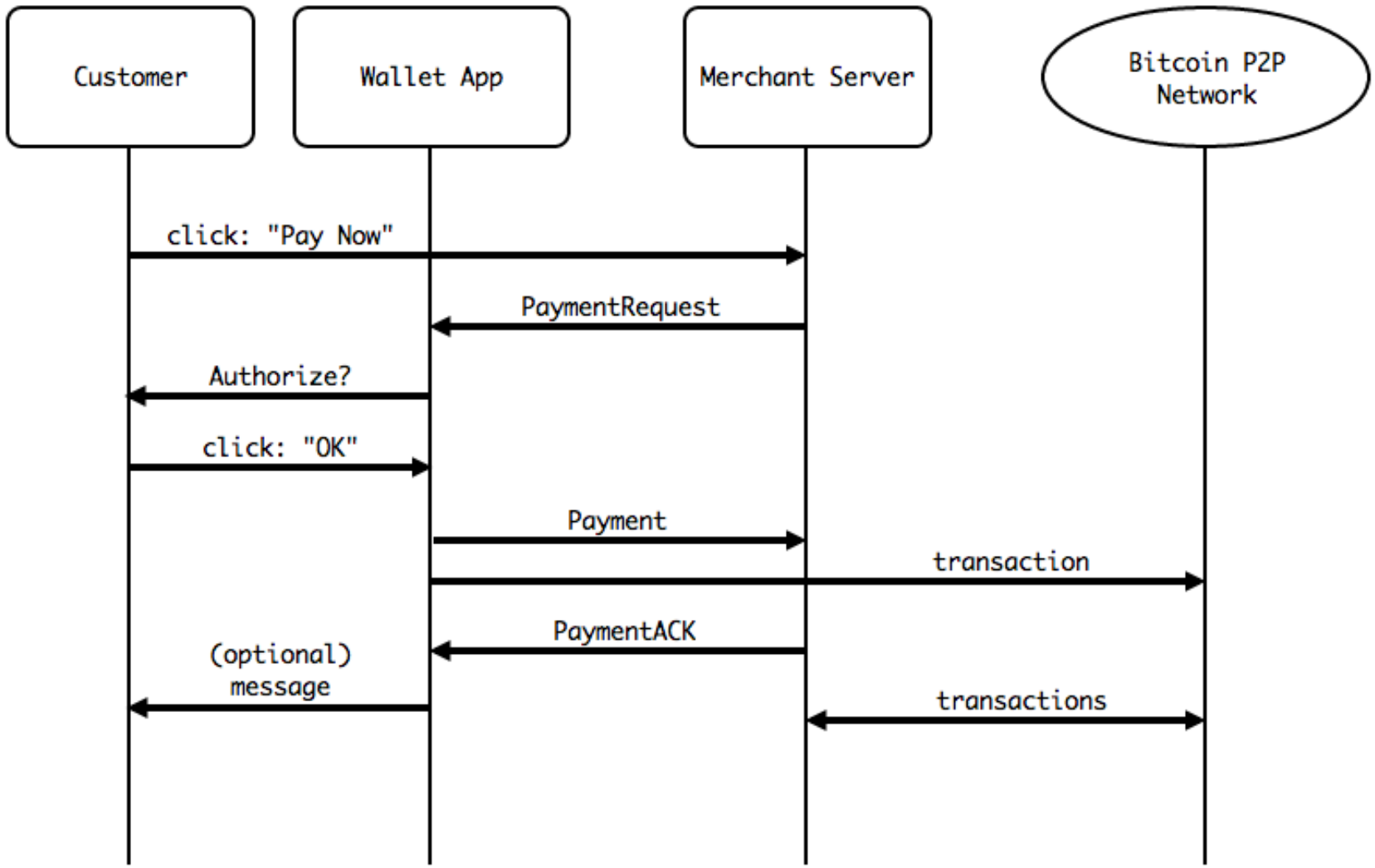
OWNERSHIP

BITCOIN PROTOCOL

E-COMMERCE

PAYMENT PROTOCOL (BIP70)

