PATRICK MURCK II BERKMAN CENTER

PROPERTY LAW & THE BLOCKCHAIN



Bitcoin is an electronic transaction network designed to settle payment obligations like physical cash transactions - quickly, securely and with finality.

COMMON ASSUMPTIONS

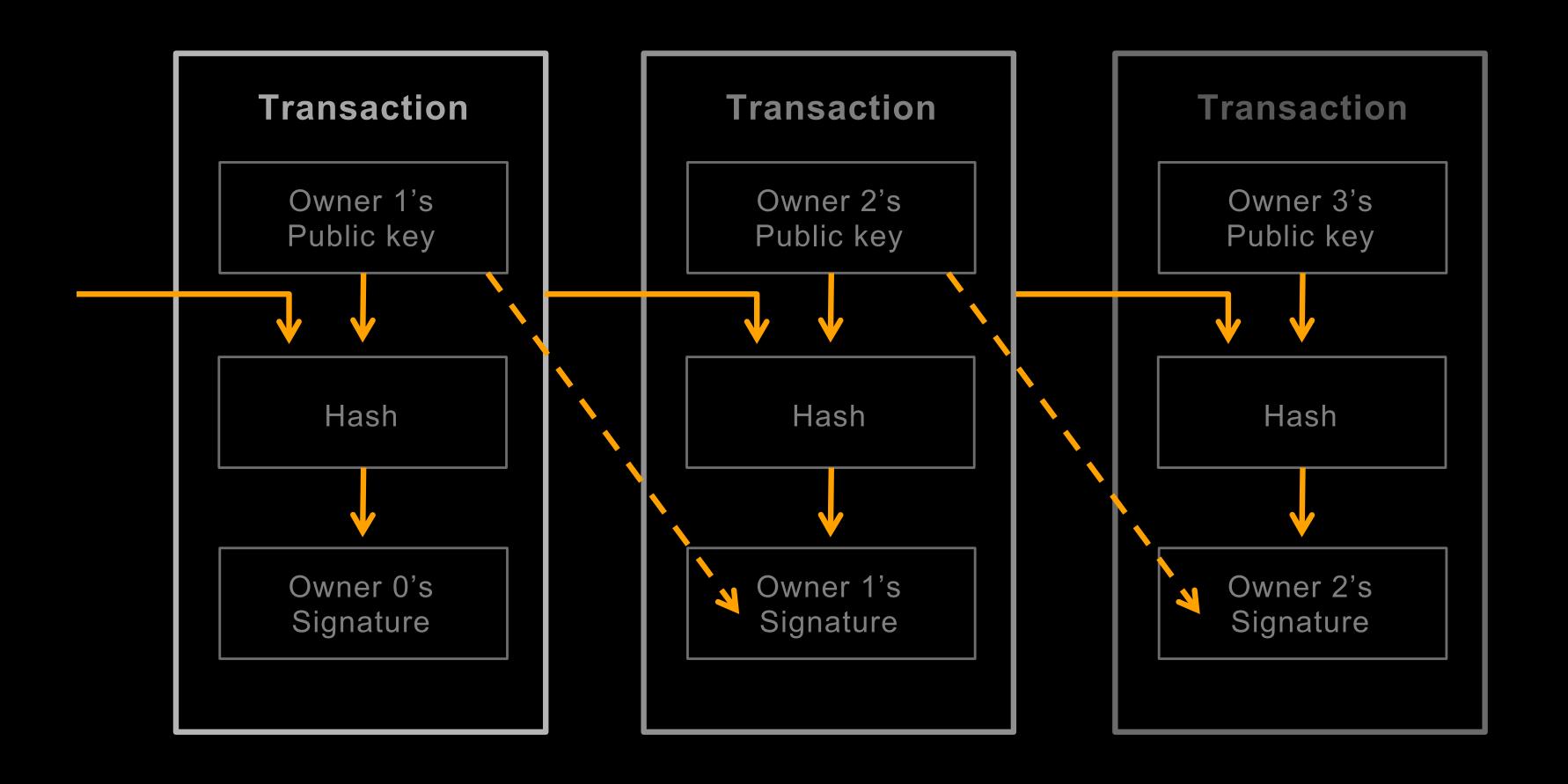
- There are discrete and identifiable "coins" that are transferred across the network from one "account" to another "account"
- These "coins" are traceable from transaction to transaction through a public "ledger"

What property right can one claim in blockchain assets?

