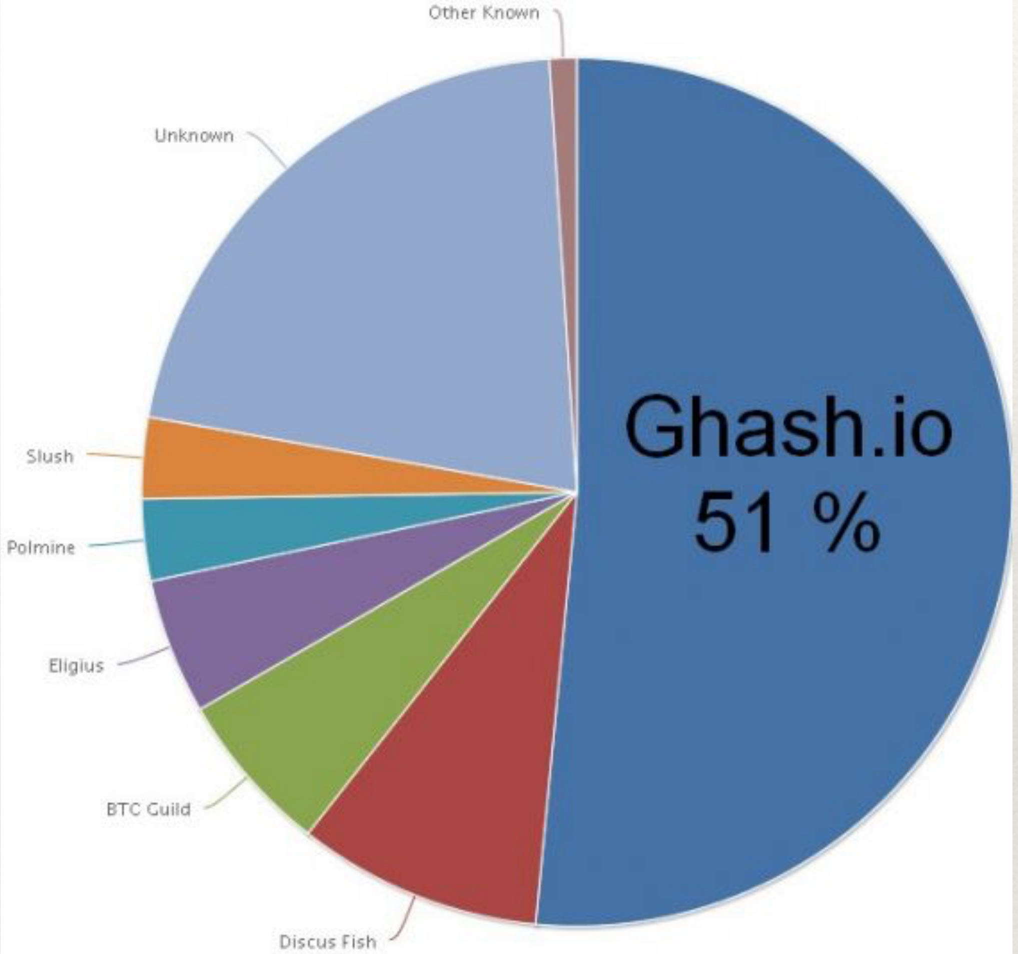
RepuCoin: Your reputation is your power

Jiangshan Yu

Joint work with David Kozhaya (*), Jérémie Decouchant, and Paulo Esteves-Veríssimo

SnT - Interdisciplinary Centre for Security, Reliability and Trust
University of Luxembourg,
Luxembourg
(*) currently at ABB Research, CH

Reality is tough



The big big challenge

In a permissionless blockchain, how to enforce, at least with a very high probability, that

