

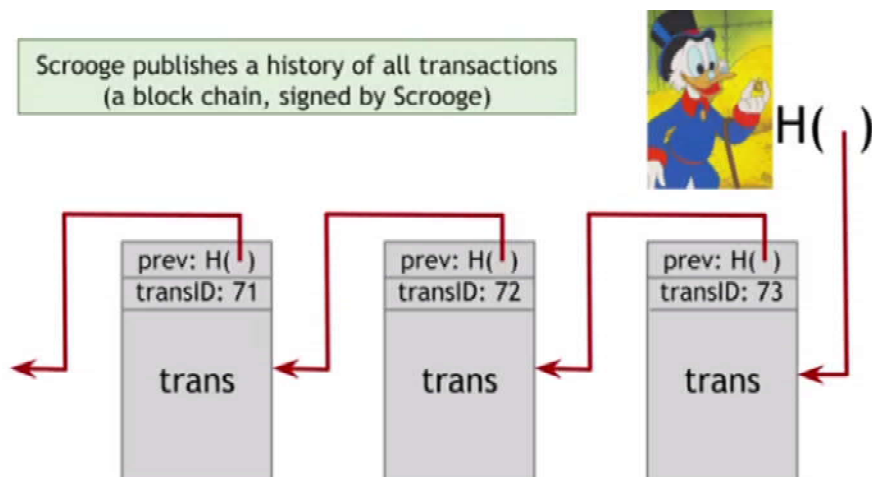
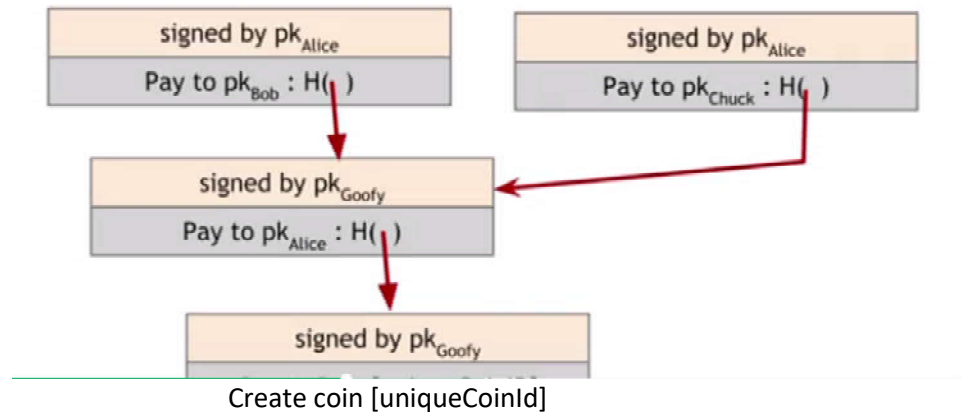
# Crypto Currency Introduction

15 August 2017 03:31 PM

Goofy Coin: (Simplest Crypto Currency)

Not Secure -- Though simple due to Double spending attack

## double-spending attack



This can prevent double spending attack as we would be able to know the History of transaction.

CreateCoins transaction creates new coins

transID: 73 type:CreateCoins		
coins created		
num	value	recipient
0	3.2	0x...
1	1.4	0x...
2	7.1	0x...

coinID 73(0)

coinID 73(1)

coinID 73(2)

Valid, because I said so.



PayCoins transaction consumes (and destroys) some coins,  
and creates new coins of the same total value

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

Valid if:  
-- consumed coins valid,  
-- not already consumed,  
-- total value out = total value in, and  
-- signed by owners of all consumed coins

SIGNATURES

=====

What if Scrooge is not honest ?

It is centralized as only scrooge can manage all coins