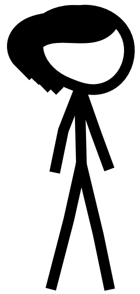
LEVERAGING WEIGHT FUNCTIONS FOR OPTIMISTIC RESPONSIVENESS IN BLOCKCHAINS

Simon Holmgaard Kamp, Bernardo Magri,
Christian Matt, Jesper Buus Nielsen,
Søren Eller Thomsen and Daniel Tschudi

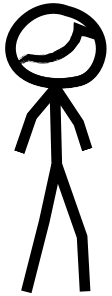
CONCORDIUM

COBRA
CONCORDIUM BLOCKCHAIN
RESEARCH CENTER AARHUS

Alice



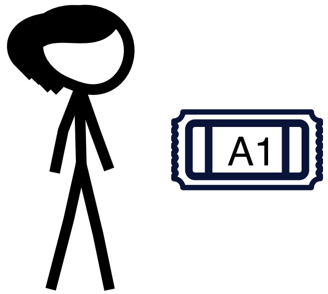
Bob



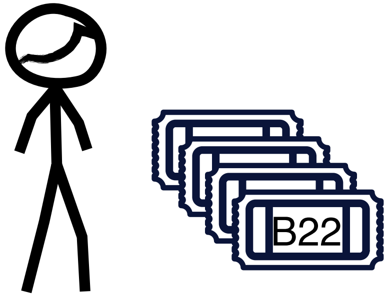
GB

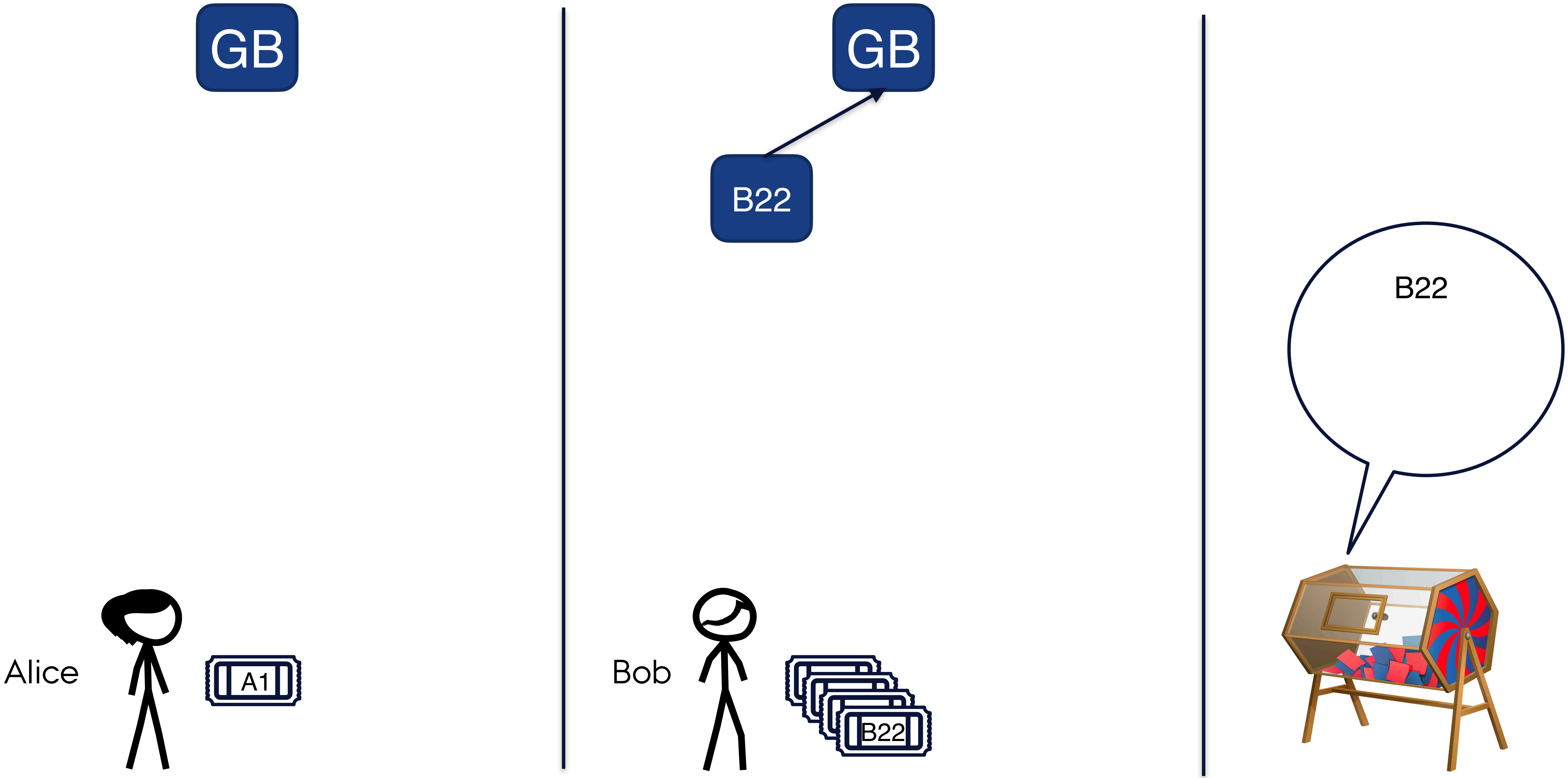
GB

Alice



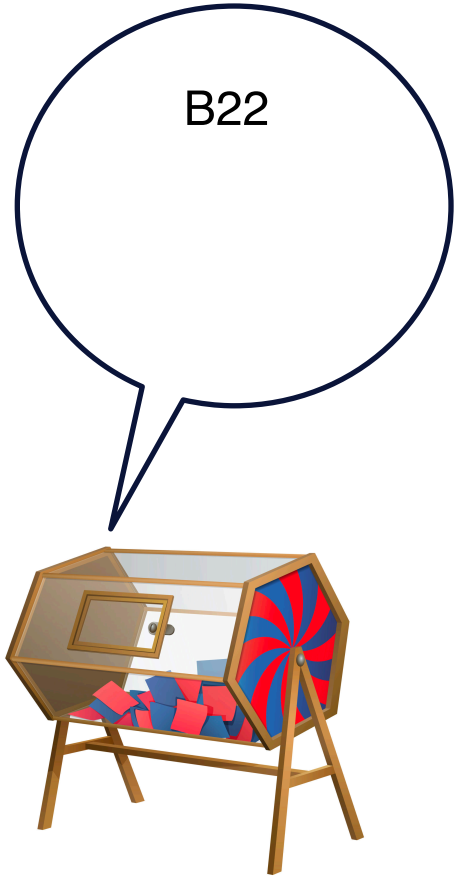
Bob

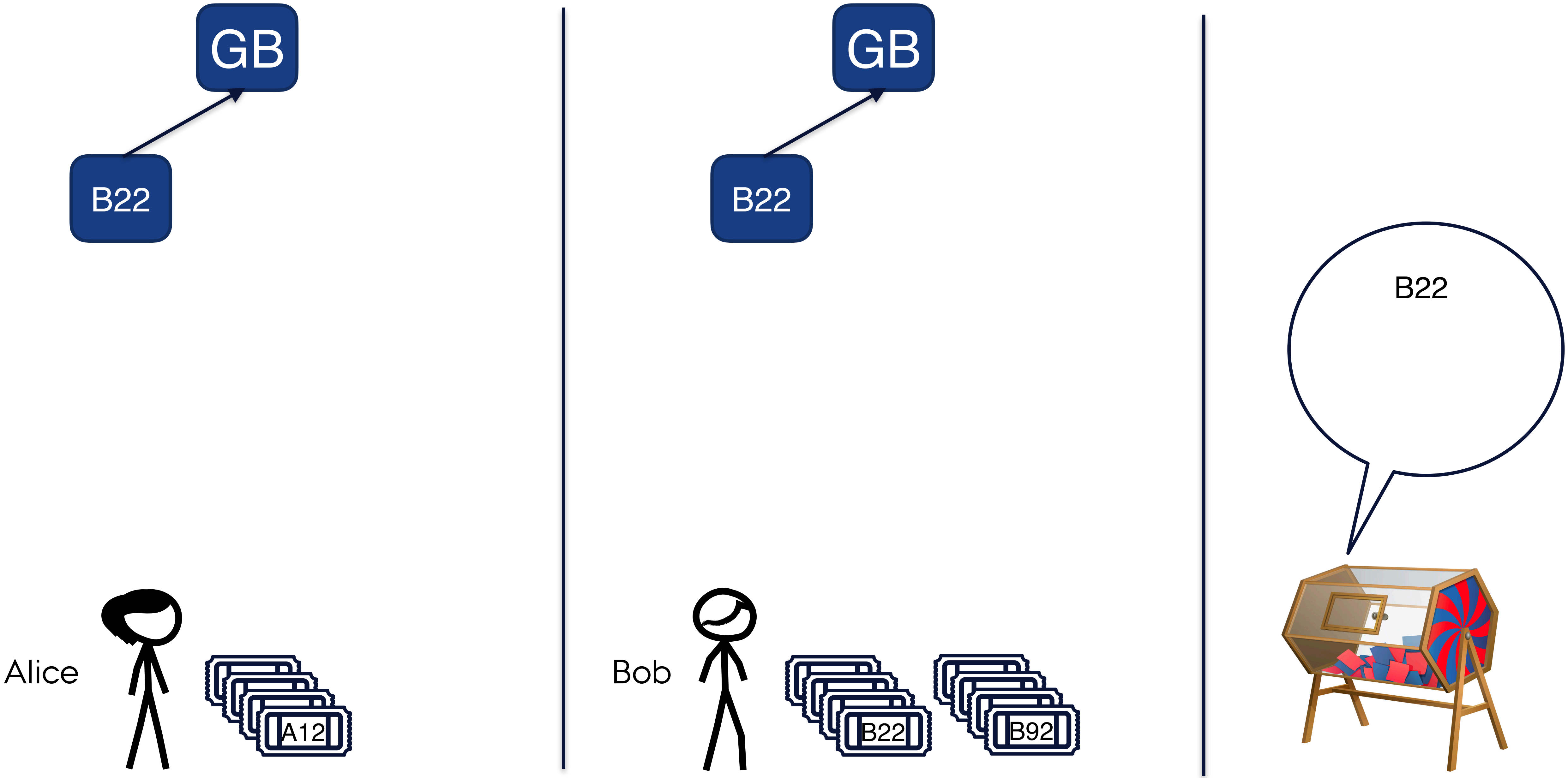