$$\# \text{ malicious\_nodes} \leq F?$$

$$\Sigma P \ \text{ malicious\_nodes} \leq P_F?$$

RepuCoin Overview

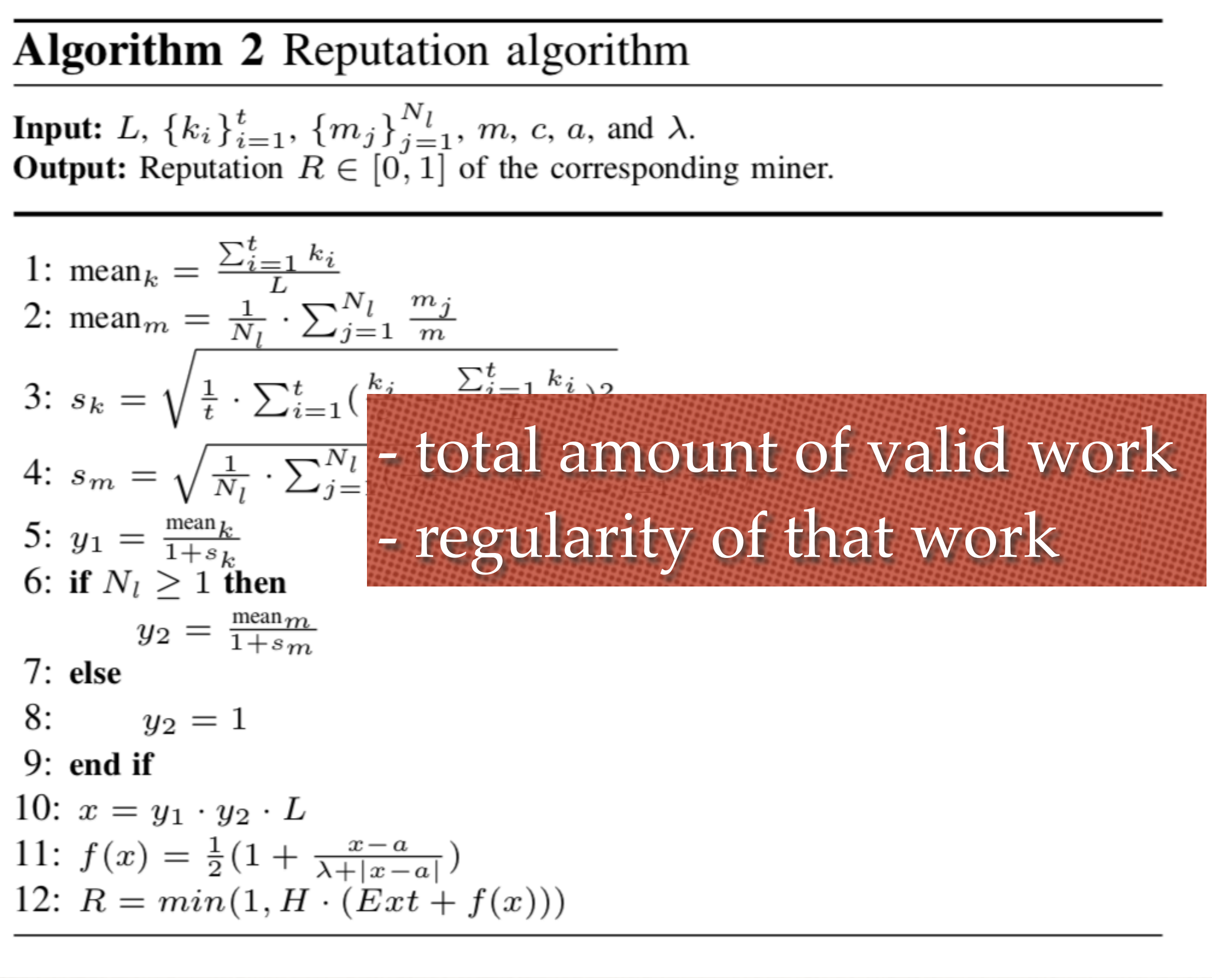
Main problems of PoW:	Our solutions:
Decision (voting) power is CPU power - **Instantaneous** power - can be gained **quickly**; - vulnerable to flash attacks.	Decision (voting) power is reputation - **Integrated** power (past performance) - can only grow **slowly with bounded rate**; - **Not** vulnerable to flash attacks.
Rationality and maliciousness - not clearly distinguished	**Rationality and maliciousness** - separate protection measures
PoW consensus is **probabilistic** - forkable BC	**PoR** consensus is **deterministic** - novel weighted voting consensus algorithm - non-forkable BC
Low (stochastic) resilience - vulnerable to selfish mining (>25%) and other attacks leveraging instantaneous power	**High** (stochastic) resilience -**Not** vulnerable to instantan. power attacks -**Non-rationality** of infiltration attacks
Low Throughput**:** - 7 TPS - 1,000 TPS (ByzCoin)	**High** Throughput: - (fast) PoR for committing transactions - 10,000 TPS (256 Byte per TX)

The logic of RepuCoin in a nutshell

- reputation-based weighted voting consensus is safe and live as long as relative decision power (given by reputation score) of attackers is below a defined threshold, fraction of the total
- max rate of decision power growth of any system participant is deterministic, bounded and known, imposed by the proof-of-reputation function
- there is no rational economic model for infiltration attacks --- compared to the cost of attacking different systems
- Attacks attacks on liveness or safety still being possible, the network achieves very high stochastic robustness against them --- i.e., attack effort to reach network control compares very favorably to previous works
- RepuCoin prevents all currently known attacks.

How does RepuCoin Work?

1. Miners gain reputation slowly with a bounded rate by contributing to the blockchain



Algorithm 2 Reputation algorithm

Input: L, $\{k_i\}_{i=1}^{t}$, $\{m_j\}_{j=1}^{N_l}$, m, c, a, and λ.
Output: Reputation $R \in [0, 1]$ of the corresponding miner.

```
mean_k = $\frac{\sum_{i=1}^{t} k_i}{L}$
mean_m = $\frac{1}{N_l} \cdot \sum_{j=1}^{N_l} \frac{m_j}{m}$
$s_k = \sqrt{\frac{1}{t} \cdot \sum_{i=1}^{t}( k_i \quad \sum_{i=1}^{t} k_i\,)^2}$
$s_m = \sqrt{\frac{1}{N_l} \cdot \sum_{j=}^{N_l}}$
$y_1 = \frac{mean_k}{1+s_k}$
if $N_l \geq 1$ then
    $y_2 = \frac{mean_m}{1+s_m}$
else
    $y_2 = 1$
end if
$x = y_1 \cdot y_2 \cdot L$
$f(x) = \frac{1}{2}(1 + \frac{x-a}{\lambda+|x-a|})$
$R = min(1, H \cdot (Ext + f(x)))$
```

