NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Shamik Sural
Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 53: Blockchain Security - II

CONCEPTS COVERED

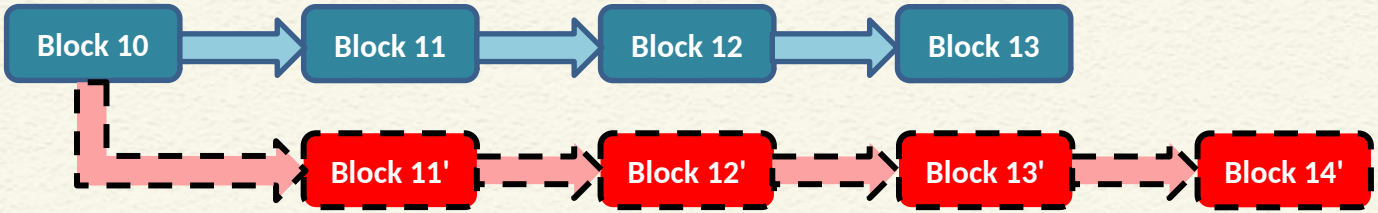
- Selfish Mining Attack
- Different Scenarios and Attacker’s Actions

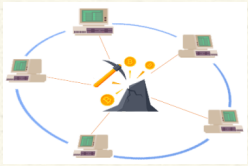
KEYWORDS

- Selfish Mining
- Attacker’s Pool
- Public Chain
- Block Suppression

Selfish Mining Attack

Others



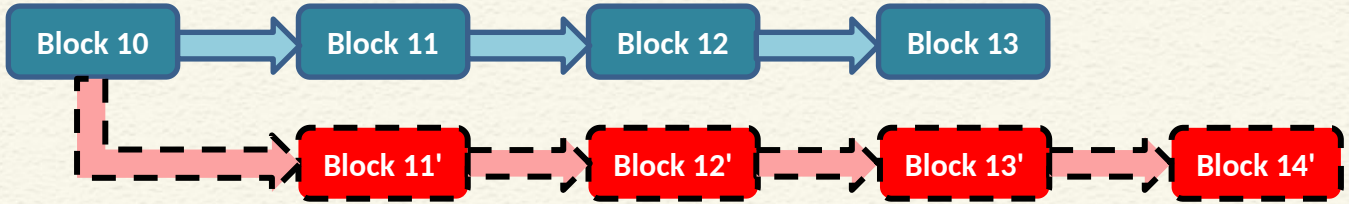


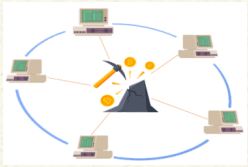
Mining Pool

"Majority Is Not Enough: Bitcoin Mining Is Vulnerable", Ittay Eyal and Emin Guen Sirer, Financial Cryptography, 2014

Selfish Mining Attack

Others





Mining Pool

Selfish Mining Attack

Pool intentionally forking the chain for keeping discovered blocks private

The honest nodes continue to mine on the public chain
The pool mines on its own private branch

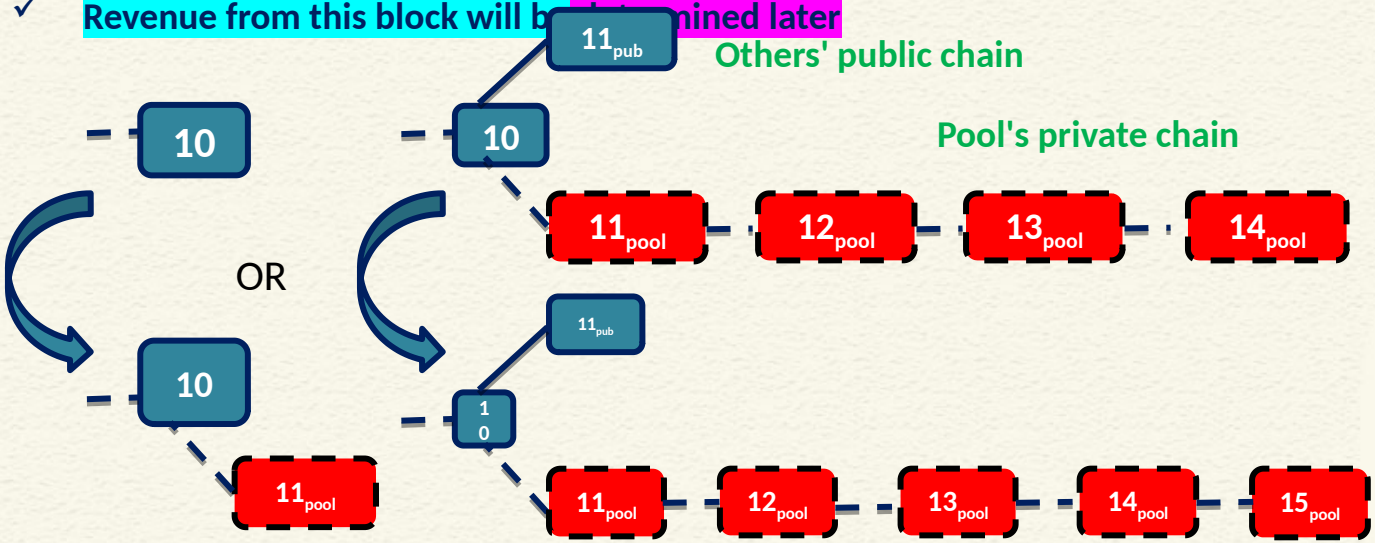
Discovering more blocks by pool develops a longer lead on the public chain, and continues to keep these new blocks private

