



# On Decentralizing Prediction Markets & Order Books

---

Jeremy Clark, Joseph Bonneau, Edward W. Felten,  
Joshua A. Kroll, Andrew Miller, & Arvind Narayanan

Remove uncertainty  
about unknown events

Politics

Sports

Weather

Market  
Share

Geo-  
politics

Product  
Completion

Scientific  
Discoveries

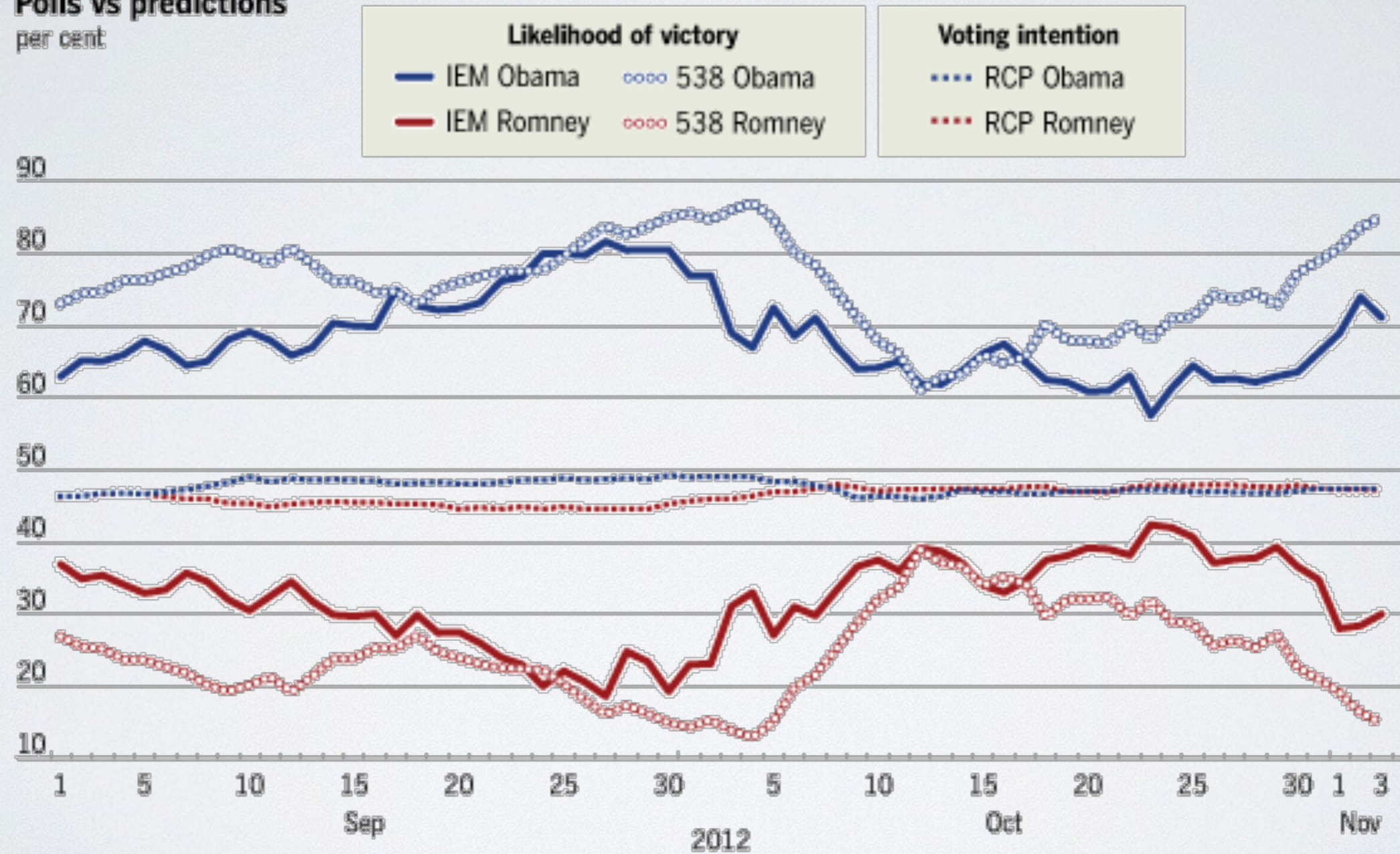
Sales

Awards

# Prediction Markets

## Polls vs predictions

per cent



Source: Real Clear Politics, Iowa Electronic Markets, FiveThirtyEight

# Prediction Markets

Obama

Romney

Johnson

Other

Winner: \$10

Losers: \$0

# Prediction Markets

Obama	\$6.10	61%		
Romney	\$3.80	38%	Winner:	\$10
Johnson	\$0.09	0.9%	Losers:	\$0
Other	\$0.01	0.1%		

