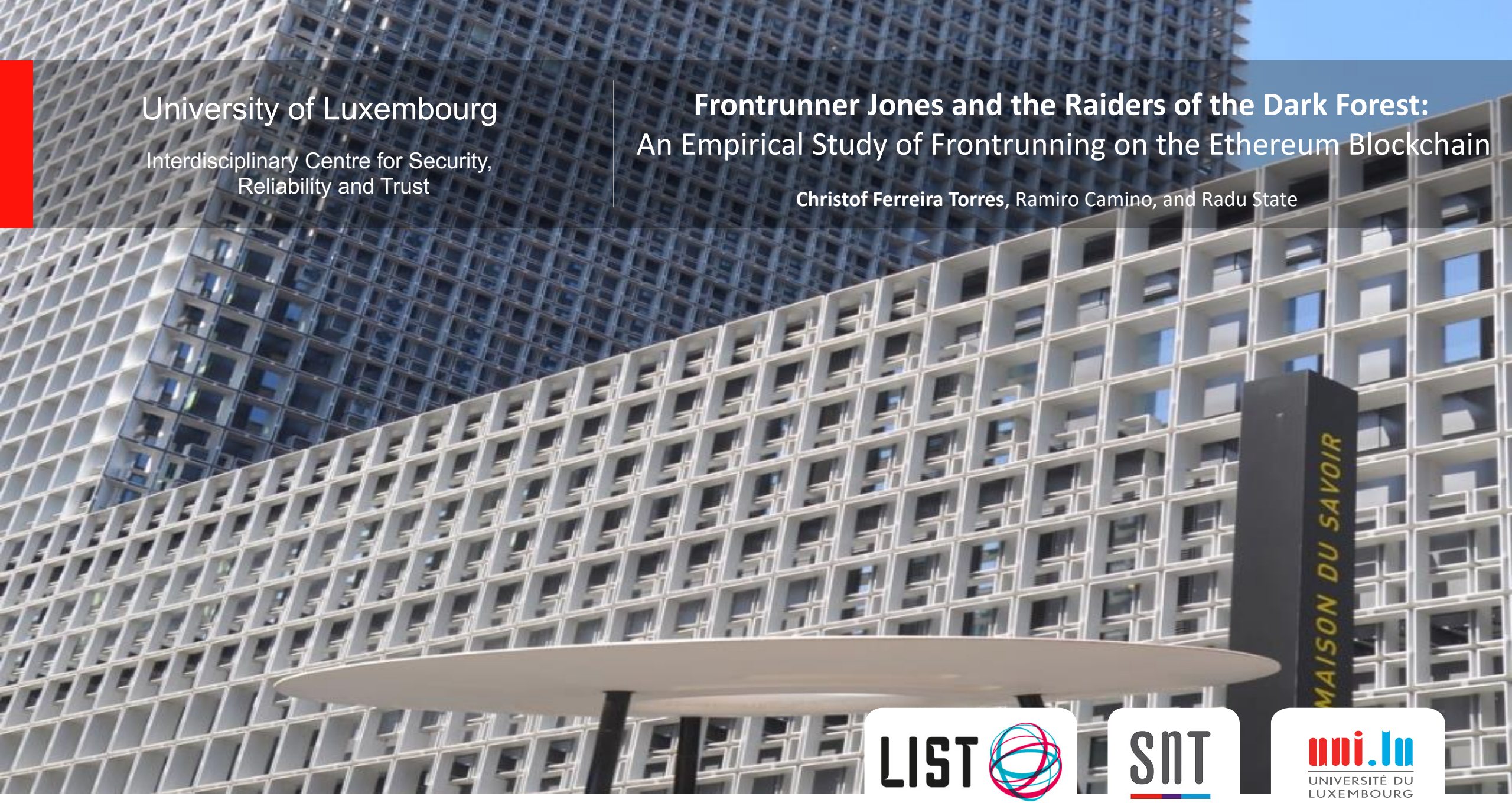



University of Luxembourg

Interdisciplinary Centre for Security, Reliability and Trust

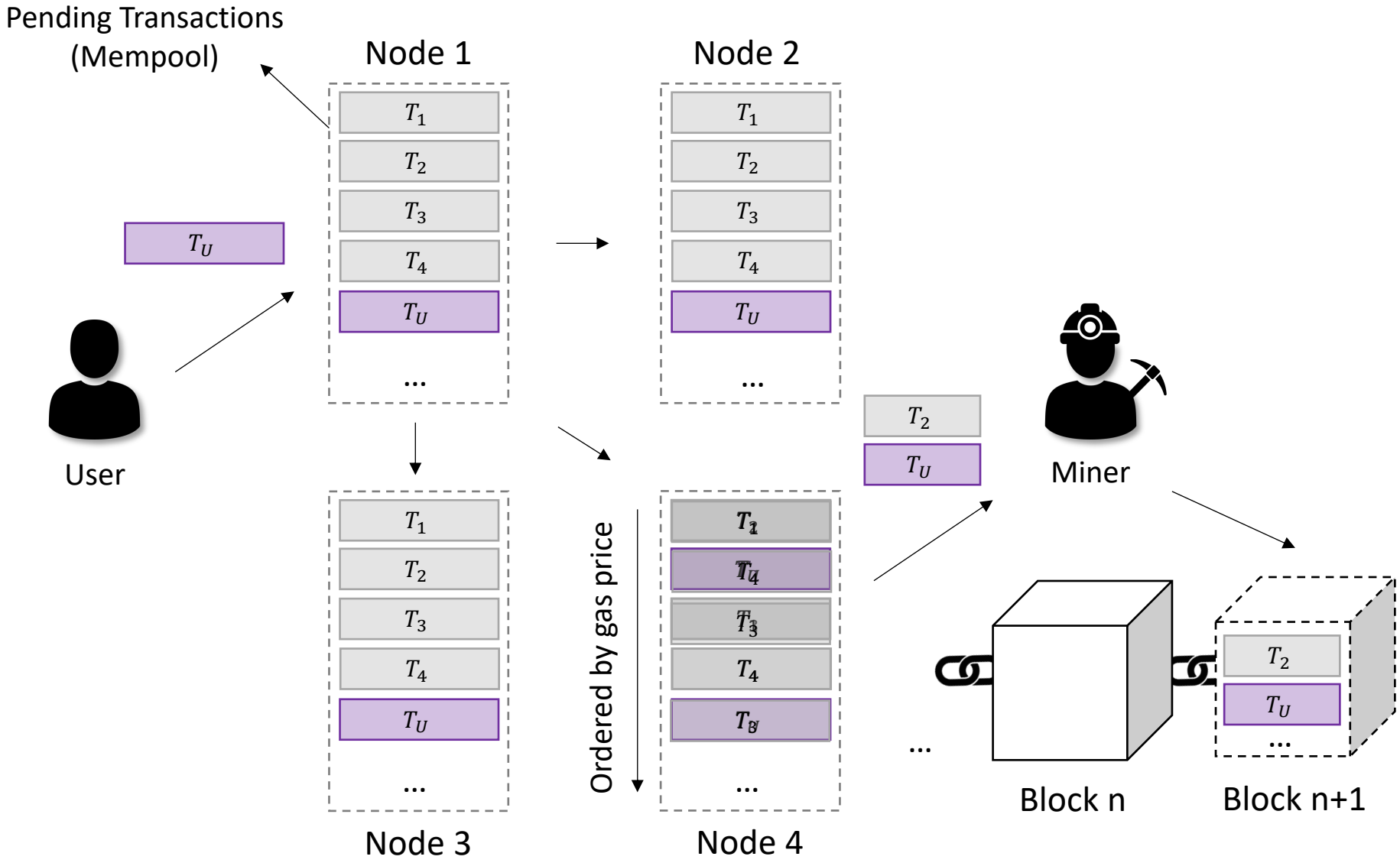
# Frontrunner Jones and the Raiders of the Dark