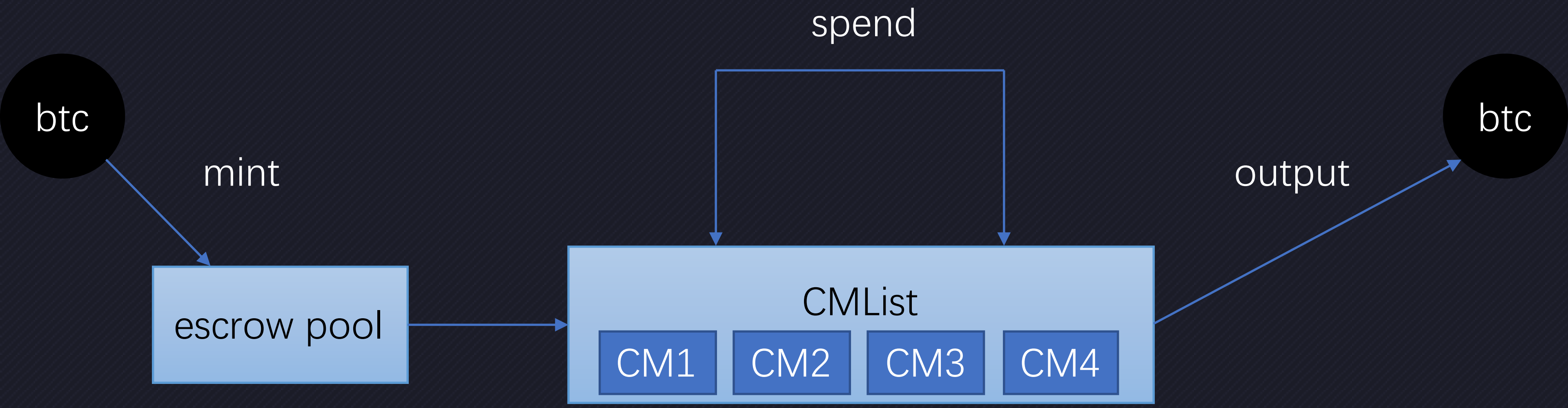
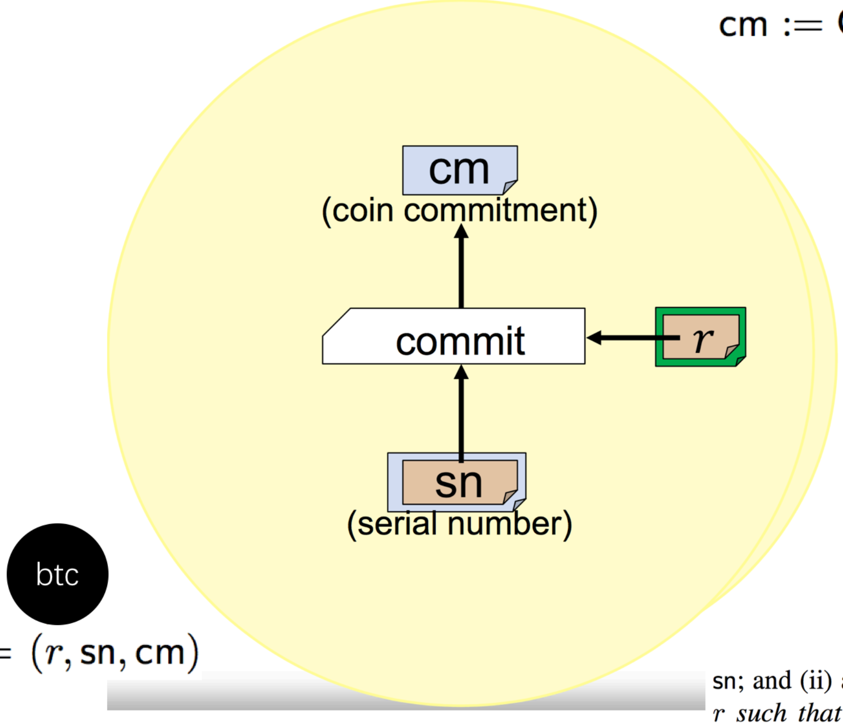
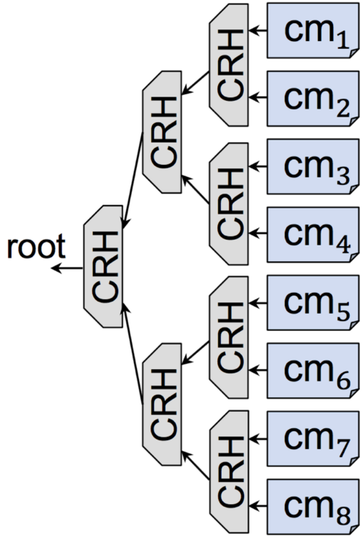
ZCash