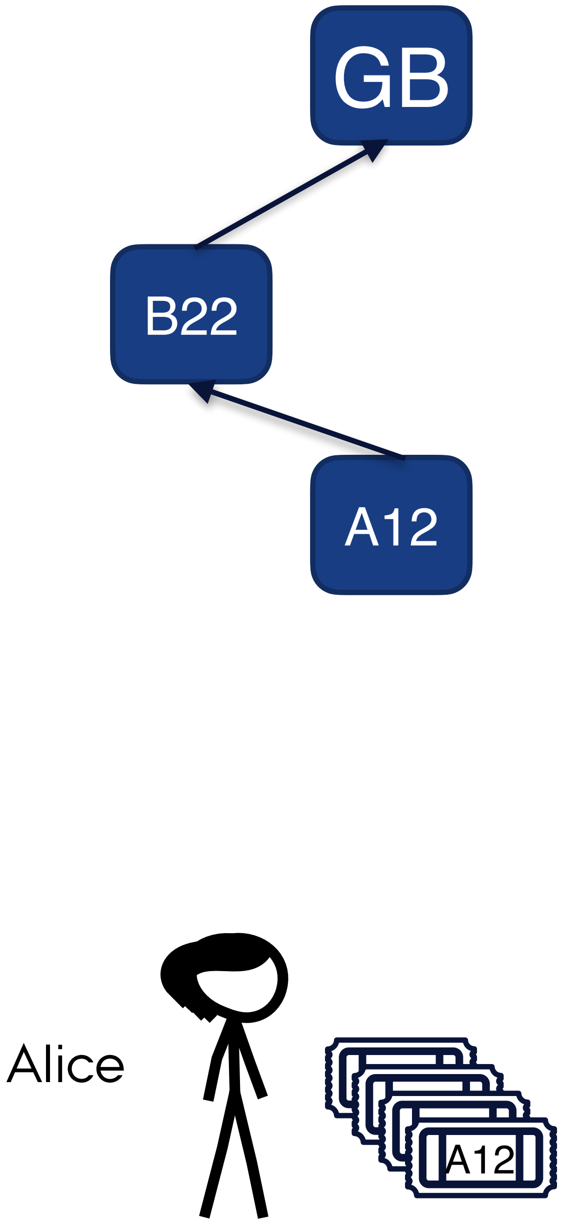

GB
Alice
A1
GB
B22
Bob
B22
B22

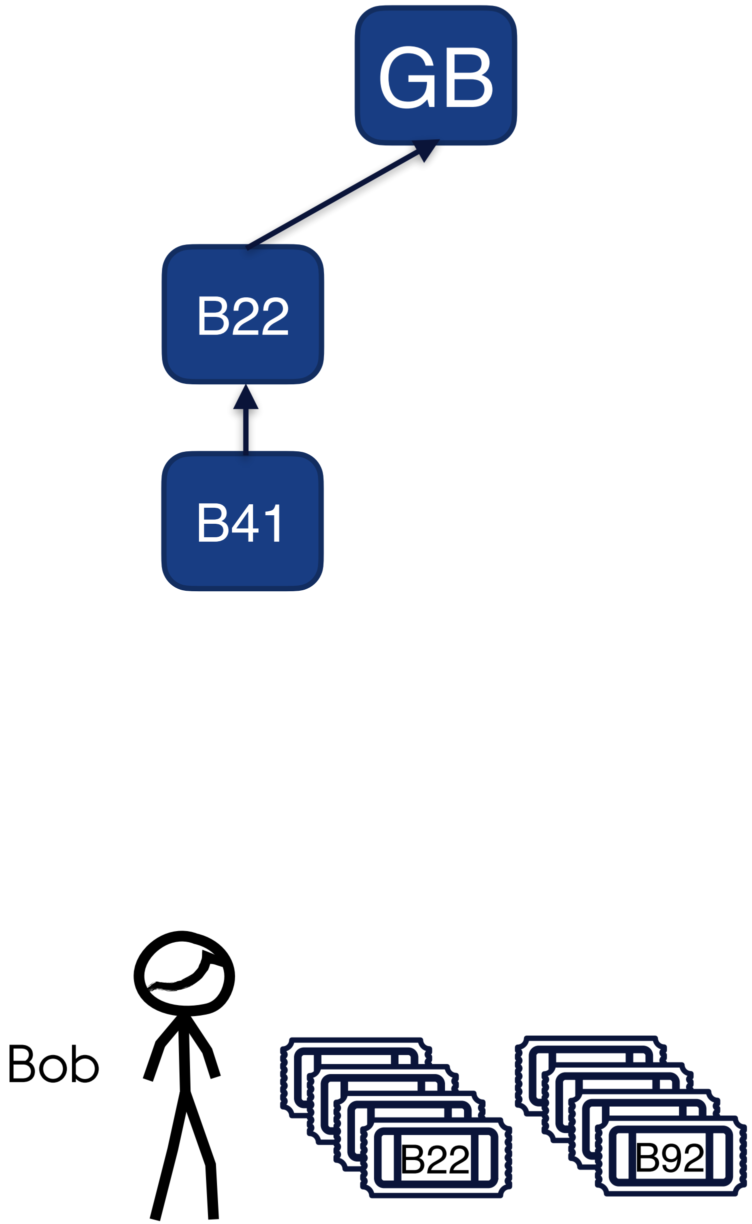

GB
B22
Alice
A1

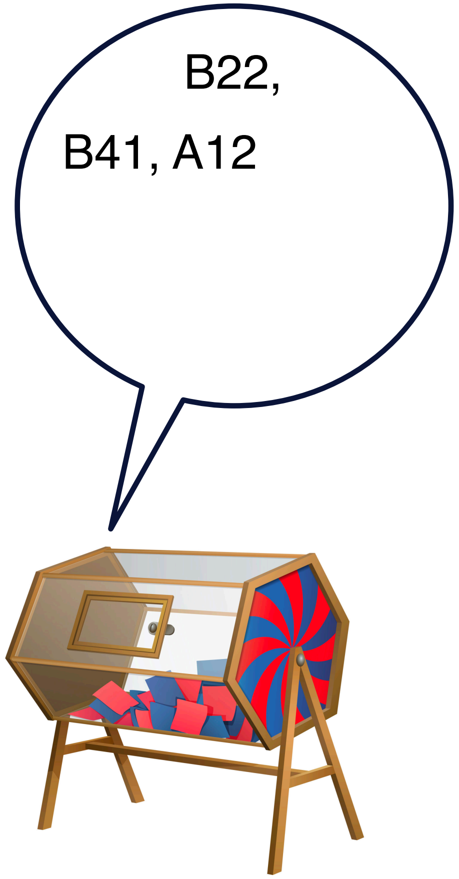

GB
B22
Bob
B22

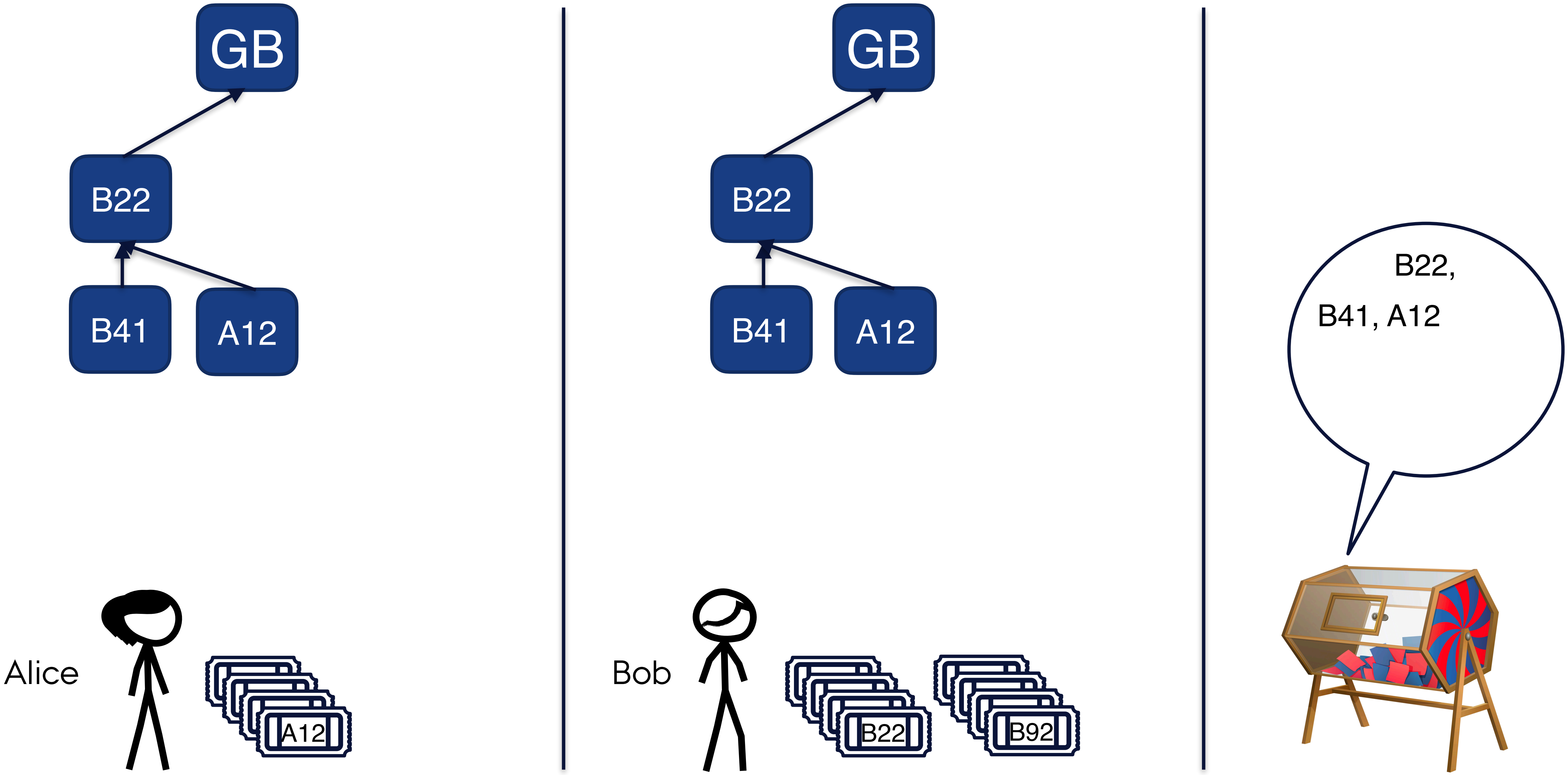

B22

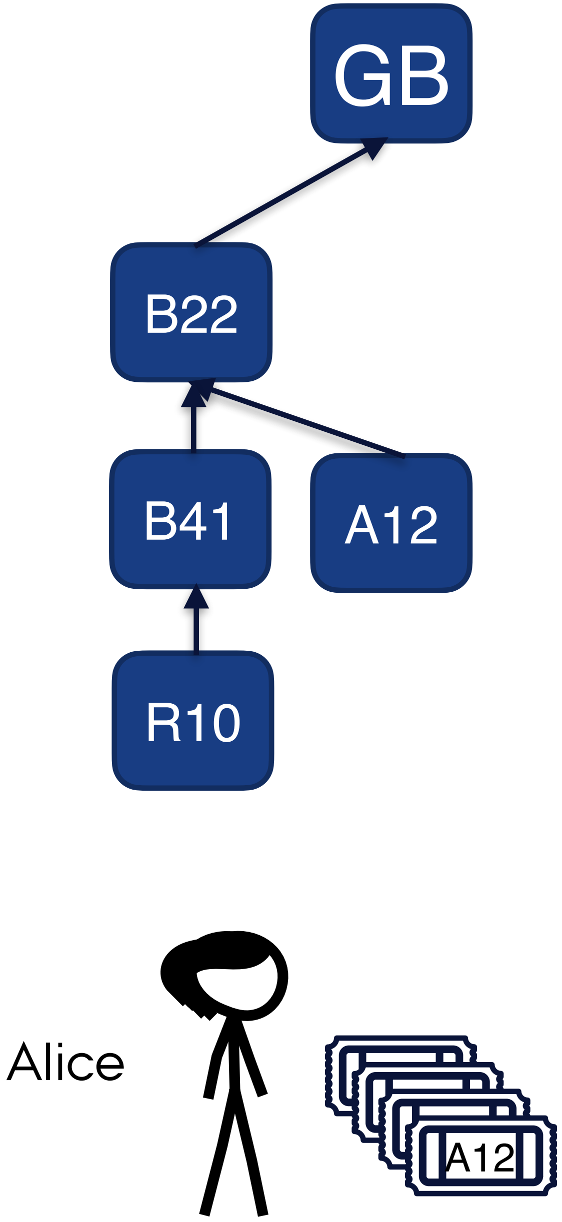