Forest:
## An Empirical Study of Frontrunning on the Ethereum Blockchain

**Christof Ferreira Torres**, Ramiro Camino, and Radu State

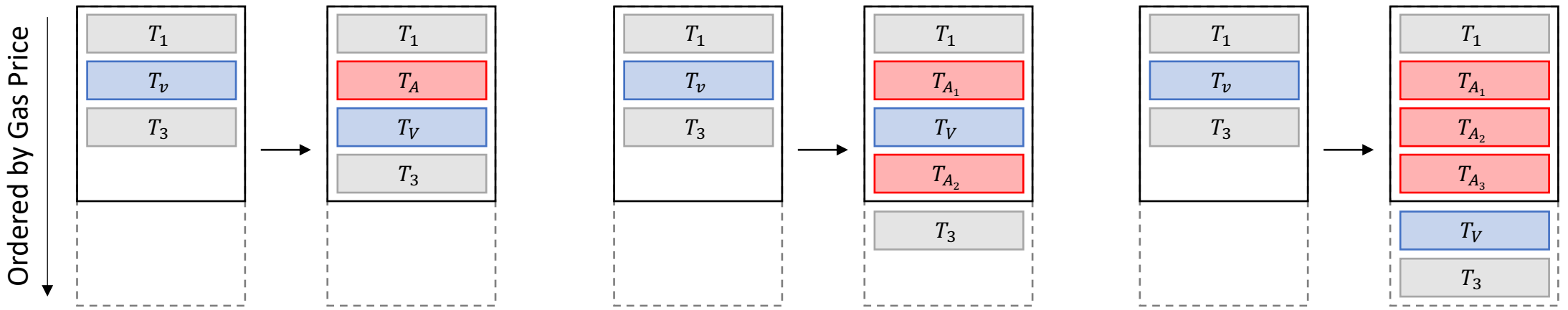
LIST SnT uni.lu UNIVERSITÉ DU LUXEMBOURG