Where do these rights attach and when?

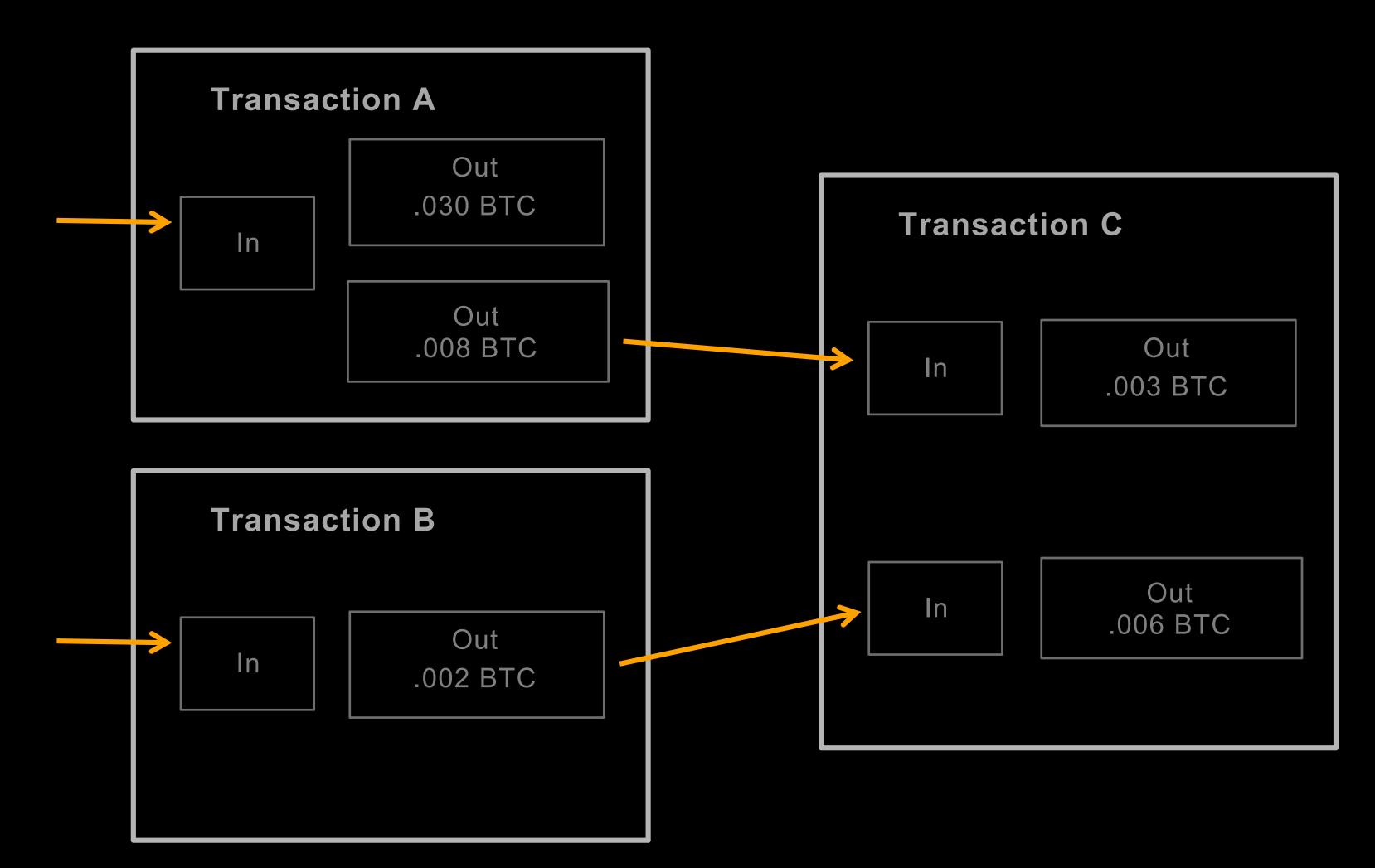
By what means can I enforce my rights and against whom?

TRACING TRANSACTIONS



TRACING COINS

- Where did the output from Transaction B go?
- How much of Transaction
 B's output went to pay transaction fees?