# Prediction Markets

Obama	\$6.10
Romney	\$3.80
Johnson	\$0.09
Other	\$0.01

# Prediction Markets

Obama	\$6.10
Romney	\$3.80
Johnson	\$0.09
Other	\$0.01

Obama

-\$6.10



# Prediction Markets

Obama	\$6.10	\$7.30
Romney	\$3.80	\$2.65
Johnson	\$0.09	\$0.04
Other	\$0.01	\$0.01

Obama

-\$6.10

# Prediction Markets

Obama	\$6.10	\$7.30
Romney	\$3.80	\$2.65
Johnson	\$0.09	\$0.04
Other	\$0.01	\$0.01

Obama

-\$6.10 +\$7.30

# Prediction Markets

Obama	\$6.10	\$7.30
Romney	\$3.80	\$2.65
Johnson	\$0.09	\$0.04
Other	\$0.01	\$0.01

Obama

$$-\$6.10 + \$7.30 = \$1.20$$

# Prediction Markets

Obama	\$6.10	\$7.30
Romney	\$3.80	\$2.65
Johnson	\$0.09	\$0.04
Other	\$0.01	\$0.01

Obama

$$-\$6.10 + \$7.30 = \$1.20$$

*Immediately Realized*

# Prediction Markets

Obama	\$6.10	\$7.30
Romney	\$3.80	\$2.65
Johnson	\$0.09	\$0.04
Other	\$0.01	\$0.01

Romney

Johnson

Other

$$-\$2.70 = \$2.65 + \$0.04 + \$0.01$$

# Prediction Markets

Obama	\$6.10	\$7.30	\$6.40
Romney	\$3.80	\$2.65	\$3.53
Johnson	\$0.09	\$0.04	\$0.06
Other	\$0.01	\$0.01	\$0.01

Romney

Johnson

Other

-\$2.70

# Prediction Markets

Obama	\$6.10	\$7.30	\$6.40
Romney	\$3.80	\$2.65	\$3.53
Johnson	\$0.09	\$0.04	\$0.06
Other	\$0.01	\$0.01	\$0.01

Romney

Johnson

Other

$$-\$2.70 + \$3.60 = \$0.90$$

# Prediction Markets

Obama	\$6.10	\$7.30	\$6.40
Romney	\$3.80	\$2.65	\$3.53
Johnson	\$0.09	\$0.04	\$0.06
Other	\$0.01	\$0.01	\$0.01

Romney

Johnson

Other

-\$2.70



# Prediction Markets

Obama	\$6.10	\$7.30	\$6.40
Romney	\$3.80	\$2.65	\$3.53
Johnson	\$0.09	\$0.04	\$0.06
Other	\$0.01	\$0.01	\$0.01

Romney

Johnson

Other

Obama

-\$2.70 -\$6.40

# Prediction Markets

Obama	\$6.10	\$7.30	\$6.40
Romney	\$3.80	\$2.65	\$3.53
Johnson	\$0.09	\$0.04	\$0.06
Other	\$0.01	\$0.01	\$0.01

Romney

Johnson

Other

Obama

$$-\$2.70 - \$6.40 + \$10.00 = \$0.90$$

# Decentralization

# Decentralization

## Centralized Market:

- Money escrowed
- Shares escrowed
- Proprietary markets
- Match orders
- Vendor lock-in
- Adjudicate outcome
- Go offline
- Potentially transparent
- High fees

## Decentralized Market:

- Hold your own money
- Hold your own shares
- Choose any market
- Open order matching
- Use any exchange
- Trust agility
- Fault tolerant
- Transparent by design
- Low fees

# Decentralization

## Centralized Market:

- Money escrowed
- Shares escrowed
- Popular markets
- Match orders
- Exchange lock-in
- Adjudicate outcome
- Easily disrupted
- Transparent by choice
- High fees

## Decentralized Market:

- Hold your own money
- Hold your own shares
- Choose any market
- Open order matching
- Use any exchange
- Trust agility
- Fault tolerant
- Transparent by design
- Low fees