ZCash

$$\mathsf{cm} := \mathsf{COMM}_r(\mathsf{sn})$$

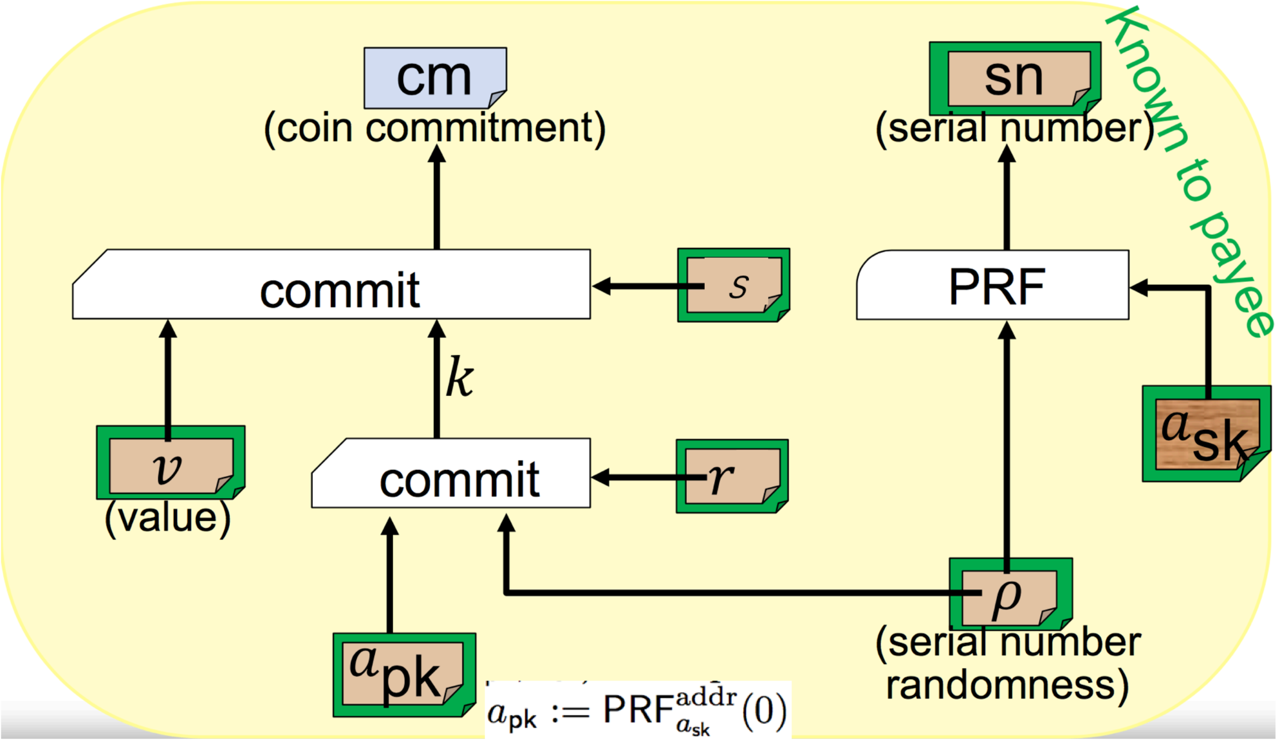




$$\mathbf{c} := (r, \mathsf{sn}, \mathsf{cm})$$

$\mathsf{tx}_{\mathsf{Spend}}$ that contains (i) the coin's serial number sn; and (ii) a zk-SNARK proof π of the NP statement *"I know r such that $\mathsf{COMM}_r(\mathsf{sn})$ appears in the list* CMList *of coin commitments"*.

