Selfish mining simulation framework for multiple attackers on various blockchains

1. Selfish minig problem

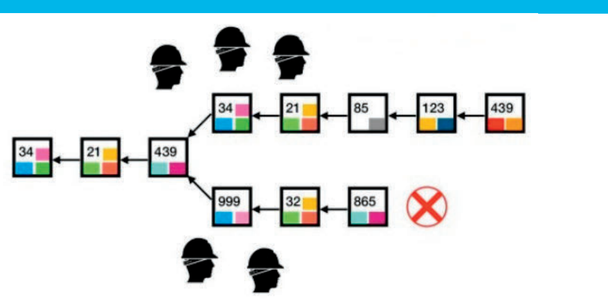
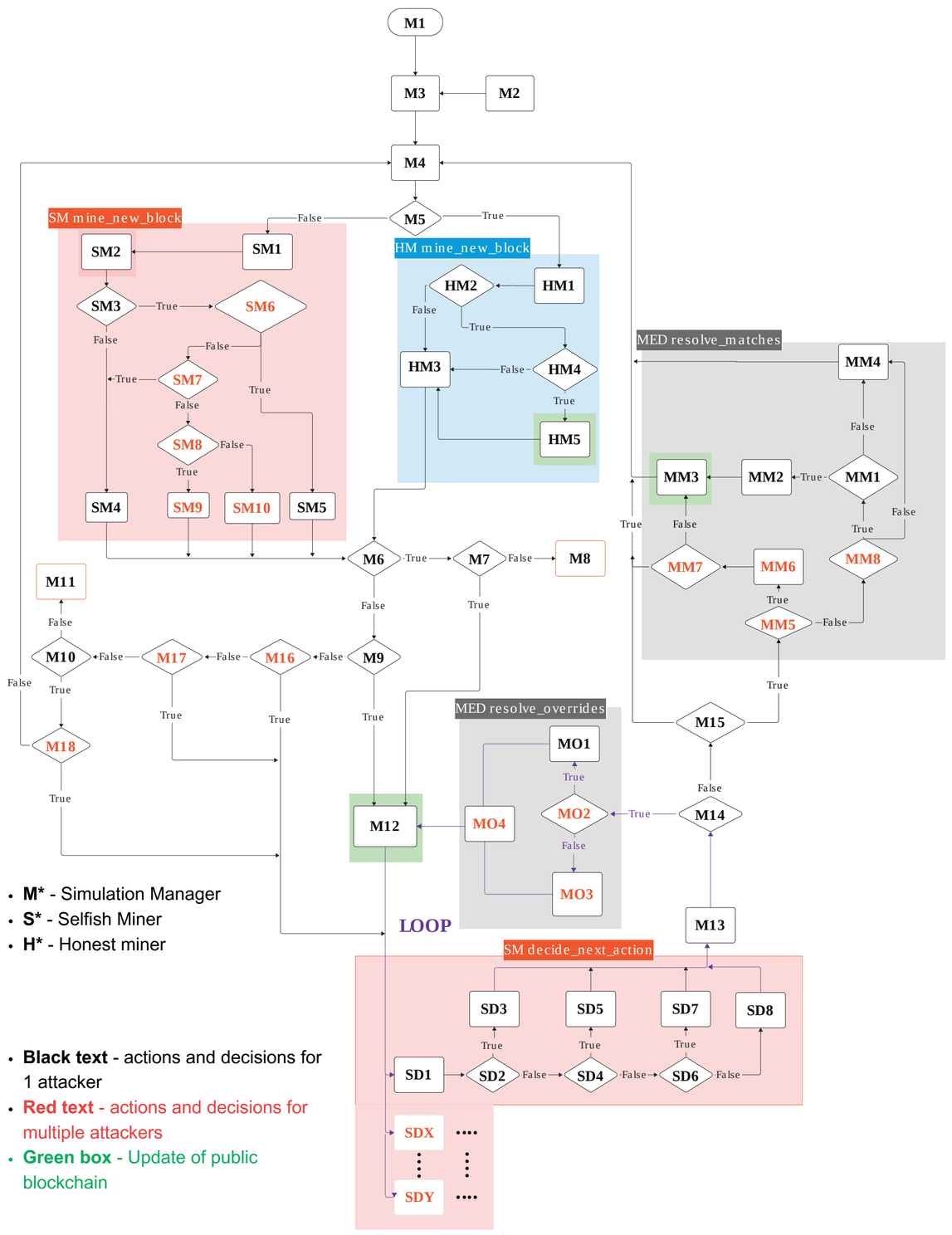


Figure 1: An example of the fork in the blockchain system [1].

- **Fork in the blockchain**
- **Selfish mining actions**
  - Override
  - Adopt
  - Match
  - Wait

2. Framework for Nakamoto consensus



- **M*** - Simulation Manager
- **S*** - Selfish Miner
- **H*** - Honest miner

- **Black text** - actions and decisions for 1 attacker
- **Red text** - actions and decisions for multiple attackers
- **Green box** - Update of public blockchain

Figure 2: Simplified workflow diagram of a simulation framework for selfish mining with multiple attackers on Nakamoto consensus.

