Blockchain Technology
(BITS F452)

BITS Pilani
Pilani Campus

Dr. Ashutosh Bhatia, Dr. Kamlesh Tiwari
Department of Computer Science and Information Systems

innovate achieve lead

BITS Pilani

Pilani Campus

A simple Cryptocurrency

Useful trick: Public key == Identity

If you see sig such a verify(pk; msg; sig) == true

Think of it as

pk says “[msg]”

To speak for **pk** you must know **sk**

Decentralized Identity Management

Anybody can make a new identity at anytime

make as many as you want

No central point of coordination

These identities are called “addresses” in Bitcoin

Privacy

Addresses not directly connected to real world identity

But observer can link together an address's activity over time

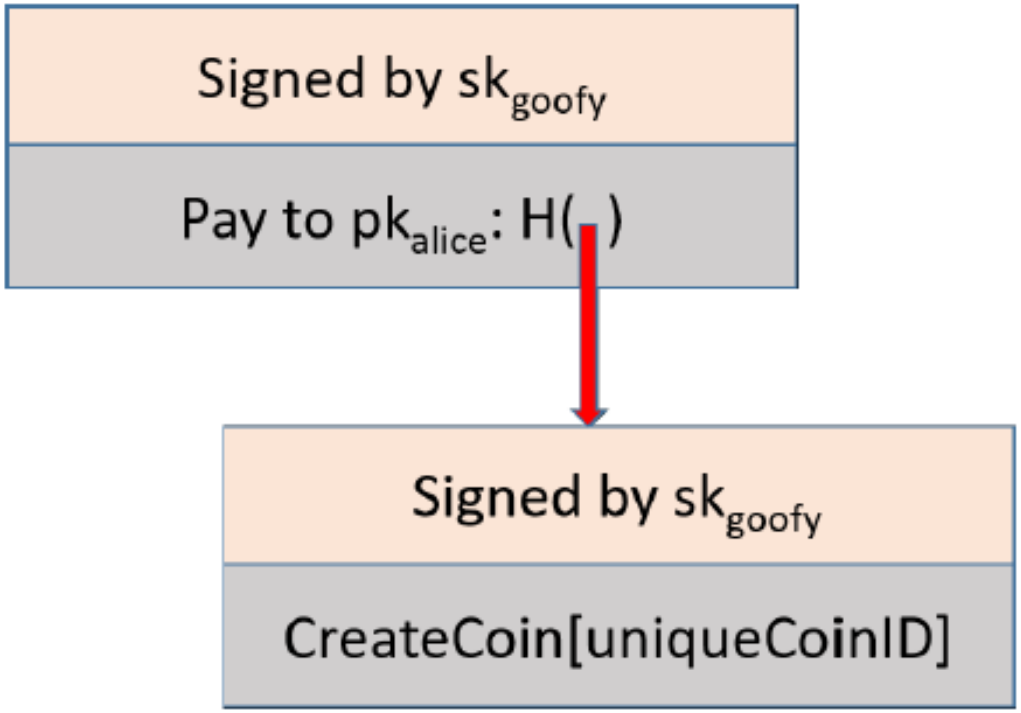
GoofyCoin

Goofy, can create new coins

Signed by sk_{goofy}
CreateCoin[uniqueCoinID]

