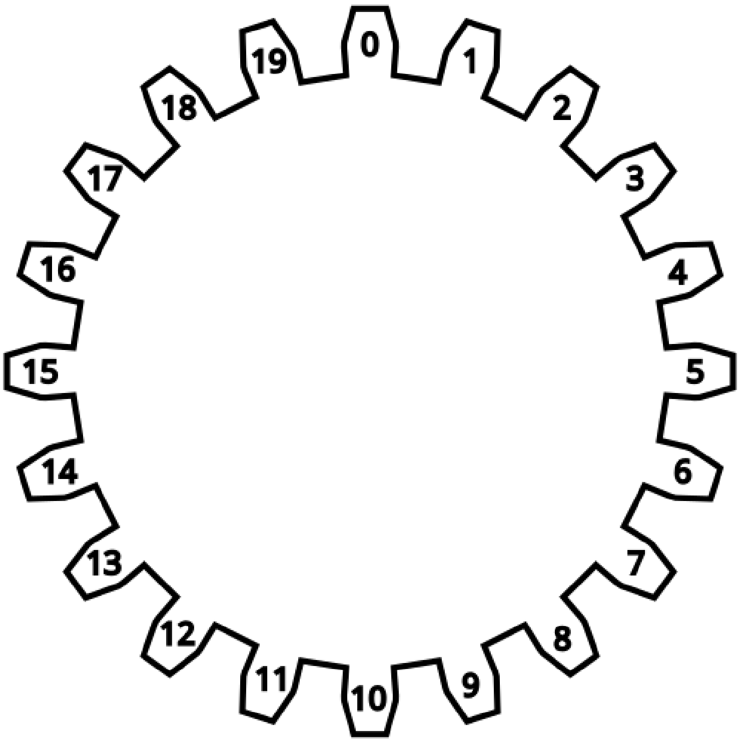
Relayer selection algorithm

BPX Bridge associates each transaction and signature to a so-called epoch - 20-minute period of time. When the epoch changes, for the same transaction, the set of selected validators will be completely different. So if a transaction cannot be completed in a given epoch due to a relayer failure, the algorithm will select a different set of relayers within 20 minutes at the latest and the transaction will not be stuck forever.

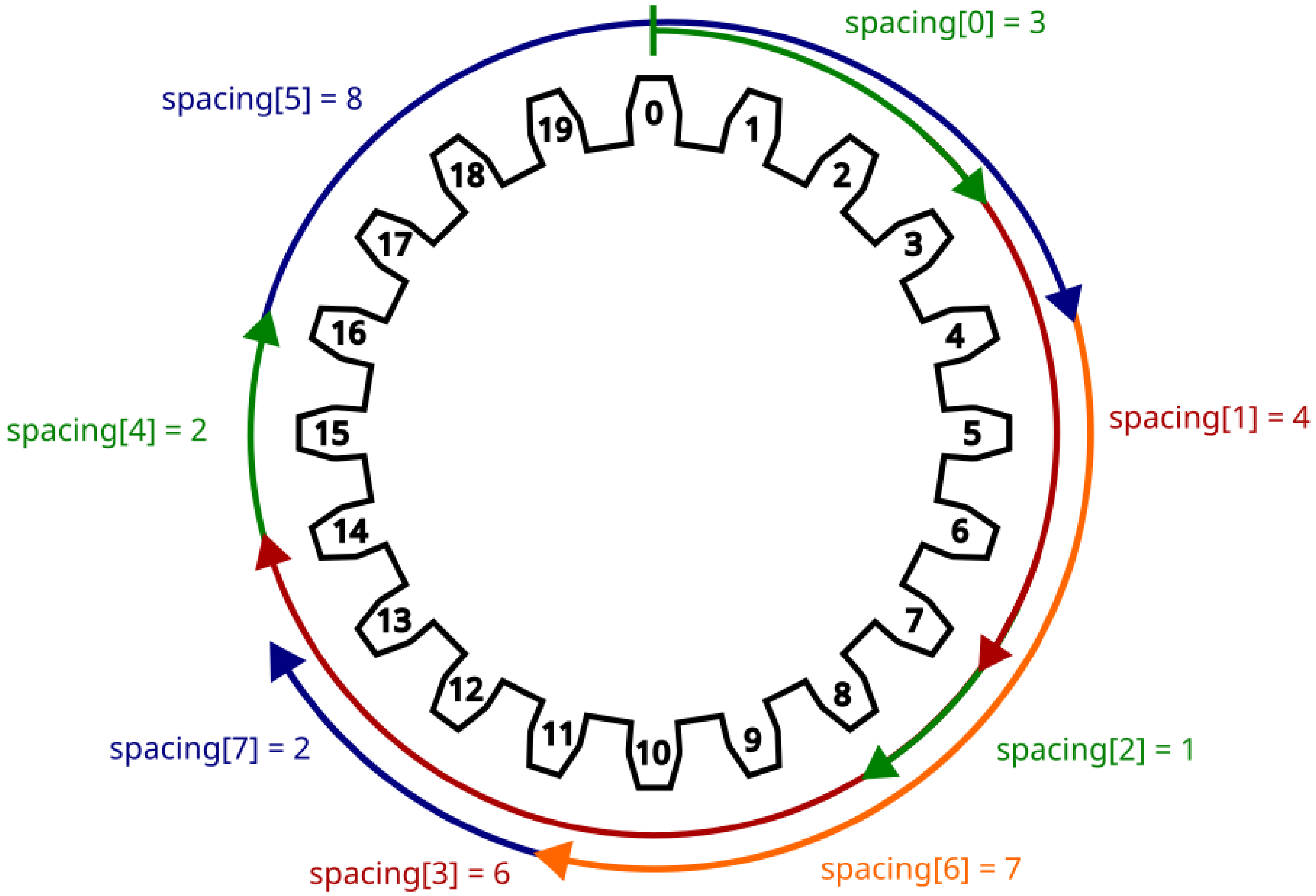
The algorithm for delegating 8 relayers for a transaction going through the bridge works as follows:

1. The bridge smart contract keeps a list of all wallet addresses that have registered as a relayer. Let’s visualize this list as a circle, because the algorithm is based on infinite shifting of the relayers list. For example, if there are 20 relayers in total, we will be adding a number 10, or 20, or 100, etc. to the index 15 to jump over the end of the list and get the relayer with index of 5 again, instead of getting non-existing relayer 25.

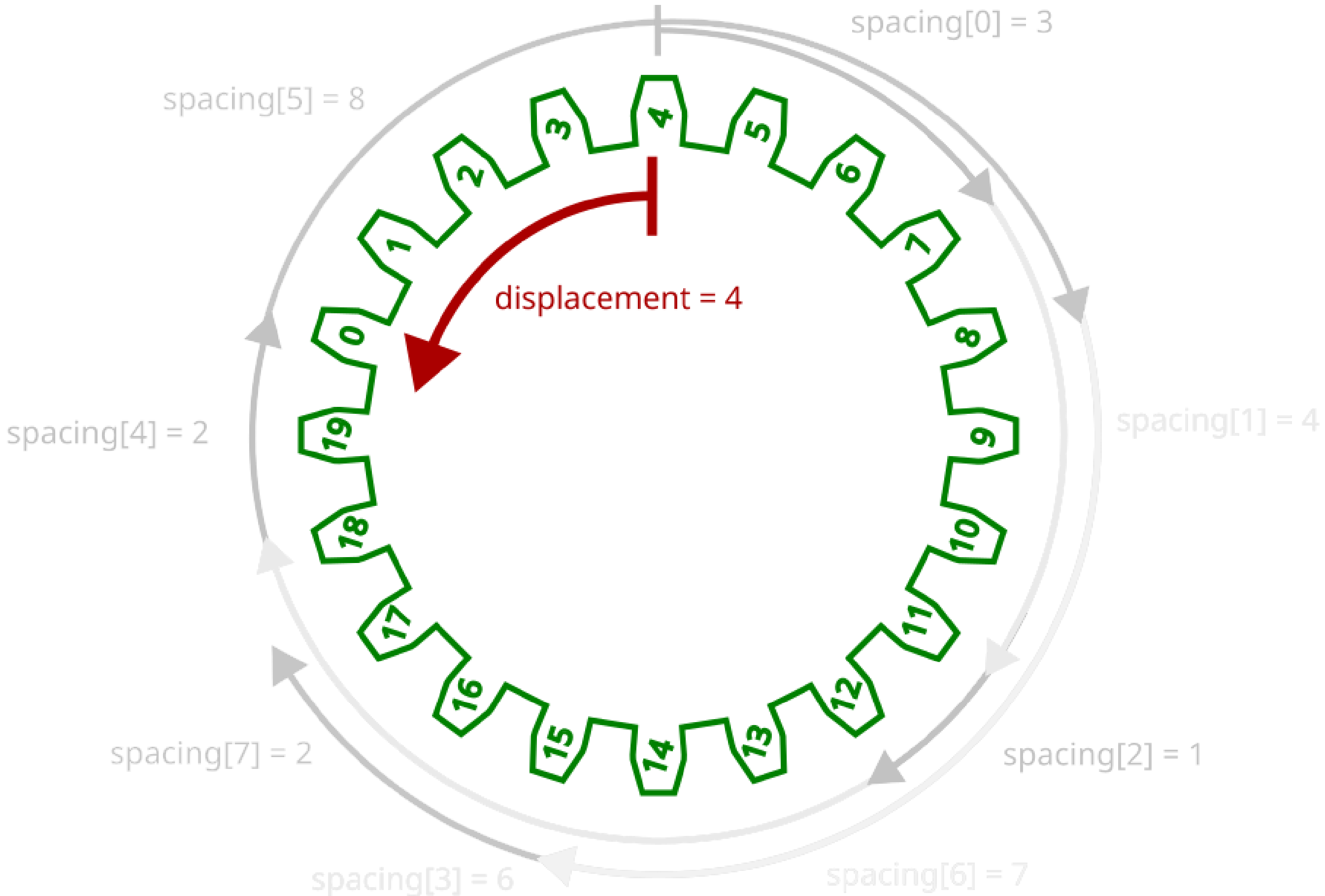


2. The smart contract picks up 8 individual spacings between relayers. These values will remain constant throughout the entire bridge epoch. To calculate these spacings, we are using transaction-independent pseudorandom data – hashes of previous blocks in the chain. Therefore