3. Supported consensus protocols

- **Nakamoto**
  - blocks
  - longest chain
  - mining powers of individual miners, gamma, simulation mining rounds
- **Subchain**
  - weak and strong blocks
  - the longest chain of strong blocks
  - mining powers of individual miners, gamma, simulation mining rounds, weak to strong block ratio
- **Strongchain**
  - weak and strong headers
  - strongest chain
  - mining powers of individual miners, simulation mining rounds, weak to strong header ratio

4. Simulation experiments

Thresholds for successfull selfish mining

Table 1: Selfish mining on **Nakamoto** consensus.

	gamma	threshold - 1	reward for threshold - 1	research thresholds	threshold	reward for threshold	threshold + 1	reward for threshold + 1
	0	32	30,7063	33	33	32,7866	34	34,86
	0.5	24	23,6487	25	25	25,0996	26	26,4018
1 attacker	1	x	x	1	1	1,0128	2	2,048
2 attackers	0.5	20	19,6278	21	21	21,0209	22	22,4901
5 attackers	0.5	13	12,8124	15	14	14,1609	15	15,5634
7 attackers	0.5	10	9,6931	12	11	11,07694286	12	12,3408

Table 3: Selfish mining on **Strongchain** consensus.

	threshold - 2	reward for threshold - 2	threshold - 1	reward for threshold - 1	research thresholds	threshold	reward for threshold
1 attackers	44	42,1228	45	43,7762	45	46	46,1311

Table 2: Selfish mining on STRONG blocks on **Subchain** consensus.

	gamma	threshold - 1	reward for threshold - 1	threshold	reward for threshold	threshold + 1	reward for threshold + 1
	0	34	32,7116	35	35,0571	36	37,8309
	0.5	26	24,8105	27	26,6223	28	28,2297
1 attacker	1	1	0,994	2	2,0402	3	3,0839
2 attackers	0.5	21	20,3494	22	21,90305	23	23,6037
5 attackers	0.5	13	12,57784	14	14,15028	15	15,66254
7 attackers	0.5	10	9,514257143	11	11,06408571	12	12,54524286

Graphs of selfish mining

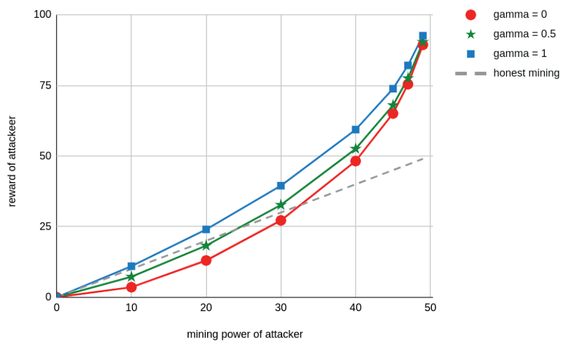


Figure 3: Selfish mining with **one attacker** on **Nakamoto** consensus for different gamma.

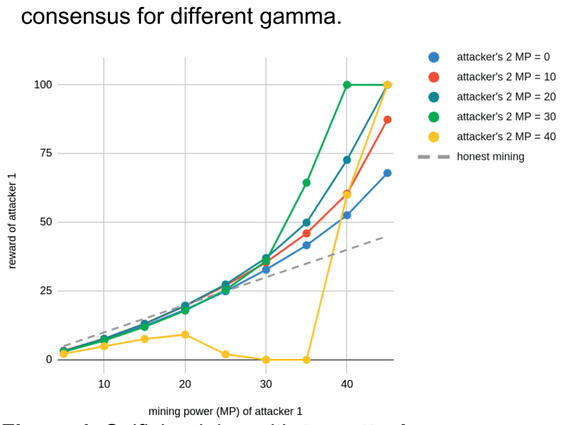


Figure 4: Selfish mining with **two attackers** on **Nakamoto** consensus for gamma = 0.5.

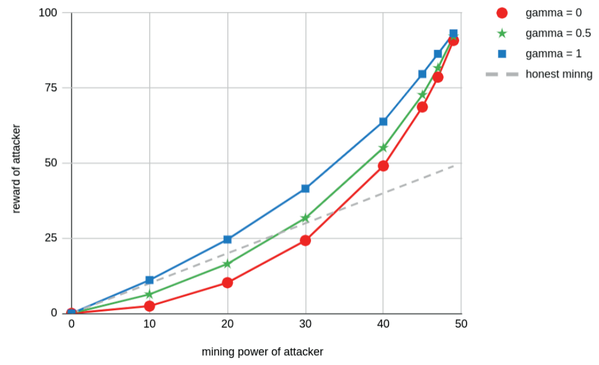


Figure 5: Selfish mining with **one attacker** on STRONG blocks on **Subchain** consensus for different gamma.

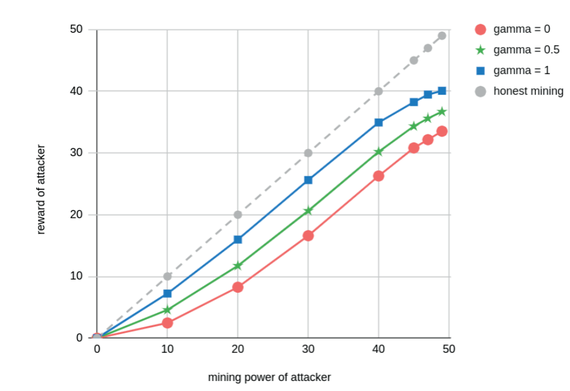


Figure 6: Selfish mining with **one attacker** on WEAK blocks on **Subchain** consensus for different gamma.

[1] Szalachowski, P., Reijsbergen, D., Homoliak, I. and Sun, S. StrongChain: Transparent and Collaborative Proof-of-Work Consensus. In: Heninger, N. and Traynor, P., ed. 28th USENIX Security Symposium, USENIX Security 2019, Santa Clara, CA, USA, August 14-16, 2019. USENIX Association, 2019, p. 819–836. ISBN 978-1-939133-06-9. Available at: https://www.usenix.org/conference/usenixsecurity19/presentation/szalachowski.

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel @FIT 2023

Author: Bc. Ján Jakub Kubík
Supervisor: Ing. Ivan Homoliak Ph.D.