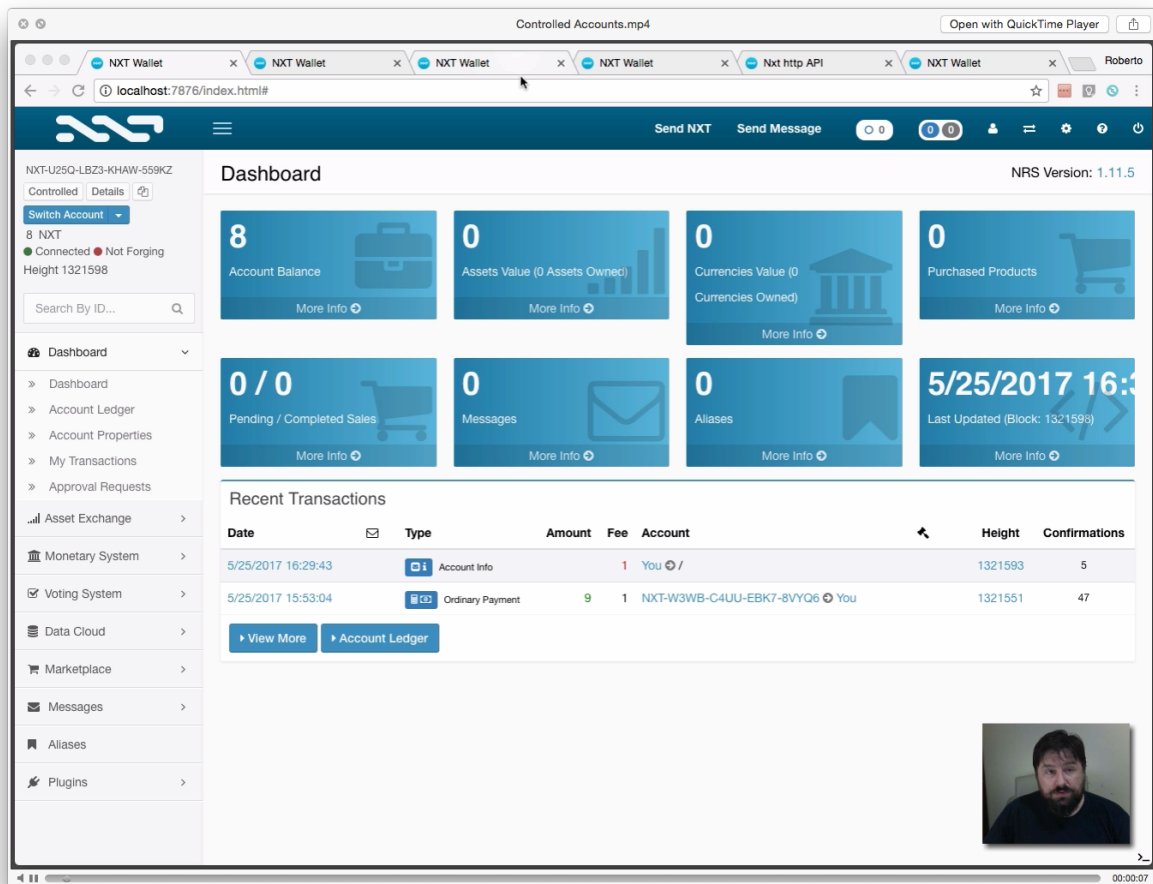


Using the Nxt blockchain  
By Roberto Capodiecì

# Emulating MultiSig in the Nxt Blockchain

## Step2step guide on how to use controlled accounts

---



NOTE: this guide is of support to the video tutorial that can be found at:

[https://www.youtube.com/watch?v=z0J1uuJL\\_5I](https://www.youtube.com/watch?v=z0J1uuJL_5I)

Last edit: 26 May 2017

---

---

## Introduction

Nxt offers Account Control: an account can be controlled by other accounts, making any transaction go through an approval of the controlling accounts. This allows, beside many other possibilities, to emulate the concept of MultiSig well known in Bitcoin and other blockchains.

### **Account Control for phased transactions.**

Any Nxt Blockchian account can be restricted to only be allowed to issue phased transactions subject to a specific voting model.

This is achieved by the account submitting a setPhasingOnly transaction using the setPhasingOnlyControl API.

The getPhasingOnlyControl API can be used to retrieve the status of an account phasing control, and getAllPhasingOnlyControls to get all accounts subject to phasing control with their respective restrictions.

Once set, the phasing only account control can only be disabled or changed with another setPhasingOnly transaction, itself subject to the currently set phasing restrictions.

Note that by-transaction and by-hash voting models are not allowed for phasing control, and setting voting model to none is used to disable the control.

To prevent deadlocks due to cyclic account control restrictions, approval transactions themselves (PhasingVoteCasting) are not subject to phasing only account control.

When setting phasing account control, a maximum fees total can be specified, limiting the total fees for currently pending phased transactions of the controlled account, and limits can be placed on minimum and maximum phasing duration allowed.

Transactions of accounts subject to phasing account control with restriction on maximum fees are throttled at one per account per block.