When the public branch approaches the pool's private branch in length,
the selfish miners reveal blocks from their private chain to the public

Selfish Mining Attack

1. Any state but two branches of length 1, pools finds a block

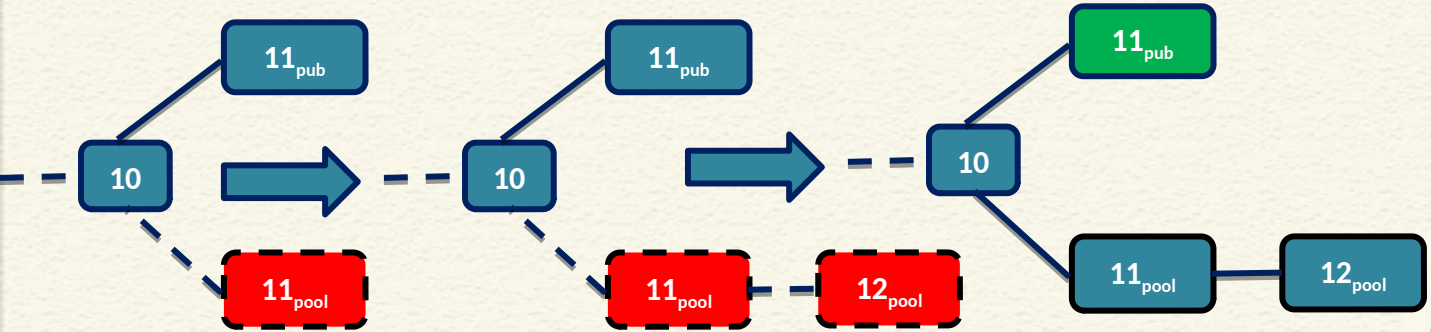
- ✓ The pool appends one block to its private branch, increasing its lead on the public branch by one
- ✓ Revenue from this block will b[illegible]mined later



Selfish Mining Attack

2. Was two branches of length 1, pool finds a block

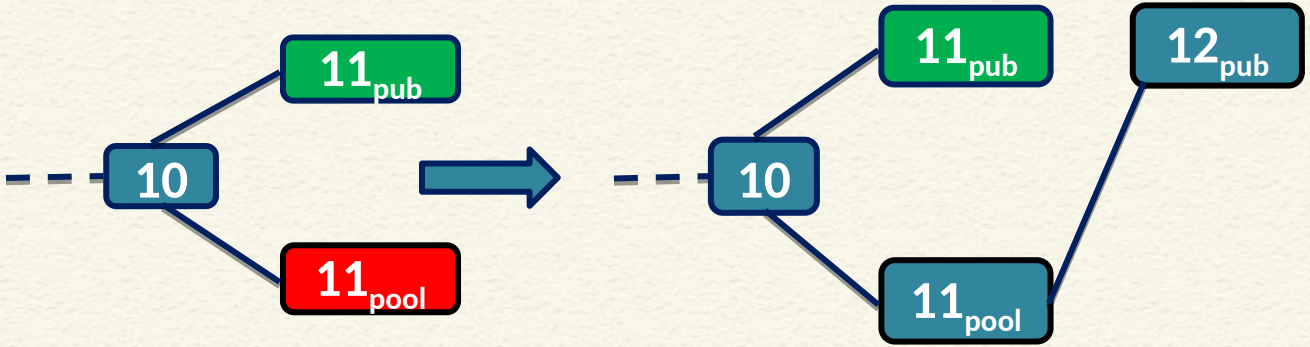
- ✓ The pool publishes its secret branch of length two
- ✓ Pool obtains a revenue of two



