

BLIND DIRIE-HELMAN KEY EXCHANGE (BDHKE)

2 BLINDING

$$B_- = Y + rG$$

DH
KEY
EXCHANGE

$$\begin{aligned} C_- &= kB_- \\ C_- &= k(Y + rG) \\ C_- &= kY + krG \end{aligned}$$

SIGNING

3

k = PRIVATE KEY - MINT

K = PUB KEY - MINT

Q = PROMISE (BLINDED SIG)

7 MINT CHECKS

$$\begin{aligned} C &\stackrel{?}{=} K \cdot \text{HASH}(x) \\ &\stackrel{!}{=} K \cdot Y \end{aligned}$$

8 MINT CONFIRMS
VALID SPEND AND
ADD x TO
THE SPENDED
LIST

6
(x, C)

5 SENDING

ALICE SENDS
(x, C)

CAROL (REFUSER)

4 UNBLINDING

$$\begin{aligned} C_- - rK &= kY + krG - rK \\ &= kY + krG - rXG \\ &= kY \\ &= C \end{aligned}$$

1

$$x \rightarrow Y = \text{hash}(x)$$

Alice (SPENDER)

x = (tx, dom, script, ^{SECRET} nonce)

r = priv key (blinding factor)

T = BLINDED MESSAGE

Z = PROOF (UNBLINDED SIGNATURE)