GB
B22
Alice
A12
GB
B22
Bob
B22
B92
B22

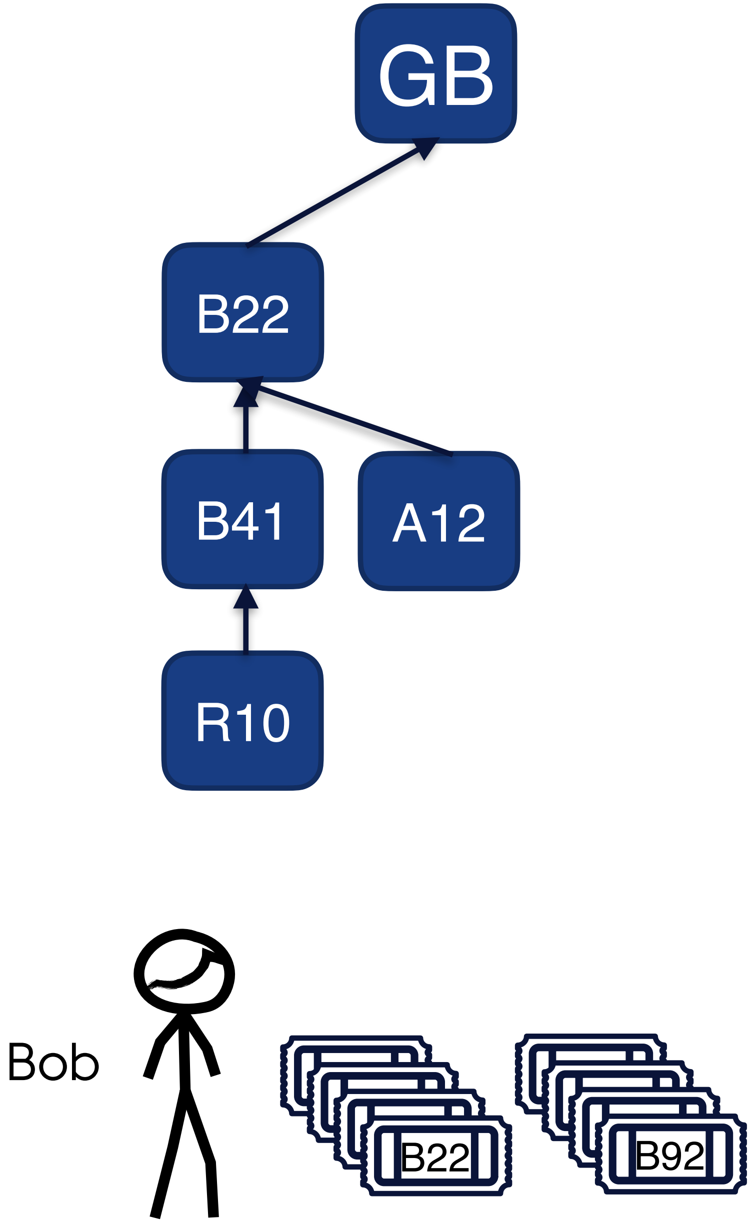

GB
B22
A12
Alice
A12

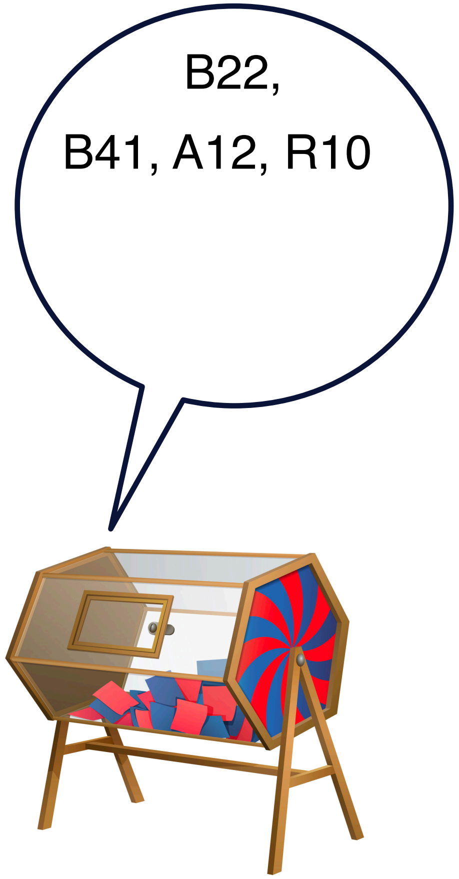

GB
B22
B41
Bob
B22
B92


B22,
B41, A12


GB
B22
B41
A12
Alice
A12
GB
B22
B41
A12
Bob
B22
B92
B22,
B41, A12


GB
B22
B41