TRACING OWNERSHIP

Unlocking Script (scriptSig)

Locking Script (scriptPubKey)

<sig> <PubK>

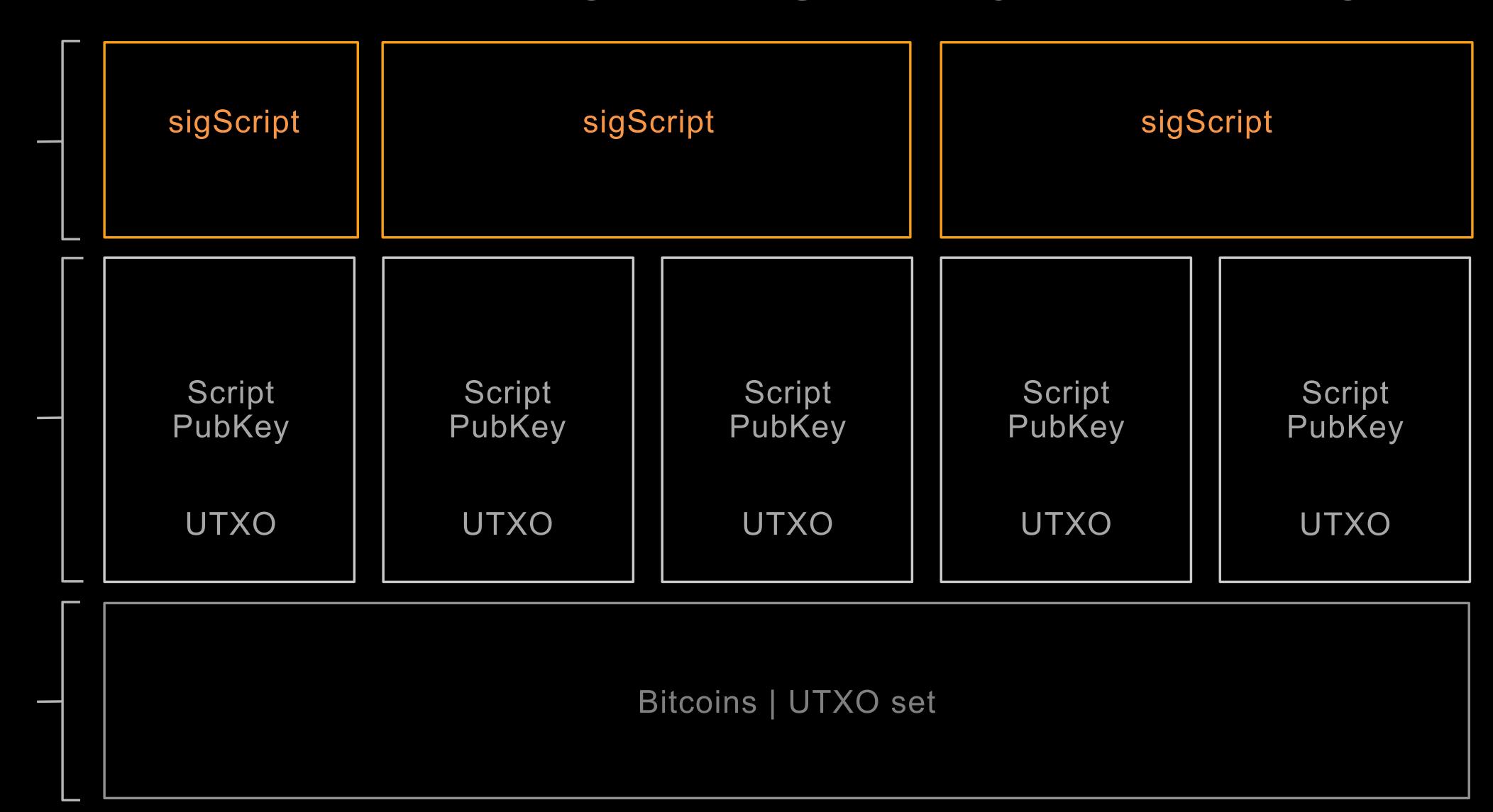
DUP HASH160 < PubKHash> EQUALVERIFY CHECKSIG