ZCash

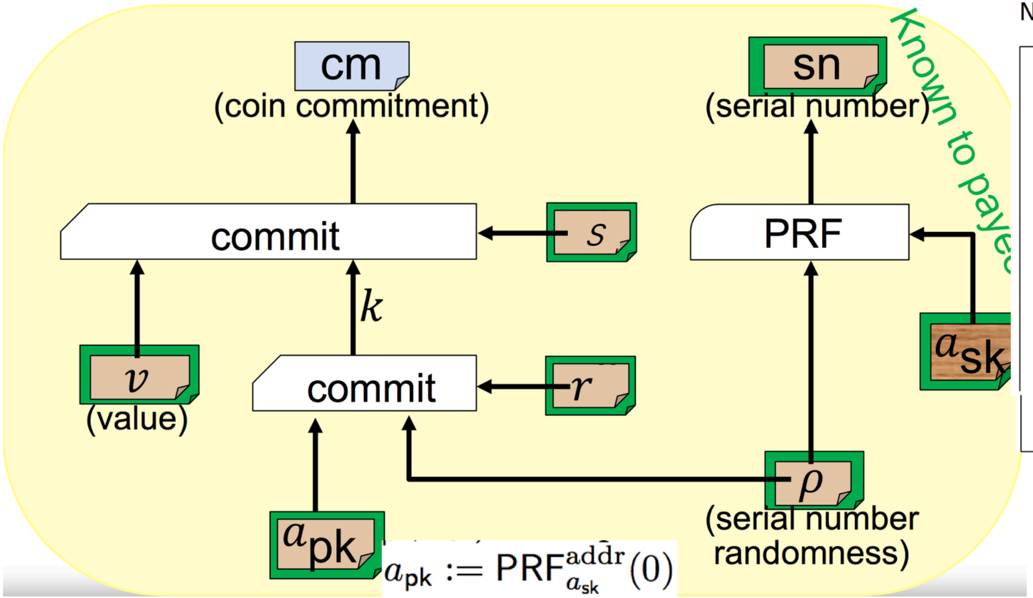


$\mathbf{c} := (a_{\mathsf{pk}}, v, \rho, r, s, \mathsf{cm})$

$\mathsf{tx}_{\mathsf{Mint}} := (v, k, s, \mathsf{cm})$

ZCash

$$\mathbf{c} := (a_{\mathsf{pk}}, v, \rho, r, s, \mathsf{cm})$$



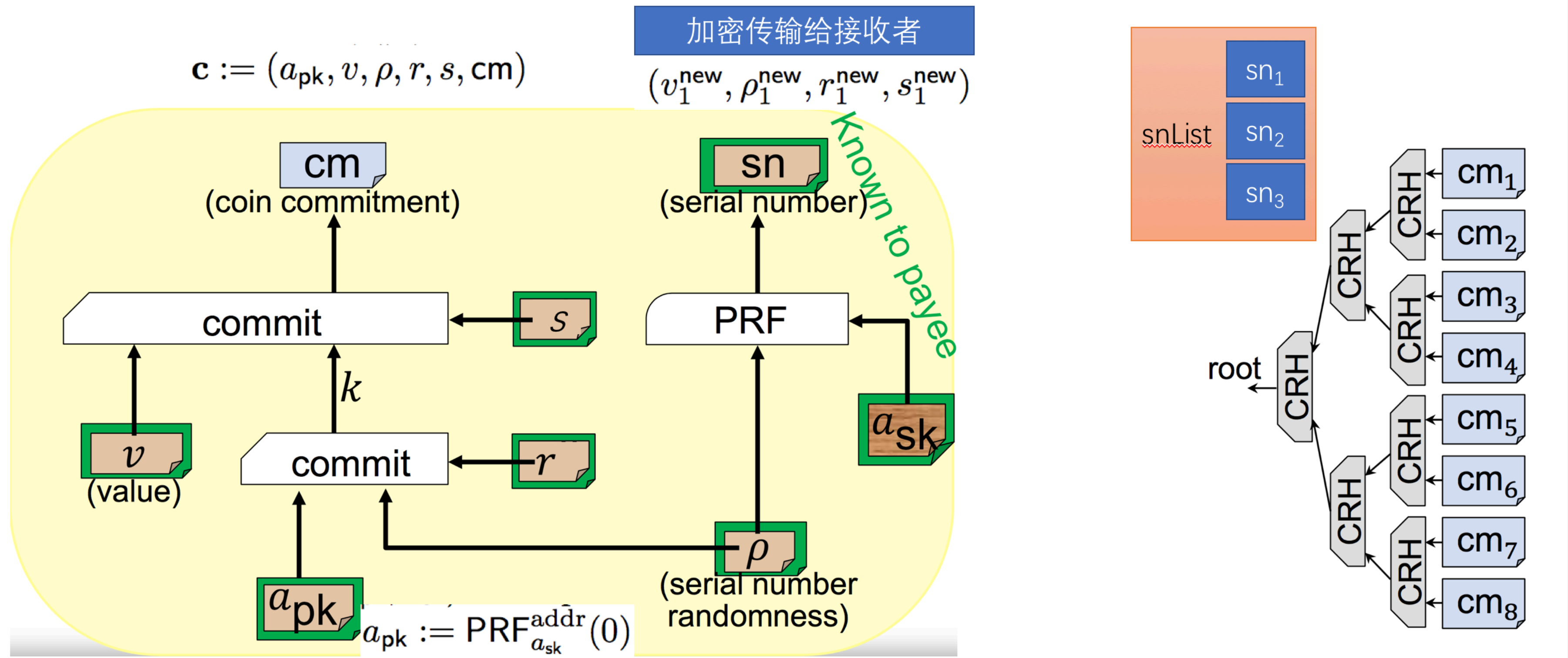
$$\mathbf{c}^{\mathsf{old}} = (a^{\mathsf{old}}_{\mathsf{pk}}, v^{\mathsf{old}}, \rho^{\mathsf{old}}, r^{\mathsf{old}}, s^{\mathsf{old}}, \mathsf{cm}^{\mathsf{old}})$$