---

## Step by step guide

Note: the images below are extracted from the video tutorial that can be found at: [https://www.youtube.com/watch?v=z0J1uuJL\\_5I](https://www.youtube.com/watch?v=z0J1uuJL_5I)

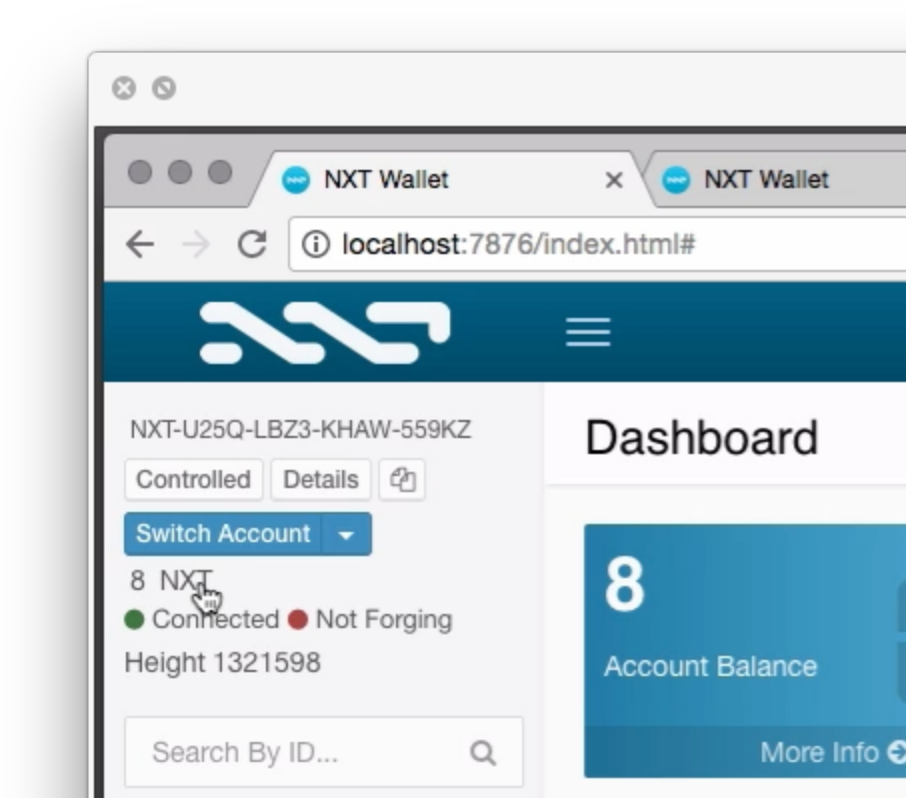
Note also that all the operations illustrated below can be executed also via API.

### Setting up the controlled account

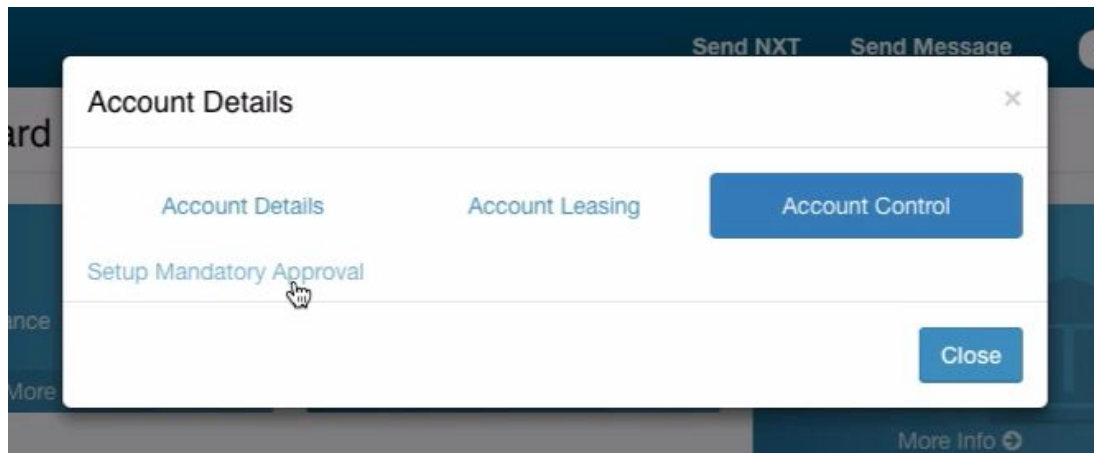
Open the wallet UI, and log in with the account you want to be controlled (the account from where the funds will leave when a MultiSignature approves it). Make sure the account has a few coins of balance as setting up the account control requires a fee,

