How are attacks handled

The peer-to-peer mechanism of blockchain frameworks is very failure proof. Each node (in FairCoin any wallet or CVN is a node) checks the behavior of other connected nodes and ranks them. If the bad behavior of a node exceeds a certain level, then it is disconnected for 24 hours. This also helps to prevent DDoS attacks.

As CVNs behave like any other nodes and their IP addresses are not listed, they can not be easily identified. The only means to find a potential CVN is to connect to a huge number of nodes and monitor all the packages and determine where you got the block/signature/nonce pool first. This becomes increasingly harder after the number of nodes grows to some thousand. To make the network even more resilient, in future we could establish a network of full nodes at trusted partners that are very well connected. Selected CVNs could connect to these nodes only, to make them totally invisible.

By keeping the signatures are unencrypted, every node can verify the message's integrity and decides if it will relay it to other hosts or bans the host the forged message was received from.

If you want to analyze the block signing mechanism, have a look at the code and raise an issue in Github for comments.