Maleficence in Traditional and Blockchain-based Financial Exchanges

Arthur Gervais
Financial Exchanges
Financial Exchanges 101
Financial Exchanges 101

Trade Matching
Financial Exchanges 101

Trade Matching

Trade Settlement
Financial Exchanges 101

Exchange

Trade Matching

Trade Settlement
Financial Exchanges 101

Exchange

Trade Matching

Trade Settlement
Financial Exchanges 101

Exchange

Trade Matching

Trade Settlement

Michaela

Jackson
Financial Exchanges 101

Exchange

Trade Matching

Trade Settlement

Michaela

Jackson
Financial Exchanges 101

Trade Matching

Trade Settlement

Exchange

Michaela

Jackson
Financial Exchanges 101

Exchange

Trade Matching

2 Matched Orders

Trade Settlement

Michaela

1

1

Exchange

Trade Matching

2 Matched Orders

Trade Settlement

Jackson

1

1
Financial Exchanges 101

Trade Matching

2 Matched Orders

Trade Settlement

Exchange
What could go wrong?
Exchange Maleficence
Security in Finance

- Front Running
- Wash Trading
- Cornering the market
- Pump and Dump
- Spoofing
- Bear Raiding
Exchange Maleficence
Security in Finance  🤔 Front Running
Exchange Maleficence
Security in Finance

Definition:

Entering into an equity trade, options or futures contracts with advance knowledge of a block transaction that will influence the price of the underlying security to capitalize on the trade. This practice is expressly forbidden by the SEC. Traders are not allowed to act on nonpublic information to trade ahead of customers lacking that knowledge.
Exchange Maleficence
Security in Finance
Exchange Maleficence
Security in Finance
Exchange Maleficence

Security in Finance  🚢 Wash Trading
Adversarial Model

Security in Finance

Who is the attacker?
Exchange Maleficence
Why is that a problem?

Unregulated Crypto Exchanges
Misbehaviour hard to detect, often impossible to prove
Potentially millions of USD in damages every year

Studies of real-world transaction reordering
Daian et al, Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges
Trade Matching

Non-Custodial Trade Settlement
## Order Book

<table>
<thead>
<tr>
<th>Market size</th>
<th>Price (US$)</th>
<th>My size</th>
<th>Market size</th>
<th>Price (US$)</th>
<th>My size</th>
</tr>
</thead>
<tbody>
<tr>
<td>21,231,360.00</td>
<td>418.40</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0.01,000,000</td>
<td>418.39</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0.01,000,000</td>
<td>418.31</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0.01,000,000</td>
<td>418.30</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0.01,000,000</td>
<td>418.29</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0.01,000,000</td>
<td>418.28</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0.01,000,000</td>
<td>418.27</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0.05,000,000</td>
<td>418.26</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0.01,000,000</td>
<td>418.23</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0.01,000,000</td>
<td>418.22</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0.01,000,000</td>
<td>418.21</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1.459,000,000</td>
<td>418.20</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0.01,000,000</td>
<td>418.19</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1.458,000,000</td>
<td>418.18</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1.458,000,000</td>
<td>418.17</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1.458,000,000</td>
<td>418.16</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1.458,000,000</td>
<td>418.15</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2.271,000,000</td>
<td>418.07</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0.06,000,000</td>
<td>418.06</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0.06,000,000</td>
<td>418.05</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1.531,000,000</td>
<td>418.04</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0.07,000,000</td>
<td>418.03</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0.07,000,000</td>
<td>418.02</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0.07,000,000</td>
<td>418.01</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0.678,000,000</td>
<td>418.00</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1.485,000,000</td>
<td>417.99</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1.483,000,000</td>
<td>417.92</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>16,487,000,000</td>
<td>417.91</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0.01,000,000</td>
<td>417.90</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1.438,000,000</td>
<td>417.89</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1.214,000,000</td>
<td>417.88</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Order Book
Order Book
Two Order Book Models

Server

On-Chain
Two Order Book Models

- Fast matching
- No fees for canceled orders
- No censorship resistance
- Exchange front running

Server

On-Chain
Two Order Book Models

Server

- Fast matching
- No fees for canceled orders
- No censorship resistance
- Exchange front running

On-Chain

- Censorship resistance
- Robust
- Slow matching
- Blockchain fees for orders
- Miner/trader front running
Two Trade Settlement Models

