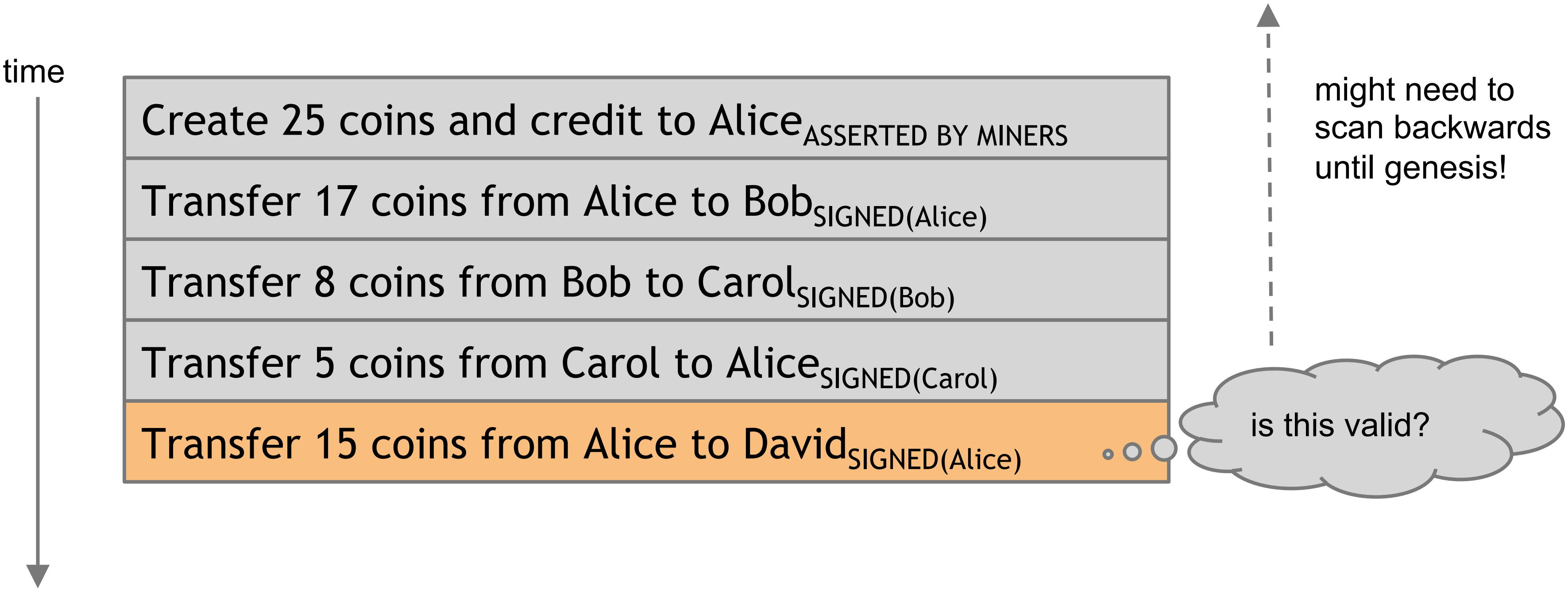


time

Create 25 coins and credit to Alice$_{\text{ASSERTED BY MINERS}}$

Transfer 17 coins from Alice to Bob$_{\text{SIGNED(Alice)}}$

Transfer 8 coins from Bob to Carol$_{\text{SIGNED(Bob)}}$

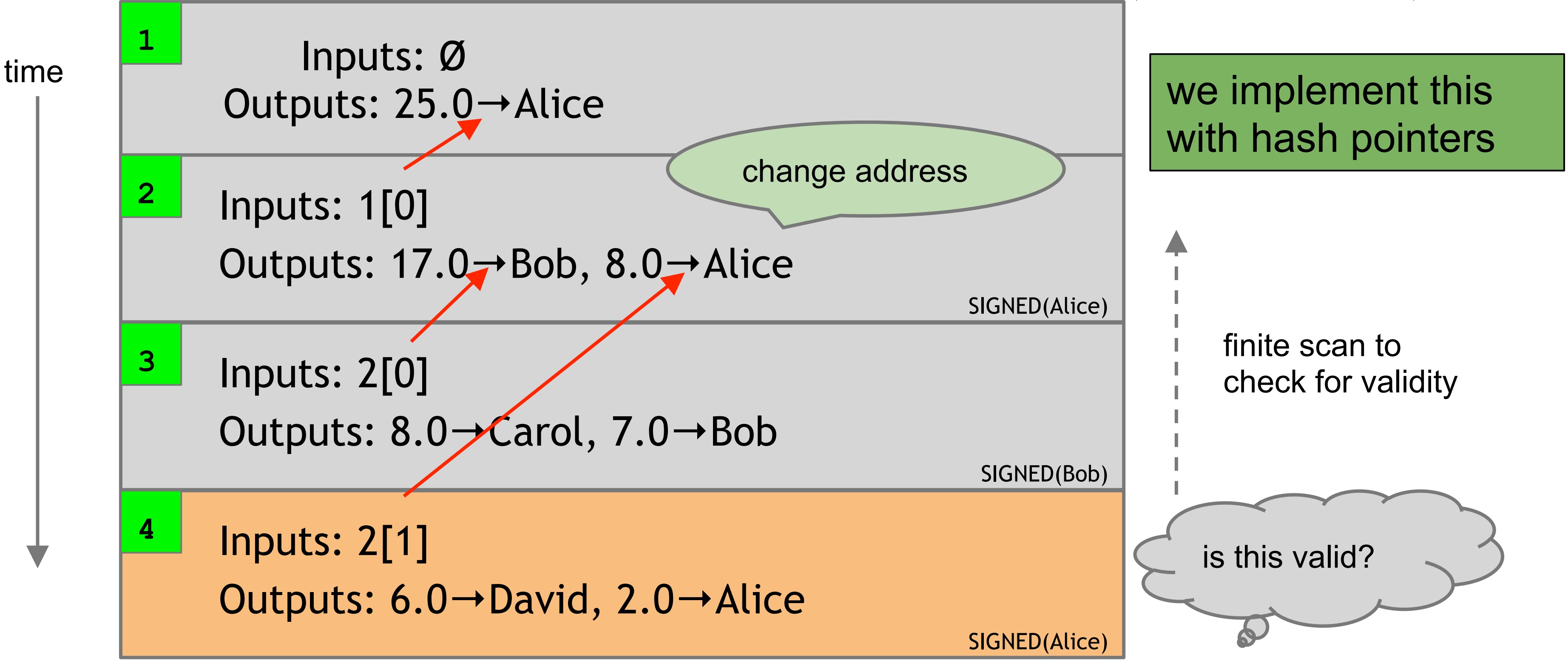
Transfer 5 coins from Carol to Alice$_{\text{SIGNED(Carol)}}$

Transfer 15 coins from Alice to David$_{\text{SIGNED(Alice)}}$