# Ethereum's Dark Forest

# Ethereum's Mining Process



# Frontrunning Taxonomy




Displacement
*(Replay Attack)*

Insertion
*(Sandwich Attack)*

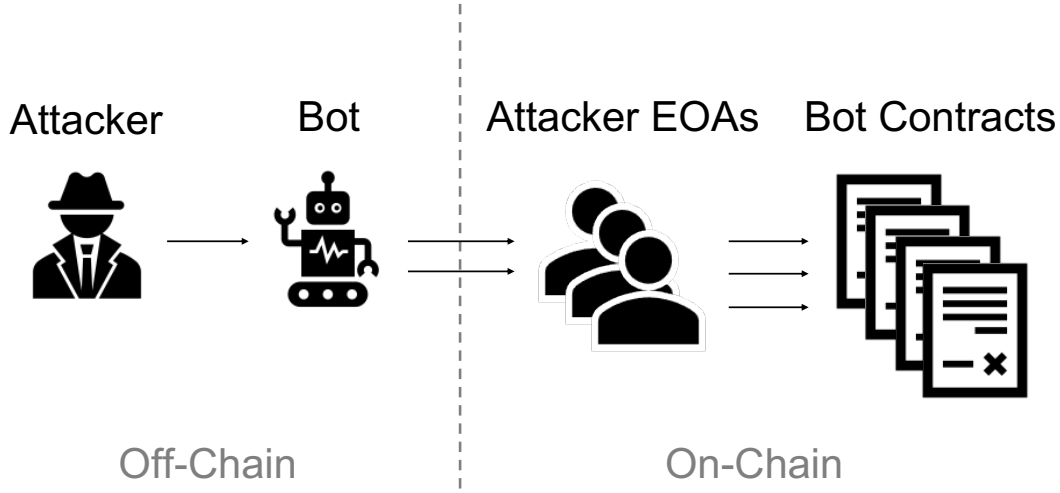
Suppression
*(Block Stuffing)*

Transaction Pool
(Pending Transactions)

Proposed Block

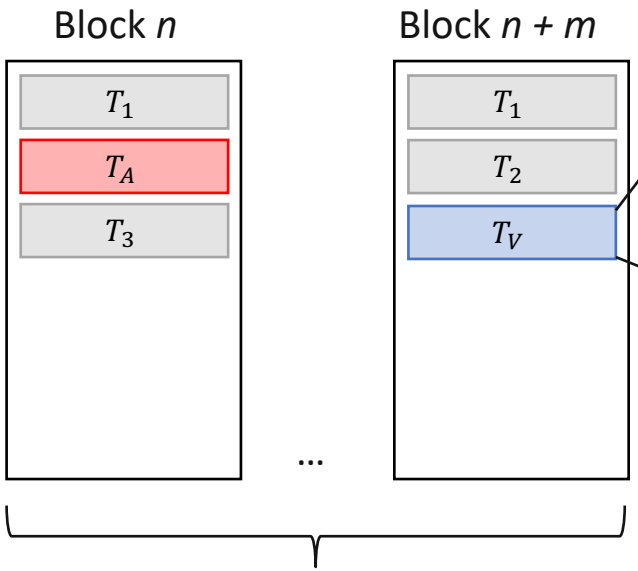
# Attacker Model

- Attackers can be miners and non-miners.
  - → We assume financially rational non-miners.
- Attackers monitor pending transactions, search for victim transaction, and create own transactions.
  - → We assume attackers automate those tasks using off-chain bot programs.
- Bots have access to Externally Owned Accounts.
  - → We assume EOAs hold a sufficiently large balance.
- We assume bots use on-chain contracts to coordinate attacks.

