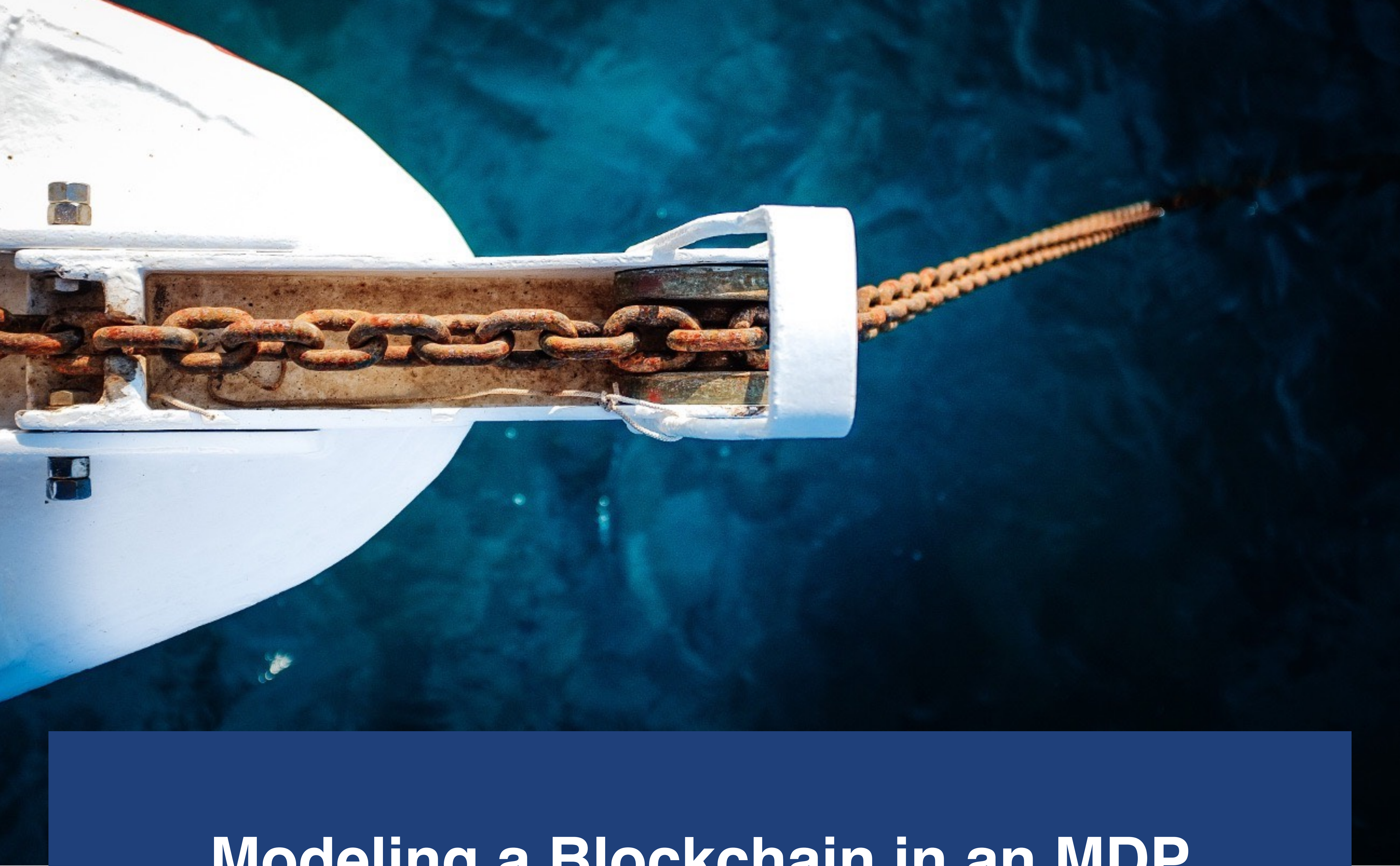


Modeling a Blockchain in an MDP

Markov Decision Process (MDP)