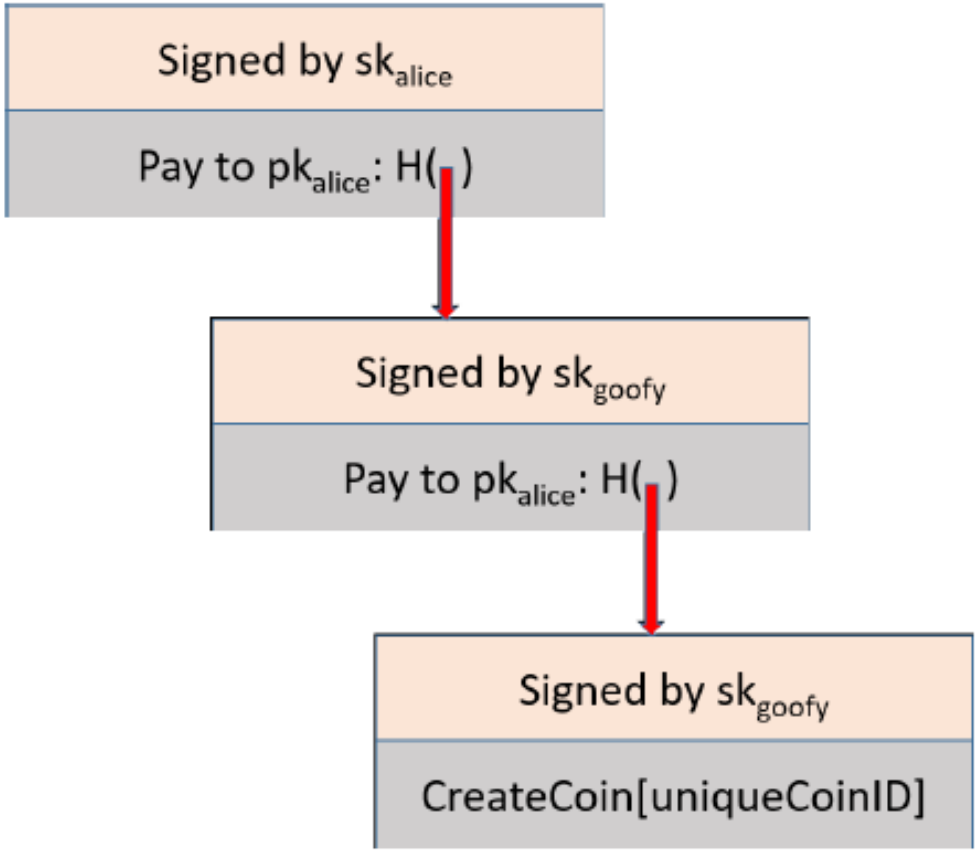
GoofyCoin

A coin's owner can spend it



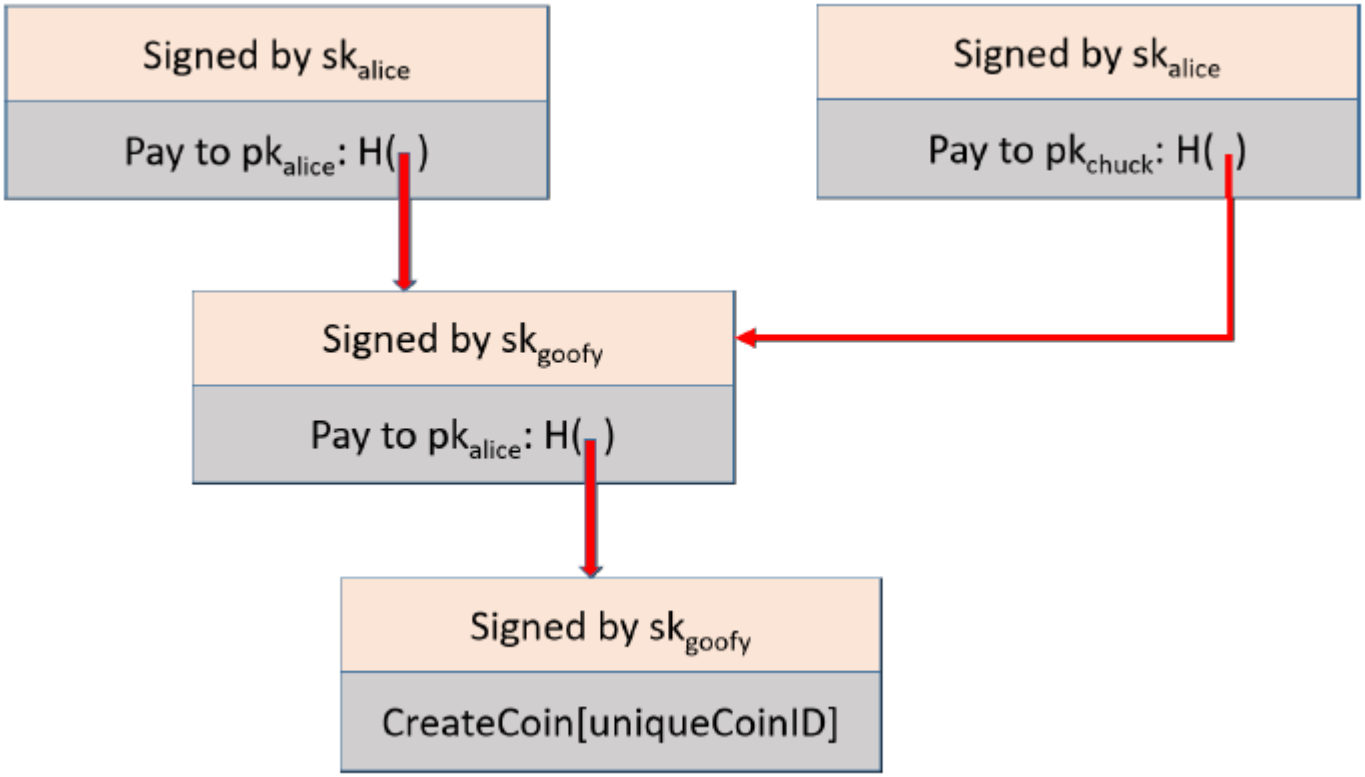
GoofyCoin

A recipient can pass the coin again



GoofyCoin

