been added to the chain.
     2. For the coinbase cancellation to be successful, a majority of Authority servers need to publish their cancellation message for a given output. When enough of the Authority Set has issued an individual Coinbase cancel message, a “[Coinbase Descriptor Cancel](https://github.com/FactomProject/FactomDocs/blob/master/factomDataStructureDetails.md#adminid-bytes)” will be added to the Admin block. It has the message type 12 and can be found in a local copy of the blockchain.
     3. To verify locally, have a factomd instance running with a copy of the blockchain. Also have factom-cli installed. Run this script to find admin blocks that have Coinbase Descriptor Cancel messages in them.

|  |
| --- |
| #!/bin/bash  for ((n=46500;n<46550;n++))  do  ABLOCK="$(factom-cli get abheight $n | grep '"adminidtype": 12,')"  if [ -z "$ABLOCK" ]  then  :  else  echo "coinbase cancel activated in block $n"  factom-cli get abheight $n  fi  done |

* + 1. The above script when run on the Community Testnet will give this output:

|  |
| --- |
| ./get\_admin\_blocks.sh  coinbase cancel activated in block 46523  {  "ablock": {  "header": {  "prevbackrefhash": "d62243cbccdd8a130188b002994d36167793f068ec05d45bf7549f636e2341db",  "dbheight": 46523,  "headerexpansionsize": 0,  "headerexpansionarea": "",  "messagecount": 11,  "bodysize": 1296,  "adminchainid": "000000000000000000000000000000000000000000000000000000000000000a",  "chainid": "000000000000000000000000000000000000000000000000000000000000000a"  },  "abentries": [  {  "adminidtype": 1,  "identityadminchainid": "8888888de45074fb3505cfdc942f80f4c9ef1ddd5c4633cd21a940288ffc89f3",  "prevdbsig": {  "pub": "d7f968a9ee264b92b6002098a6072fd8619a572c18d80f55fff4790665b061dd",  "sig": "8f7c844fa71766d419e13223c2958ae8af4bbbef96802e008f057110fc47f946c6579d05b8c0cf9b5f8013fe146dd16b93a7adc82c750c7226ec123946f52201"  }  },  {  "adminidtype": 1,  "identityadminchainid": "8888889822cf1d5889aa8dc11ad210b67d582812152de568fabc5f8505989c0f",  "prevdbsig": {  "pub": "591b76f87bbea9ea5bbacb79ee10603bffac0a728999a25b2afac936fbeb3a39",  "sig": "0944a92d5710df1625e28760877ef2d3a849c52af6c28e68f71aaa2fec427545a3dcecc613e09caa467237ec453b03defd1260d44c2f1b64211b074c0de9fc0c"  }  },  {  "adminidtype": 1,  "identityadminchainid": "8888889fff41615e89c718e6a08d28107ff50aa99e72197c6efd40fb202a5803",  "prevdbsig": {  "pub": "6d9be060bed2a53a3498a2918934a62768b0c109c3ceb3d0b3697d2f5c92f8a0",  "sig": "c965c52fe1dcd58f35c66fb7aef756071c606f94834ee62875592c600470ef1457776d3d4629e1228138db50c8073fabb931778fd6acb54927ffafcfeaf34f08"  }  },  {  "adminidtype": 1,  "identityadminchainid": "888888dc16a02e27f184353ac046e8ca2e052be873809af3dc86907bdae98b96",  "prevdbsig": {  "pub": "db0429a7caf8b93b387688e5172df591731acc862ac7440d85c01657c672b2c0",  "sig": "73668add6295563d619ede67844879ab35068d512a98ff2883c82244e0d89a05393487604ae2e3c02fbf472fd57efc9402ee28e7ce0191f49203ee422233ee0e"  }  },  {  "adminidtype": 1,  "identityadminchainid": "888888dcb1aacf764c1d15e1f6bc883831160db626cb8f46bdc86c1fcf5c019e",  "prevdbsig": {  "pub": "462c856ad698491eed4f59d5c848ada06a81893856d3b965a19502d2d807ad07",  "sig": "4ebe31564431ab74aa59817db09edfaf69a00d9d555b9f1ede3285b872dfd630b33434eef77f1c4d30d6cba4c45ef8cbfcd5cc993d2adb437d60b5bc172c390e"  }  },  {  "adminidtype": 1,  "identityadminchainid": "888888f1dd02afef9715456811a8db5cd409619b3c5e3cd612bbfd6d16c94d48",  "prevdbsig": {  "pub": "f476310b7fa47eb6436f31710ce2a1db1caeb3a2b2638295df9eaab1370228c4",  "sig": "a74e5ec5b14af310fb905628d23cacad85603245e24014046eaa464f60c7153e09745e2467d4f48db70b76a8d17222339d70bc18b86aa6853bf31b6fbd36d409"  }  },  {  "adminidtype": 1,  "identityadminchainid": "8888880732ebbec169b8e583c6ac6f9a348692aca6457cab5025e104fbadc282",  "prevdbsig": {  "pub": "08ec6928e010c1694763d571e9a0142c697f524cc40d33ca7bd911d8685a1921",  "sig": "e909c3c0d0a65e352d5a9c9de015fe33ebebc5b42db42de2754b93703ce7e94bdcaee4d30f5b9ec7988c9d22e0ae658e27abba2c59155b0792c0ead13f480e03"  }  },  {  "adminidtype": 1,  "identityadminchainid": "8888881c98618455b818cbe56b924374d87445ffdc7263363302292974dc3f94",  "prevdbsig": {  "pub": "0de6369919f526225a14c38b7cf7081287e4029471e000b5c4336c041b233253",  "sig": "0f54b16d99e9c89ba838b55ac637d39e789e3b9ee043381abb5092cf55ec32298ed4e08ac264da09d2ecf7cb1dadba613201c9892c7f27ed256f24c66284b70d"  }  },  {  "adminidtype": 1,  "identityadminchainid": "888888745c880f62e73da38a03519134c895cbc806feebc73f321cc00681b126",  "prevdbsig": {  "pub": "dcaf4ab9040b17248fa15defcfecdd7bdbd018776c5a01b92c7e391077658699",  "sig": "2d6349dc386bfe918e73893b34ba66d74abe24f2322a935dd0627575b10a81239f3d5ac278749a7ac7f0fcdf1db6ca493ee3e2a9ed49244fd0772b8980f6ab01"  }  },  {  "adminidtype": 1,  "identityadminchainid": "88888877a43c37ce2ca73845684fcdda340fdc72857a6029d1f33c665dc6e092",  "prevdbsig": {  "pub": "15772114e000072a2fb703fa96aa4eb8825bf42f4b398b6de480b638fd2eb755",  "sig": "bc3d6ae30484651e876617acb7714d75167a6cd66985d8e7e811c5625a2e5033dbf70be8473b2c7619186992c4e6659fc47110dcf4bebb84c1a12c8c0fb2ca0e"  }  },  {  "adminidtype": 12,  "descriptor\_height": 46460,  "DescriptorIndex": 8  }  ],  "backreferencehash": "b493590959eea4944ea51e7066a5d8c1d905f0ce4113710bba639ae660afc7bb",  "lookuphash": "dcd88117e8233efe279c371eb54bc0c73bc2c8627a9c5a8be3de74b8b9afa2d4"  },  "rawdata": ""  } |