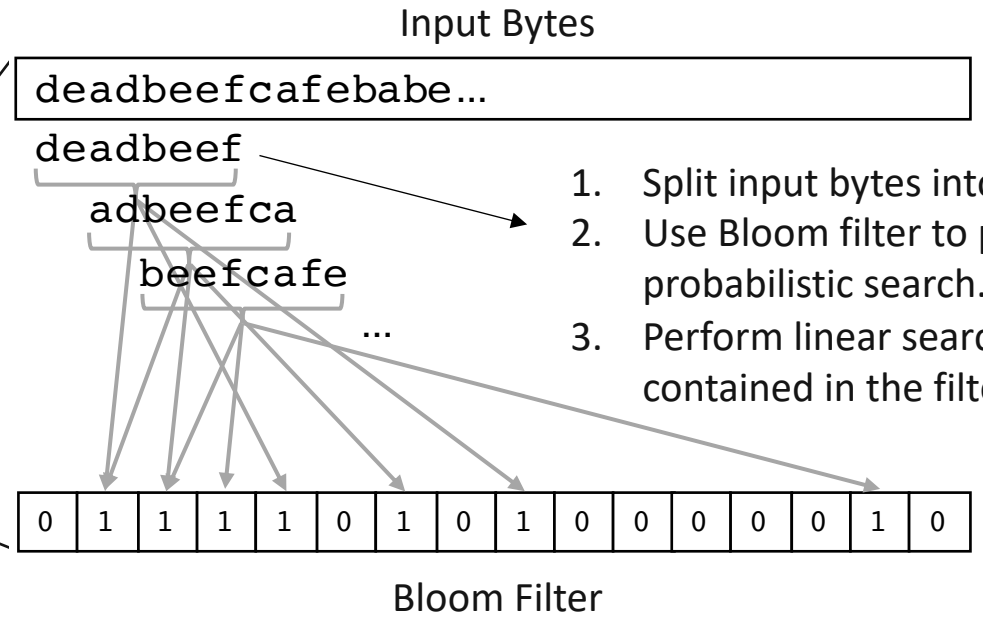


# Detecting Frontrunning Attacks

# Detecting Displacement




Split range of blocks to be analyzed into windows of 100 blocks with an offset of 20 blocks.




1. Split input bytes into n-grams of 4 bytes.
2. Use Bloom filter to perform quick probabilistic search.
3. Perform linear search if 95% of *n*-grams are contained in the filter.

Heuristics:

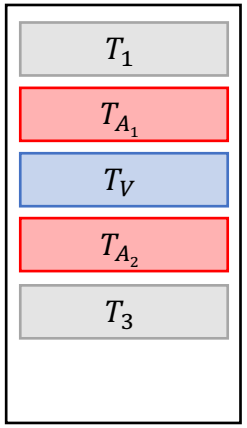
$H_1$: sender and receiver of $T_A$ and $T_V$ must be different.

$H_2$: gas price $T_A$ > gas price $T_V$.

$H_3$: 25% of $T_V$'s input bytes must conform with those of $T_A$.

Check if executing $T_A$ before $T_V$ results in a different state than execution $T_A$ after $T_V$.

# Detecting Insertion




Get ERC-20 token *Transfer* events for all transactions.

$H_3: c_{A1} = c_V = c_{A2}$ $H_5: i_{A1} > i_V > i_{A2}$

| Event | From | To | Amount | Contract | Hash | Index | Gas Price |
|---|---|---|---|---|---|---|---|
| $T_{A1}$ | 0x0984… | 0x0bfe… | 50000 | 0xab67… | 0x4393… | 0 | 150 Gwei |
| $T_V$ | 0x0984… | 0x14ca… | 100000 | 0xab67… | 0x74ab… | 10 | 60 Gwei |
| $T_{A2}$ | 0x0bfe… | 0x0984… | 50000 | 0xab67… | 0x15bc… | 11 | 59 Gwei |