# Decentralization



Bitcoin

# Bitcoin

$K_A$

$K_B$

# Bitcoin

$K_A$

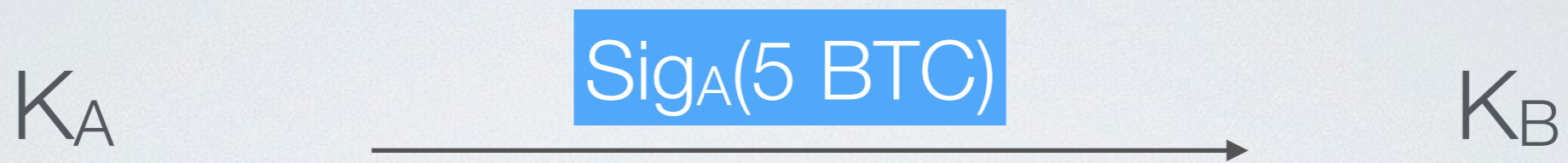
$K_B$

<i>From</i>	<i>To</i>	<i>Amount</i>
K	K	10 BTC
K	K	5 BTC
K	K	18 BTC

Ledger



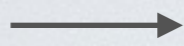
# Bitcoin



<i>From</i>	<i>To</i>	<i>Amount</i>
K	K	10 BTC
K	K	5 BTC
K	K	18 BTC
K	K	5 BTC

Ledger

$K_A$



T-9833

$K_B$



Miners

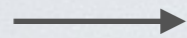
T-2351

T-4528

T-9636

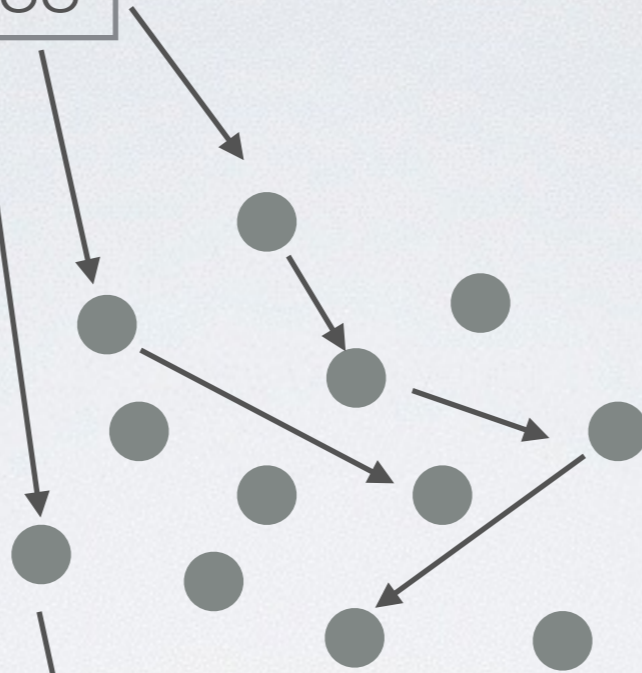
T-9833

$K_A$



T-9833

$K_B$



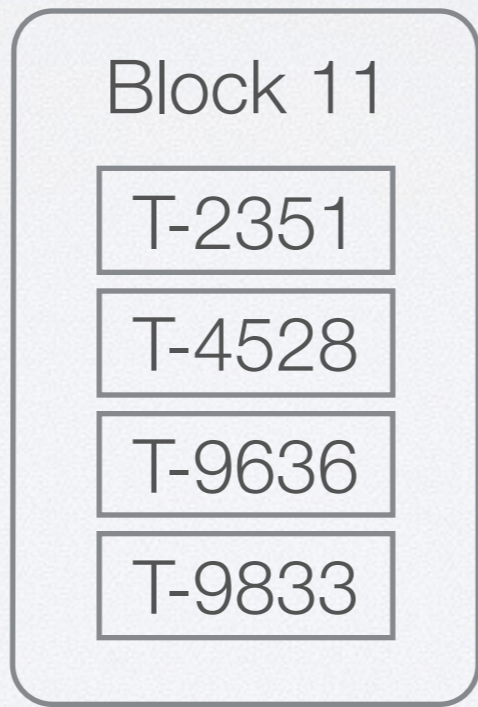
T-2351

T-4528

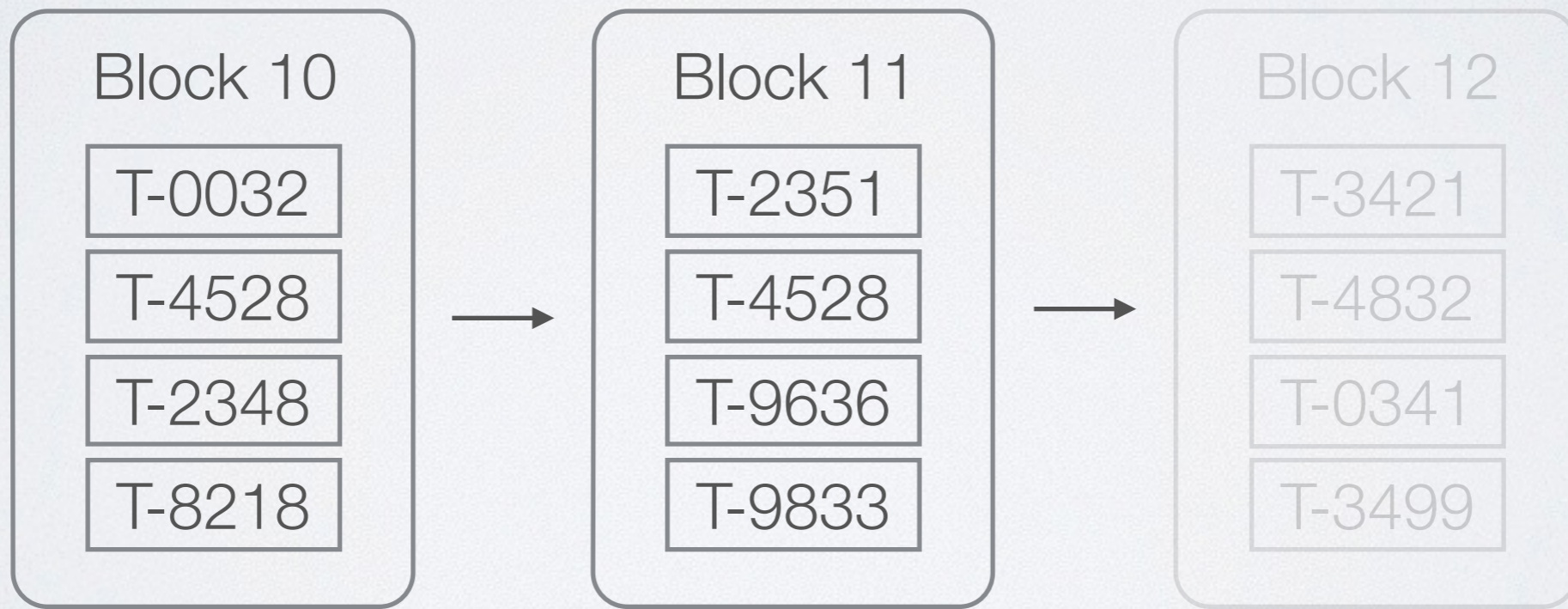
T-9636

T-9833

Transaction Pool



Ledger



Ledger

# Design Decisions

Underlying digital currency & block chain

- Extend Bitcoin
- [Altcoin \(XFT\)](#)
- Colored Coins

# Design Decisions

How to Declare a Winner:

- Machine-readable feed
- Trusted (human) arbiter
- Miners vote
- Users vote

# Design Decisions

## How to Declare a Winner:

- Machine-readable feed
- Trusted (human) arbiter
- Miners vote
- Users vote

## Threats:

- Wrong decision -> profitable
- No decision -> DoS



# Design Decisions

## How to Declare a Winner:

- Machine-readable feed
- **Trusted (human) arbiter**
- Miners vote
- Users vote

## Arbiters:

- Choose who you trust (agility)
- Low barrier to entry
- History & external reputation
- Trustworthiness built into price

# Design

## New Operations (Simplified)

- `OpenMarket()` Description & Arbiter, signed by arbiter
- `CloseMarket()` Outcome, signed by arbiter