Selfish Mining Attack

3. Was two branches of length 1, others find a block after pool head

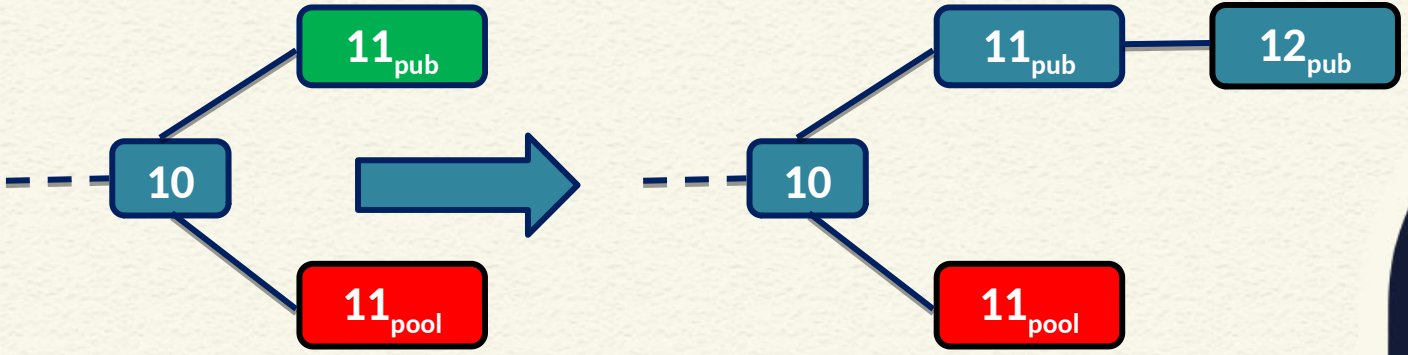
- ✓ The pool and the others obtain a revenue of one each - the others for the new head, the pool for its predecessor



Selfish Mining Attack

4. Was two branches of length 1, others find a block after others' head

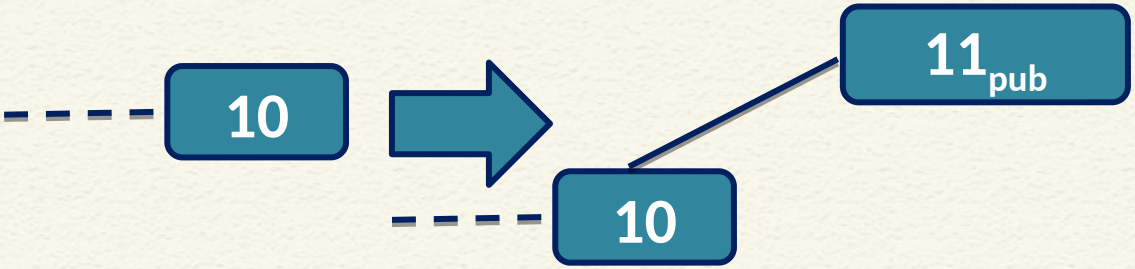
- ✓ **The others obtain a revenue of two**