#### Step 1: Open a special dialog window and choose the Account Control tab

Click on the account balance to open the dialog to set the Account Control

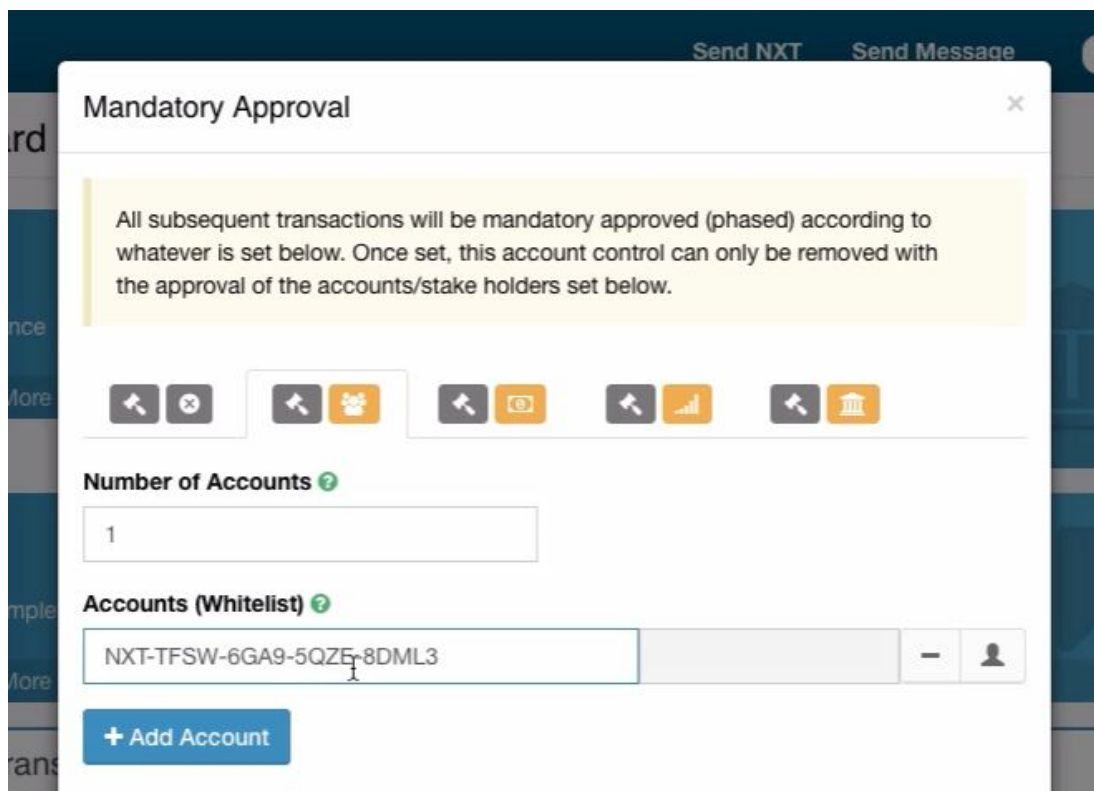


## Step 2: Open the Account Control Mandatory Approval Setup



In this dialog go to the third tab “Account Control” and click on it. If the account has no Account Control set up already, you should see the link “Setup Mandatory Approval”. Click on it to open the setting dialog to set up Account Control.

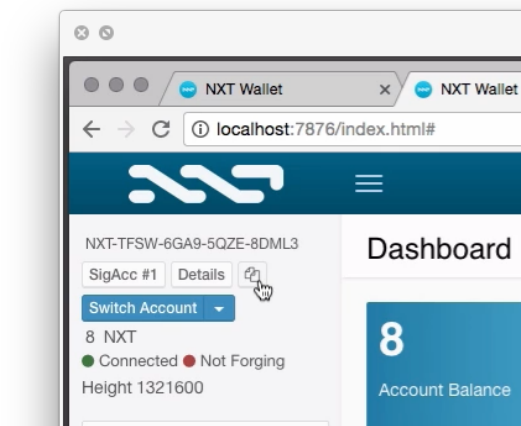
## Step 3: Choose the second control option out of the 5 available



---

In this tab you can start adding the list of the accounts that are authorised to sign to approve a transaction.

#### Step 4: Copy all the accounts ID from and paste them in the list



To copy an account ID simply click on the copy icon in the account, and paste the account ID in an email or wherever necessary to get it available to the person setting up the Account control.

#### Step 5: Set account list and qurum for transactions approval

List as many account IDs as you need and chose how many approvals are necessary to authorise a transaction. For example, if you have 10 authorised account to sign, you can chose that only 6 are necessary to approve the transaction



Click on “+ Add Account” to list more accounts,

The screenshot shows a web interface with a top navigation bar containing several icons. Below the navigation bar, there is a section titled "Number of Accounts" with a text input field containing the number "1". Below this is a section titled "Accounts (Whitelist)" containing a table with three rows. Each row has a text input field for an account ID, a greyed-out input field, a minus sign icon, and a person icon. The account IDs are "NXT-TFSW-6GA9-5QZE-8DML3", "NXT-JJ2X-NLWL-EV6A-8EZZS", and "NXT-N4DR-EYWU-B5K8-AUAQ2". Below the table is a blue button labeled "+ Add Account". At the bottom, there is a section titled "Min Balance Type".

