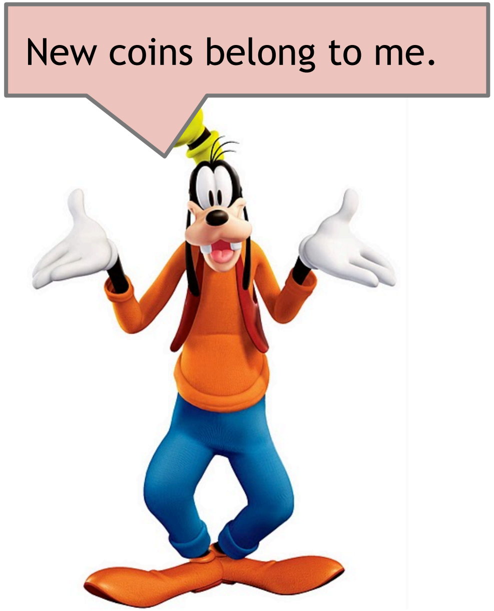
GoofyCoin

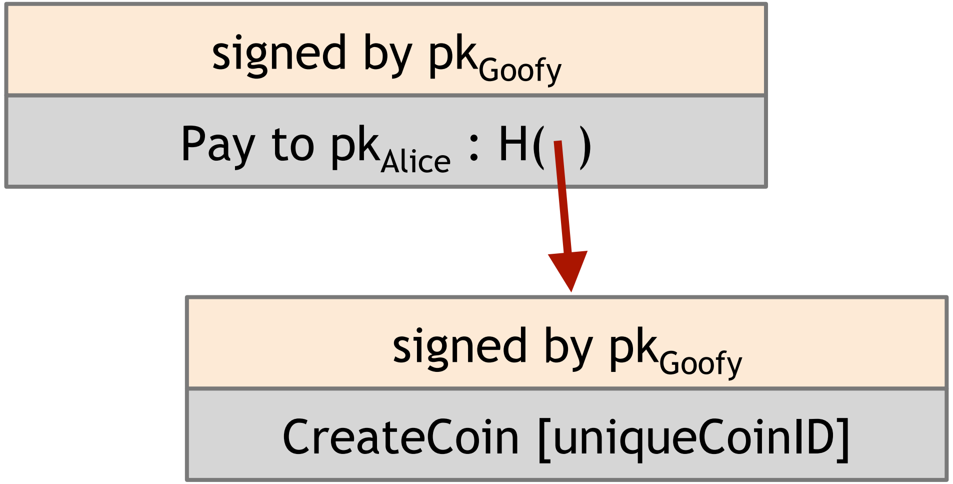
Goofy can create new coins

signed by pk_{Goofy}

CreateCoin [uniqueCoinID]



A coin’s owner can spend it.



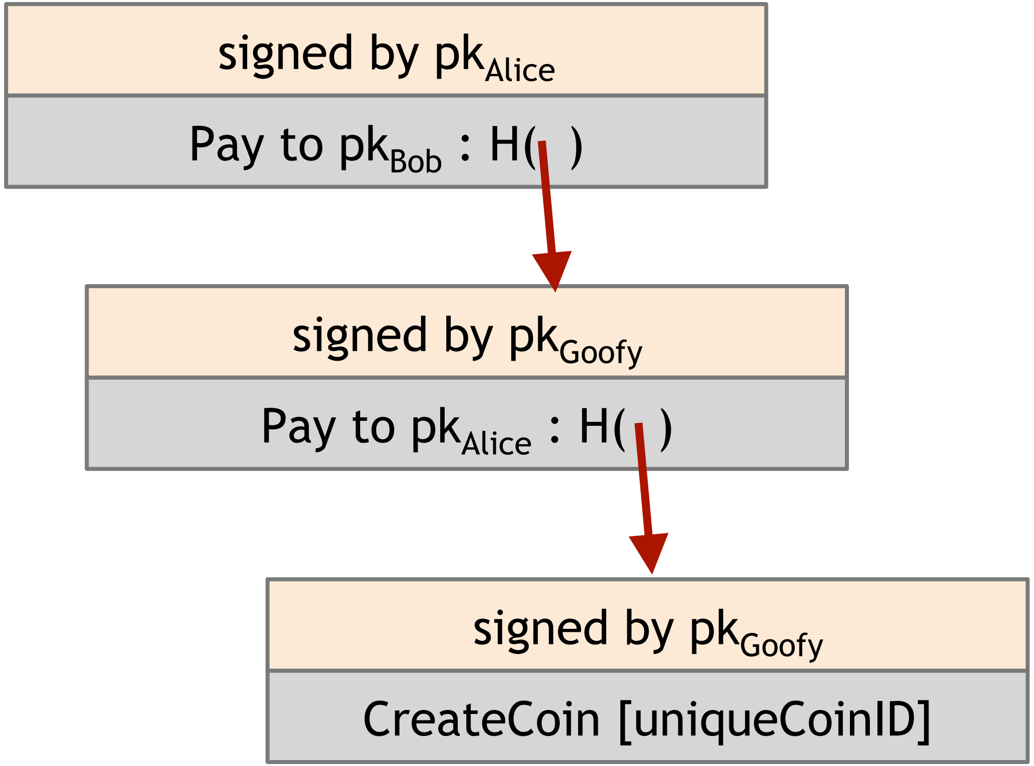
signed by pk_{Goofy}

Pay to pk_{Alice} : H( )

signed by pk_{Goofy}

CreateCoin [uniqueCoinID]