is this valid?

might need to scan backwards until genesis!

SIMPLIFICATION: only one transaction per block



time

1

Inputs: Ø

Outputs: 25.0→Alice

2

Inputs: 1[0]

Outputs: 17.0→Bob, 8.0→Alice

SIGNED(Alice)

change address

3

Inputs: 2[0]

Outputs: 8.0→Carol, 7.0→Bob

SIGNED(Bob)

4

Inputs: 2[1]

Outputs: 6.0→David, 2.0→Alice

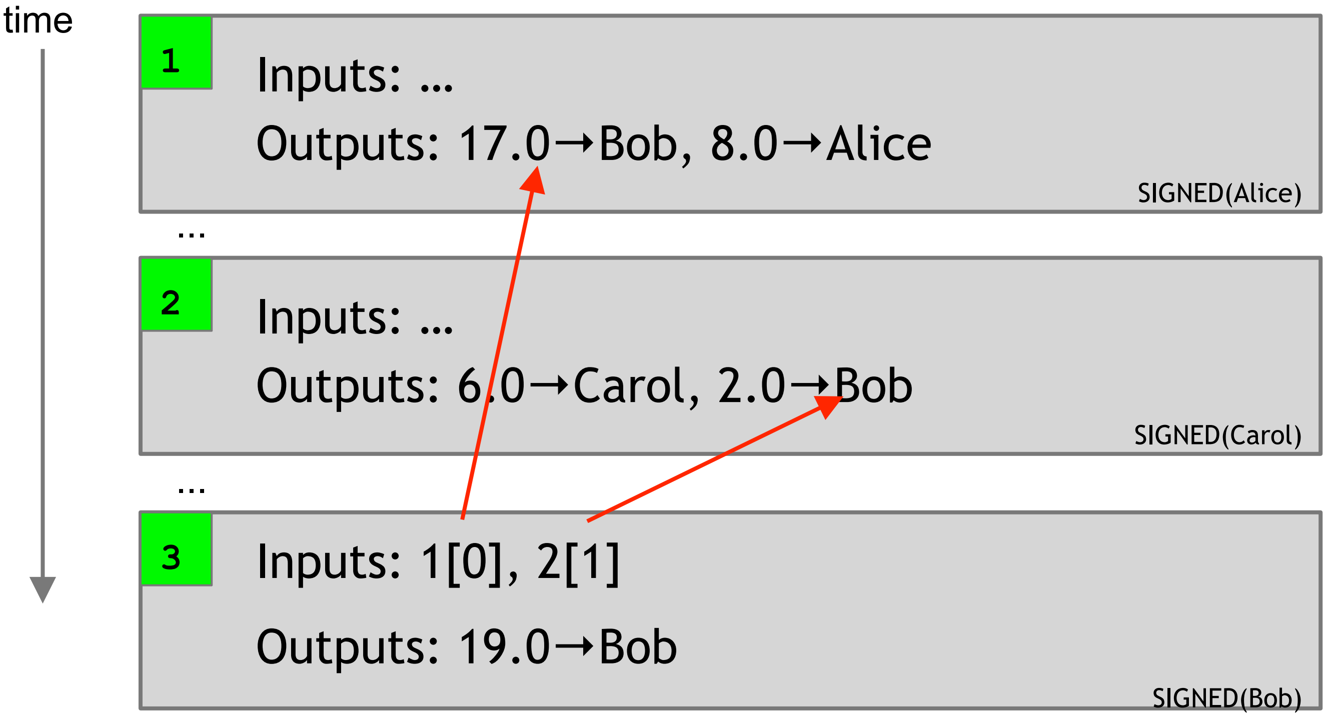
SIGNED(Alice)