# Design

## New Operations (Simplified)

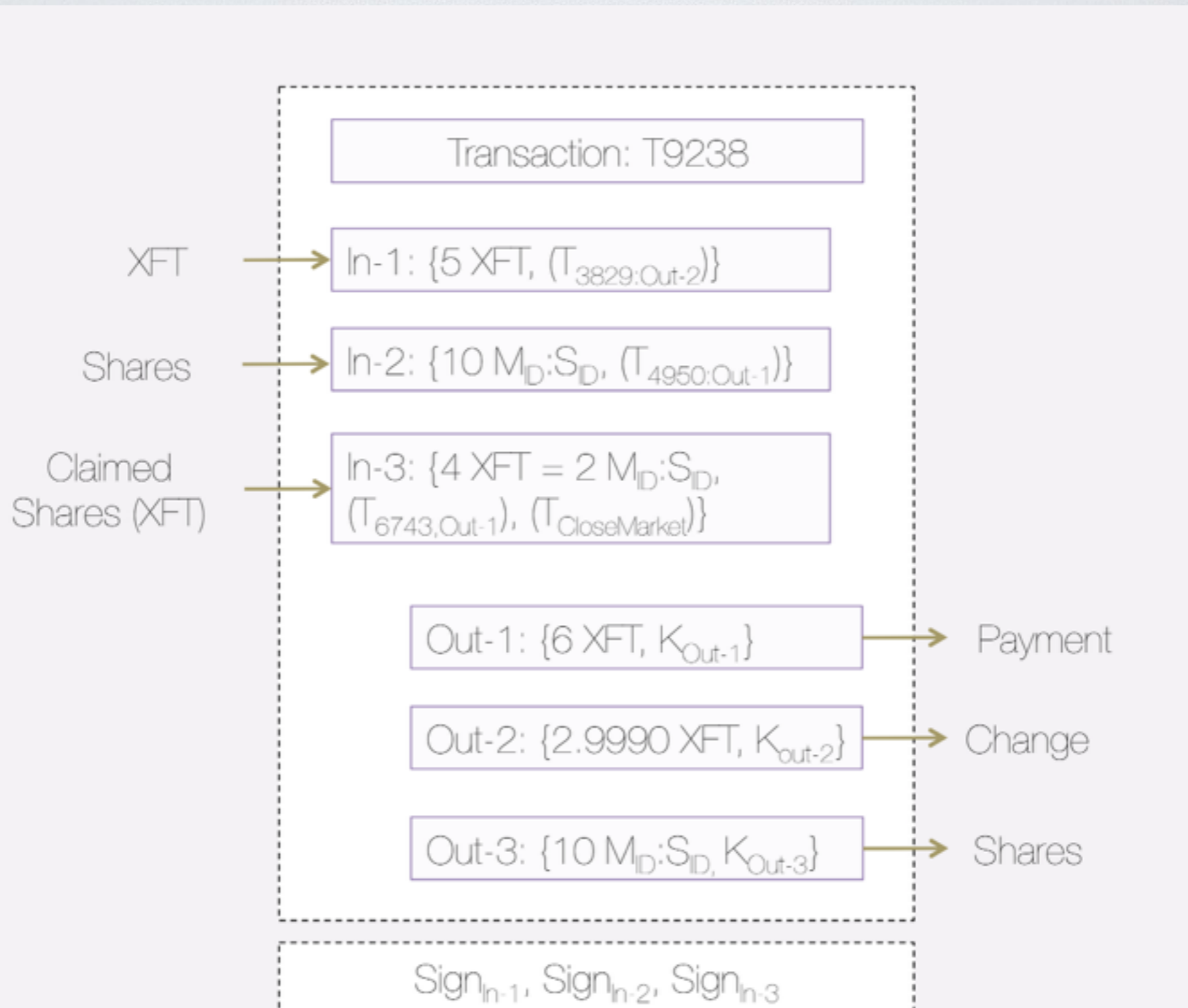
- `OpenMarket()` Description & Arbiter, signed by arbiter
- `CloseMarket()` Outcome, signed by arbiter
  
- `BuyPortfolio()` Convert 1 XFT into complete set of shares, signed by currency holder
- `SellPortfolio()` Convert complete set for 1 XFT, signed by share holder

# Design

## New Operations (Simplified)

- `OpenMarket()` Description & Arbiter, signed by arbiter
- `CloseMarket()` Outcome, signed by arbiter
- `BuyPortfolio()` Convert 1 XFT into complete set of shares, signed by currency holder
- `SellPortfolio()` Convert complete set for 1 XFT, signed by share holder
- `Exchange()` Exchange shares for XFT between two parties, signed by both parties

# Design



# Order Book

Most common: continuous, price-time priority

Broadcast orders to Bitcoin-style network:

- Nodes drop competitive orders
- No way to establish time
- Blockchain: updated in batches
- Miners drop competitive orders
- Miners front-run well-priced orders

# Order Book

- Nodes drop competitive orders
- No way to establish time
- Blockchain: updated in batches
- Miners drop competitive orders
- Miners front-run well-priced orders

The best we can + support external exchanges

# Order Book

- Nodes drop competitive orders
- No way to establish time
- Blockchain: updated in batches
- Miners drop competitive orders
- Miners front-run well-priced orders

Broadcast to all known neighbours



# Order Book

- Nodes drop competitive orders
- No way to establish time
- Blockchain: updated in batches
- Miners drop competitive orders
- Miners front-run well-priced orders