- total amount of valid work
- regularity of that work

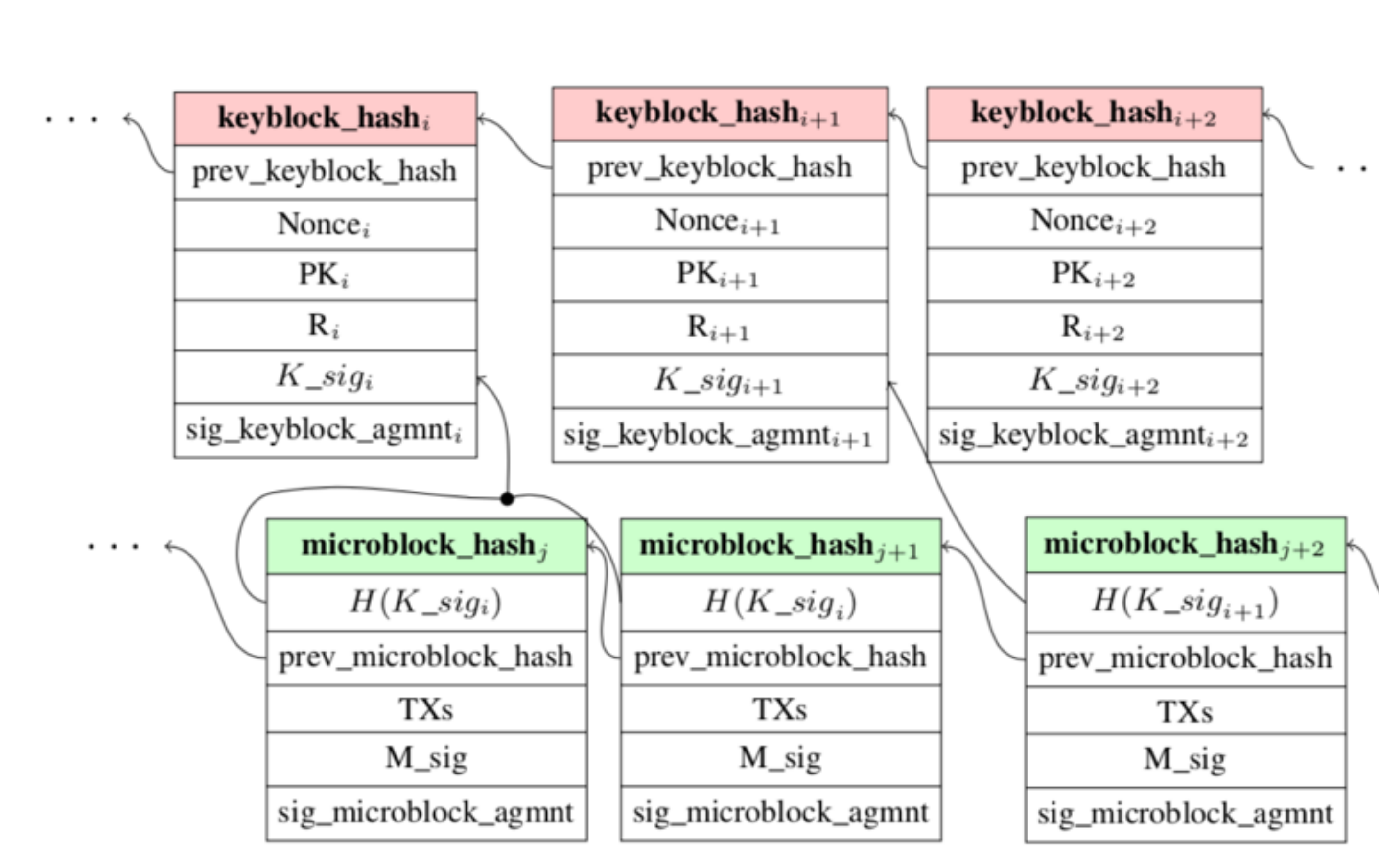
How does RepuCoin Work?

1. Miners gain reputation slowly with a bounded rate by contributing to the blockchain

2. Top reputed miners dynamically form a consensus committee

How does RepuCoin Work?

1. Miners gain reputation slowly with a bounded rate by contributing to the blockchain
2. Top reputed miners dynamically form a consensus committee
3. The committee votes through reputation-based weighted voting protocol to pin keyblocks;
4. A randomly elected leader proposes microblocks to the committee for their approval;



How does RepuCoin Work?