Account ID			
NXT-TFSW-6GA9-5QZE-8DML3		-	
NXT-JJ2X-NLWL-EV6A-8EZZS		-	
NXT-N4DR-EYWU-B5K8-AUAQ2		-	

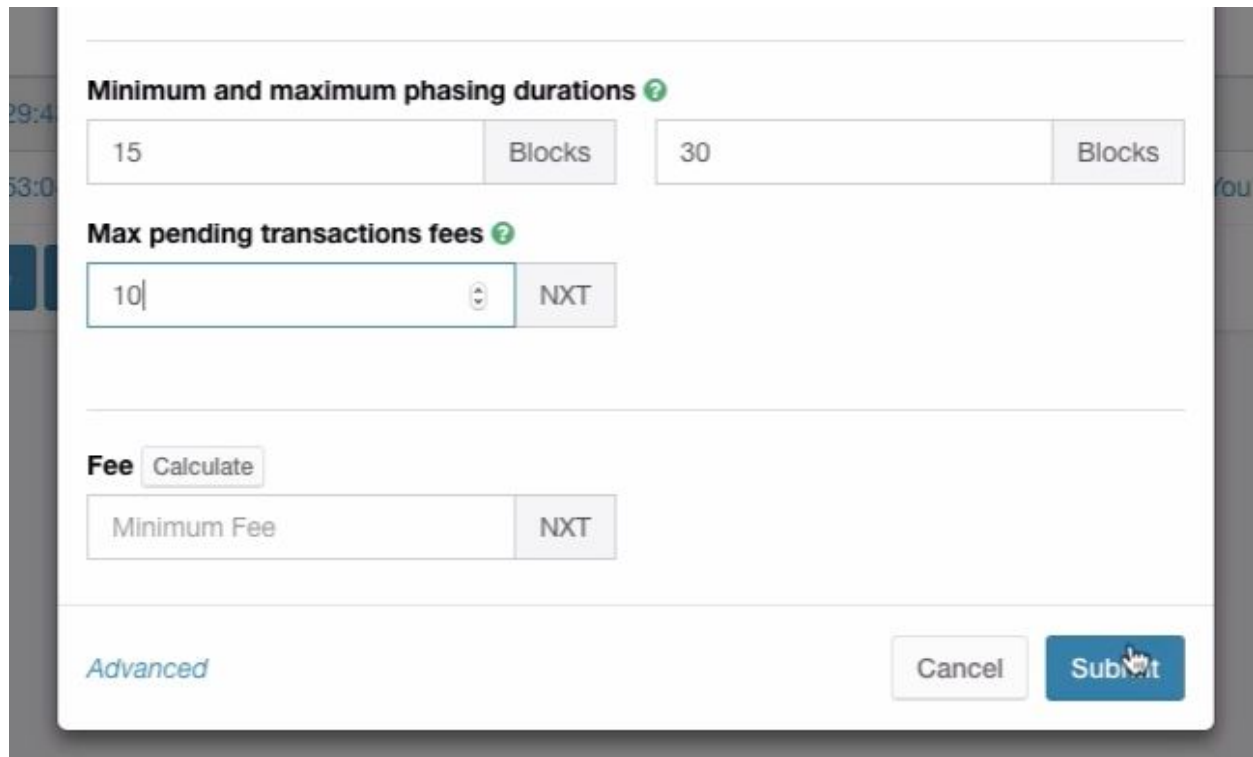
and set the number of minimum account approvals to approve the transaction in “number of accounts”

The screenshot shows the same web interface as the previous one, but with the "Number of Accounts" text input field now containing the number "2". The "Accounts (Whitelist)" table remains the same, with the same three rows and account IDs. The "+ Add Account" button and "Min Balance Type" section are also visible.

Account ID			
NXT-TFSW-6GA9-5QZE-8DML3		-	
NXT-JJ2X-NLWL-EV6A-8EZZS		-	
NXT-N4DR-EYWU-B5K8-AUAQ2		-	

---

## Step 6: Choose when the transaction will be executed



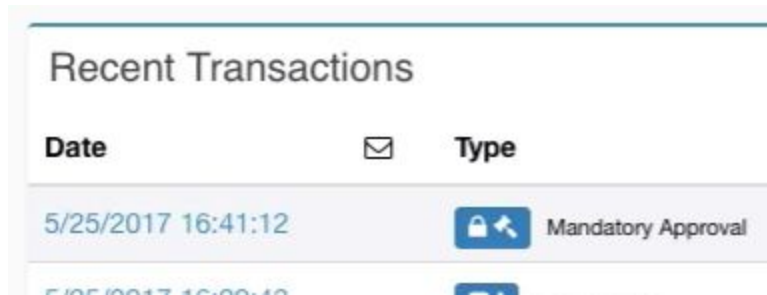
The screenshot shows a web interface for configuring transaction execution. It features two input fields for 'Minimum and maximum phasing durations' with values 15 and 30, both labeled 'Blocks'. Below these is a 'Max pending transactions fees' field with a value of 10 and a unit selector set to 'NXT'. A 'Fee' section includes a 'Calculate' button and a 'Minimum Fee' field with a unit selector set to 'NXT'. At the bottom, there is a blue 'Advanced' link, a 'Cancel' button, and a blue 'Submit' button.

In the “Minimum and maximum phasing duration” fields you can set, in blocks (1 block equals 1 minute circa) the starting and ending time of the window when the transaction will be executed. For example, following the image above, the transactions set by the controlled accounts will be executed (if the necessary amount of approvals is reached) between 15 to 30 minutes after the submission. This means that if all the necessary approvals (co-signatures) are achieved in 5 minutes after the transaction has been submitted, the transaction will be executed anyways after 15 minutes. If past 15 minutes not enough approvals have been submitted, the transaction keep waiting until 30 minutes from its submission to execute. If in this window of time the quorum of approval is reached, then the transaction will be executed immediately, else it will fail and not be executed.