Selfish Mining Attack

5. No private branch, others find a block

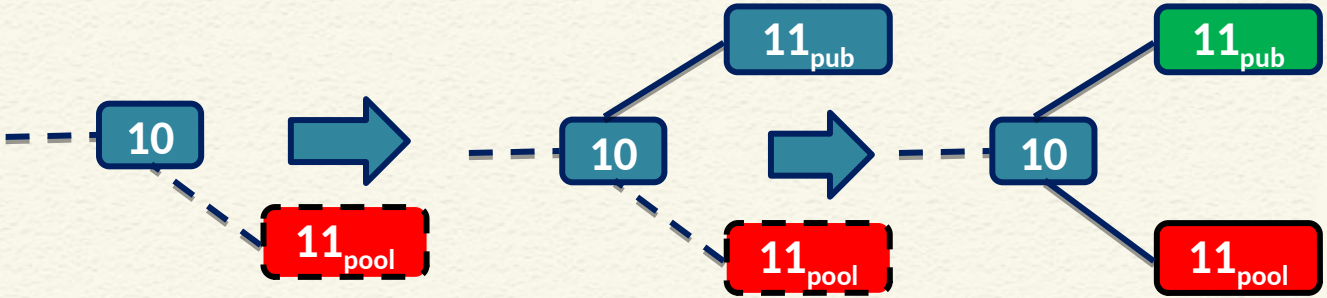
- ✓ Both the pool and the others start mining on the new head
- ✓ The others obtain a revenue of one



Selfish Mining Attack

6. Lead was 1, others find a block

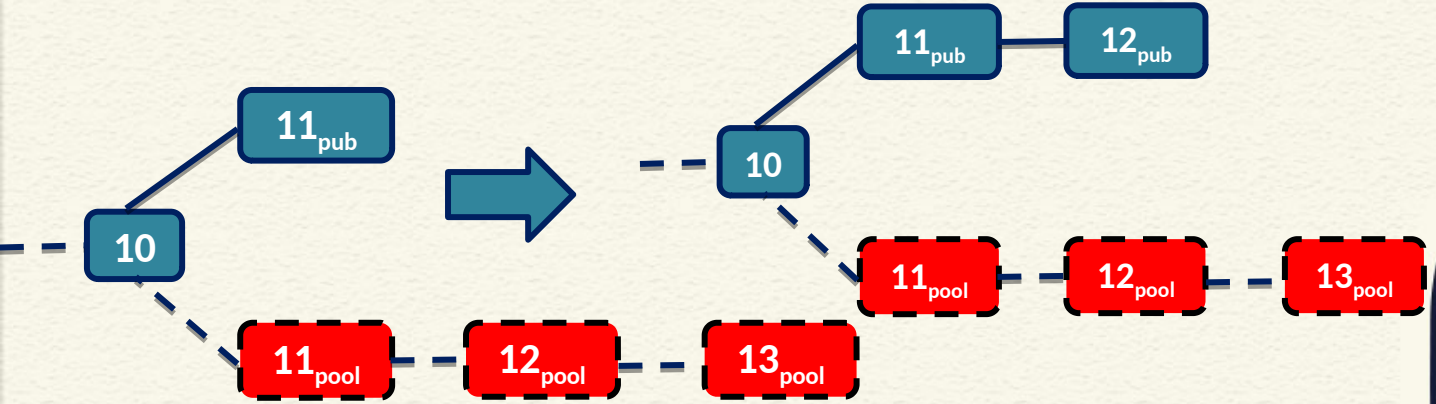
- ✓ There are two branches of length one, and the pool publishes its single secret block
- ✓ The revenue from this block cannot be determined yet



Selfish Mining Attack

7. Lead was 2, others find a block

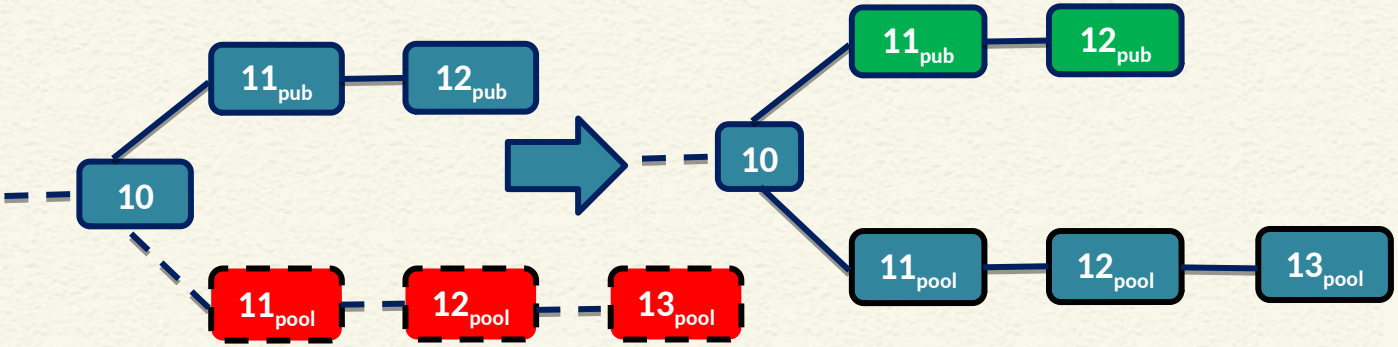
- ✓ The pool publishes its secret blocks, causing everybody to start mining at the head of the previously private branch
- ✓ Pool obtains a revenue of two