A12
R10
Alice
A12

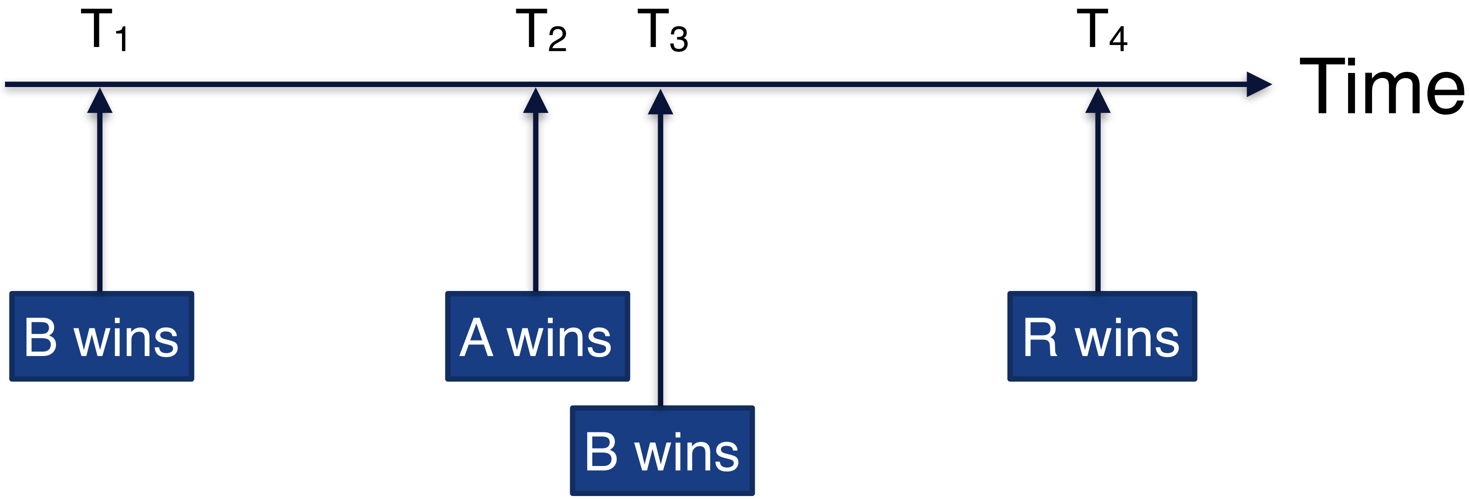

GB
B22
B41
A12
R10
Bob
B22
B92

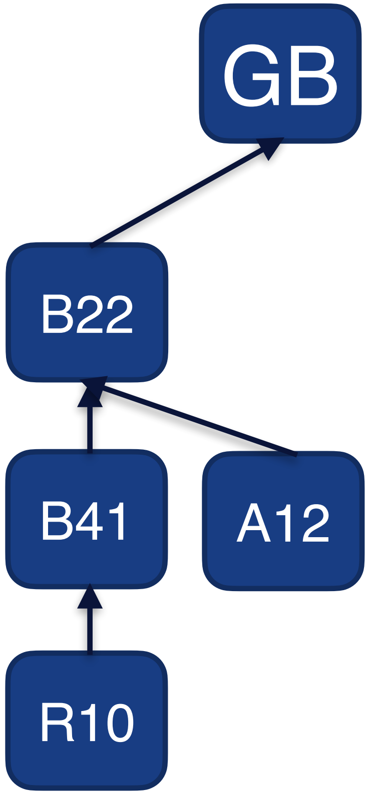

B22,
B41, A12, R10

INTUITION FOR CORRECTNESS

Observation 1: $T_2 - T_1 > \Delta_{Net}$ => Good thing happens

Observation 2: $T_3 - T_2 < \Delta_{Net}$ => Bad thing happens





THE LOTTERY DILEMMA

You need to guess the Δ_{Net} in order to instantiate the lottery that ensures a secure protocol.

If your guess is too low your protocol will not be secure!

If your guess is too high your protocol will be slow by construction!

