

On the Feasibility of Automating Stock Market Manipulation

Carter Yagemann, Simon Chung, Erkam Uzun,
Sai Ragam, Brendan Saltaformaggio, Wenke Lee

December 10th, 2020

CREATING THE NEXT®

Markets change with technology…





Unknowns of automated market manipulation…

- What can bots automate?
- How can they automate, communicate?
- Who will they compromise?
- How will they evade detection?

CREATING THE NEXT®

Agenda…

- What is *layering* manipulation? How does it work?
- What are the current defenses?
- How could a trading malware work?
- What would its impact be?
- The future…

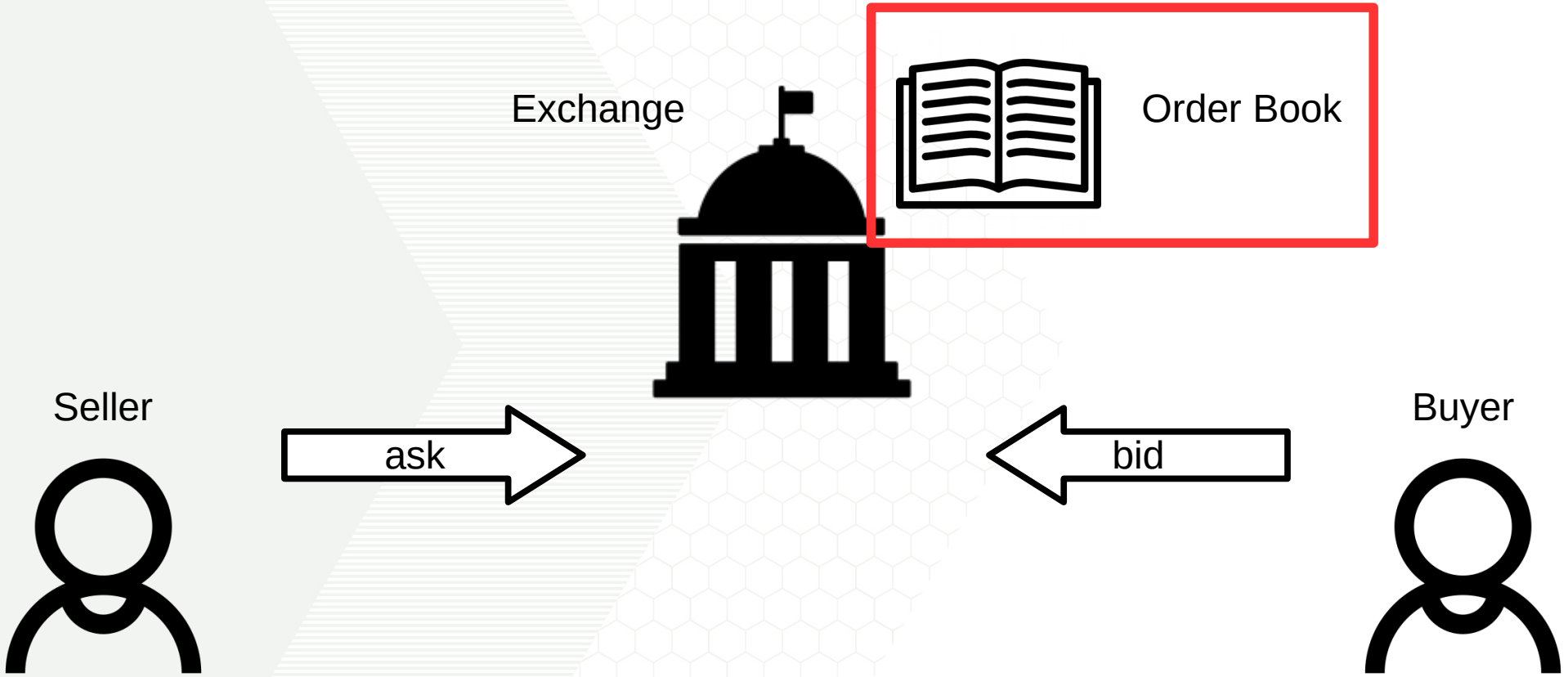
CREATING THE NEXT®

Agenda…

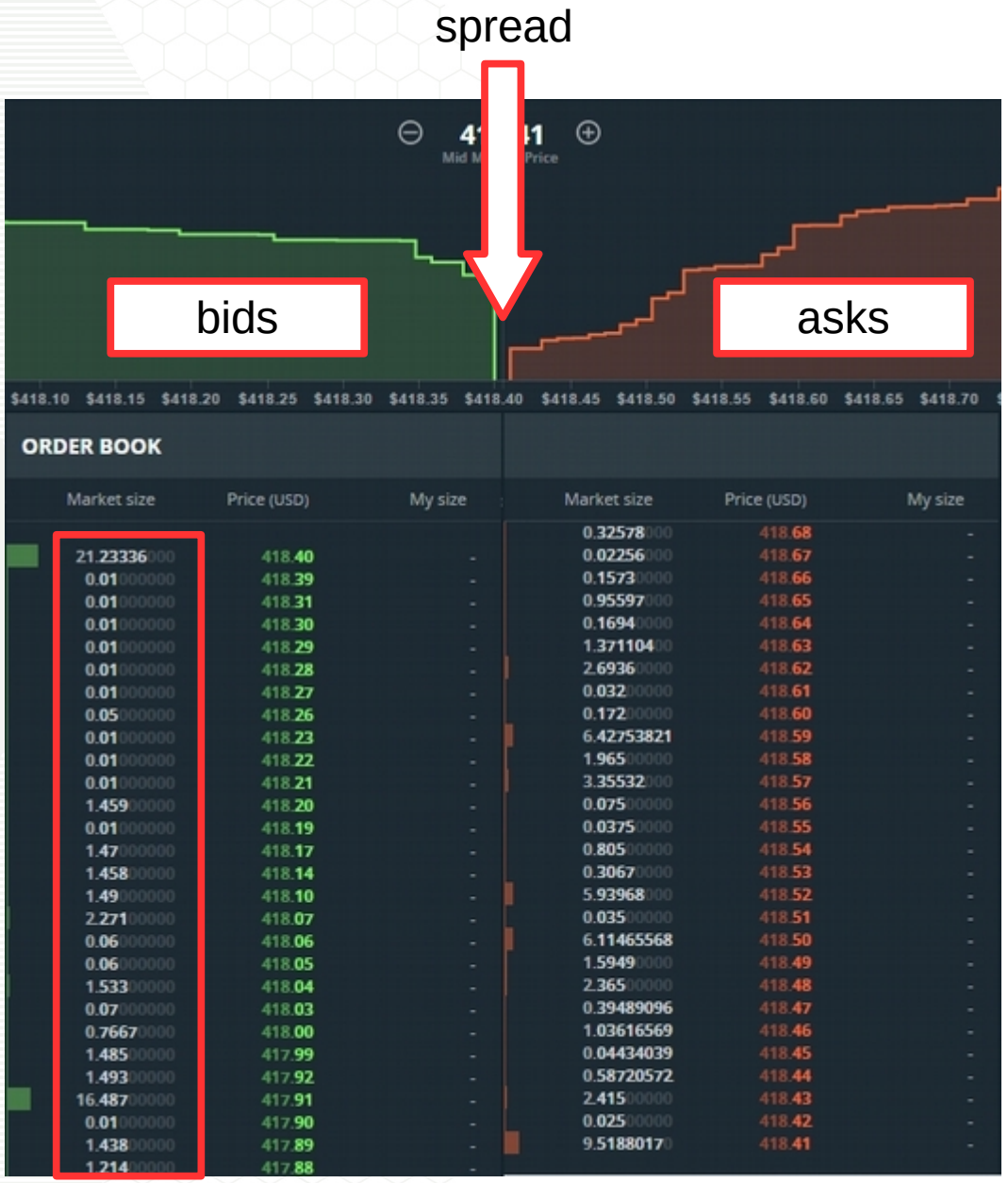
- What is *layering* manipulation? How does it work?
- What are the current defenses?
- How could a trading malware work?
- What would its impact be?
- The future…