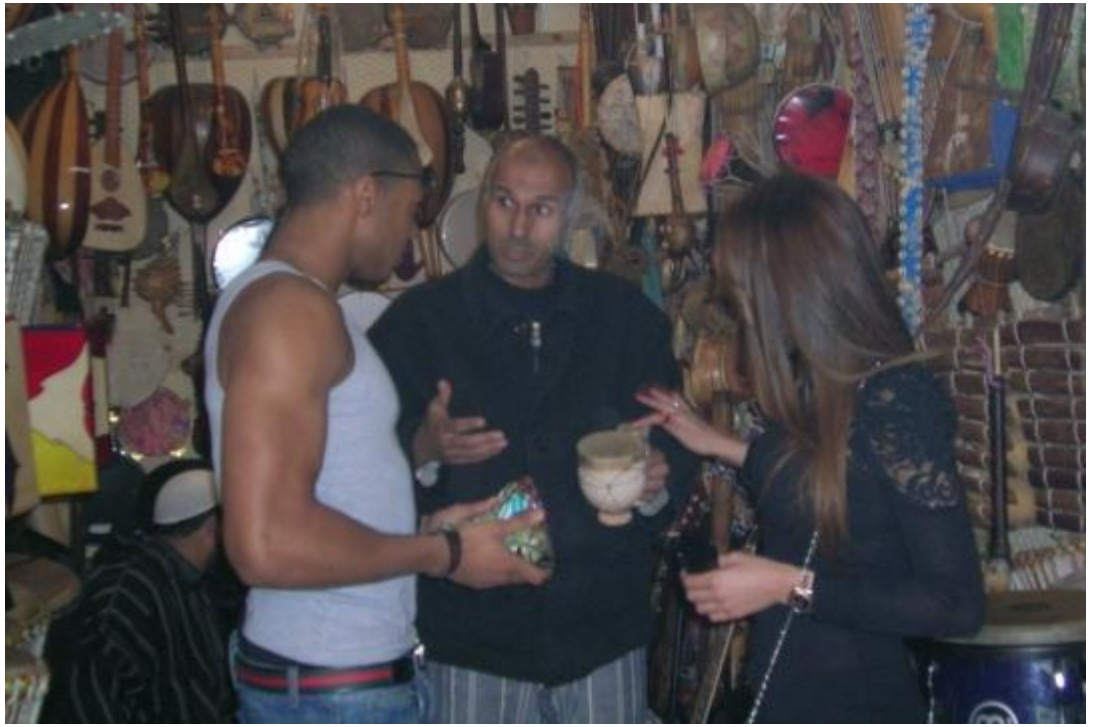

Customer
Wallet App
Merchant Server
Bitcoin P2P Network
click: "Pay Now"
PaymentRequest
Authorize?
click: "OK"
Payment
transaction
PaymentACK
(optional) message
transactions

THIS IS GOOD BUT…

SOME SHOPS ARE DIFFERENT

WITH DIFFERENT TRADE MODELS

BARGAINING



THE BARGAINING PROTOCOL

DURING THE NEGOTIATION,
BUYER & SELLER ITERATE TO CREATE
INVALID TRANSACTIONS

$$\sum \text{txin} < \sum \text{txout}$$

(TRANSACTION WILL BE REJECTED IF BROADCAST TO THE NETWORK)

