bitmarkets

anonymous decentralized markets
with no trusted third parties

problem

centralized markets
censorship
no privacy
high fees
winner takes all

solution

decentralized markets
no censorship
more privacy
no fees
market diversity

implementation

privacy via tor

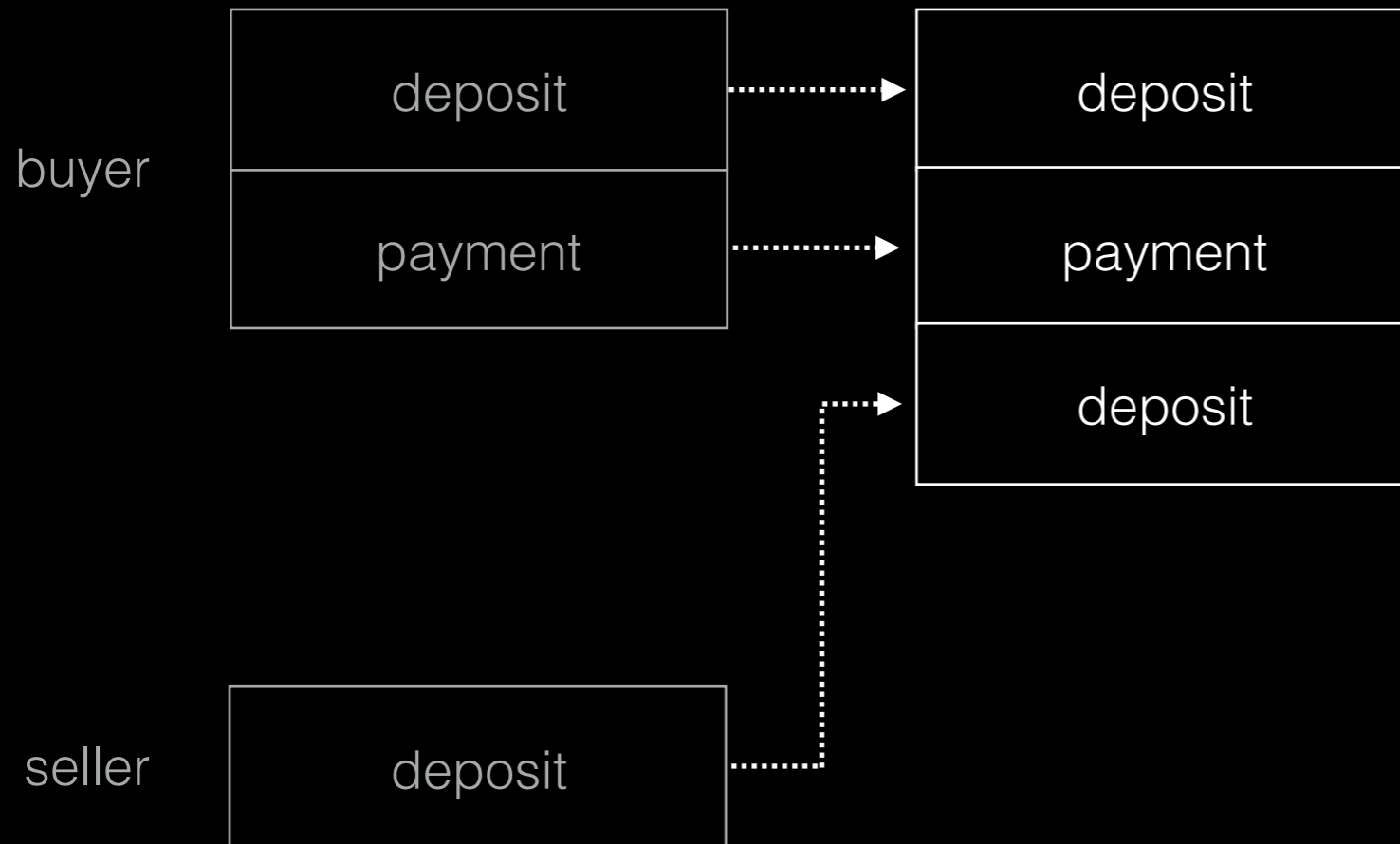payments via bitcoin