CREATING THE NEXT®

Market basics (simplified)…

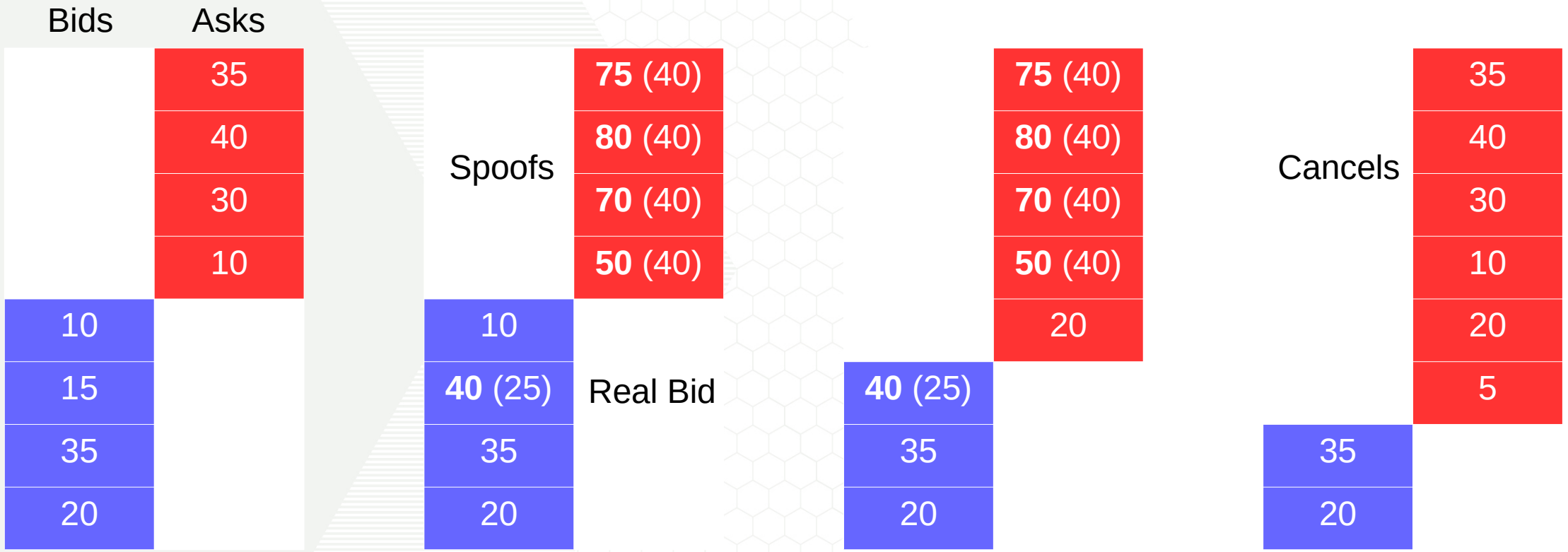


Order book…



layers

Layering example…



CREATING THE NEXT®

Agenda…

- What is *layering* manipulation? How does it work?
- What are the current defenses?
- How could a trading malware work?
- What would its impact be?
- The future…

CREATING THE NEXT®

Market basics (expanded)…

Government
(ex: SEC)



We'll come back to them at the end

- Anomaly detection (per-account)
- 2FA (optional)
- Notifications (default: email)

- Anomaly detection (global)

Seller



Brokerage



Broker



Exchange



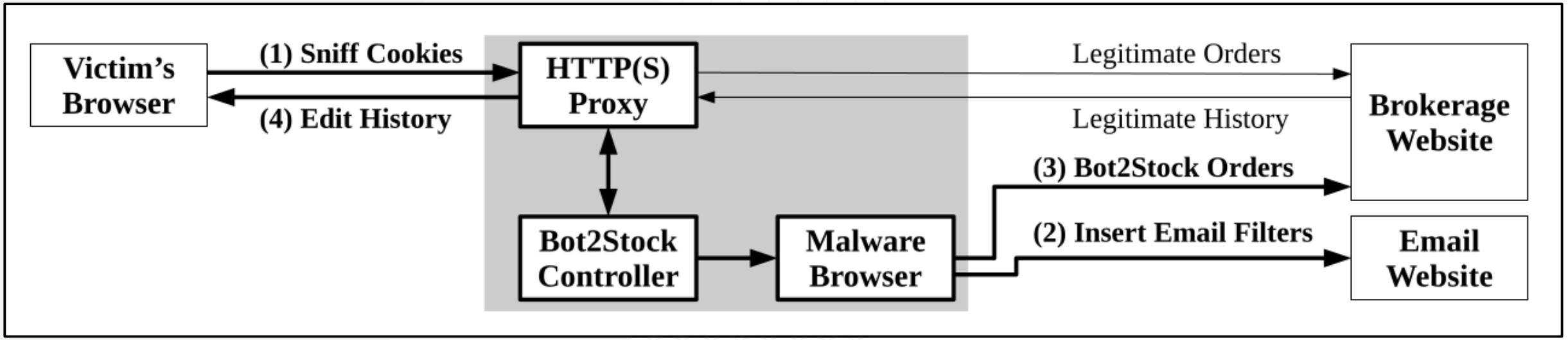
Incomplete views poorly suited to detecting large-scale collusion.