This yields the coins $\mathbf{c}^{\mathsf{new}}_1 := (a^{\mathsf{new}}_{\mathsf{pk},1}, v^{\mathsf{new}}_1, \rho^{\mathsf{new}}_1, r^{\mathsf{new}}_1, s^{\mathsf{new}}_1, \mathsf{cm}^{\mathsf{new}}_1)$ and $\mathbf{c}^{\mathsf{new}}_2 := (a^{\mathsf{new}}_{\mathsf{pk},2}, v^{\mathsf{new}}_2, \rho^{\mathsf{new}}_2, r^{\mathsf{new}}_2, s^{\mathsf{new}}_2, \mathsf{cm}^{\mathsf{new}}_2)$. Next, u produces a zk-SNARK proof $\pi_{\mathtt{POUR}}$ for the following NP statement, which we call `POUR`:

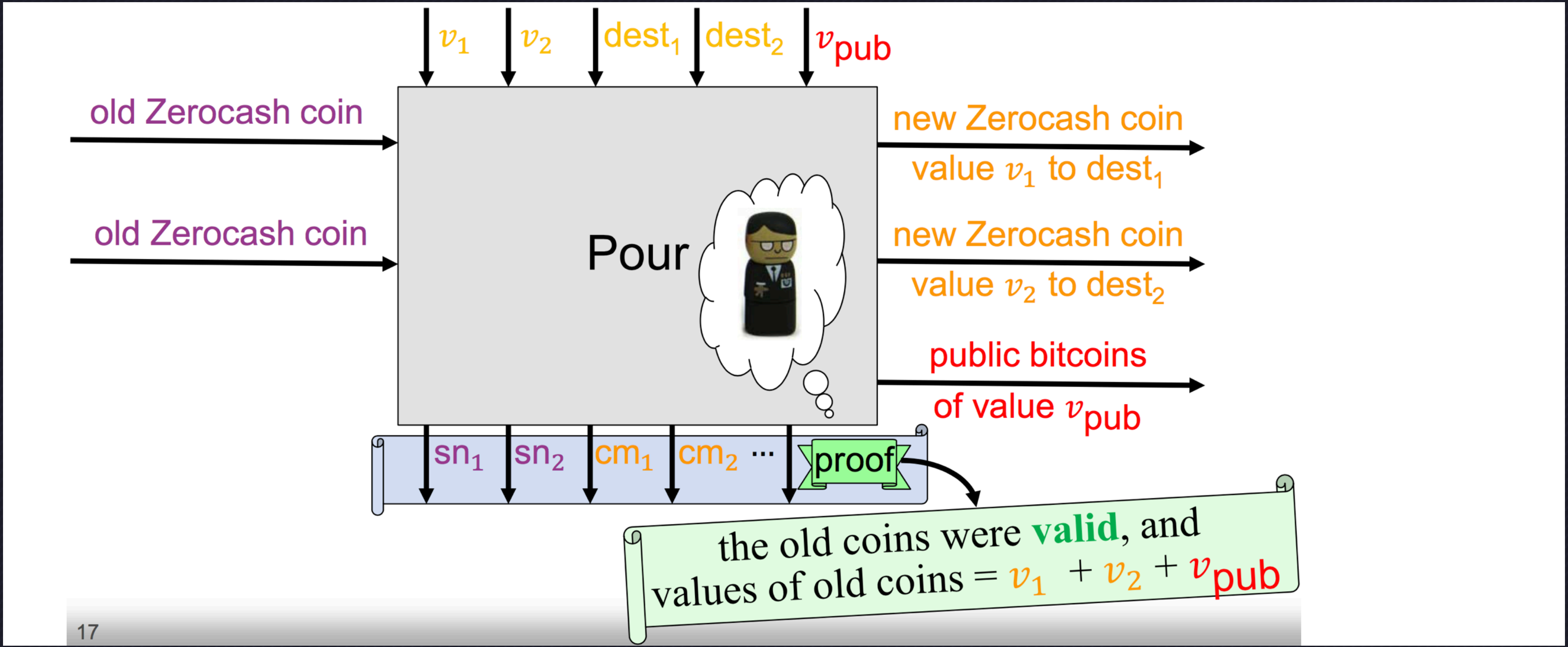
"Given the Merkle-tree root rt*, serial number* $\mathsf{sn}^{\mathsf{old}}$*, and coin commitments* $\mathsf{cm}^{\mathsf{new}}_1, \mathsf{cm}^{\mathsf{new}}_2$*, I know coins* $\mathbf{c}^{\mathsf{old}}, \mathbf{c}^{\mathsf{new}}_1, \mathbf{c}^{\mathsf{new}}_2$*, and address secret key* $a^{\mathsf{old}}_{\mathsf{sk}}$ *such that:*

