

EVE

ALICE

TREES
 $H(\text{"TREES"}) \rightarrow C \longrightarrow$

C

\leftarrow GUESS

ANSWER \rightarrow

"TREES" \longrightarrow
"CLOUDS" \longrightarrow

$H(\text{"TREES"}) \stackrel{?}{=} C$
 $H(\text{"CLOUDS"}) \stackrel{?}{=} C$

EVE

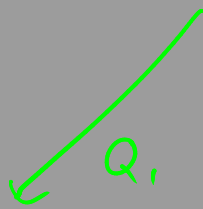
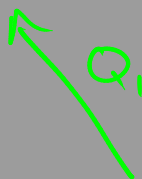
sk_E, vk_E



Q_1 ~~T_{Q_1}~~ σ_{Q_1}



A_1 ~~$SIGN_{sk_A}(A_1) = \sigma_{A_1}$~~
 ~~$MAC_K(A_1) = T_{A_1}$~~



TTP

(BLOCKCHAIN)

Q_1 A_1

Q_2 A_2

\vdots

sk_A, vk_A
ALICE

ALICE'S sk_A

$SIGN_{sk_A}(Q_1) = \sigma_{Q_1}$

Q_1 ~~$MAC_K(Q_1) = T_{Q_1}$~~

A_1 T_{A_1} σ_{A_1}

$VERIFY_{vk}(A_1, \sigma_{A_1})$

$T_{Q_1} \leftarrow A_1 \leftarrow T_{Q_2}$



LOTS OF PEOPLE KEEP
TRACK.

SID

EVE sk_E, vk_E, vk_A

SID

ALICE sk_A, vk_A, vk_E

Q_1, σ_{Q_1}

$Q_1, \sigma_{Q_1} = \text{SIGN}_{sk_A}(\underbrace{Q_1}_{H(Q_1)})$

$A_1, \sigma_{A_1} = \text{SIGN}_{sk_E}(\underbrace{A_1, Q_1}_{H(A_1, Q_1)})$

A_1, σ_{A_1}

Q_2, σ_{Q_2}

$Q_2, \sigma_{Q_2} = \text{SIGN}_{sk_A}(\underbrace{Q_2, \sigma_{A_1}}_{H(Q_2, \sigma_{A_1})})$

$A_2, \sigma_{A_2} = \text{SIGN}(A_2, \sigma_{Q_2})$

SIGNED



Q_1

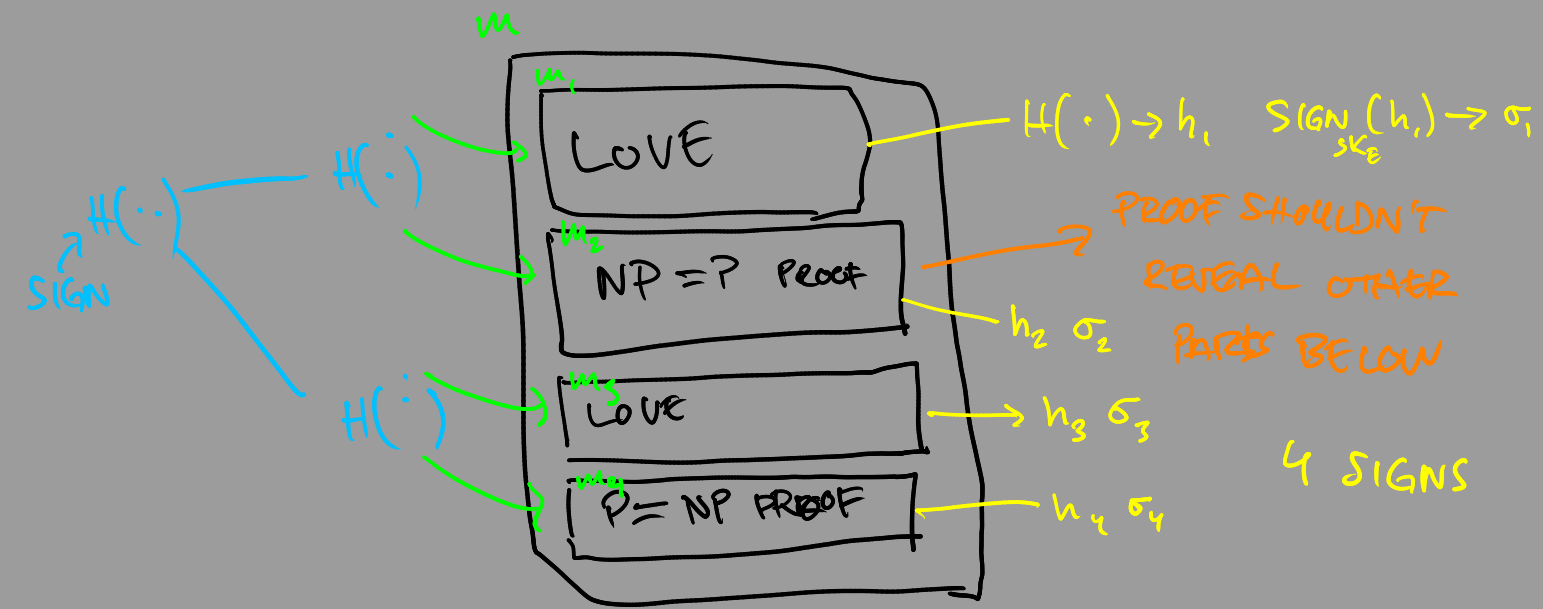
SIGNED



A_1

Q_2

A_2



$$H(m) \rightarrow h_m \quad \text{SIGN}(h_m) \rightarrow \sigma_m$$

$$\text{SIGN}(h_1, h_2, h_3, h_4) \rightarrow \sigma_m$$

$$H(h_1, h_2, h_3, h_4) \rightarrow h_{all}$$