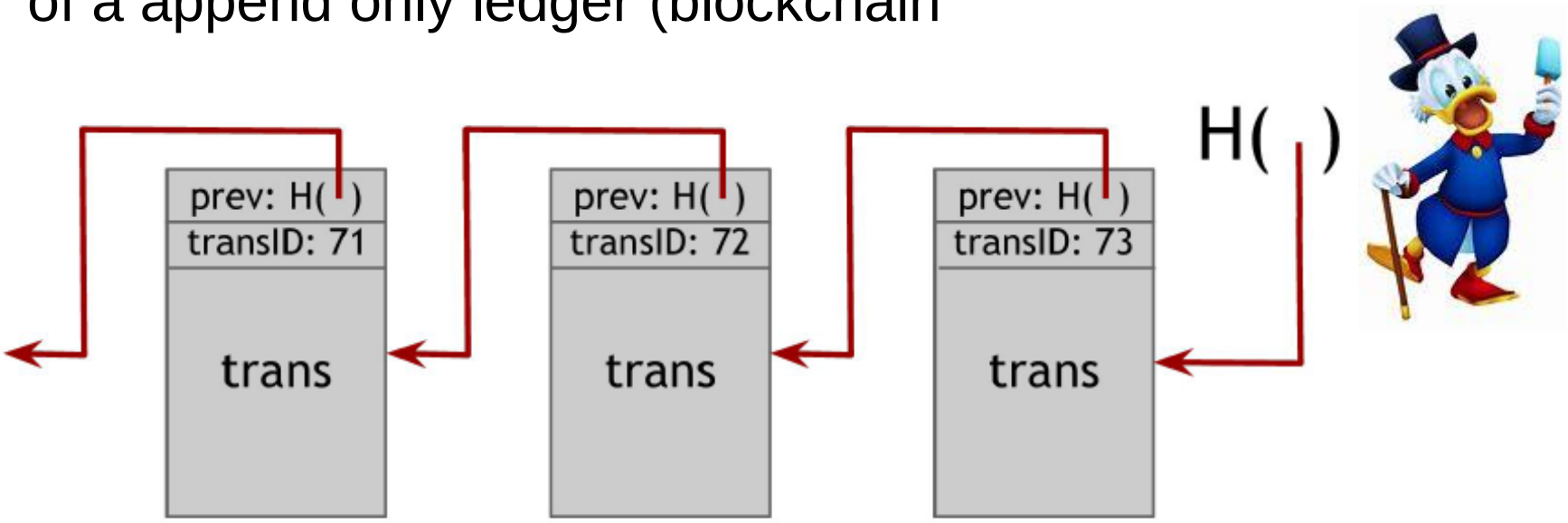
Double Spending Problem



ScroogeCoin

ScroogeCoin: Solving Double Spending Problem

Scrooge publishes a history of all the transactions in form of a append only ledger (blockchain