communication via bitmessage

trust via two party escrow

two party escrow

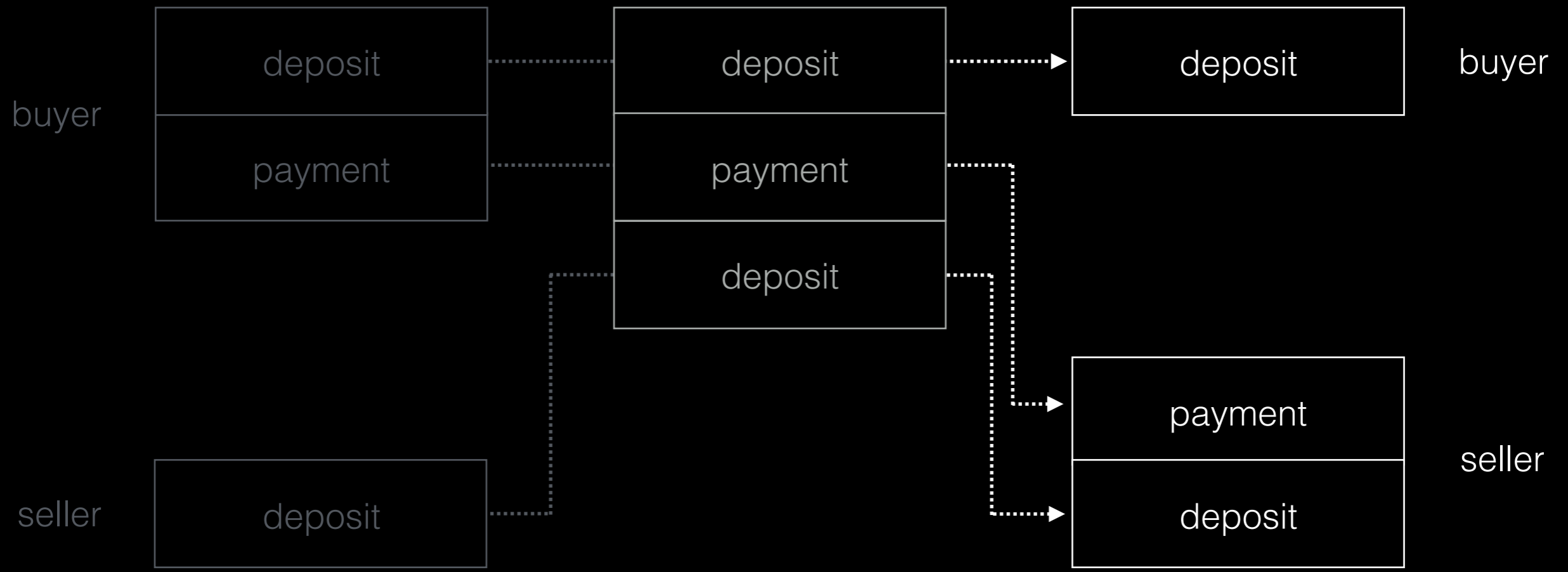both parties lock mutual deposits and buyer payment in a transaction both must sign to release.

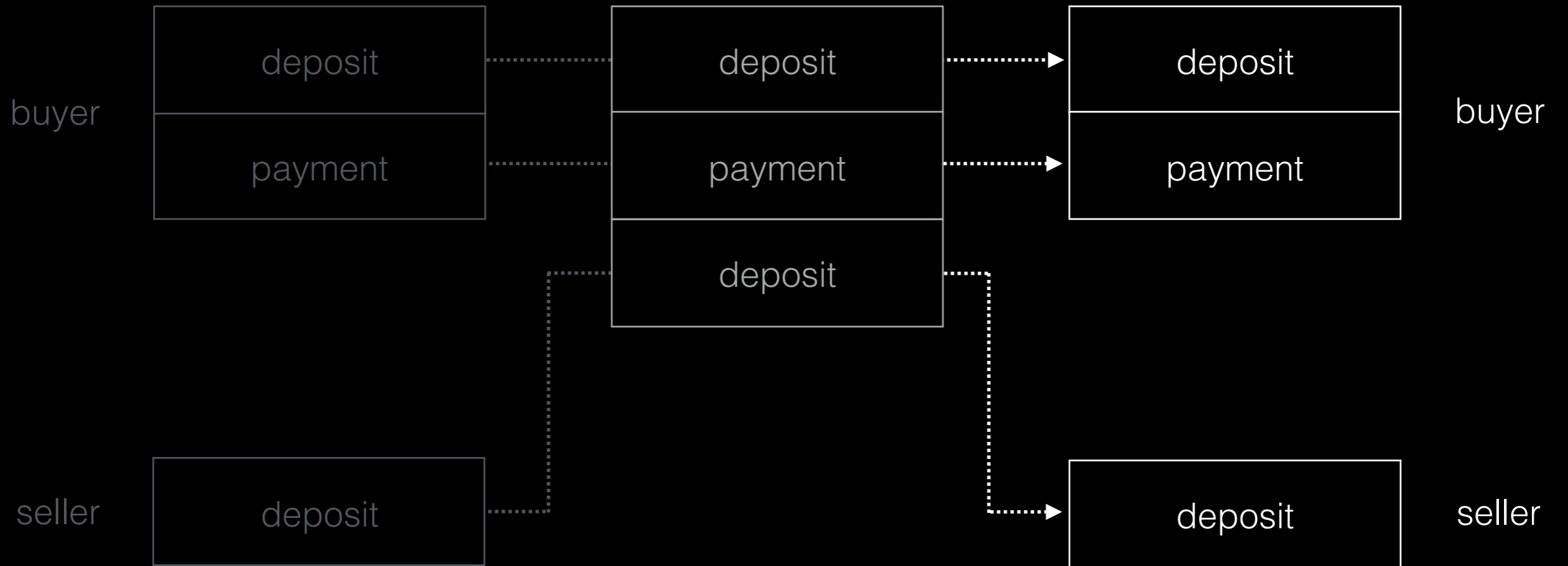once locked, neither can profitably defraud the other.

