Revisiting Double-Spending Attacks on the Bitcoin Blockchain: New Findings

Jian Zheng, Huawei Huang, Canlin Li, Zibin Zheng, Song Guo*
School of Computer Science and Engineering, Sun Yat-Sen University, Guangzhou, China
*Department of Computing, The Hong Kong Polytechnic University, Hong Kong.

Presentation for IWQoS 2021
Double-Spending Attack

☐: Block mined by an honest miner
○: Block mined by the attacker

① Target TX is released
② Forking attack
③ Pack the target TX
④ Confirmation position
⑤ Release all blocks
Our contribution

• **Adaptive DSA**: Adaptive Double-Spending Attack

• Profit-maximized attack strategy by Stochastic Dynamic Programming (SDP)

• Analytical model for simulation
An unfavourable situation to the attacker

- The attacker is mining
- Honest miners are mining

- The transaction has not been confirmed in $S_{1,5}$.

- Should the attacker give up?
Attack decision: Quit or Keep

- **0**: Quit attacking

- **i = 3**
  - **j = 2**
  - Case-1

- **i = 1**
  - **j = 2**
  - Case-2

- **i = 2**
  - **j = 2**
  - Case-3
Attack decision: Quit or Keep

- 1: Keep attacking

$p, q$: the probabilities of state transition

$p: S_{i,j} \rightarrow S_{i+1,j}$

$q: S_{i,j} \rightarrow S_{i,j+1}$
Attack-Decision Matrix

- Variables: \( d_{i,j} \in \{0, 1\} \)
  - 0: Quit attacking
  - 1: Keep attacking

- Profit: \( f(\{d_{i,j}\}) \)

- Tools:
  - Occurrence-Probability Matrix
  - Reward Matrix

<table>
<thead>
<tr>
<th>(d_{ij})</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Occurrence-Probability Matrix

\[ P_{i,j} = \begin{cases} 
1, & \text{if } i = j = 0; \\
d_{i-1,j} \cdot p \cdot P_{i-1,j}, & \text{if } j = 0 \text{ or } i = z; \\
d_{i,j-1} \cdot q \cdot P_{i,j-1}, & \text{if } i = 0 \text{ or } j = z; \\
d_{i-1,j} \cdot p \cdot P_{i-1,j} + d_{i,j-1} \cdot q \cdot P_{i,j-1}, & \text{otherwise.} 
\end{cases} \] (1)

\[ P_{i,j} \begin{array}{ccccccc} 
 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
\end{array} \]
\[ R_{i,j} = \begin{cases} 
- (i + j) \cdot \text{cost}, & \text{if } i < j; \\
i \cdot d - (i + j) \cdot \text{cost}, & \text{if } z > i > j; \\
p \cdot i \cdot d - (i + j) \cdot \text{cost}, & \text{if } z > i = j; \\
p[b + d(z + 1) - (i + j + 1) \cdot \text{cost}] + q \cdot R_{i,j+1}, & \text{if } i = z, j \leq z - 2; \\
p[b + d(z + 1) - (i + j + 1) \cdot \text{cost}] + q[p(b + z \cdot d) - 2z \cdot \text{cost}], & \text{if } i = z, j = z - 1. 
\end{cases} \]
Profit-Maximization Problem

- **0**: Quit attacking
- **1**: Keep attacking

\[ d_{i,j} \in \{0, 1\} \]

\[
\max f(\{d_{i,j}\}) = \sum_{i=0}^{z} \sum_{j=0}^{z} (1 - d_{i,j}) \cdot P_{i,j} \cdot R_{i,j}
\]
• $d_{i,j}=0$, quit attacking

$$J_n(s_{i,j}) = J_{n+1}(s'_{i,j}) = \begin{cases} 0, & \text{if } 0 \leq i < j \leq z - 1; \\ i \cdot d, & \text{if } 0 \leq j < i \leq z - 1; \\ p \cdot i \cdot d, & \text{if } 0 \leq i = j \leq z - 1. \end{cases}$$

<table>
<thead>
<tr>
<th>$J_n(s_{i,j})$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
</table>
Stochastic Dynamic Programming (SDP)

• $d_{i,j} = 1$, keep attacking

$$J_n(s_{i,j}) = -\text{cost} + p \cdot J_{n+1}(s_{i+1,j}) + q \cdot J_{n+1}(s_{i,j+1})$$

$p, q$: the probabilities of state transition
Performance Evaluation

The proportion of the hashpower controlled by the attacker (represented by $p$)
Performance Evaluation

The proportion of the hashpower controlled by the attacker (represented by $\rho$)
Conclusion

• **Adaptive DSA**: new threat to PoW-based blockchains

• 50% is not enough

• More strategies in the double-spending attack
Thanks

HuangLab@SYSU  http://xintelligence.pro/