Selfish Mining Attack

7. Lead was 2, others find a block (Contd.)

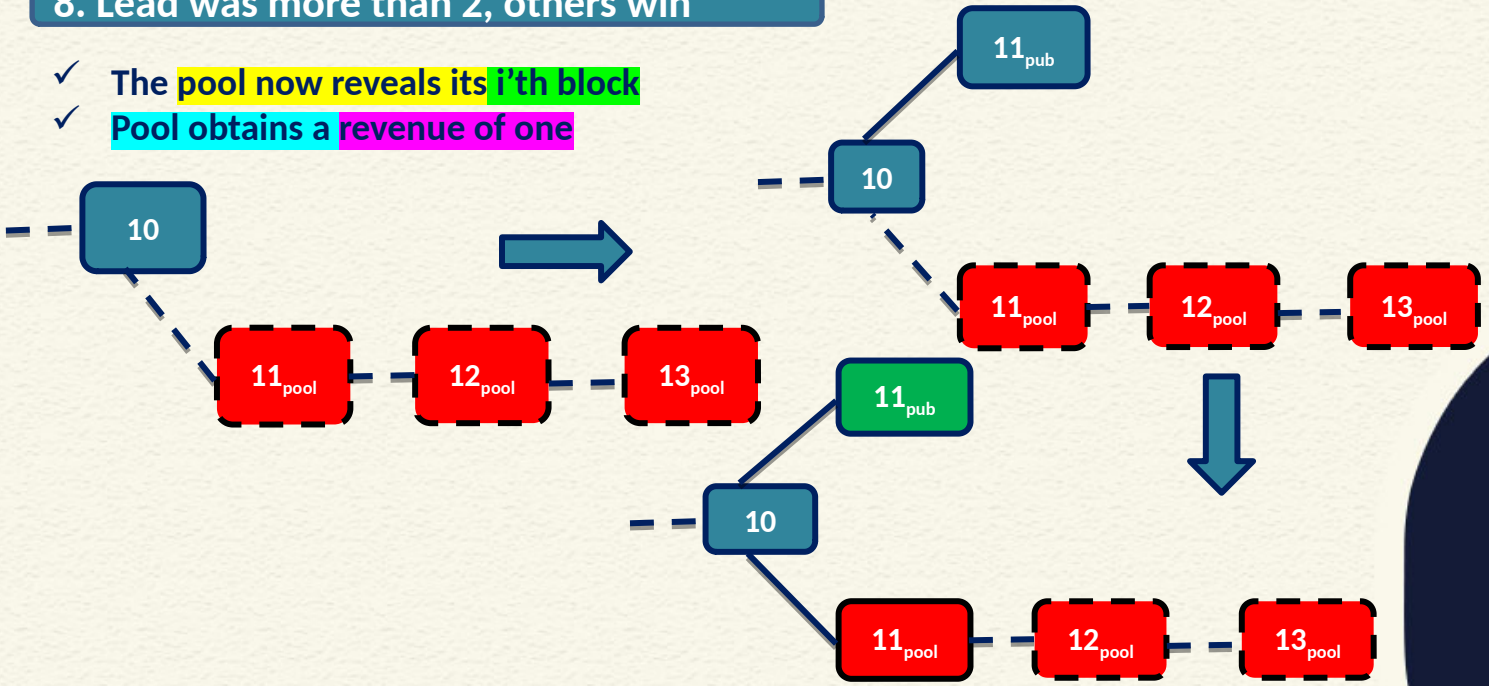
- ✓ The pool publishes its secret blocks, causing everybody to start mining at the head of the previously private branch
- ✓ Pool obtains a revenue of two



Selfish Mining Attack

8. Lead was more than 2, others win

- ✓ The pool now reveals its i'th block
- ✓ Pool obtains a revenue of one



CONCLUSIONS

- Discussed selfish mining attack in detail
- Decisions of the attacker under different conditions

REFERENCES

- Web resources as mentioned from time to time


Thank
you