1. Miners gain reputation slowly with a bounded rate by contributing to the blockchain

2. Top reputed miners dynamically form a consensus committee

3. The committee votes through reputation-based weighted voting protocol to pin keyblocks;

4. A randomly elected leader proposes microblocks to the committee for their approval;

5. Mis-behaved miners will be punished, and they lose reputation

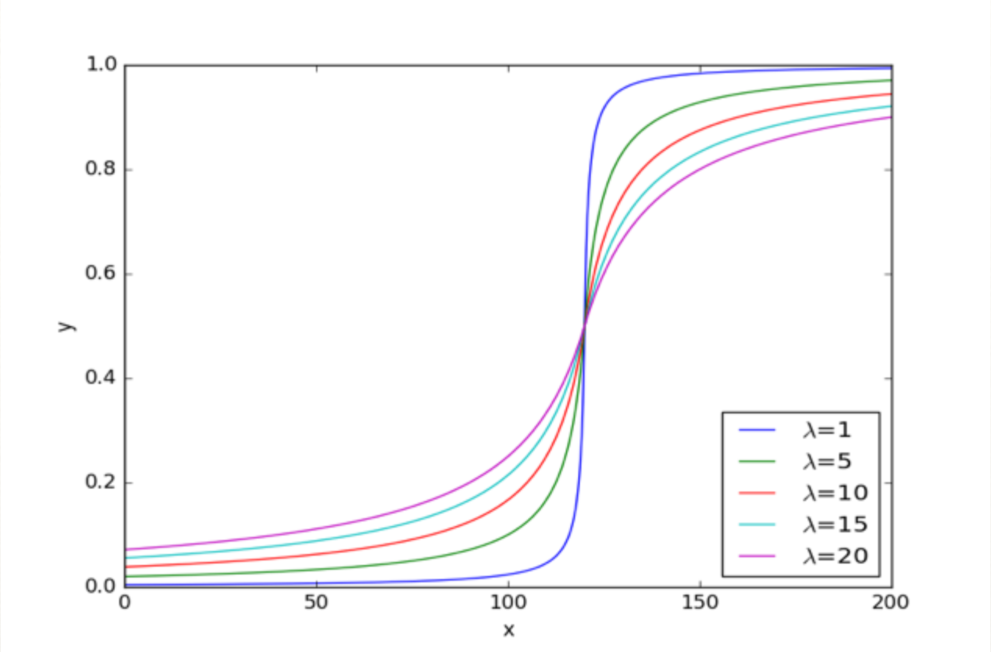
Reputation is your power

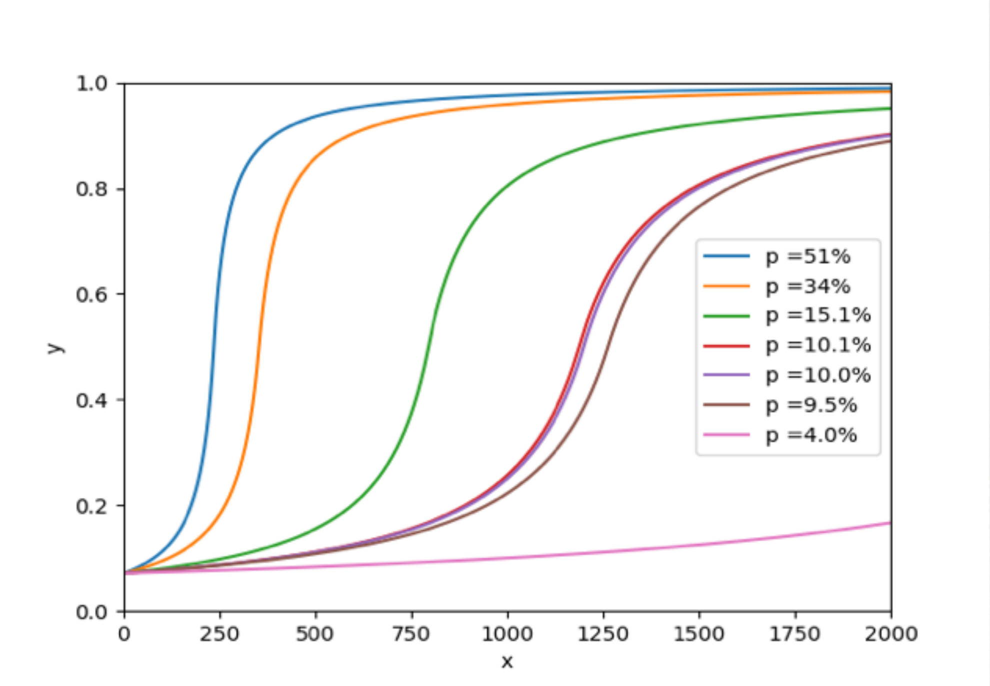
The **social objectives** of reputation:

i. **careful start**, through an initial slow increase;

ii. potential for quick reward of mature participants, through **fast increase in mid-life**;

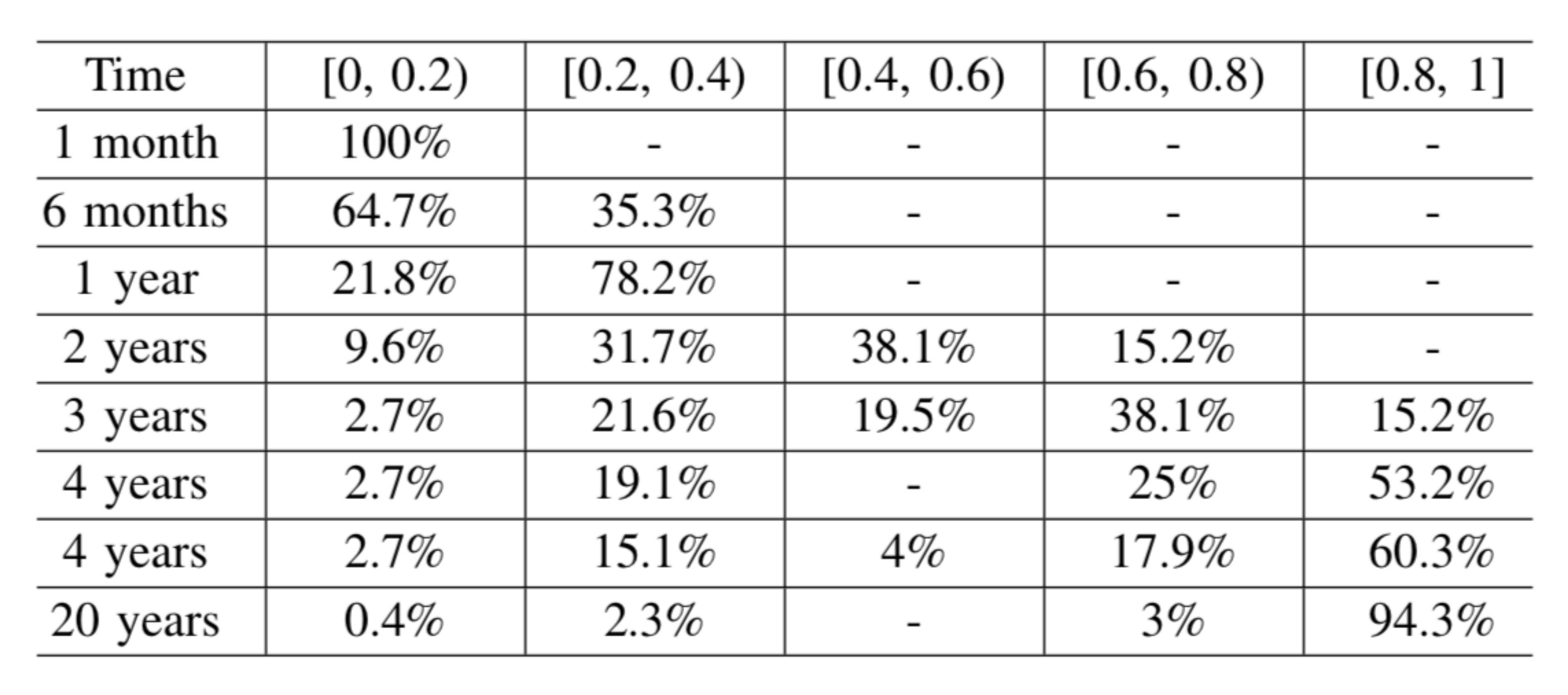
iii. prevention of over-control, by **slow increase near the top**