The “Max pending transactions fees” is the maximum amount of fees, per block, that the controlled account can spend (for example to issue new transactions that will need to be approved). It is important to leave at least 2, as controlled accounts transactions cost 2 in fees, but not a too high amount either, as someone with the secret phrase of that account can abuse it spending all the funds in fees.

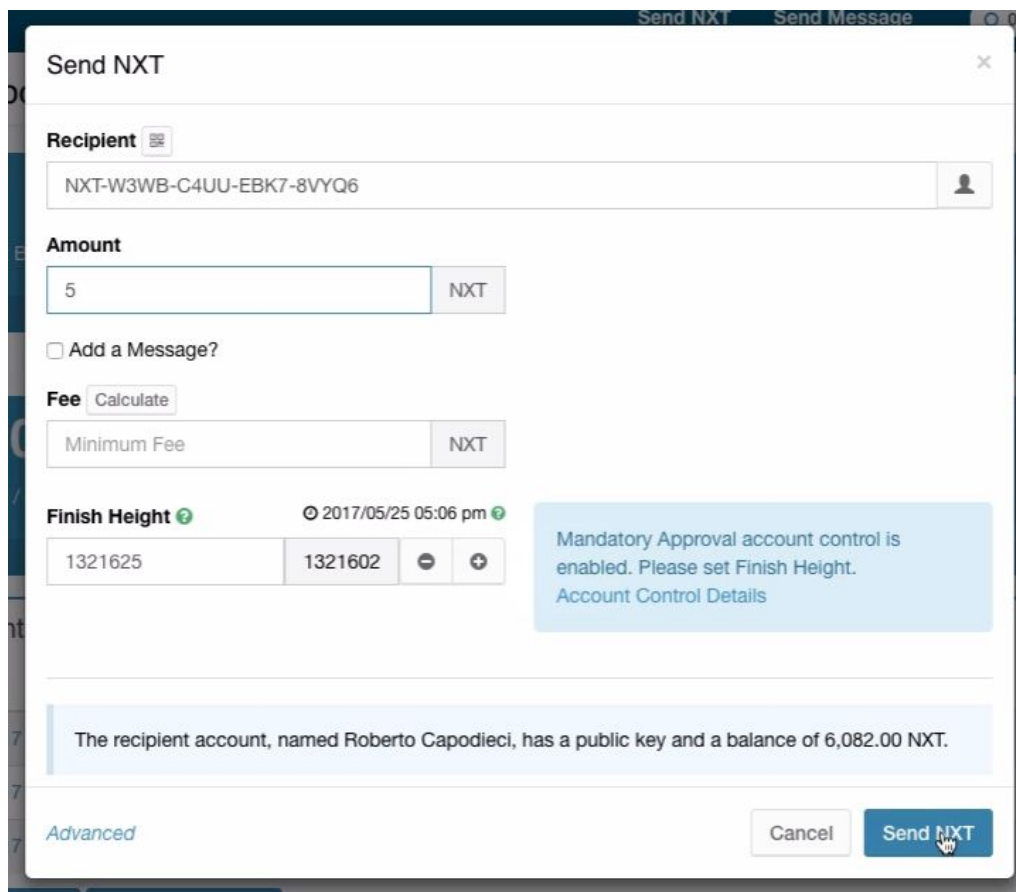
---

## Step 7: Submit the form



In the main control panel check that the controlled Account setting are submitted and registered in the blockchain (there is at least 1 or more confirmations)

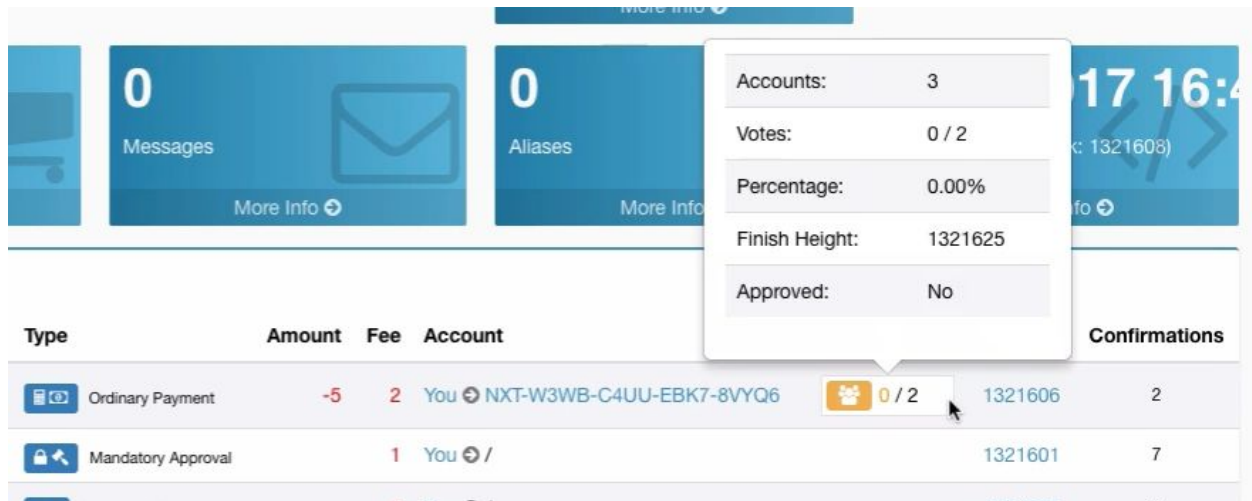
## Posting a transaction from the controlled account



When posting a transaction from the controlled account a warning appears.