Off-Chain

On-Chain
Two Trade Settlement Models

Off the blockchain, but **secured by** the blockchain

**Off-Chain**

**On-Chain**
Two Trade Settlement Models

Off-Chain

- Off the blockchain, but secured by the blockchain

On-Chain

- Censorship resistance
- Robust
- No scale/Slow settlement
- Blockchain fees for orders
- Miner/trader front running
Two Trade Settlement Models

Off-Chain

- Fast, scalable trading
- No blockchain fees
- No miner/trader front running
- No censorship resistance
- Exchange operator front running

Off the blockchain, but secured by the blockchain

On-Chain

- Censorship resistance
- Robust
- No scale/Slow settlement
- Blockchain fees for orders
- Miner/trader front running
Summary

Exchange

Trade Matching

Non-Custodial Trade Settlement

Server

On-Chain

Off-Chain

On-Chain
TEX - Trustless Exchange

Exchange

Trade Matching

Non-Custodial Trade Settlement

Server

Off-Chain

* Kahlil et al. Eprint 2019
TEX - Trustless Exchange

Exchange

Trade Matching

Non-Custodial Trade Settlement

Server

- Immune to front-running from miner/trader
- Exchange operator could front run

Off-Chain

- Immune to front-running from miner/trader
- Scales

* Kahlil et al. Eprint 2019
Front Running Resilient
Order book
Front running resilient Orderbook
A commit and reveal protocol for limit order

Difficult to DoS the exchange

Hide the order content before the exchange commits, while guaranteeing its validity

The faster the exchange commits, the better (the less likely there was front running)
Time Lock Puzzle

- Puzzles are solvable with a predetermined amount of computation
- The puzzle's difficulty to decrypt must be sequential

Adversary with parallel resources should not decrypt a time-lock puzzle faster than a hardware-restrained adversary.

Possible technique: **Repeated squaring** in an RSA group [Rivest et al.’96]
Moonwalk Order

Zero Knowledge Proof

Encrypted Order

Time Lock Puzzle
Moonwalk Order

To prove the order is valid

To hide the order contents

To allow the exchange to decrypt the order after time $T$ (e.g. repeated squaring)

Zero Knowledge Proof

Encrypted Order

Time Lock Puzzle
Front running resilient order book
Front running resilient order book

(1) Create Moonwalk order

- ZKP
- Encrypted Order
- Time Lock Puzzle

Michaela (Trader)

Trade Matching & Off-chain settlement

TEX Smart Contract

Parent-Chain
Front running resilient order book

1. Create Moonwalk order
2. Encrypted order

- ZKP
- Encrypted Order
- Time Lock Puzzle

Michaela (Trader)

Trade Matching & Off-chain settlement

TEX Smart Contract

Parent-Chain

Trade Matching & Off-chain settlement
Front running resilient order book

1. Create Moonwalk order
2. Encrypted order

- ZKP
- Encrypted Order
- Time Lock Puzzle

Michaela (Trader)

Parent-Chain

TEX Smart Contract

Trade Matching & Off-chain settlement
Front running resilient order book

1. Create Moonwalk order
2. Encrypted order
3. Construct Merkel Tree Commitment adding newest order

- ZKP
- Encrypted Order
- Time Lock Puzzle

Michaela (Trader)

TEX Smart Contract
Parent-Chain

Trade Matching & Off-chain settlement
Front running resilient order book

1. Create Moonwalk order
2. Encrypted order
3. Construct Merkel Tree Commitment adding newest order
4. Receive MT receipt

- ZKP
- Encrypted Order
- Time Lock Puzzle

TEX Smart Contract

Trade Matching & Off-chain settlement

Michaela (Trader)

Parent-Chain
Front running resilient order book

1. Create Moonwalk order
2. Encrypted order
3. Construct Merkel Tree Commitment
4. Receive MT receipt

TEX Smart Contract

Parent-Chain

Trade Matching & Off-chain settlement

Michaela (Trader)
Front running resilient order book

1. Create Moonwalk order
2. Encrypted order
3. Construct Merkle Tree Commitment
4. Receive MT receipt
5. Reveal key

Trade Matching & Off-chain settlement
TEX Smart Contract
Parent-Chain

ZKP
Encrypted Order
Time Lock Puzzle

Michaela (Trader)
Front running resilient order book

1. Create Moonwalk order
2. Encrypted order
3. Construct Merkel Tree Commitment adding newest order
4. Receive MT receipt
5. Reveal key
6. New order submission authorization