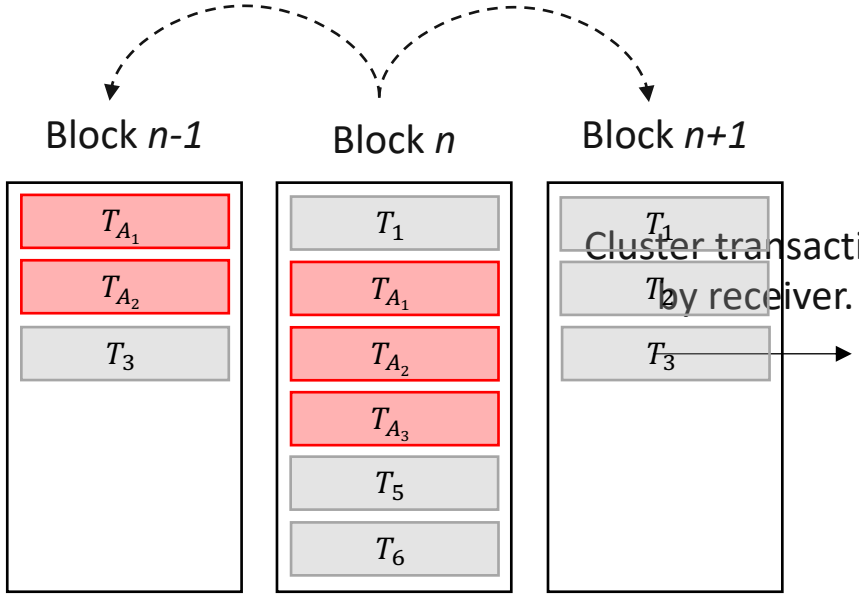
$H_1: s_{A1} = s_V = r_{A2} \wedge r_{A1} = s_{A2}$

$H_4: h_{A1} \neq h_V \neq h_{A2}$ $H_6: g_{A1} > g_V \geq g_{A2}$

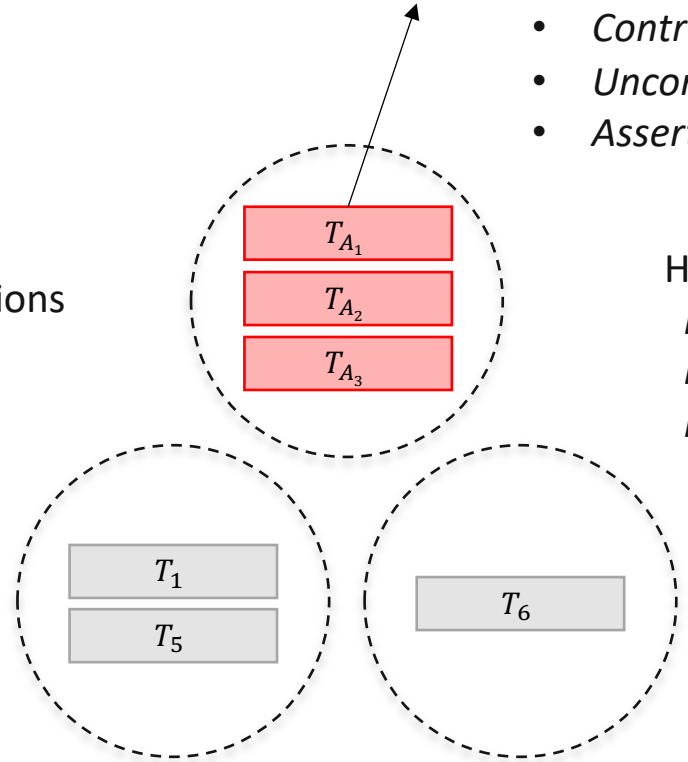
$H_2: \frac{|aA_1 \_ aA_2|}{\max(aA_1, aA_2)} \leq 0.01$

# Detecting Suppression

Does one of the neighbouring blocks contain a cluster that satisfies the same heuristics?




Cluster transactions by receiver.




Check if execution trace of first transaction employs one of the 3 suppression strategies:

- *Controlled gas loop*
- *Uncontrolled gas loop*
- *Assert*

Heuristics:

$H_1$: transactions > 1.

$H_2$: each transaction consumes > 21,000 gas.

$H_3$: gas used / gas limit > 99% for all transactions.

# Analyzing Frontrunning Attacks

LIST SnT uni.lu UNIVERSITÉ DU LUXEMBOURG

# Analyzing Cost And Profit

2,983 Attacks

| | Cost (USD) | Profit (USD) |
|---|---|---|
| mean | 14.28 | 1,537.99 |
| std | 18.25 | 7,162.80 |
| min | 0.01 | 0.00 |
| 25% | 4.36 | 1.14 |
| 50% | 9.48 | 158.53 |
| 75% | 16.64 | 851.04 |
| max | 311.69 | 223,150.01 |

Displacement

196,691 Attacks

| | Cost (USD) | Profit (USD) |
|---|---|---|
| mean | 19.41 | 65.05 |
| std | 51.15 | 233.44 |
| min | 0.01 | -10,620.61 |
| 25% | 4.09 | 7.86 |
| 50% | 7.74 | 24.07 |
| 75% | 15.23 | 62.92 |
| max | 1,822.22 | 20,084.01 |

