Contents

1 zerocash notes, and highlights

1.1 zerocoin drawbacks

zerocoin isn't used in daily transaction due to performance limitations, but rather for anonymization, or laundrying coins through decentralized mix. performance bottleneck is that redeeming zerocoins requires double-discrete-logarithm proofs of knowledge which have size that exceeds 45kb, and 450ms to verify(at the 128-bit security level), it uses fixed denominations, can't pay in zerocoin directly, provides anonymity for the original address only.

2 minting

minting coin $c := ((a_{pk}, PK_{enc}), v, \rho, r, s, cm)$ is:

$$tx_{mint} := (v, k, s, cm)$$

$$cm := COMM_s(v||k)$$

$$a_{pk} := PRF^{addr}_{a_{sk}}(0)$$

$$k := COMM_r(a_{pk}||\rho)$$

3 spending

Spending the coin c:

$$tx_{spend} := (cm, sn, \pi)$$

$$sn := PRF^{sn}_{a_{sk}}(\rho)$$

3.0.1 pouring

pouring $coin^{old}$ into $coin^{new}_1$, $coin^{new}_2$. with $v^{old} = v_{pub} + v^{new}_1 + v^{new}_2$ as follows:

$$tx_{pour} := (rt, sn^{old}, cm^{new}_1, cm^{new}_2, \pi_{pour}, enc_{pk^{new}_{enc,1}}(C_1), enc_{pk^{new}_{enc,2}}(C_2)$$

$$C_i = (v^{new}_i, \rho^{new}_i, r^{new}_i, s^{new}_i)$$

π_{pour} is the pouring sk-snark proof of the spending/pouring process. address for each participant is the pair $(addr_{pk}, addr_{sk})$, $addr_{pk} = (a_{enc}, pk_{enc})$, $addr_{sk} = (a_{sk}, sk_{enc})$