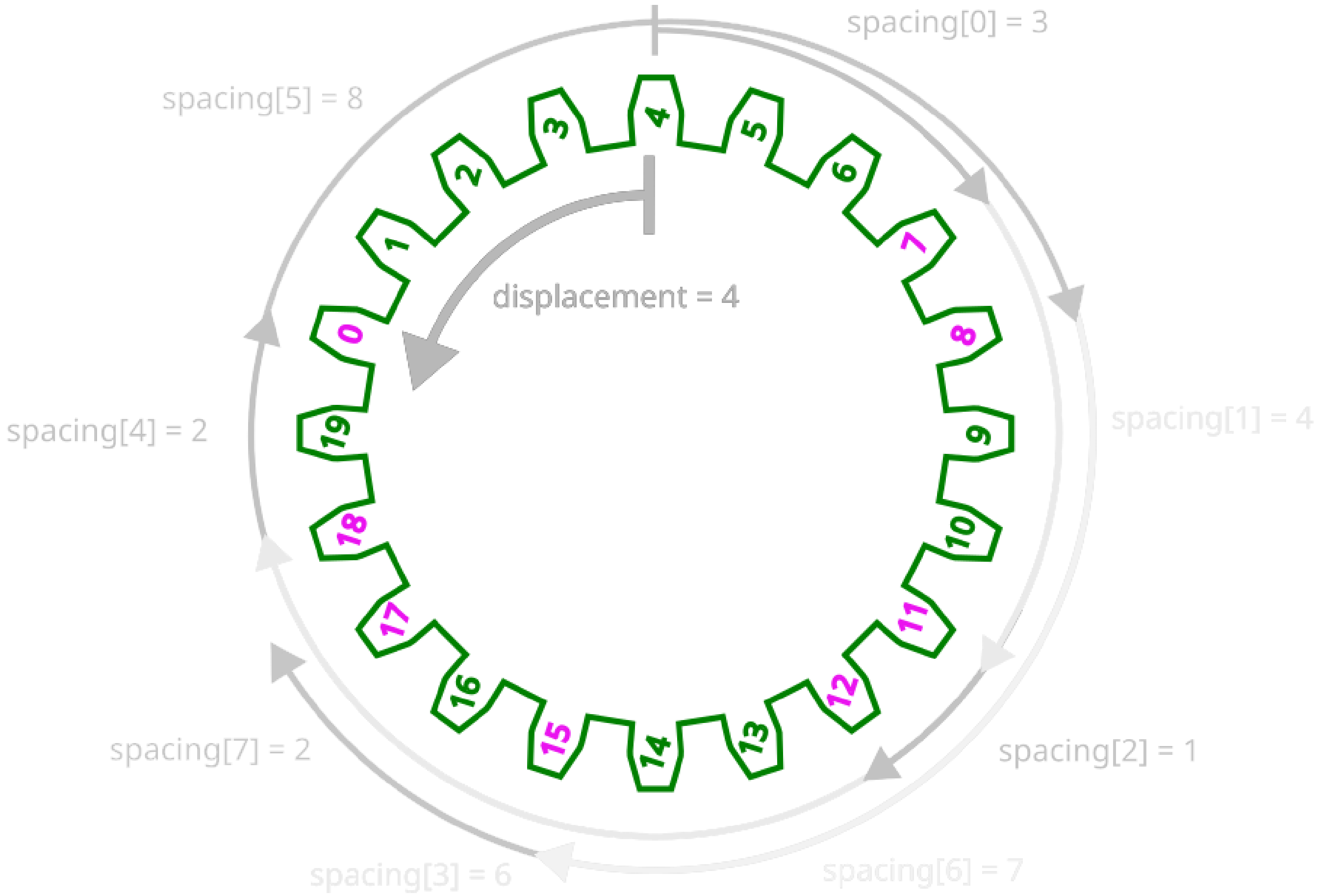
the bridge user has no influence on the calculated values. If we relied on transaction-dependent data, a hostile user could craft the transaction parameters in a such way, that only hostile relayers under his full control were delegated to validate the transaction. In our example, the calculated spacings have the following values: 3, 4, 1, 6, 2, 8, 7, 2.



3. For each transaction, the displacement of relayers list is calculated. We are shifting the entire list by a value based on transaction-dependent data, so each transaction, even in the same epoch, has a different set of relayers. Potential hostile bridge user can influence the calculated displacement by modifying the transaction parameters, but is still unable to modify the spacings from the previous step.



4. After applying the displacement, relayers selected to validate the transaction are as follows: 7, 11, 12, 18, 0, 8, 15, 17. The order is important - the signatures will be invalid if they are swapped.



> If the algorithm happens to select the same relayer twice or more, the next available relayer in the list is selected instead.

Revision #6
Created 20 May 2024 10:15:52 by Admin
Updated 21 May 2024 13:38:33 by Admin