THIS TALK

1. Weighted PoW lottery

2. Security of weighted lotteries

3. A specific weight-function that provides optimistic responsiveness

THE WEIGHT LOTTERY

Lottery	
Valid blocks	$\mathsf{Hash}(B) > T$
Contribution to chain	1
Best chain	Longest chain

THE WEIGHT LOTTERY

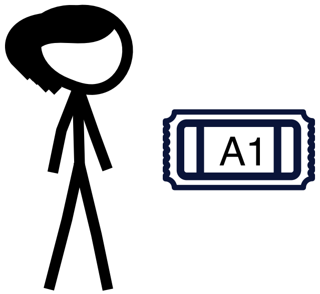
Lottery		Weight lottery
Valid blocks	$\text{Hash}(B) > T$	Everything
Contribution to chain	1	$w : \mathscr{H} \to \mathbb{R}$
Best chain	Longest chain	Heaviest chain

THE WEIGHT LOTTERY

Lottery	₿	Weight lottery	₿-Weight lottery
Valid blocks	$\text{Hash}(B) > T$	Everything	Everything
Contribution to chain	1	$w : \mathscr{H} \to \mathbb{R}$	$w(h) = \begin{cases} 0, & \text{if } h \leq T \\ 1, & \text{else} \end{cases}$
Best chain	Longest chain	Heaviest chain	Heaviest chain