Call Market: Market opens, orders pile up, randomly close market, match orders

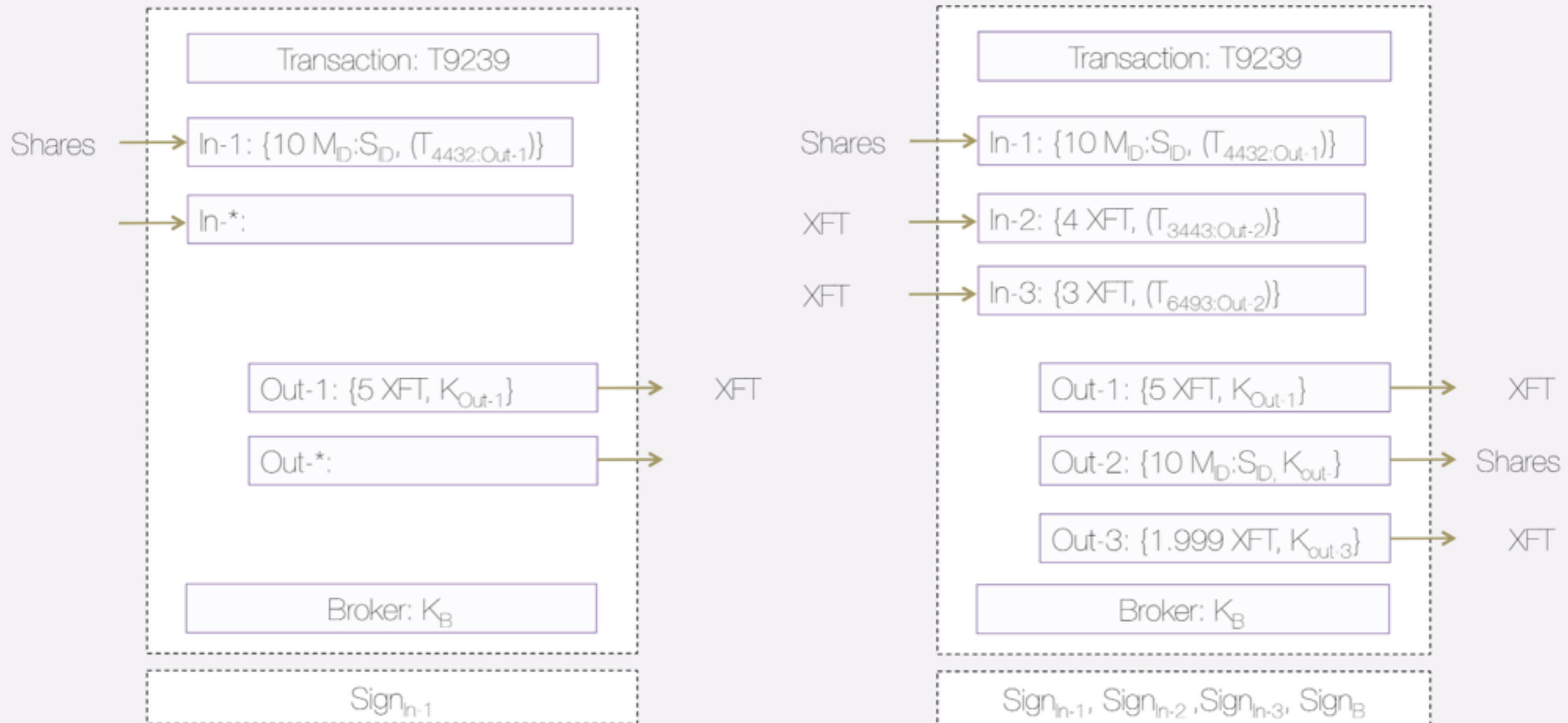
Matching: Lowest ask matched to highest bid until no more matching possible

# Order Book

- Nodes drop competitive orders
- No way to establish time
- Blockchain: updated in batches
- Miners drop competitive orders
- Miners front-run well-priced orders

Miners keep spread: spreads can replace fees & miners can execute at best price (added perk)

# Order Book



# Discussion

Design landscape, not a specific proposal

Regulatory issues: not attempting regulatory avoidance

Platform for other financial exchanges

Not suitable for forecasts about underlying currency



# Questions?

---

[@PulpSpy](#)

[@josephbonneau](#)

[@EdFelten](#)

[@realjoshkroll](#)

[@socrates1024](#)

[@random\\_walker](#)