Reputation is your power

Reputation distribution of miners over time.



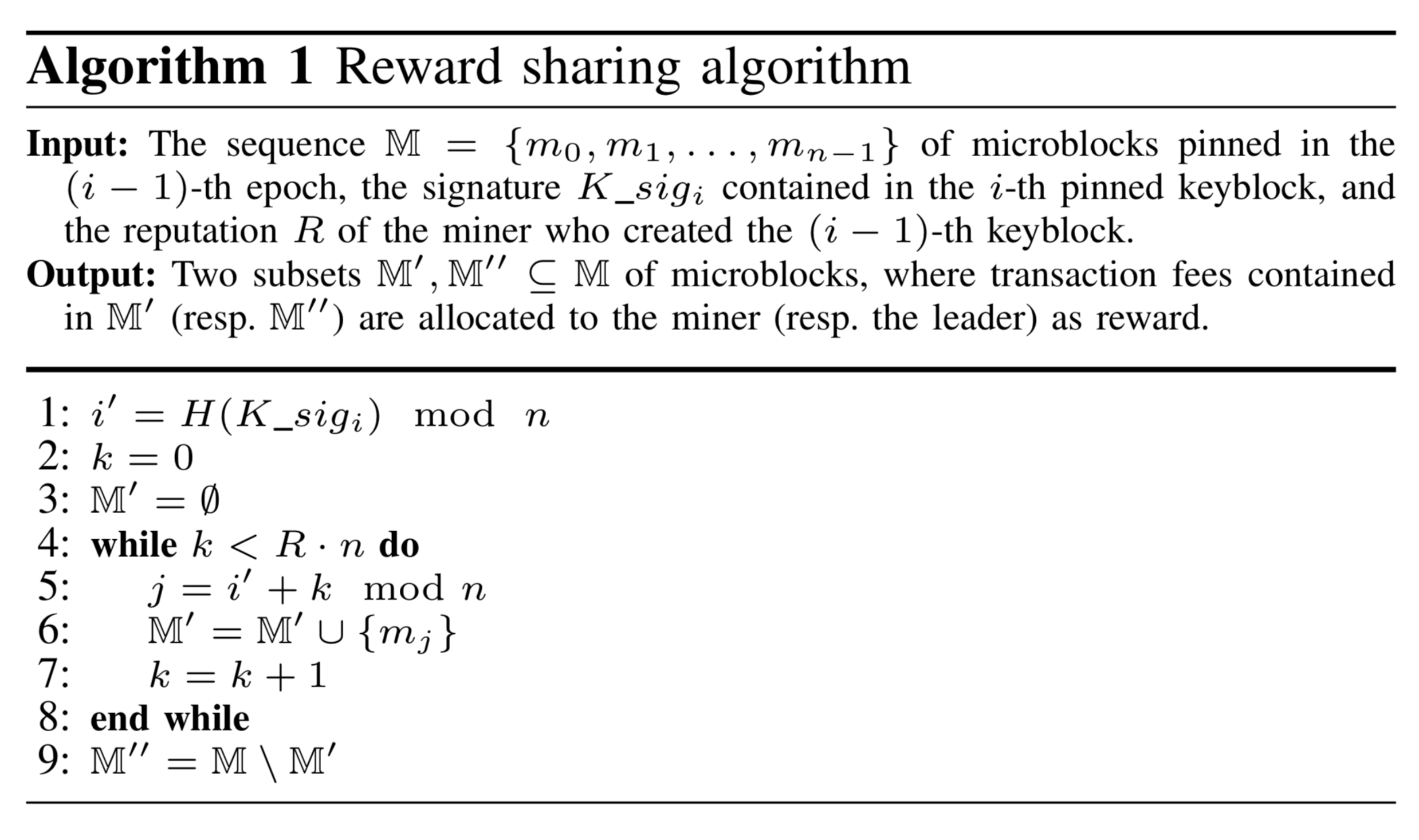
Time	[0, 0.2)	[0.2, 0.4)	[0.4, 0.6)	[0.6, 0.8)	[0.8, 1]
1 month	100%	-	-	-	-
6 months	64.7%	35.3%	-	-	-
1 year	21.8%	78.2%	-	-	-
2 years	9.6%	31.7%	38.1%	15.2%	-
3 years	2.7%	21.6%	19.5%	38.1%	15.2%
4 years	2.7%	19.1%	-	25%	53.2%
4 years	2.7%	15.1%	4%	17.9%	60.3%
20 years	0.4%	2.3%	-	3%	94.3%