Insertion

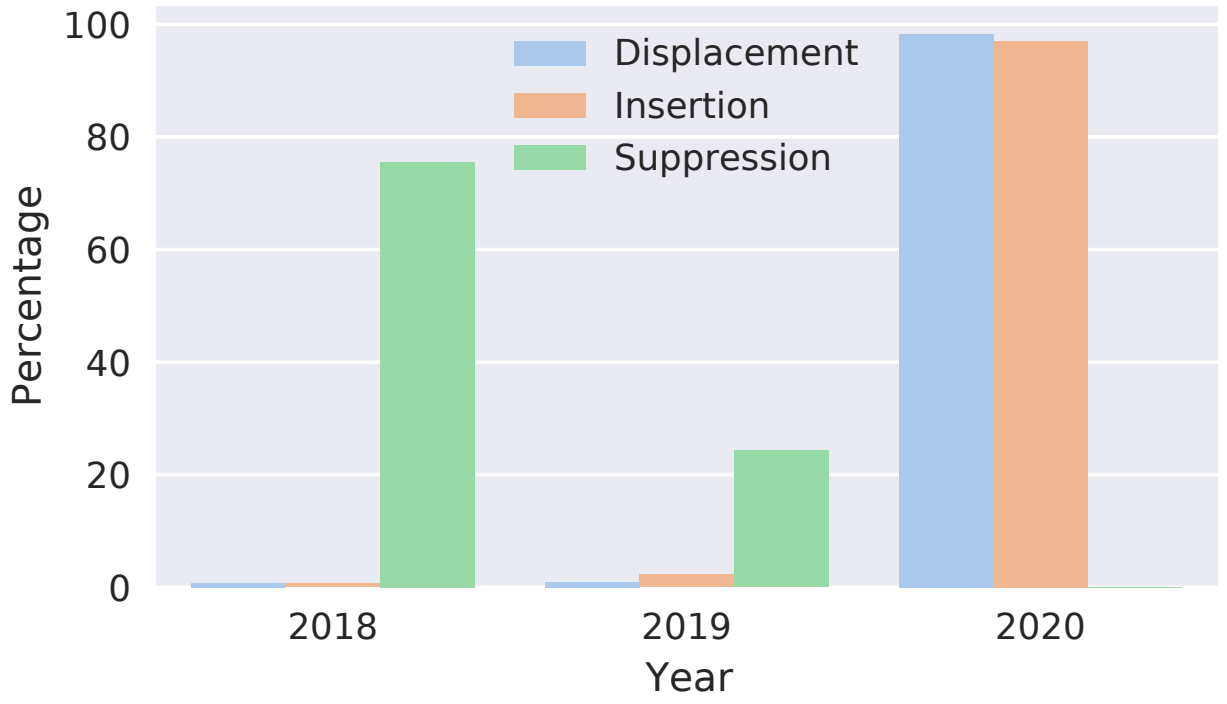
50 Attacks

| | Cost (USD) | Profit (USD) |
|---|---|---|
| mean | 2,349.65 | 20,725.24 |
| std | 3,331.21 | 113,598.58 |
| min | 4.67 | -10,741.12 |
| 25% | 221.87 | -1,893.26 |
| 50% | 896.68 | -284.81 |
| 75% | 2,719.69 | -14.93 |
| max | 10,741.12 | 791,211.86 |