Trade Matching & Off-chain settlement

TEX Smart Contract

Parent-Chain
Front running resilient order book

1. Create Moonwalk order

2. Encrypted order

3. Construct Merkel Tree Commitment

4. Receive MT receipt

5. Reveal key

6. New order submission authorization

7. Repeat with new order, to test if the exchange is inspecting orders

Trade Matching & Off-chain settlement

TEX Smart Contract

Parent-Chain

(4) receive MT receipt

(2) Encrypted order

(3) Construct Merkel Tree Commitment adding newest order

(5) Reveal key

(6) New order submission authorization

(7) Repeat with new order, to test if the exchange is inspecting orders

 shortages (null) (null) (null) (null)
Front running resilient order book

1. Create Moonwalk order
2. Encrypted order
3. Construct Merkle Tree Commitment adding newest order
4. receive MT receipt
5. reveal key
6. new order submission authorization
7. Repeat with new order, to test if the exchange is inspecting orders
8. checkpoint constant size order state

Trade Matching & Off-chain settlement

TEX Smart Contract

Parent-Chain

Michaela (Trader)
Building trust

- Operator can decrypt the order in $T$ seconds
- If it takes $T$ seconds, front running can happen
- Users issue $k$ fake (small value) orders
Actions against misbehaviour

- Challenge on Parent Chain (fraud proof)
- Time for the operator to answer
- Operator punished if no or a bad response
Assumptions, Drawbacks

No side channels (IP address/Browser Fingerprinting/etc)

Fraud Proof: the blockchain always has sufficient space to issue challenges

Such exchange is likely not suitable for HFT (high frequency trading)
Trade Settlement Layer
Why is off-chain exciting?

0 or 1 tx to
join
off-chain protocol

1000+ tx securely
off-chain

0 or 1 tx to
leave
off-chain protocol

No consensus latency or mining fees, while still achieving non-custodial security

Backward compatibility!
Which off-chain solution?

Off-Chain

Commit-Chains
- NOCUST
- Plasma

Channel Networks
- State Replacement
  - One-way channel
  - State channel
- Sync
  - HTLC
  - Routing
Which off-chain solution?

Off-Chain

Commit-Chains

Channel Networks

NOCUST

Sync

HTLC

Routing

SoK: Off The Chain Transactions

Lewis Gudgin
Imperial College London
l.gudgin4@imperial.ac.uk

Patrick McCorry
King’s College London
patrick.mccorry@kcl.ac.uk

Pedro Moreno-Sanchez
TU Wien
pedro.sanchez@tuwien.ac.at

Arthur Gervais
Imperial College London, Liquidity Network,
Lancaster University of Applied Sciences and Arts
a.gervais@imperial.ac.uk

Stefanie Roos
TU Delft
s.roos@ tudelft.nl

Abstract—Blockchains have the potential to revolutionize markets and services, yet, currently exhibit high latency and fail to handle high volume to those managed by traditional custodial financial systems. Layer-two protocols, built on top of layer-one blockchains, avoid saturating every transaction to the whole network by sending transactions off-chain and instead utilize the blockchain only as a reserve for disputes. The promise of layer-two protocols is to complete transactions in sub-seconds, reduce fees, and allow blockchains to scale.

With this Systematization of Knowledge, we are the first to structure the complex rich and multifaceted body of research on layer-two transactions. Cataloging the research into payment and state channels as well as on-chain-side channels, we provide a foundational structure for future research. Based on this study, a Systematization of the associated synchronization and routing protocols along with their privacy and security aspects. Contrary to common belief in the Blockchain community, we show that layer-two can scale blockchains; that layer-two protocols are secure without full decentralization; that privacy of layer-two transactions is not granted by default; and that fees depend on the transmitted transaction value. The SoK shows the layer-two fog, highlights the potential of layer-two solutions and identifies their unsolved challenges and promising avenues of future work.
Which off-chain solution?

Off-Chain

Commit-Chains
- NOCUST
- Plasma

Channel Networks
- State Replacement
  - One-way channel
  - State channel
- Sync
  - HTLC
  - Routing
Thank You!