BUT THEY TRY TO REACH AN AGREEMENT

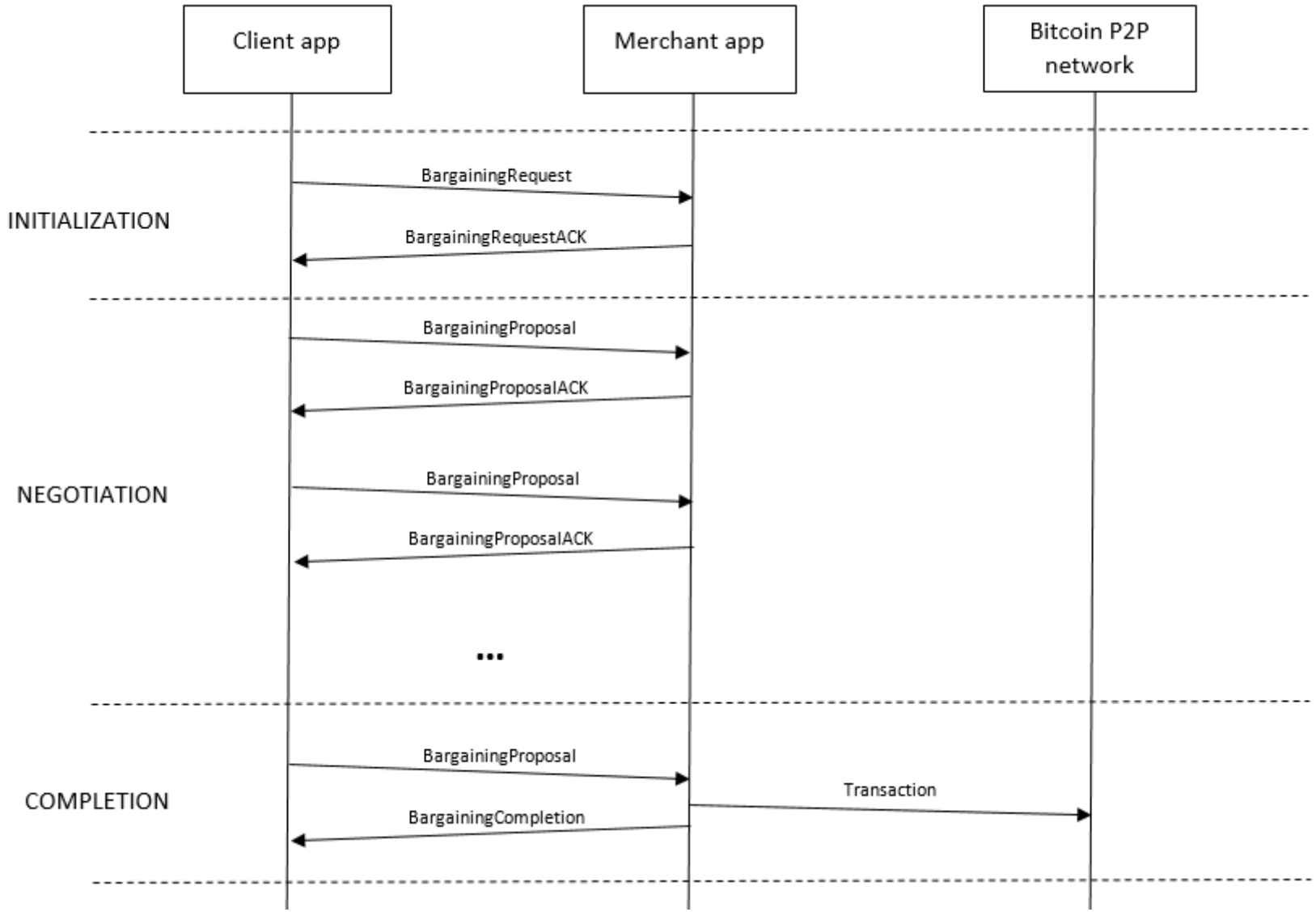
$$\text{Buyer} : \sum \text{txin}(t+1) \geq \sum \text{txin}(t)$$

$$\text{Seller} : \sum \text{txout}(t+1) \leq \sum \text{txout}(t)$$

(OR IT ABORTS THE NEGOTIATION)

…TILL THEY CONVERGE TO A VALID TRANSACTION

$$\sum \text{txin} \geq \sum \text{txout}$$


Client app
Merchant app
Bitcoin P2P network
INITIALIZATION
BargainingRequest
BargainingRequestACK
BargainingProposal
BargainingProposalACK
NEGOTIATION
BargainingProposal
BargainingProposalACK
...
BargainingProposal
COMPLETION
Transaction
BargainingCompletion

IN THE WILD

OUTPUT SCRIPTS CAN BE

2-OF-3 MULTISIG

(SELLER, BUYER, ESCROW)

MAIN BENEFITS

PROVABLE NEGOTIATION

EACH MESSAGE IS SIGNED IN A CHAIN OF SIGNATURES

SIGN(HASH(PREV_MSG + MSG))

TERMS OF THE NEGOTIATION CAN’T BE FORGED

TRUST-FREE NEGOTIATION

SELLER CAN CHECK IN THE BLOCKCHAIN
THAT BUYER OWNS FUNDS TO COVER THE PLEDGE

(AT EACH ITERATION)

ALLOWS ADVANCED USE CASES

ASYNCHRONOUS NEGOTIATION

ALLOWS ADVANCED USE CASES

1-TO-N NEGOTIATION

(BUYER CHALLENGES SEVERAL SELLERS, …)

USE CASES

HUMAN TO HUMAN

ONLINE BAZAAR

...

COMPUTER TO COMPUTER

AUTOMATED NEGOTIATION OF RESOURCES
(ON-DEMAND CLOUD SERVICE PROVISIONS)

DYNAMIC NEGOTIATION STRATEGIES (A.I.)

HUMAN TO COMPUTER

LASTMINUTE.COM

NEGOTIATION ASSISTANT