## Step 1: Post a transaction as usual



The screenshot shows a dashboard with two main cards: 'Messages' (0) and 'Aliases' (0). Below these is a table of transactions. A tooltip is visible over the '0 / 2' icon in the first row.

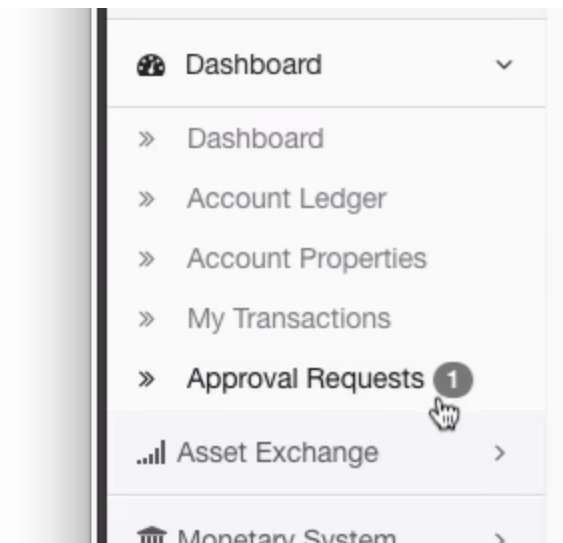
Type	Amount	Fee	Account	Confirmations
Ordinary Payment	-5	2	You  NXT-W3WB-C4UU-EBK7-8VYQ6	2
Mandatory Approval	1	You  /		7

Tooltip details:

- Accounts: 3
- Votes: 0 / 2
- Percentage: 0.00%
- Finish Height: 1321625
- Approved: No

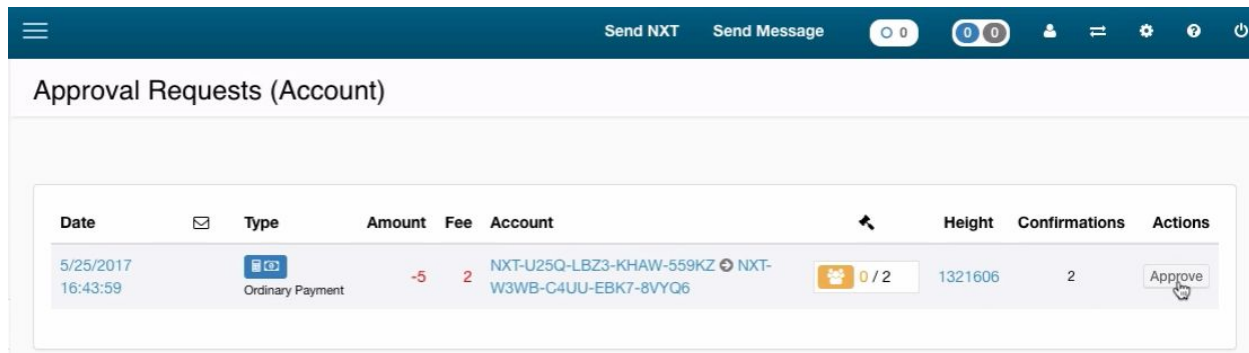
Once posted, a transaction appears in the main dashboard, showing how many approval have already been received. Mouse over the icon to get details on the finish height and status of the transaction

## Approving a Transaction (cosigning the MultiSig)



Once that the controlled account posts a transaction, the controller accounts (the account to co-sign the MultiSig transaction) will receive a notice of "Approval Request".