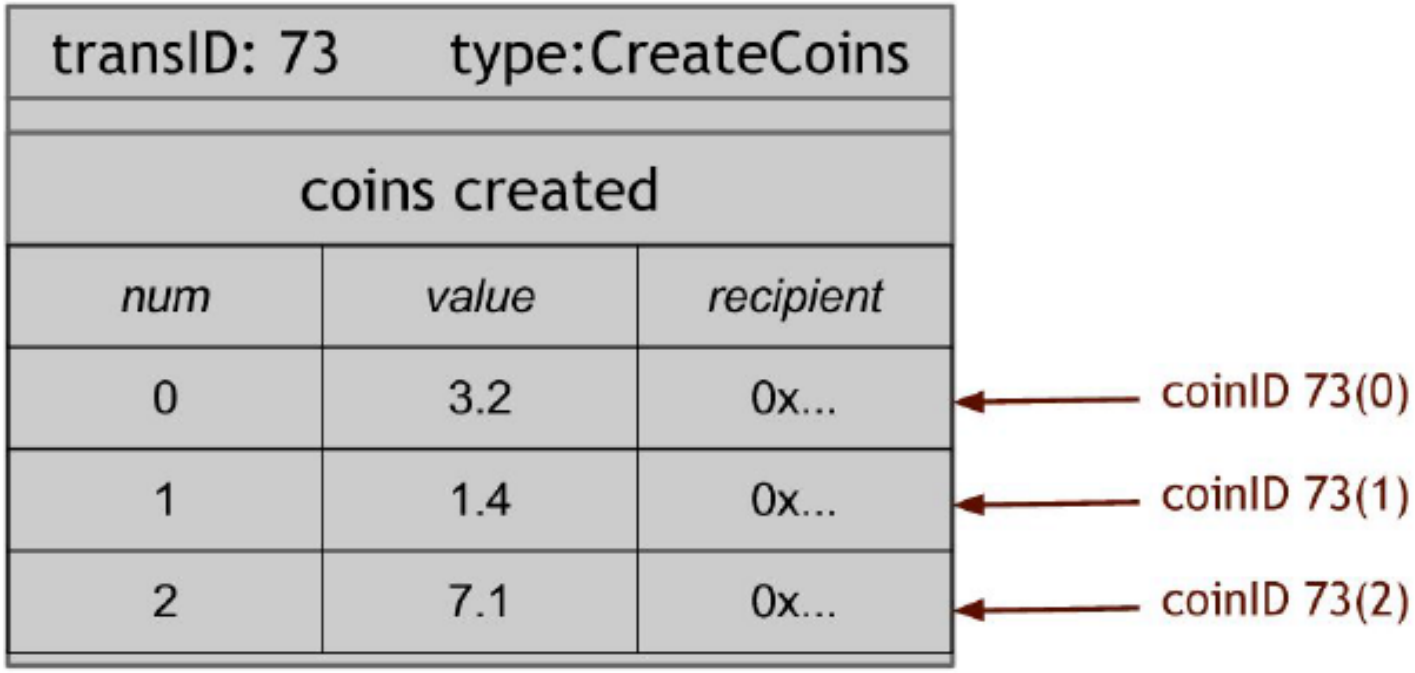


Optimization: put multiple transactions in the same block

ScroogeCoin

innovate achieve lead

CreateCoin Transaction create a new coin



ScroogeCoin

A Paycoin transaction consumes some coins and creates new coins of the same value

transID: 73 type:PayCoins		
consumed coinIDs: 68(1), 42(0), 72(3)		
coins created		
num	*value*	*recipient*
0	3.2	0x...
1	1.4	0x...
2	7.1	0x...
signatures		

Valid if

- ✓ Consumed coins are valid
- ✓ Not already consumed
- ✓ total value out = total value in
- ✓ signed by owners of all consumed coins

ScroogeCoin

Problem with the scrooge coin

Coins can’t be transferred, subdivided or combined

but you can get the same effect by using transactions to sub divide:

create a new transaction, consume your coin and pay out two new coins to yourself.

ScroogeCoin

Crucial Question

Can we de-scoogify the currency and operate without a trusted third party

We need to figure out:

How every one agree upon a single public block chain

How every one agree upon which transactions are valid

How to assign IDs to coins in a decentralized manner.