The recipient can pass on the coin again.



signed by pk_{Alice}

Pay to pk_{Bob} : H( )

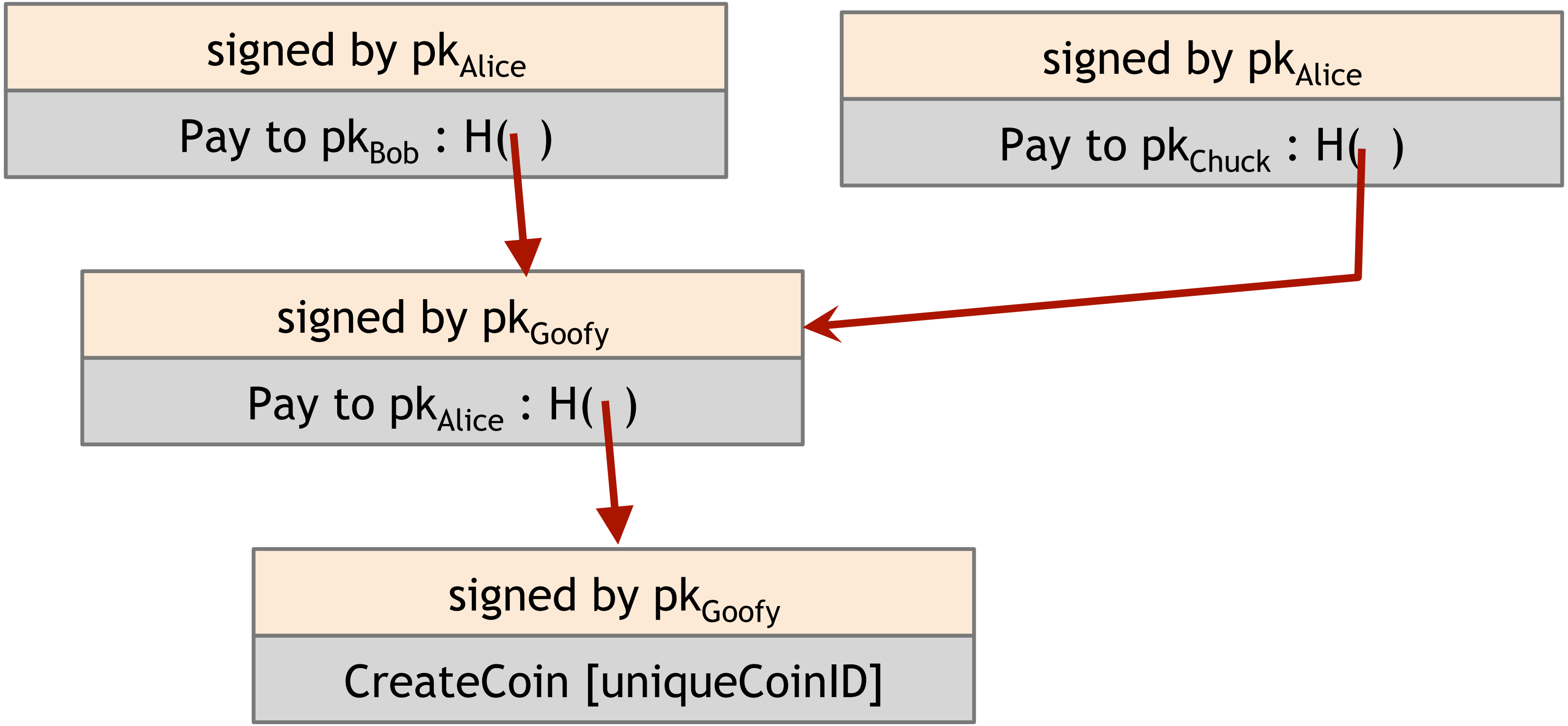
signed by pk_{Goofy}

Pay to pk_{Alice} : H( )

signed by pk_{Goofy}

CreateCoin [uniqueCoinID]

double-spending attack



signed by pk_{Alice}

Pay to pk_{Bob} : H( )

signed by pk_{Alice}

Pay to pk_{Chuck} : H( )

signed by pk_{Goofy}

Pay to pk_{Alice} : H( )

signed by pk_{Goofy}

CreateCoin [uniqueCoinID]