

Bitmarkets

anonymous decentralized markets
based on two party escrow

no fees, no middle men, no altcoin,
open protocol and source
working and available today

Steve Dekorte, lead at voluntary.net

“I've been working on a new
electronic cash system that's
fully peer-to-peer, with
no trusted third party.”

first public words of Satoshi Nakamoto

“I've been working on a new
electronic cash system that's
fully peer-to-peer, with
no trusted third party.”

Can we make markets like this?

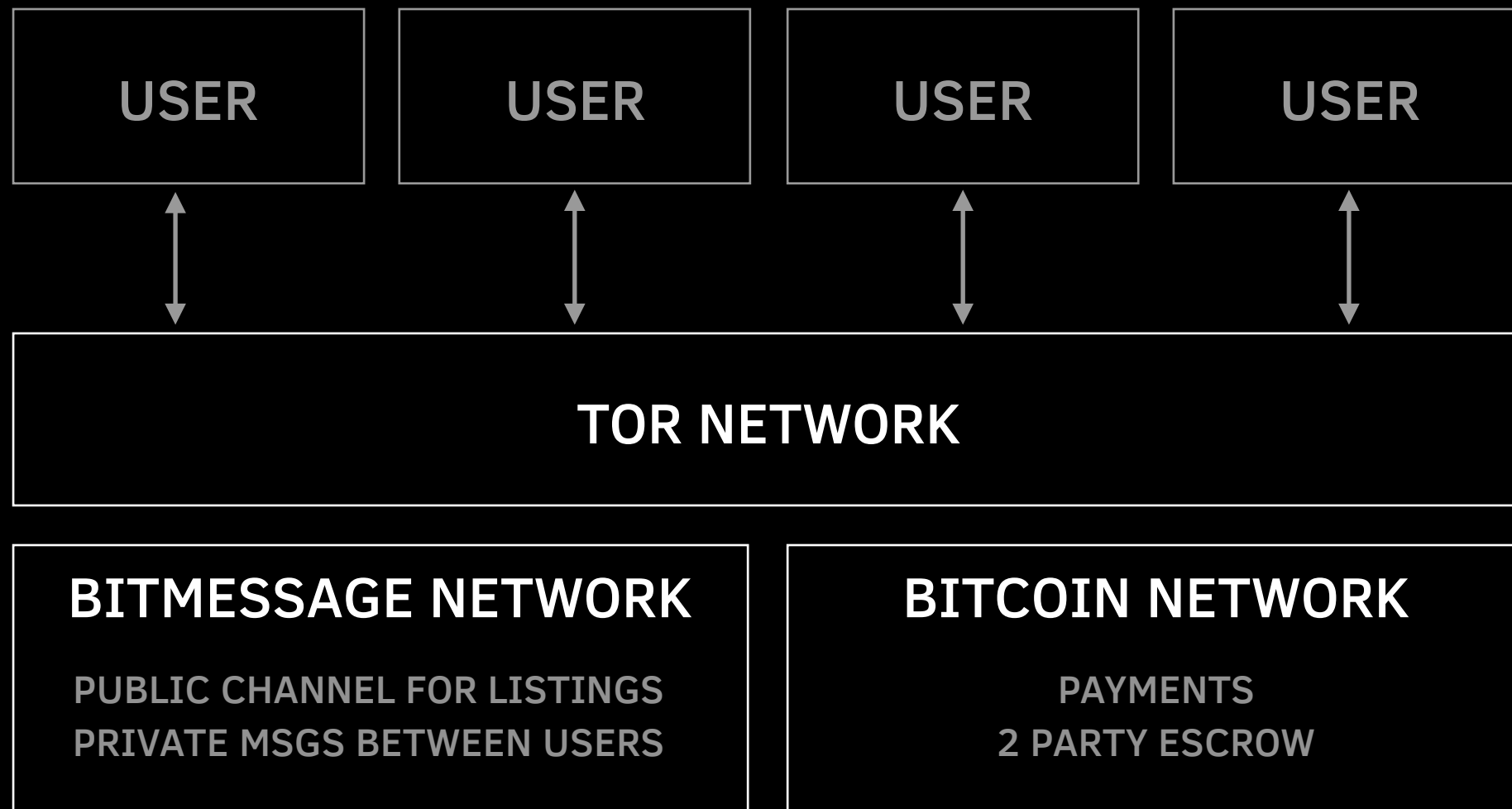
CENTRALIZED MARKETS

NO PRIVACY, HIGH FEES



P2P ORDER BOOK & PAYMENTS

FULL PRIVACY, NO FEES



P2P 2 PARTY ESCROW

BUYER PUTS UP 2X,
SELLER PUTS UP 1X
ITEM PRICE

FROM
BUYER

BUYER DEPOSIT
BUYER PAYMENT

FROM
SELLER

SELLER DEPOSIT

LOCK TWO PARTY ESCROW



FROM
BUYER

BUYER DEPOSIT

BUYER PAYMENT

BOTH SIGN TX
TO LOCK ESCROW

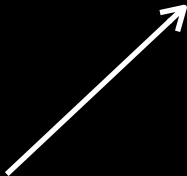
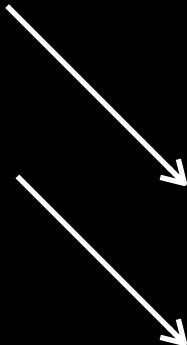
BUYER DEPOSIT