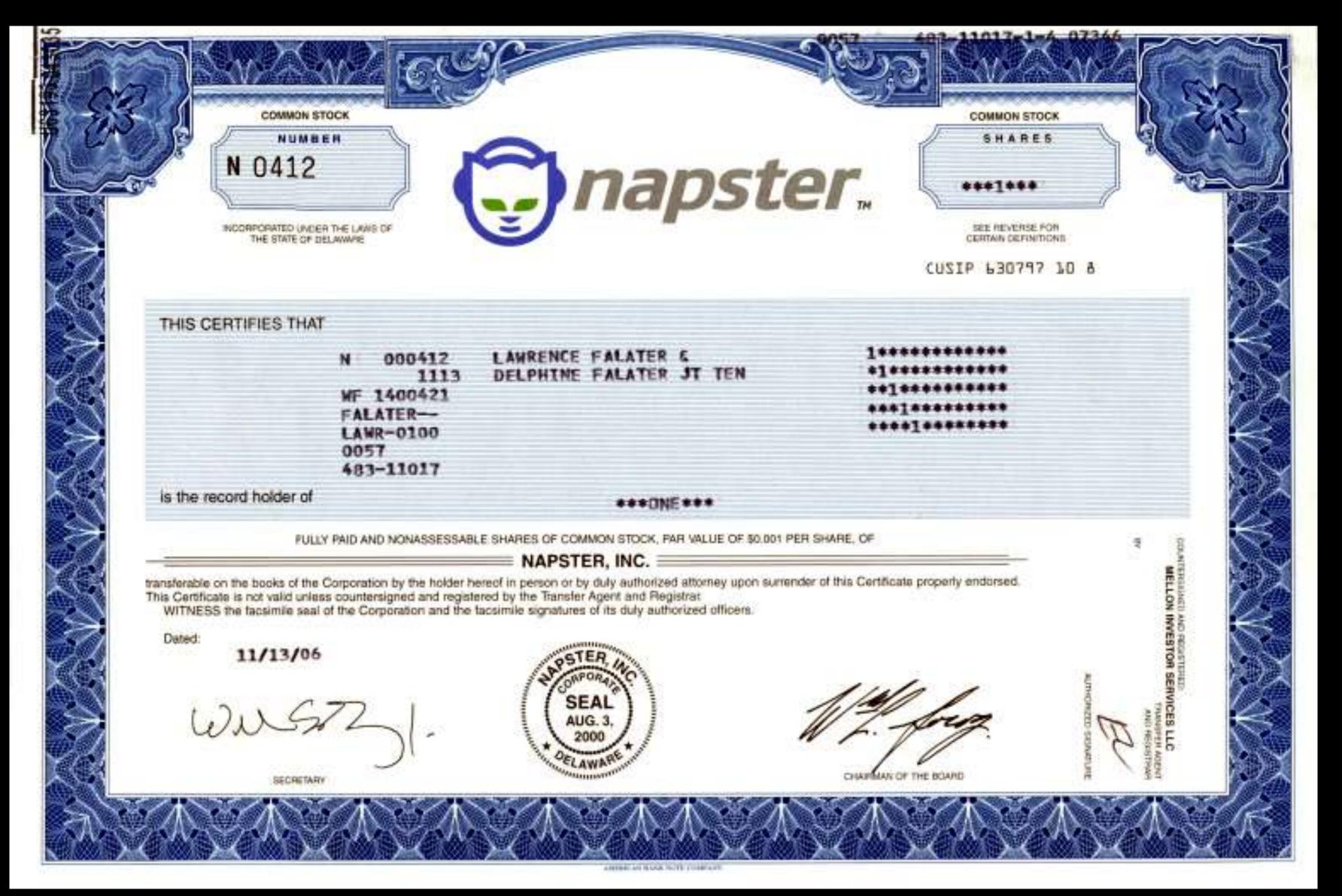
Unlock Script (scriptSig) is provided by the user to resolve the encumbrance

Lock Script (scriptPubKey) is found in a transaction output and is the encumbrance that must be fulfilled to spend the output



WHERE DO RIGHTS ATTACH?





BITCOIN FUNDAMENTALS

- The ScriptPubKey and sigScript are a unique combination that form the basis for every bitcoin transaction
- While transactions are traceable, the "coins" attached to those transactions are not traceable

THANK YOU!

PATRICK MURCK | @VIRTUALLYLAW | PMURCK@CYBER.LAW.HARVARD.EDU