we implement this with hash pointers

finite scan to check for validity

is this valid?

SIMPLIFICATION: only one transaction per block



time

1

Inputs: ...

Outputs: 17.0→Bob, 8.0→Alice

SIGNED(Alice)

...

2

Inputs: ...

Outputs: 6.0→Carol, 2.0→Bob

SIGNED(Carol)

...

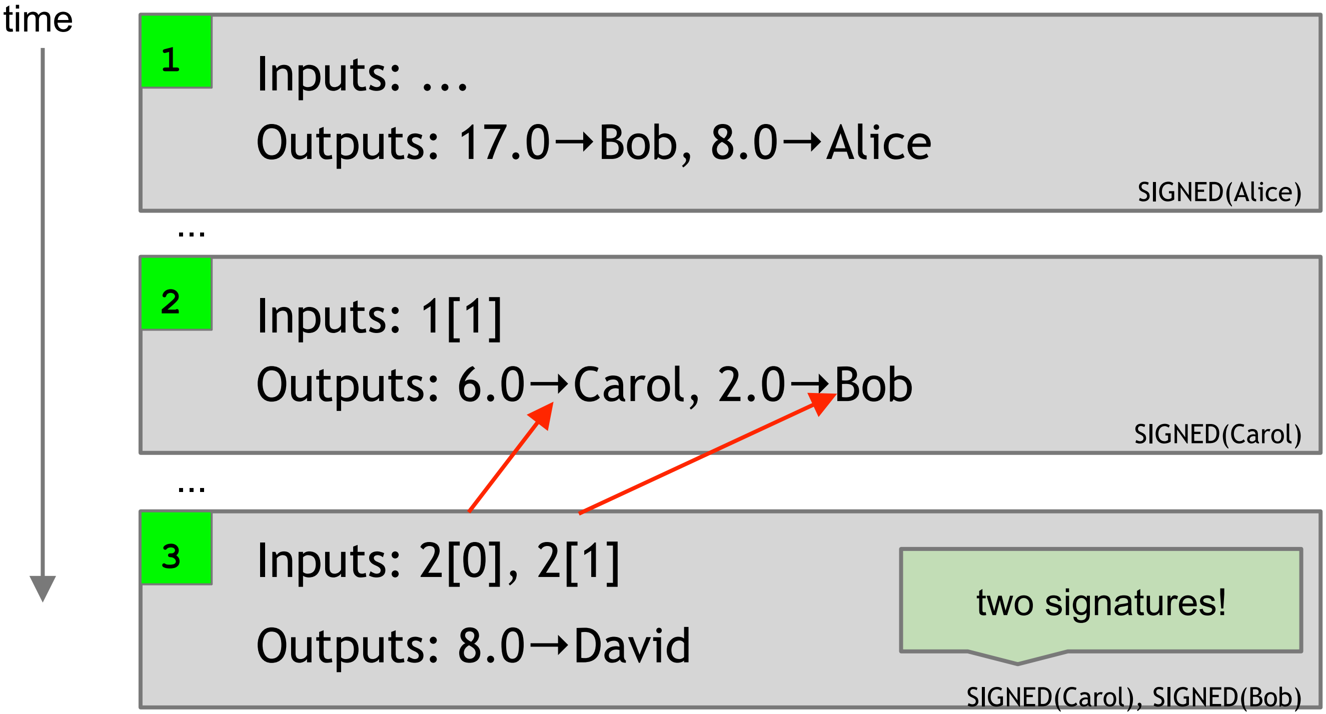
3

Inputs: 1[0], 2[1]

Outputs: 19.0→Bob

SIGNED(Bob)

SIMPLIFICATION: only one transaction per block



time

1

Inputs: ...

Outputs: 17.0→Bob, 8.0→Alice

SIGNED(Alice)

...

2

Inputs: 1[1]

Outputs: 6.0→Carol, 2.0→Bob

SIGNED(Carol)

...

3

Inputs: 2[0], 2[1]

Outputs: 8.0→David

two signatures!

SIGNED(Carol), SIGNED(Bob)

SIMPLIFICATION: only one transaction per block