BUYER PAYMENT

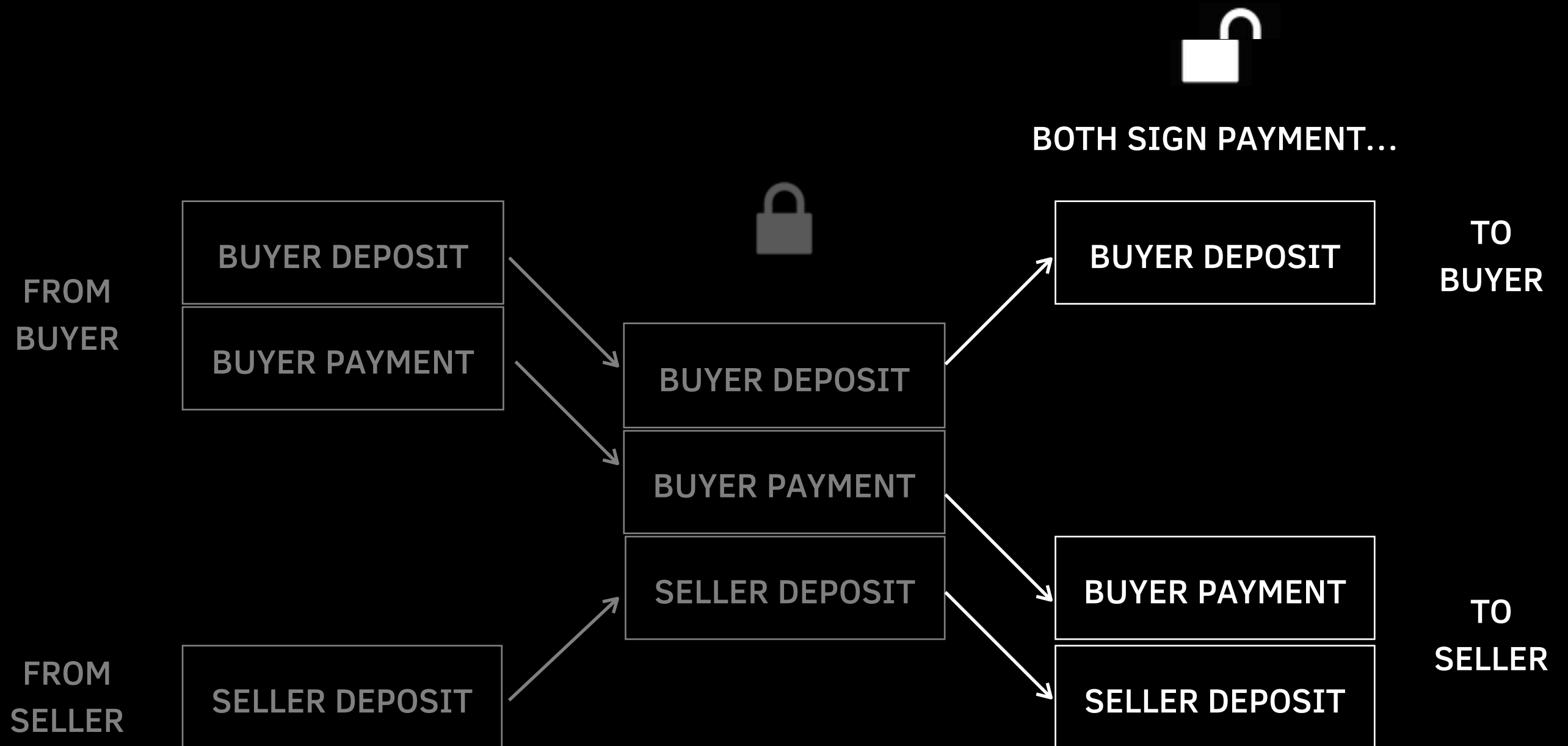
SELLER DEPOSIT

FROM
SELLER

SELLER DEPOSIT



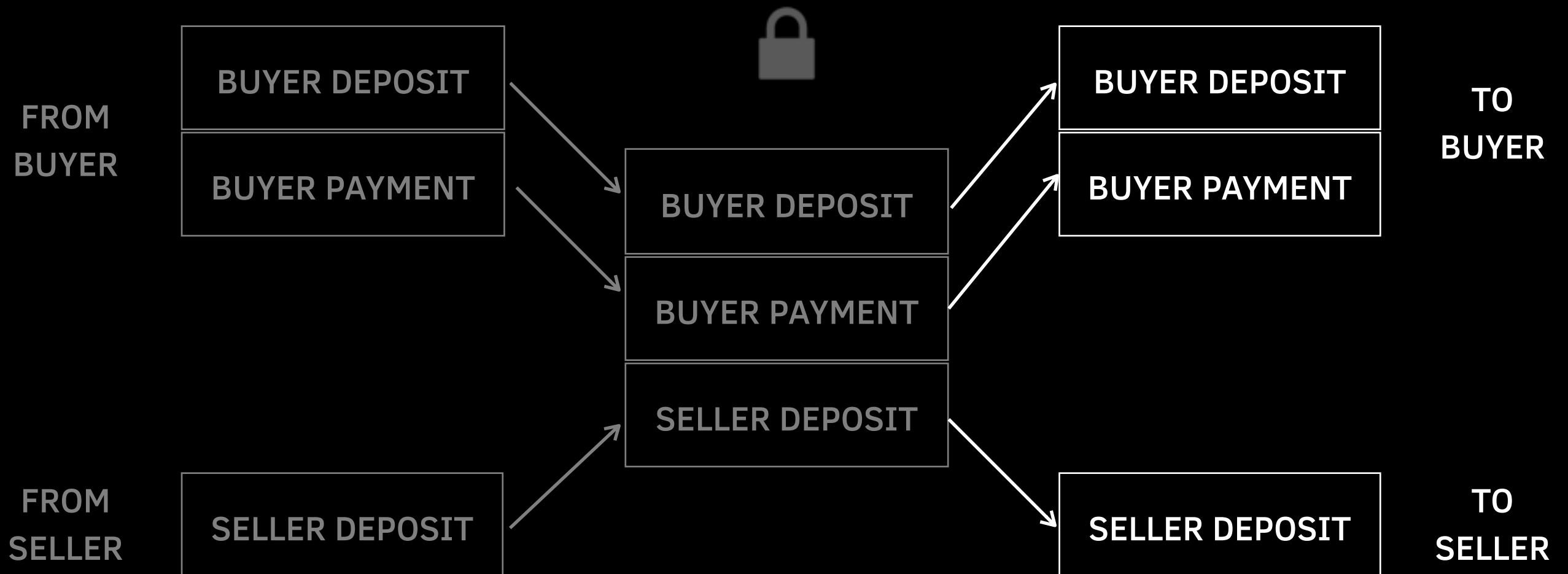
RELEASE PAYMENT



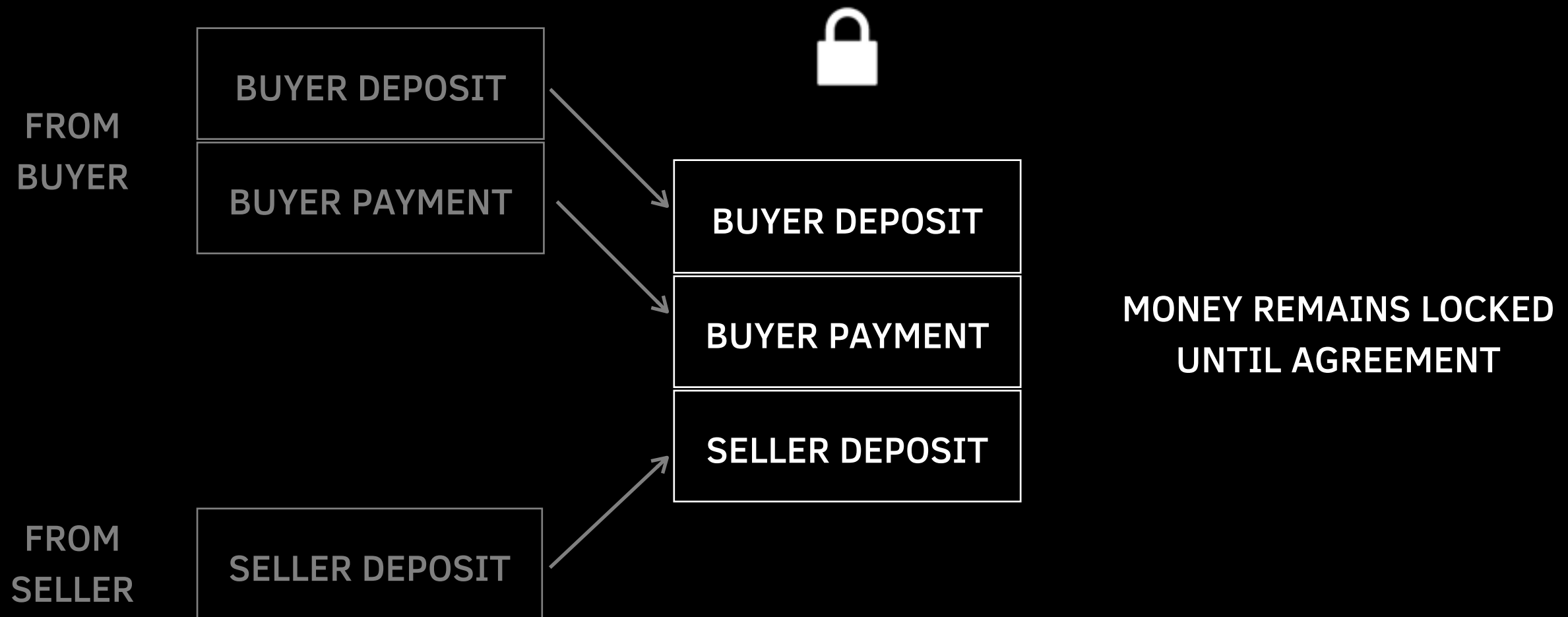
RELEASE REFUND



OR BOTH SIGN REFUND...



NO AGREEMENT



PERMANENTLY UNRESOLVED DISPUTES REDUCE BTC MONEY SUPPLY
TRANSFERRING THE PURCHASING POWER TO ALL OTHER BTC HOLDERS

TWO PARTY ESCROW

SELLER

BUYER

-1x

LOSES DEPOSIT
KEEPS ITEM

SELLER FRAUD

DOESN'T SEND ITEM
OR SIGN REFUND

-2x

LOSES DEPOSIT
LOSES PAYMENT

-2x

LOSES DEPOSIT
LOSES ITEM

BUYER FRAUD

DOESN'T SEND PAYMENT

-1x

LOSES DEPOSIT
GAINS ITEM

NO FRAUD

GAINS ITEM

GAINS PAYMENT

NEITHER CAN PROFITABLY DEFRAUD OTHER.
REPEATED BAD ACTORS GO BANKRUPT.

WHY NOT USE ESCROW AGENTS?

NO MEANS OF FAIRLY RESOLVING DISPUTES

buyer's vs seller's word

delivery receipt != quality item delivered

GAME THEORY

If $>50\%$ of people act punitively,