- *The coins are well-formed: for* $\mathbf{c}^{\mathsf{old}}$ *it holds that* $k^{\mathsf{old}} = \mathsf{COMM}_{r^{\mathsf{old}}}(a^{\mathsf{old}}_{\mathsf{pk}} \| \rho^{\mathsf{old}})$ *and* $\mathsf{cm}^{\mathsf{old}} = \mathsf{COMM}_{s^{\mathsf{old}}}(v^{\mathsf{old}} \| k^{\mathsf{old}})$*; and similarly for* $\mathbf{c}^{\mathsf{new}}_1$ *and* $\mathbf{c}^{\mathsf{new}}_2$*.*
- *The address secret key matches the public key:* $a^{\mathsf{old}}_{\mathsf{pk}} = \mathsf{PRF}^{\mathrm{addr}}_{a^{\mathsf{old}}_{\mathsf{sk}}}(0)$*.*
- *The serial number is computed correctly:* $\mathsf{sn}^{\mathsf{old}} := \mathsf{PRF}^{\mathrm{sn}}_{a^{\mathsf{old}}_{\mathsf{sk}}}(\rho^{\mathsf{old}})$*.*
- *The coin commitment* $\mathsf{cm}^{\mathsf{old}}$ *appears as a leaf of a Merkle-tree with root* rt*.*
- *The values add up:* $v^{\mathsf{new}}_1 + v^{\mathsf{new}}_2 = v^{\mathsf{old}}$*."*

ZCash


加密传输给接收者
$\mathbf{c} := (a_{\mathsf{pk}}, v, \rho, r, s, \mathsf{cm})$
$(v_1^{\mathsf{new}}, \rho_1^{\mathsf{new}}, r_1^{\mathsf{new}}, s_1^{\mathsf{new}})$
cm
(coin commitment)
sn
(serial number)
Known to payee
commit
s
PRF
k
v
(value)
commit
r
a_{sk}
ρ
(serial number randomness)
a_{pk}
$a_{\mathsf{pk}} := \mathsf{PRF}^{\mathrm{addr}}_{a_{\mathsf{sk}}}(0)$
snList
sn1
sn2
sn3
root
CRH
cm1
cm2
cm3
cm4
cm5
cm6
cm7
cm8

ZCash


v_1
v_2
dest_1
dest_2
v_{pub}
old Zerocash coin
old Zerocash coin
Pour
new Zerocash coin
value v_1 to dest_1
new Zerocash coin
value v_2 to dest_2
public bitcoins
of value v_{pub}
sn_1 sn_2 cm_1 cm_2 ···
proof
the old coins were **valid**, and
values of old coins = $v_1 + v_2 + v_{\text{pub}}$
17