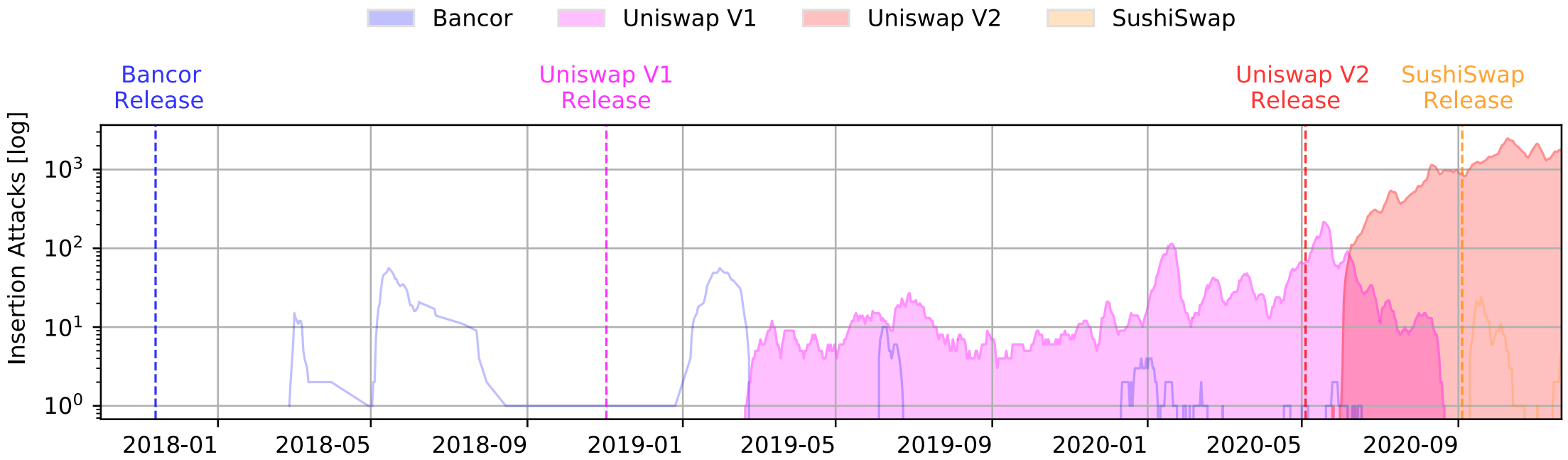
Suppression

Total Attacks: 199,725
Accumulated Profit: 18.41M USD

# Analyzing Trends

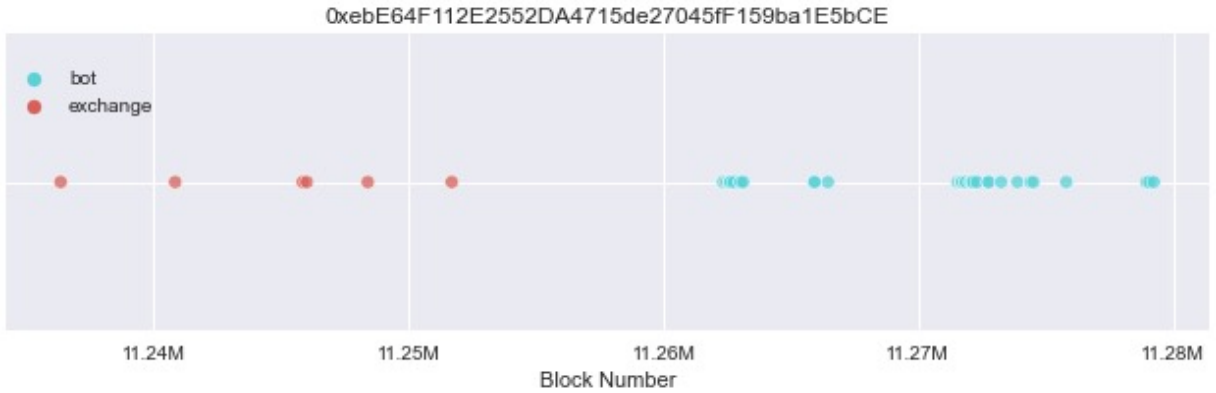


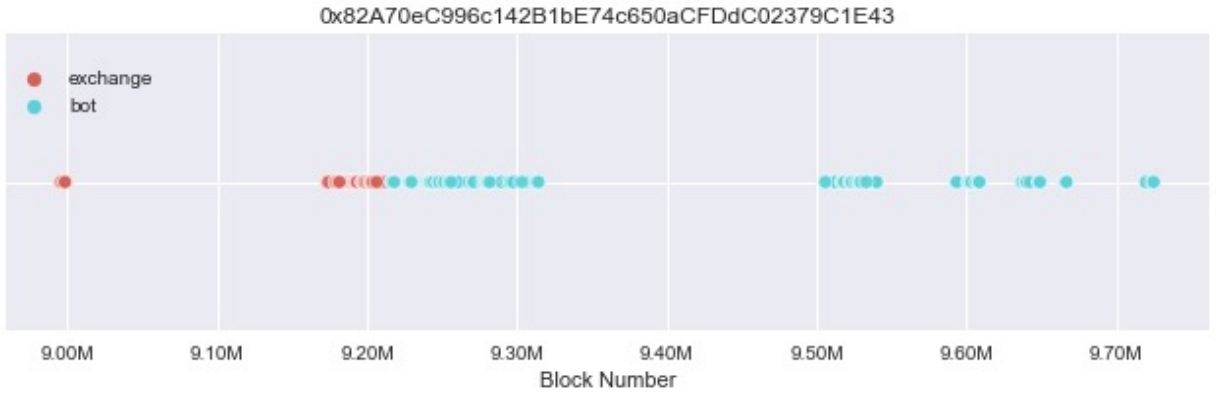
# Analyzing Insertion Attacks on DEXes



# Analyzing Insertion Attacks on DEXes

| Exchange Combination | Attacker Clusters |
|---|---|
| Uniswap V2 | 72 |
| Uniswap V1 | 16 |
| SushiSwap, Uniswap V2 | 4 |
| Bancor | 3 |
| Uniswap V1, Uniswap V2 | 2 |
| Bancor, SushiSwap, Uniswap V1, Uniswap V2 | 1 |



# Analyzing Suppression Victims and Strategies

| Suppressed Contract Address | Contract Name | Attacks | Rounds | Transactions | Attackers | Bot Contracts | Attacker Clusters |
|---|---|---|---|---|---|---|---|
| 0xDd9fd6b6F8f7ea932997992bbE67EabB3e316f3C | Last Winner | 16 | 20 | 304 | 27 | 5 | 2 |
| 0xA62142888ABa8370742bE823c1782D17A0389Da1 | FoMo3Dlong | 12 | 188 | 5875 | 81 | 8 | 4 |
| 0x5D0d76787D9d564061dD23f8209F804a3b8AD2F2 | Peach Will | 6 | 52 | 1105 | 26 | 5 | 2 |
| 0x2c58B11405a6a8154FD3bbC4CcAa43924f2BE769 | ERD | 3 | 3 | 207 | 20 | 2 | 1 |
| 0x42CeaD70158235a6ca4868F3CFAF600c7A7b0ebB | ETH CAT | 2 | 23 | 929 | 20 | 2 | 1 |
| 0xB7C2e4047Fb76508D4137BE787DaF28B013F00E6 | Escape plan | 2 | 3 | 67 | 20 | 2 | 1 |
| 0x29488e24cFdAA52a0b837217926C0c0853Db7962 | SuperCard | 1 | 25 | 319 | 17 | 1 | 1 |
| 0xB4a448387403554616eB5B50aa4C48f75243a015 | Mobius2Dv2 | 1 | 4 | 82 | 19 | 1 | 1 |
| 0x3e22bB2279d6Bea3Cfe57f3Ed608fC3B1DeaDADf | Star3Dlong | 1 | 3 | 66 | 6 | 1 | 1 |
| 0xD15E559f6BD5C785Db35E550F9FbC80045b0a049 | FDC | 1 | 3 | 44 | 18 | 1 | 1 |