cheating is money losing strategy.

A “rational” actor would accept cheating
to get deposit back, but do humans?

Answer: NO

For even 10% cheating, Ultimatum Game psychology
experiment shows 60% act punitively.

Similar results in chimps & bonobos.
Our social instincts evolved for repeated interactions.

“Game theory is very weak as a security model, but on internet probably superior to reputation, and certainly to assuming trusted third parties.”

Nick Szabo on two party escrow

PROBLEMS WITH REPUTATION

PROXY ATTACKS

automated script can gain reputation
by proxying agent, buyer or seller orders

leave bad reviews for competitors &
leave good reviews for attacker ids

2 of 3 exit scam using ids

UNSTABLE EQUILIBRIUM

as reputation increases,
so does potential exit scam profit

AGENT MARKETS NOT SOLUTION

many agents no different than
many markets acting as agents
lowers costs of proxy attacks

PSUSEDONYMOUS ESCROW AGENT SCAMS

NOT A THEORETICAL PROBLEM

“I am so sorry, but Verto and Kimble have f*ed us all,”

NSWGreat on Evolution

“I can’t believe mdparity has decided to exit scam now”

MrDoe on BlankBank

Prediction: fraud will continue
until move to two party escrow

WALLET

syncing with bitmessage network - 8 connections, 1506 messages processed

Markets 8

Sells 8

Buys

Wallet
1.5000 BTC

About

Balance

1.5000BTC 355.3USD 319.0EUR

Deposit

Withdraw

Time	Confirms	Type	Description	Amount
2014-12-17 16:18	20372	Deposit	1jwuqYuTu9cGkvHpon2aTdXXira8BwAZL	+ 1.5000 BTC

BROWSING POSTS

syncing with bitmessage network - 8 connections, 1595 messages processed

Markets

Sells

Buys

Wallet
1.5000 BTC

About

Global

US

Canada

Austria

Belgium

Bulgaria

Croatia

Czech Rep

Denmark

Finland

France

Automotive

Currencies

Electronics

Fashion 4

Home

Media & Games 1

Other 1

Services

Sporting

Tests 2

Tickets

Games
Cards, Board Games...