Reputation is your power

Reputation-based incentives lead miners to work diligently and honestly

A successful miner

1. gets all mining rewards
2. shares transaction fees with a randomly selected leader, according to the reputation.
3. gets >60 times better transaction fees than BTC, due to high throughput



Algorithm 1 Reward sharing algorithm

Input: The sequence $\mathbb{M} = \{m_0, m_1, \ldots, m_{n-1}\}$ of microblocks pinned in the $(i-1)$-th epoch, the signature K_sig_i contained in the i-th pinned keyblock, and the reputation R of the miner who created the $(i-1)$-th keyblock.

Output: Two subsets $\mathbb{M}', \mathbb{M}'' \subseteq \mathbb{M}$ of microblocks, where transaction fees contained in $\mathbb{M}'$ (resp. $\mathbb{M}''$) are allocated to the miner (resp. the leader) as reward.

```
$i' = H(K\_sig_i) \mod n$
$k = 0$
$\mathbb{M}' = \emptyset$
while $k < R \cdot n$ do
    $j = i' + k \mod n$
    $\mathbb{M}' = \mathbb{M}' \cup \{m_j\}$
    $k = k + 1$
end while
$\mathbb{M}'' = \mathbb{M} \setminus \mathbb{M}'$
```

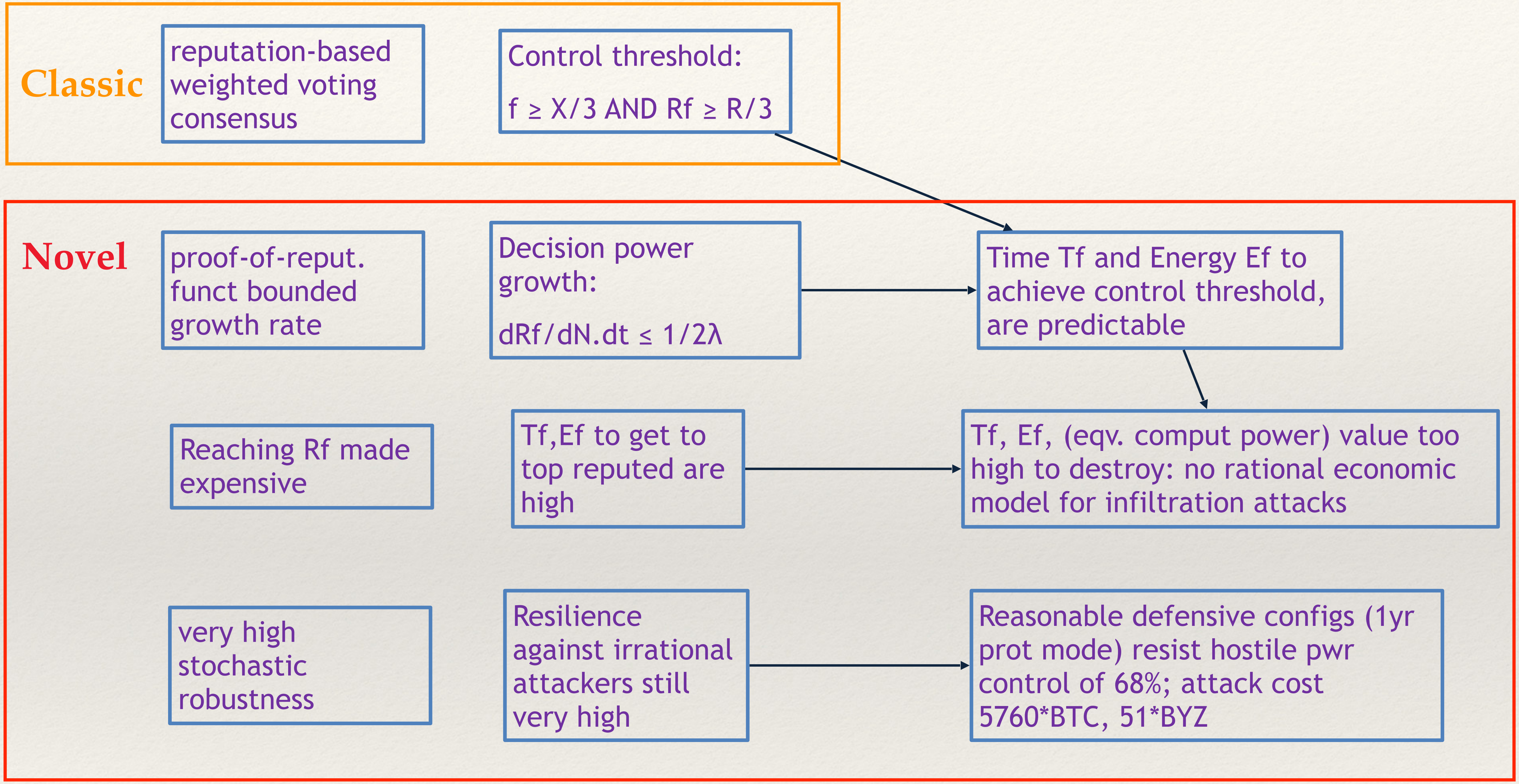
What do we enforce?