## Step 1:

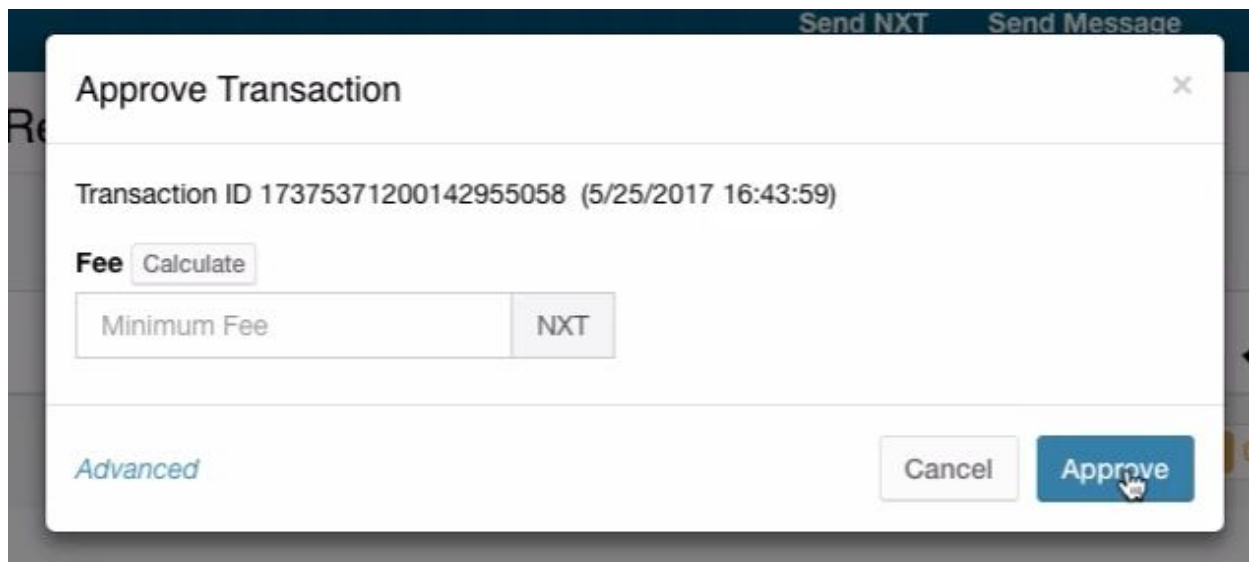


The screenshot shows a web application interface for 'Approval Requests (Account)'. At the top, there's a dark blue header with 'Send NXT' and 'Send Message' buttons, and a status bar showing '0 0'. Below the header, the title 'Approval Requests (Account)' is displayed. A table lists transactions with columns: Date, Type, Amount, Fee, Account, Height, Confirmations, and Actions. One transaction is visible, dated 5/25/2017 16:43:59, of type 'Ordinary Payment' with an amount of -5 and a fee of 2. The account ID is NXT-U25Q-LBZ3-KHAW-559KZ. The height is 1321606 and there are 2 confirmations. An 'Approve' button is in the Actions column.

Date	Type	Amount	Fee	Account	Height	Confirmations	Actions
5/25/2017 16:43:59	Ordinary Payment	-5	2	NXT-U25Q-LBZ3-KHAW-559KZ W3WB-C4UU-EBK7-8VYQ6	1321606	2	Approve

Clicking on the approval request notification a page with all the transactions that need approval will open. The cosigning account holder can verify that is all ok, and press on the “approve” button on the right.

## Step 2: confirming the approval



The screenshot shows a dialog box titled 'Approve Transaction'. It displays the transaction ID 17375371200142955058 (5/25/2017 16:43:59). Below the ID, there's a 'Fee' section with a 'Calculate' button and a 'Minimum Fee' input field. The 'NXT' label is next to the input field. At the bottom, there are 'Cancel' and 'Approve' buttons. The 'Approve' button is highlighted with a mouse cursor. There is also a link labeled 'Advanced' at the bottom left.

Approve Transaction

Transaction ID 17375371200142955058 (5/25/2017 16:43:59)

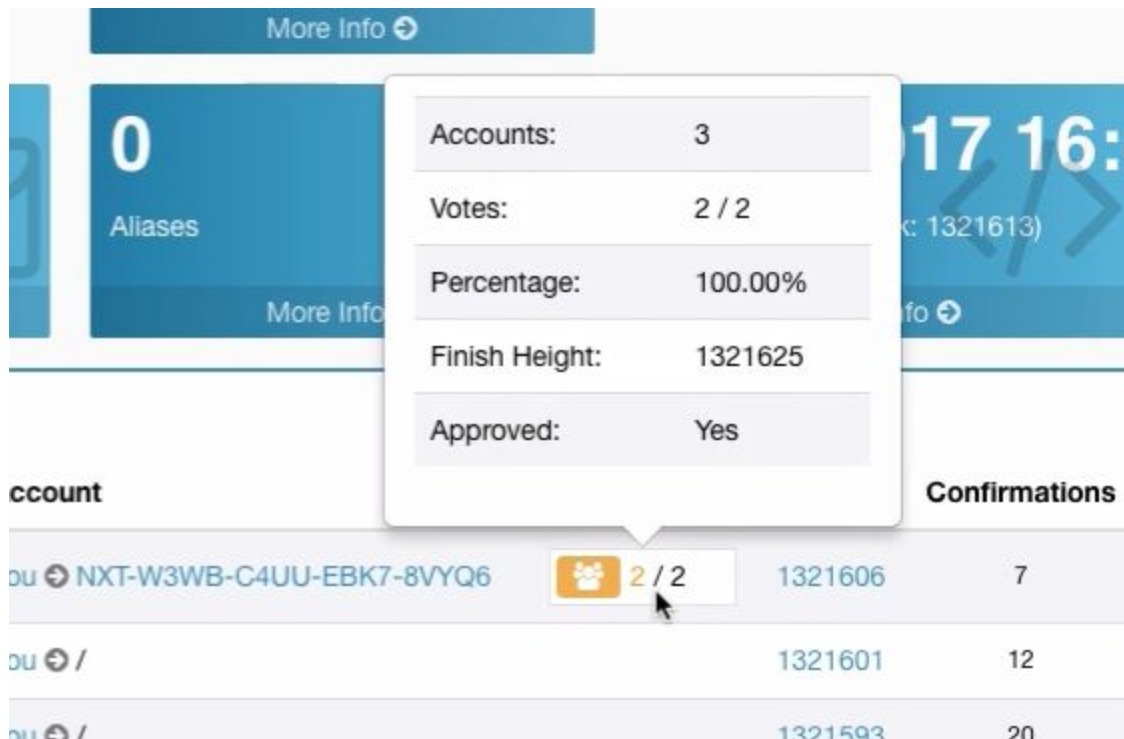
Fee Calculate

Minimum Fee NXT

Advanced Cancel Approve

A dialog will open requesting to approve the transaction and offering additional options.