Instruments
Musical Instruments

Paper
Books, Magazine... 1

Plastic
DVD, CD, Vinyl

Video Gaming
Games and Gear

Cool Tools Book by Kevin Kelly
0.0427BTC

Cool Tools Book by Kevin Kelly
0.0427BTC 10.1USD 9.1EUR


Buy

Perfect condition. This item is \$25USD on Amazon.
Shipping in US only.

Shipping within US

BM-2cTUgr97vPRASYUGvU83CAQToLpwGQ8NHf

Media & Games / Paper



TRACKING YOUR SALES

syncing with bitmessage network - 8 connections, 1273 messages processed

Markets8

Sells8

Buys

Wallet1.5000 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

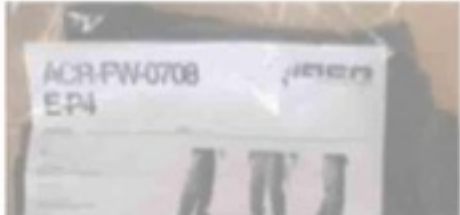
The medium of these was a bit too small for me (I'm a 32 waist).

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

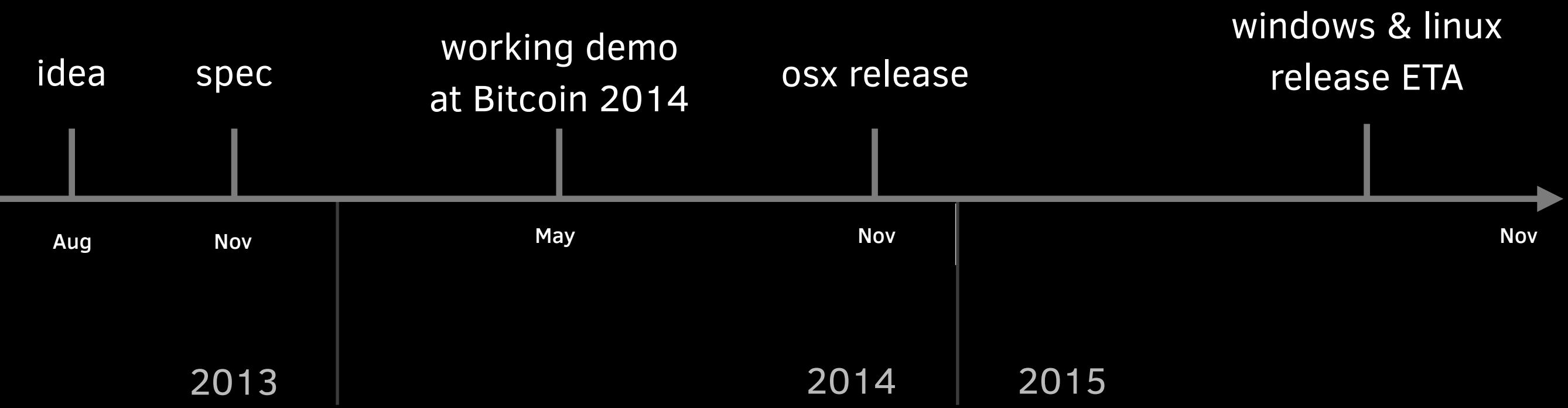
📍 Shipping within US

👤 BM-2cTUgt97vPRASYUGvU83CAQToLpwGQ8NHF

▶ Fashion / Men's / Pants



Bitmarkets History



Two party escrow makes fraud
unprofitable without
trusted third parties,
courts or threat/use of force.

A voluntary economy.

app, source, white paper and
protocol spec available at

bitmarkets.org

users & contributors welcome!

Who are we?

Chris Robinson UI Designer

Rich Collins Bitcoin integration

Adam Thorsen Bitmessage & Tor integration

Steve Dekorte UI implementation & lead

Greg Casamento Windows & Linux port
& **Riccardo Mottola**

Differences with OpenBazaar?

can't fairly resolve disputes

makes fraud profitable

gameable reputation

sellers must run servers

not based on tor

no goal of anonymity

Is seller deposit a significant burden?

