Which digital signatures schemes are being used

We now use EC-Schnorr signatures for two aspects of FairCoin:

1. chain signatures - which legitimize the next creator to create its block
2. block signatures - proof that an actual CVN created the block and not some malicious entity

In this context, the current EC-Schnorr implementation is safe to use. It is very efficient and generates shotz signatures. But it can not be used for transaction signing. Here we still use the same elliptic curve signature scheme as Bitcoin does: ECDSA. We are currently looking also at Curve25519.