Agenda…

- What is *layering* manipulation? How does it work?
- What are the current defenses?
- How could a trading malware work?
- What would its impact be?
- The future…

CREATING THE NEXT®

Bot2Stock…



CREATING THE NEXT®

Agenda…

- What is *layering* manipulation? How does it work?
- What are the current defenses?
- How could a trading malware work?
- What would its impact be?
- The future…

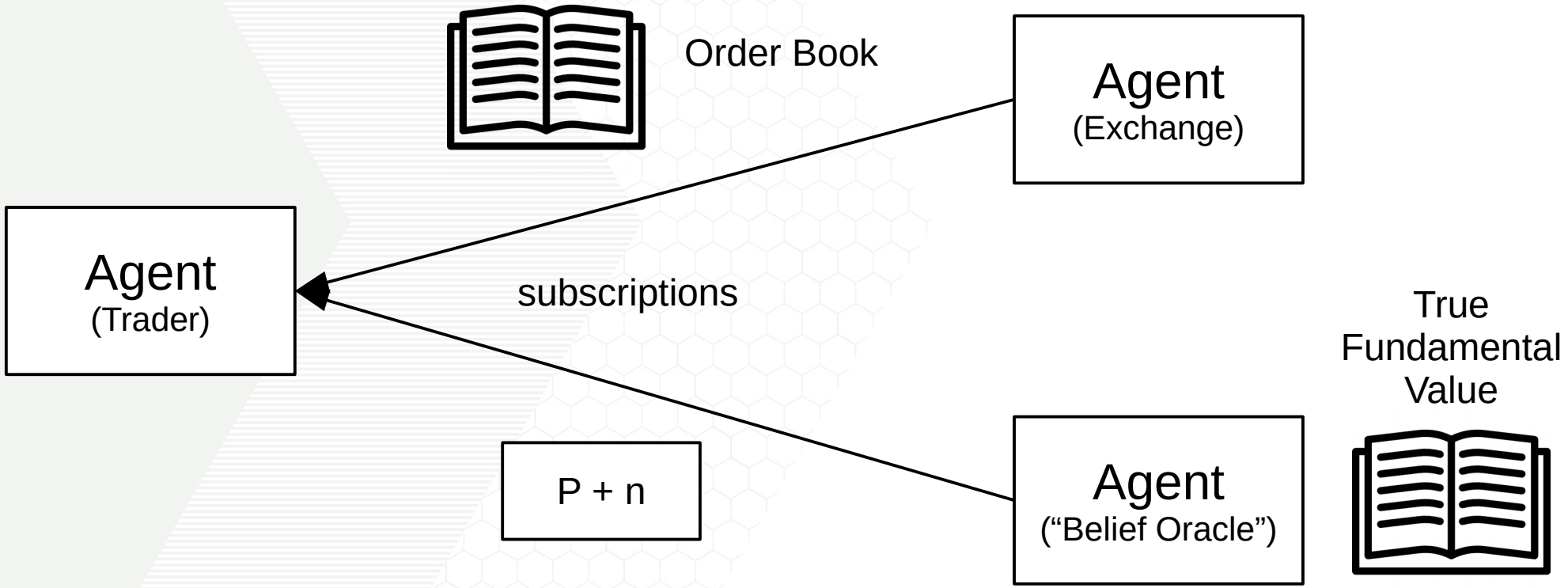
CREATING THE NEXT®

Simulation challenges…

- Modeling slippage
- Stock value beliefs
- Factoring computation, communication

CREATING THE NEXT®

Value beliefs…



Findings…

- Attack Duration: < 1 minute
- Network Latency Tolerance: > 200% added (3x)
- Required Trade Volume: 1.5%
- Per-Session ROI: 2.8% ROI
- **Annual ROI: 1022%**

Example…

- IBM, March 2020: 9,120 shares traded per minute
- 9,120 x 1.5% x Market Price = ~$5,000/session
- 2.8% ROI x 1 session per day x 252 trading days x $100k initial investment
- **Profit: > $1 million**
- **Botnet Loss: Commission Fees**
- **Self-Sustaining**

Agenda…

- What is *layering* manipulation? How does it work?
- What are the current defenses?
- How could a trading malware work?
- What would its impact be?
- The future…

CREATING THE NEXT®

The future…

- Mandating 2FA? No.
- More brokerage anomaly detection? Suboptimal.
- Improve alerting? Yes!
- Consolidated Audit Trail (CAT)