The increase of any miner's voting power is bounded by "physics"!

$$\frac{dPd}{dN \cdot dt} = \frac{1}{2} \frac{\lambda}{(\lambda + |x - a|)^2} \leq \frac{1}{2\lambda}$$

λ and a are system parameters, and x is defined in the reputation algorithm.

RECAP: The logic of RepuCoin in a nutshell



Classic

reputation-based weighted voting consensus

Control threshold:

$f \geq X/3$ AND $Rf \geq R/3$

Novel

proof-of-reput. funct bounded growth rate

Decision power growth:

$dRf/dN.dt \leq 1/2\lambda$

Time Tf and Energy Ef to achieve control threshold, are predictable

Reaching Rf made expensive

Tf,Ef to get to top reputed are high

Tf, Ef, (eqv. comput power) value too high to destroy: no rational economic model for infiltration attacks

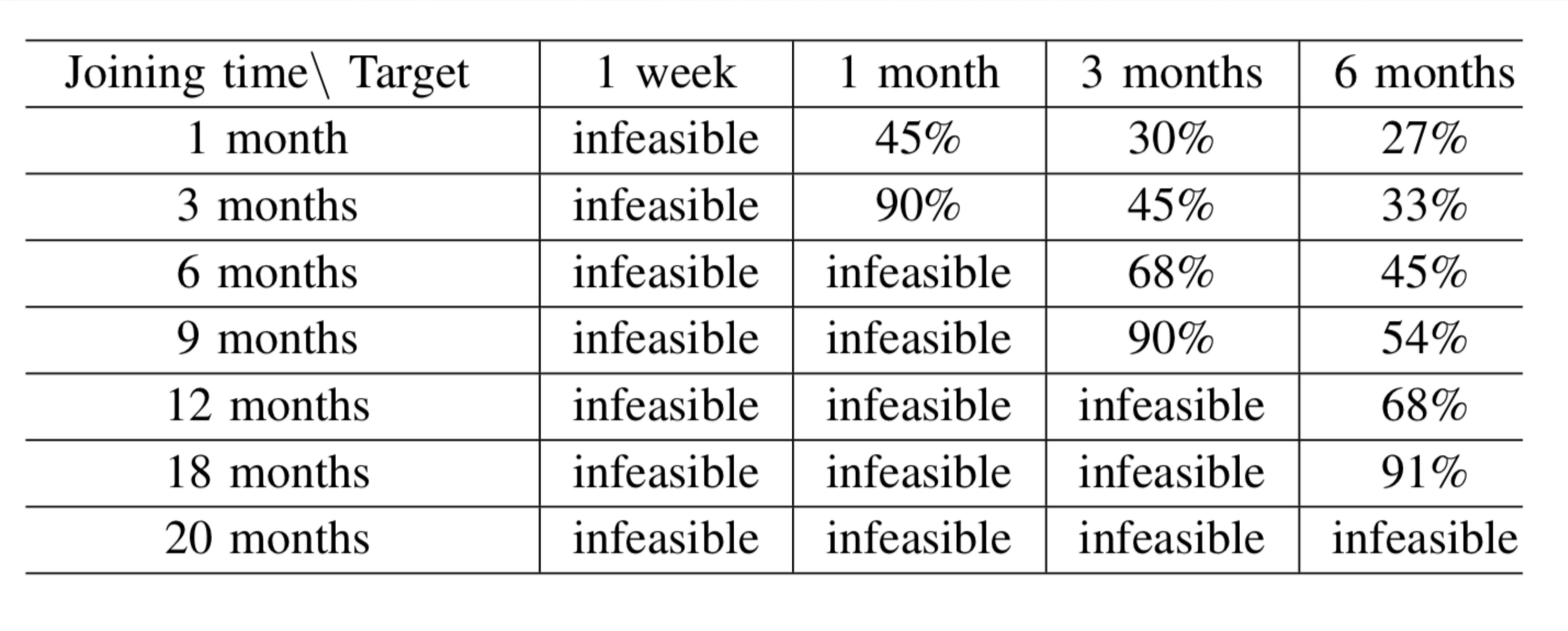
very high stochastic robustness

Resilience against irrational attackers still very high

Reasonable defensive configs (1yr prot mode) resist hostile pwr control of 68%; attack cost 5760*BTC, 51*BYZ

Security and Dependability:

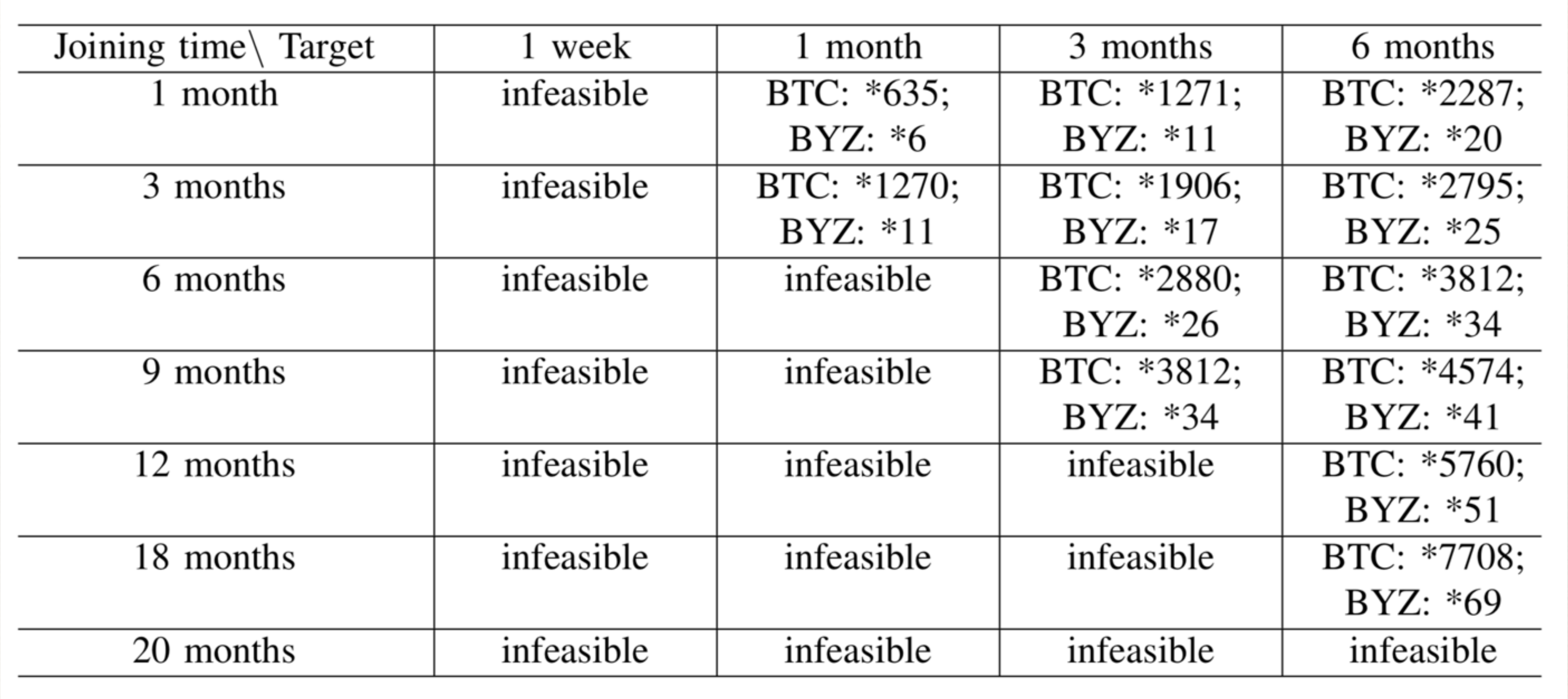
The minimum cost of successfully attacking RepuCoin



Joining time\ Target	1 week	1 month	3 months	6 months
1 month	infeasible	45%	30%	27%
3 months	infeasible	90%	45%	33%
6 months	infeasible	infeasible	68%	45%
9 months	infeasible	infeasible	90%	54%
12 months	infeasible	infeasible	infeasible	68%
18 months	infeasible	infeasible	infeasible	91%
20 months	infeasible	infeasible	infeasible	infeasible

Security and Dependability:

The minimum cost of successfully attacking RepuCoin



Joining time\ Target	1 week	1 month	3 months	6 months
1 month	infeasible	BTC: *635; BYZ: *6	BTC: *1271; BYZ: *11	BTC: *2287; BYZ: *20
3 months	infeasible	BTC: *1270; BYZ: *11	BTC: *1906; BYZ: *17	BTC: *2795; BYZ: *25
6 months	infeasible	infeasible	BTC: *2880; BYZ: *26	BTC: *3812; BYZ: *34
9 months	infeasible	infeasible	BTC: *3812; BYZ: *34	BTC: *4574; BYZ: *41
12 months	infeasible	infeasible	infeasible	BTC: *5760; BYZ: *51
18 months	infeasible	infeasible	infeasible	BTC: *7708; BYZ: *69
20 months	infeasible	infeasible	infeasible	infeasible

Comparison

Attacks/Features	BitCoin	BitCoin-NG	ByzCoin	RepuCoin
Double spending attacks	☠	☠	👌	👌
Selfish mining attack	☠	☠	☠	👌
Bribery/flash attack	☠	☠	☠	👌
Eclipse attacks	☠	☠	😐	😐
Non-forkable chain	☠	☠	👌	👌
Liveness	👌	👌	☠	👌
Throughput	7 tps	?	1,000 tps	10,000 tps

256 Bytes / TX
13 nodes
1KB / Kblock
2 MB / Mblock

👌 The system is secure against this attack

☠ The system is vulnerable to this attack

😐 The system can prevent double spending, but its throughput maybe reduced.

Thank you!

Jiangshan Yu

jiangshan.yu@uni.lu
www.jiangshanyu.com

CRITIX @SnT, *Critical and Extreme Security and Dependability*

We're hiring bright post-docs and research associates
willing to address these challenges!

J.Yu,D.Kozhaya,J.Decouchant,and P.Esteves-Verissimo,"Repucoin: Your reputation is your power," Cryptology ePrint Archive, Report 2018/239, 2018, https://eprint.iacr.org/2018/239.