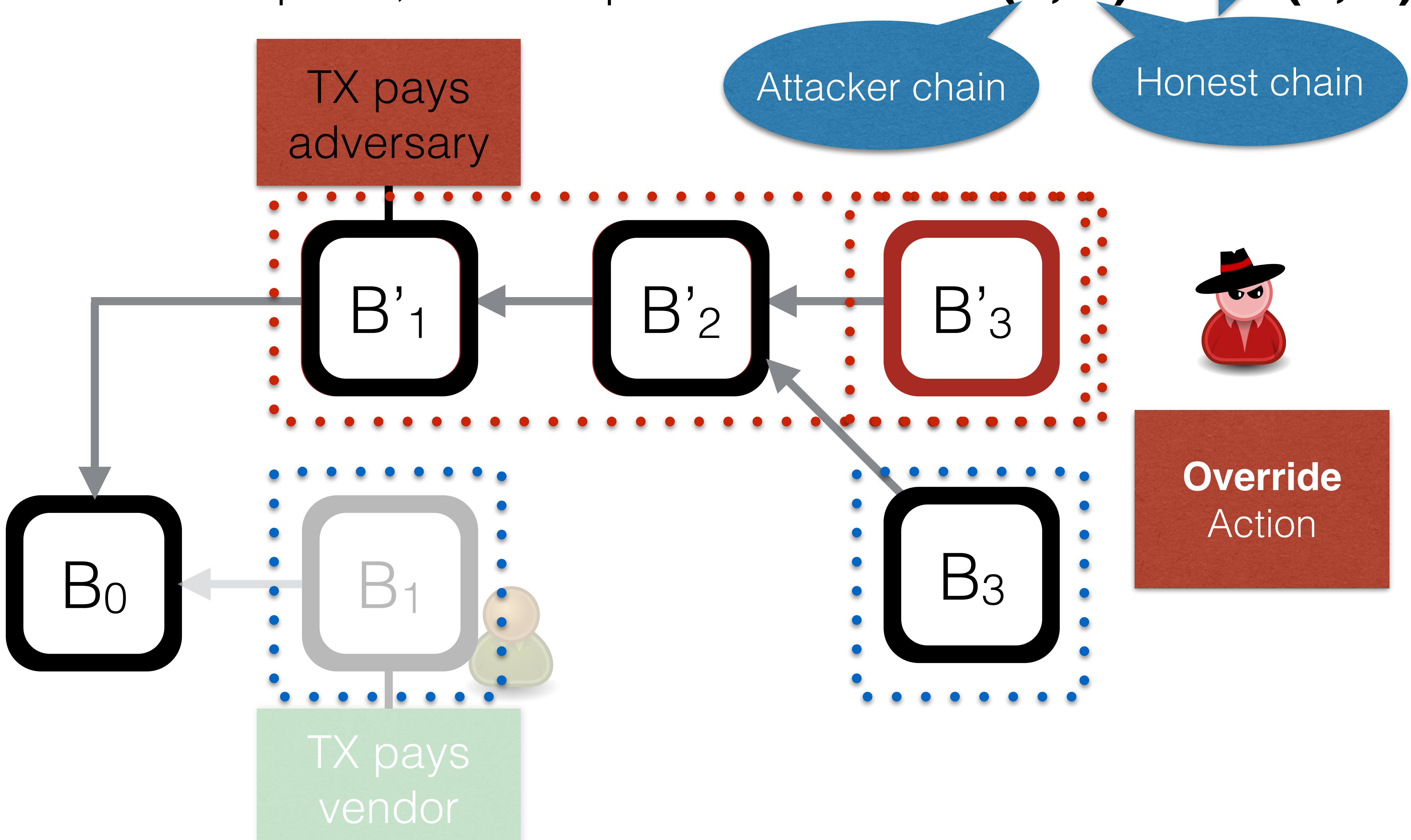
+ double-spending value

Extension of Markov Chains

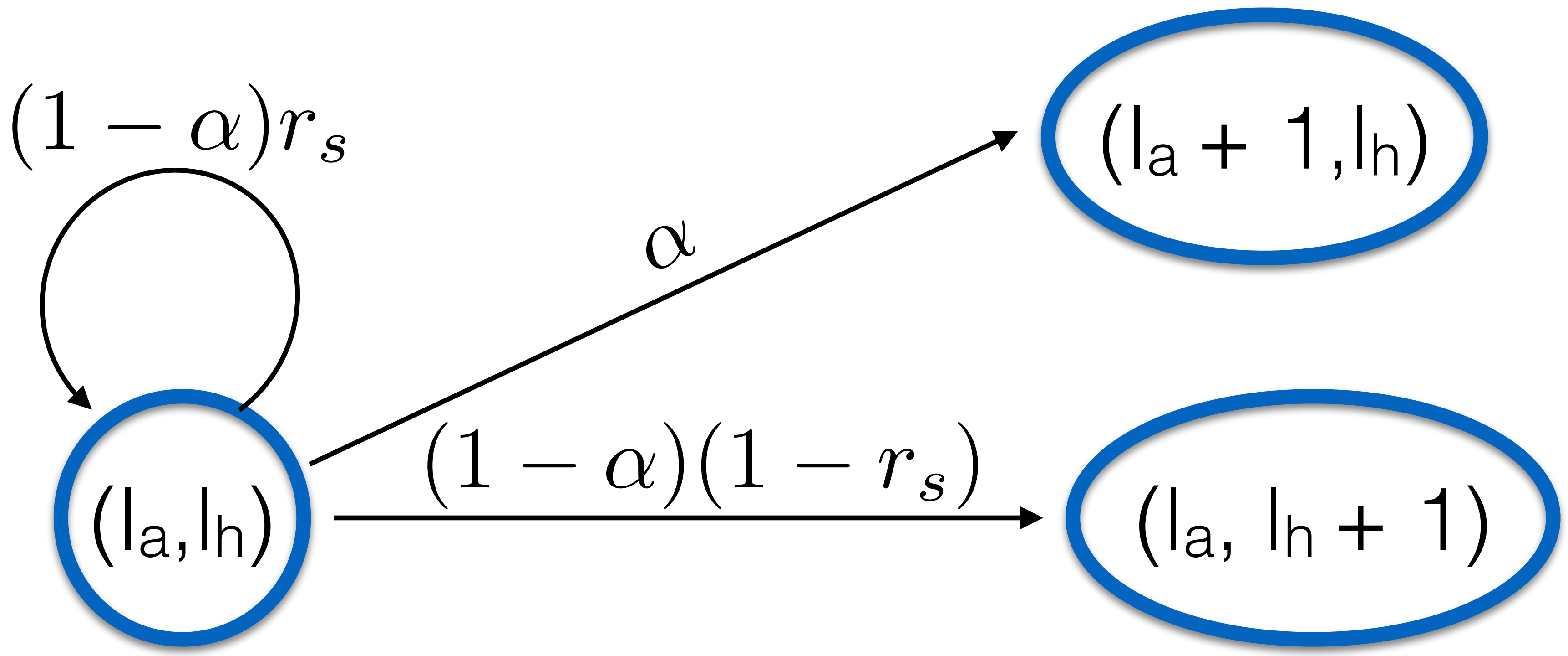
- Actions, Rewards
- State space, action space

Reward for adversary: 2

State: (3, 1) → (1, 1)