both sign to lock

🔒

buyer

| deposit |
| payment |

| deposit |
| payment |
| deposit |

seller deposit

money remains locked until agreement

both sign payment…

buyer

buyer

deposit
payment

deposit
payment
deposit

deposit	buyer

seller

seller

deposit

payment	seller
deposit	

or both sign refund

buyer

deposit

payment

deposit

payment

deposit

buyer

seller

deposit

payment

deposit

deposit

deposit

seller

if seller doesn't send item

seller -1x (keeps item but loses deposit)

buyer -2x (loses deposit & payment)

if buyer doesn't send payment

seller -2x (losses item & deposit)

buyer -1x (gets item but looses deposit & payment)

game theory
users need to be willing to take a loss
to punish fraud, but will they?

ultimatum game experiments
suggests they will

why no escrow agent?
agent only has one party's word
against the other and therefore
no means of fairly resolving disputes

what about reputation?

pseudonymous reputation
vulnerable to sybil and proxy attack

reputation is useful when tied to real
identities as they are immune to such
attacks, but this comes at the cost of
privacy

proxy attacks

proxy orders to gain reputation

sybil attacks

leave bad reviews for competitors &

leave good reviews for attacker

these can be automated

reputation
can be stolen
can be bought & sold
exit scam incentive increases with reputation
eventually, everyone retires…

escrow agent markets?
replacing markets-as-agents
with market-of-agents
lowers costs of proxy attacks

trusting pseudonymous agents

30% of hidden service markets

have been exit scams

two party escrow

guarantees fraud unprofitable

safe from reputation attacks

safe from exit scams

no middle men

browsing posts

tracking sales

Markets	8
Sells	**8**
Buys	
Wallet	
1.5000 BTC	
About	

ACR-FW-0708 E-P...	
1.2000BTC	•
ACR-FW-1213 P9-...	
1.2000BTC	•
ACR-FW-1213-DS-...	
0.8000BTC	•
Banana Republic...	
0.0443BTC	•
Cool Tools Book b...	
0.0427BTC	•
Test	
0.0100BTC	•
Test 2	
0.0100BTC	•
Test 3	
0.0070BTC	•

Listed ✓ | Bids • | Lock Escrow | Dispatch | Release Escrow | Complete
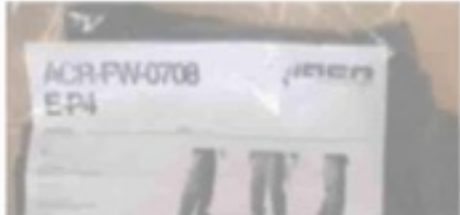
Status
Awaiting bids.

Accept First Bid   **Remove Listing**

ACR-FW-0708 E-P4, BLK (M)
1.2000BTC   284.3USD   255.2EUR

The medium of these was a bit too small for me (I'm a 32 waist).

For more info on this brand, see:
http://www.acronym.de/collections.php

⚲ Shipping within US
👤 BM-2cTUgt97vPRASYUGvU83CAQToLpwGQ8NHF
▶ Fashion / Men's / Pants

app, source, white paper and protocol spec available at

bitmarkets.org

team

chris robinson designer

rich collins bitcoin integration

adam thorsen bitmessage & tor work

steve dekorte ui & lead