| 0x9954fF17909893B443E2EE825066373960c2735A | F3DPRO | 1 | 1 | 41 | 18 | 1 | 1 |
| 0xC75506dEAe7c01F47BCd330B324226CE9ba78e30 | FomoXP | 1 | 3 | 39 | 19 | 1 | 1 |
| 0x0fe2247a20E779a879c647D2b9deA1b896FC0ccf | EFS | 1 | 1 | 33 | 16 | 1 | 1 |
| 0xbAbED6ca5C86B2347D374e88251Ca8007C417f55 | The rabbit | 1 | 1 | 15 | 13 | 1 | 1 |
| 0xb178EA2c9023bb2DD500a607505D2aa121F92A35 | RichKey | 1 | 1 | 9 | 8 | 1 | 1 |

| Suppression Strategy | Attacks | Successful | Failed |
|---|---|---|---|
| Assert | 20 | 2 | 18 |
| Controlled Gas Loop | 18 | 8 | 10 |
| Uncontrolled Gas Loop | 12 | 3 | 9 |

# Conclusion

# Conclusion

- We presented an efficient methodology to detect **displacement, insertion,** and **suppression** attacks on Ethereum's past transaction history.
- We performed an extensive measurement study on the Ethereum blockchain and analyzed more than **11M blocks** (roughly 5 years) for frontrunning attacks.
- We identified almost **200K frontrunning attacks** performed by over 1.5K **attacker accounts** and more than **500 bots** with an accumulated **profit of over 18.41M USD** for the attackers.
- We found that attacker accounts and bots can be grouped into **137 unique attacker clusters**.
- We discussed frontrunning implications and discovered that miners made a **profit of over 300K USD** due to frontrunners.

# Questions?

All **code** & **data** is available on GitHub:

https://github.com/christoftorres/Frontrunner-Jones

Contact information:

christof.torres@uni.lu

Supported by:

ripple | University Blockchain Research Initiative

Luxembourg National Research Fund