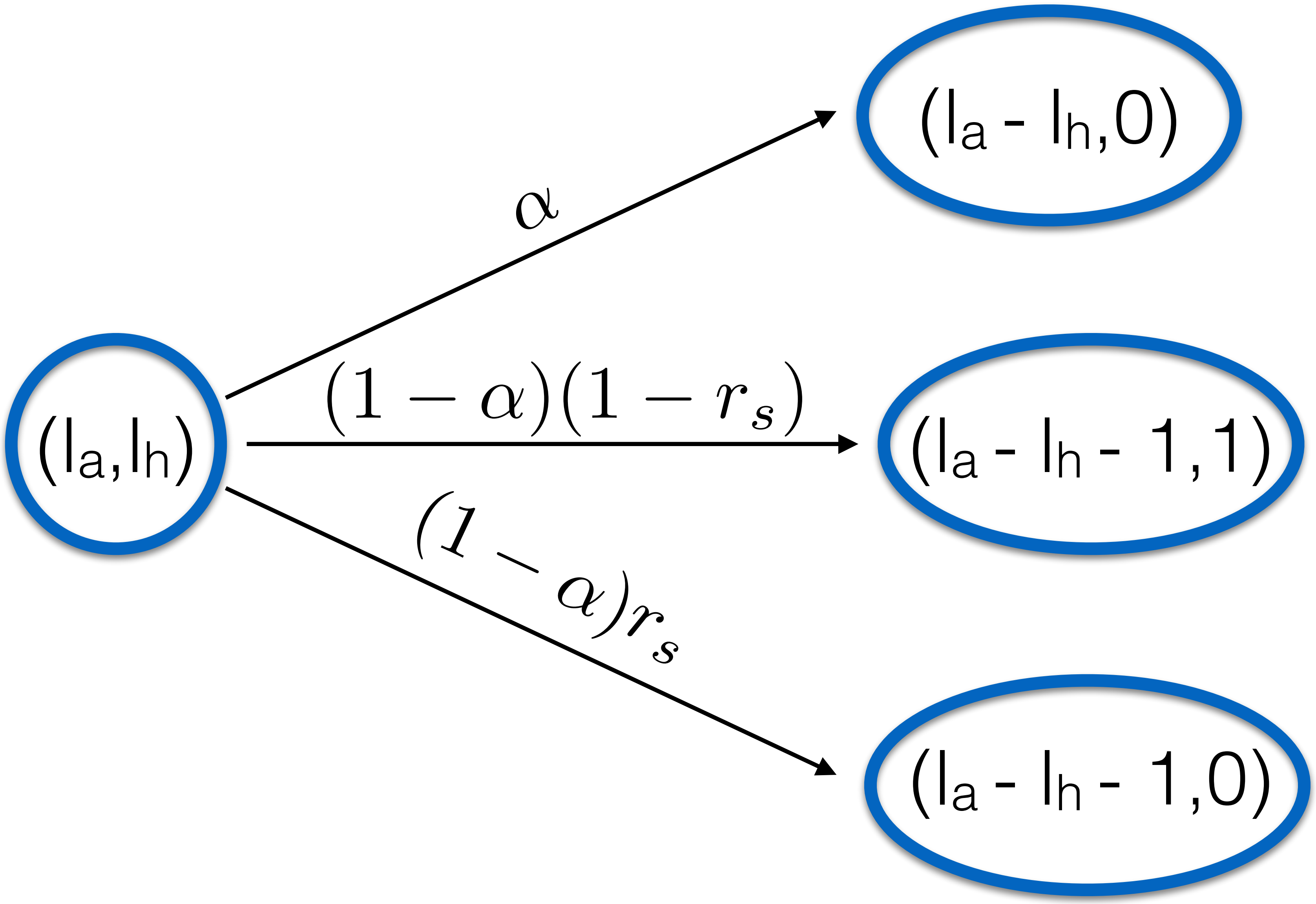


MDP model (simplified) - Wait Action



$r_a=0$, $r_h=0$

MDP model (simplified) - Override Action



Reward for adversary: l_h+1

Action iif $l_a>l_h$

MDP - State Transitions and Rewards

State × Action	Resulting State	Probability	Reward (in Block reward)
$(l_a, l_h, b_e, \cdot)$, adopt	$(1, 0, 0, i)$ $(1, 0, 1, i)$ $(0, 1, 0, r)$ $(0, 0, 0, i)$	α ω $(1-\alpha-\omega)\cdot(1-r_s)$ $(1-\alpha-\omega)\cdot r_s$	$(-c_m, l_h)$ $(-c_m, l_h)$ $(-c_m, l_h)$ $(-c_m, l_h)$
$(l_a, l_h, b_e, \cdot)$, override	$\left(l_a - l_h, 0, b_e - \lceil (l_h+1)\frac{b_e}{l_a} \rceil, i\right)$ $\left(l_a - l_h, 0, b_e - \lceil (l_h+1)\frac{b_e}{l_a} \rceil + 1, i\right)$ $\left(l_a - l_h - 1, 1, b_e - \lceil (l_h+1)\frac{b_e}{l_a} \rceil, r\right)$ $\left(l_a - l_h - 1, 0, b_e - \lceil (l_h+1)\frac{b_e}{l_a} \rceil, i\right)$	α ω $(1-\alpha-\omega)\cdot(1-r_s)$ $(1-\alpha-\omega)\cdot r_s$	$\left(\lfloor (l_h+1)\frac{l_a-b_e}{l_a} \rfloor - c_m, 0\right)$ $\left(\lfloor (l_h+1)\frac{l_a-b_e}{l_a} \rfloor - c_m, 0\right)$ $\left(\lfloor (l_h+1)\frac{l_a-b_e}{l_a} \rfloor - c_m, 0\right)$ $\left(\lfloor (l_h+1)\frac{l_a-b_e}{l_a} \rfloor - c_m, 0\right)$
(l_a, l_h, b_e, i), wait (l_a, l_h, b_e, r), wait	(l_a+1, l_h, b_e, i) (l_a+1, l_h, b_e+1, i) (l_a, l_h+1, b_e, r) (l_a, l_h, b_e, i)	α ω $(1-\alpha-\omega)\cdot(1-r_s)$ $(1-\alpha-\omega)\cdot r_s$	$(-c_m, 0)$ $(-c_m, 0)$ $(-c_m, 0)$ $(-c_m, 0)$
(l_a, l_h, b_e, a), wait (l_a, l_h, b_e, r), match	(l_a+1, l_h, b_e, a) (l_a+1, l_h, b_e+1, a) $(l_a - l_h, 1, b_e - \lceil (l_h)\frac{b_e}{l_a} \rceil, r)$ (l_a, l_h+1, b_e, r) (l_a, l_h, b_e, a)	α ω $\gamma\cdot(1-\alpha-\omega)\cdot(1-r_s)$ $(1-\gamma)\cdot(1-\alpha-\omega)\cdot(1-r_s)$ $(1-\alpha-\omega)\cdot r_s$	$(-c_m, 0)$ $(-c_m, 0)$ $\left(\lfloor (l_h)\frac{l_a-b_e}{l_a} \rfloor - c_m, 0\right)$ $(-c_m, 0)$ $(-c_m, 0)$
$(l_a, l_h, b_e, \cdot)$, exit	exit	1	$(l_a - b_e + v_d, 0)$