## Verifying that the transaction went through



Both sender (controlled account) and recipient can see the status of the approval.

## The emulation of a MultiSig on the Nxt Blockchain

While this is not technically a multisignature as per cryptographic definition, the way Nxt treats Account Controls offers many more opportunities on how a transaction is authorised and by who out of the full pool of users in the blockchain.

This tutorial has been limited to the emulation of a MultiSig account in the Nxt Blockchain, and had no intention to go into other details.

For more info check the Nxt Wiki: <https://nxtwiki.org/wiki/Phasing>

Watch the tutorial video here: [https://www.youtube.com/watch?v=z0J1uuJL\\_5I](https://www.youtube.com/watch?v=z0J1uuJL_5I)

Roberto Capodiecì

## Addendum

Two more items that deserve attention: changing account control and using the API to manage Account Control.

### Freeing an account from being “controlled”

The screenshot shows a 'Mandatory Approval' dialog box with a close button (X) in the top right corner. A yellow warning box contains the text: 'All subsequent transactions will be mandatory approved (phased) according to whatever is set below. Once set, this account control can only be removed with the approval of the accounts/stake holders set below.' Below this is a row of five icons, each with a back arrow: a crossed-out square, a cat, a coin, a bar chart, and a bank building. The text 'Process without approval.' is below the icons. The 'Fee' section has a 'Calculate' button and a 'Minimum Fee' input field with an 'NXT' unit selector. The 'Finish Height' section shows a current value of 1321636, a target value of 1321613, and minus/plus buttons. A timestamp '2017/05/25 05:12 pm' is next to it. A blue information box states: 'Mandatory Approval account control is enabled. Please set Finish Height. Account Control Details'. At the bottom left is the word 'Advanced' in blue. At the bottom right are 'Cancel' and 'Submit' buttons.

Send NXT Send Message

**Mandatory Approval** X

All subsequent transactions will be mandatory approved (phased) according to whatever is set below. Once set, this account control can only be removed with the approval of the accounts/stake holders set below.

Process without approval.

**Fee** Calculate

Minimum Fee NXT

**Finish Height** ? 2017/05/25 05:12 pm ?

1321636 1321613 - +

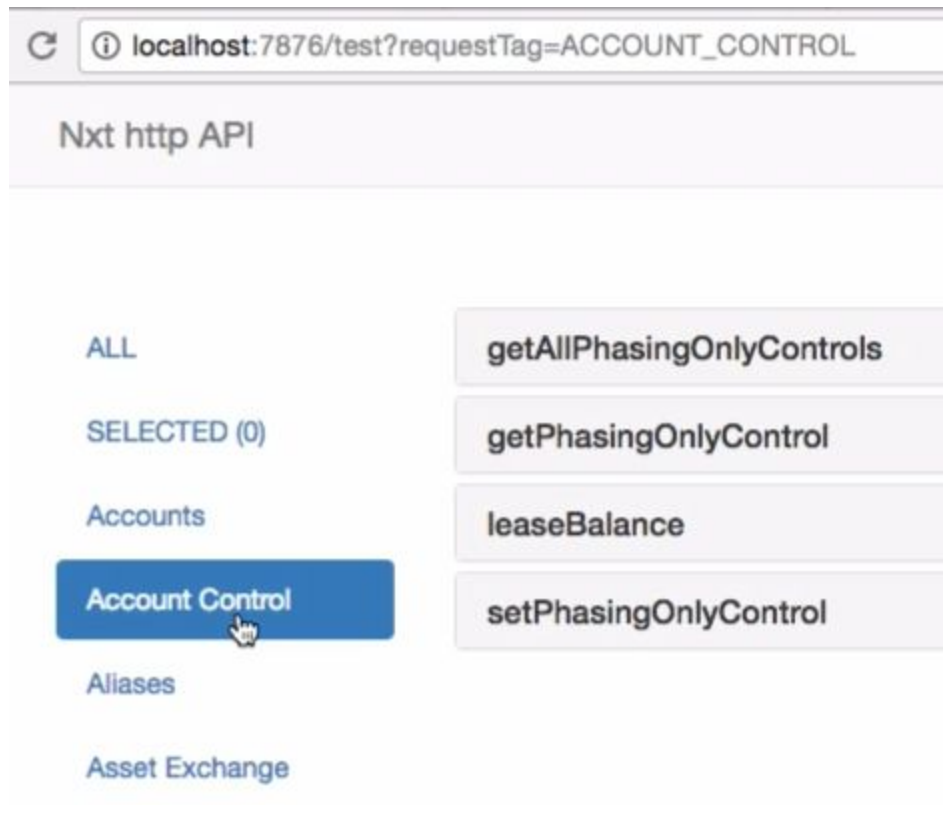
Mandatory Approval account control is enabled. Please set Finish Height.  
Account Control Details

Advanced Cancel Submit

This seems quite obvious, but better making it clear: to remove or edit the way an account is controlled the approval of the controlling accounts is necessary.

---

## All you saw above, but via API



The API set to set and manage Account Control are available at the url /test of the node address being used.

From LocalHost, for example, to check the status of the account control of an account, simply use:

`http://localhost:7876/nxt?requestType=getPhasingOnlyControl&account=[ACCOUNTID]`