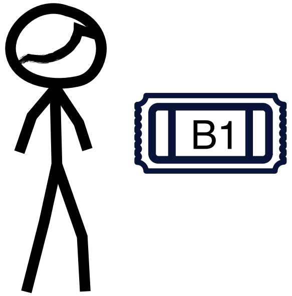
GB

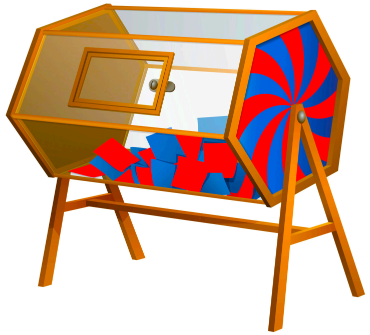
Alice



GB

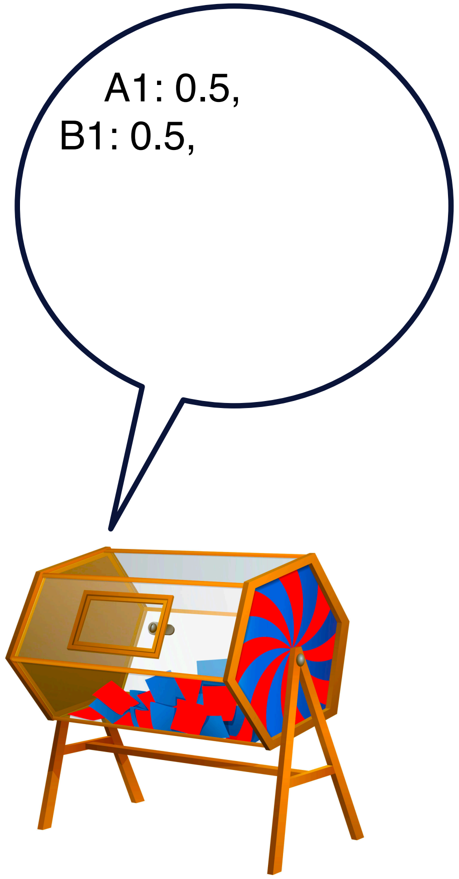
Bob

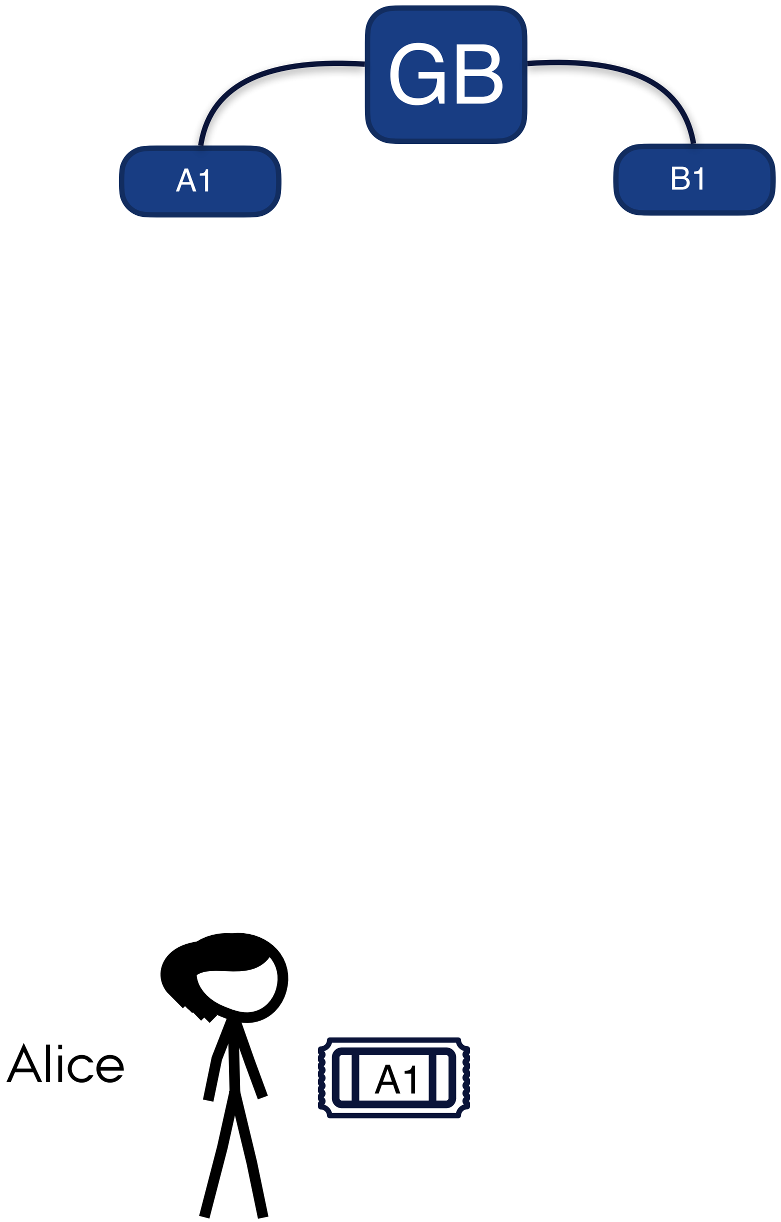




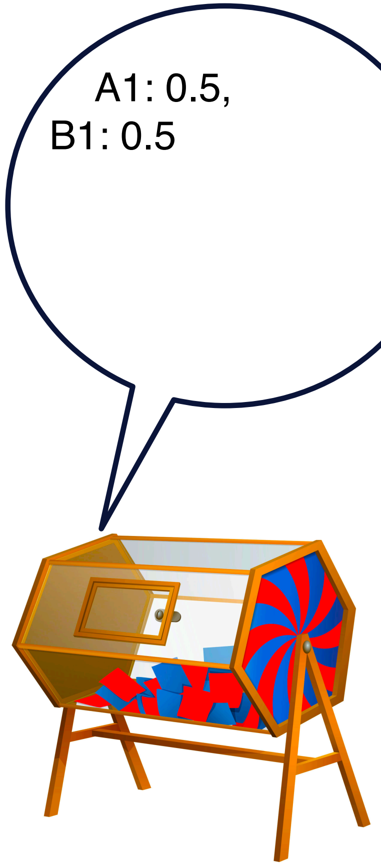

GB
A1
Alice
A1

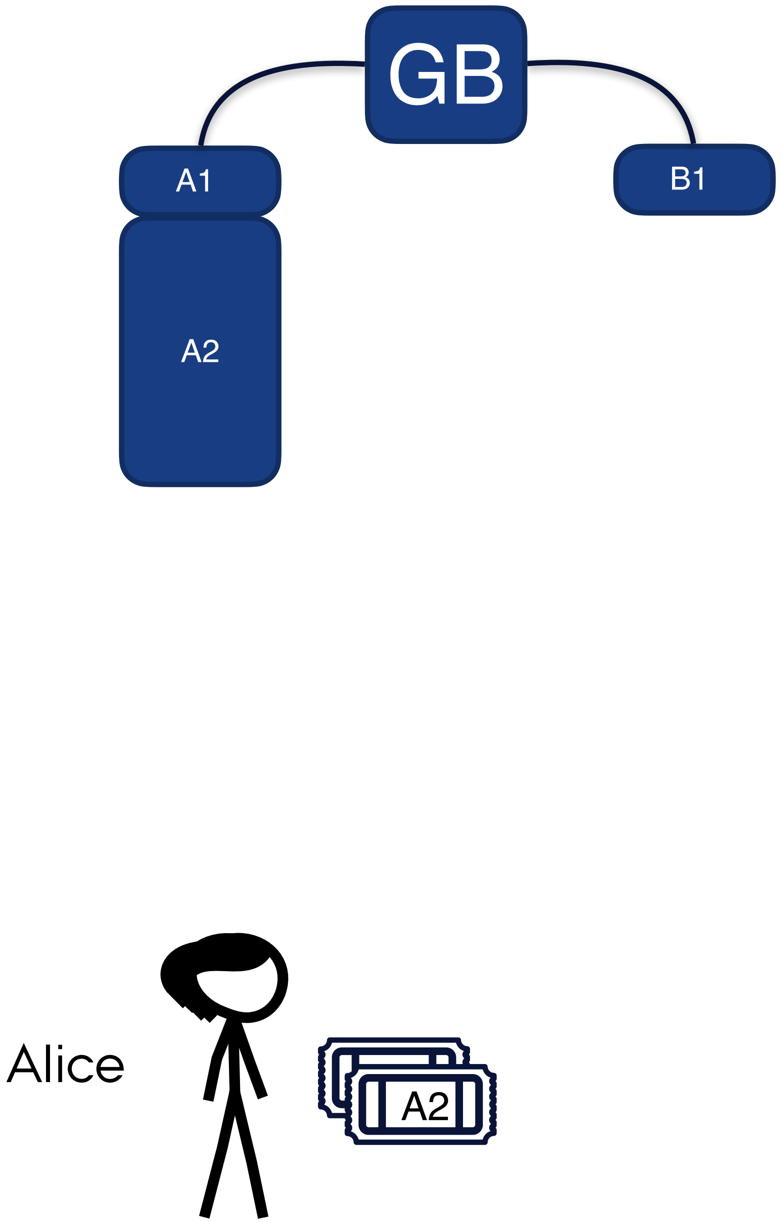

GB
B1
Bob
B1

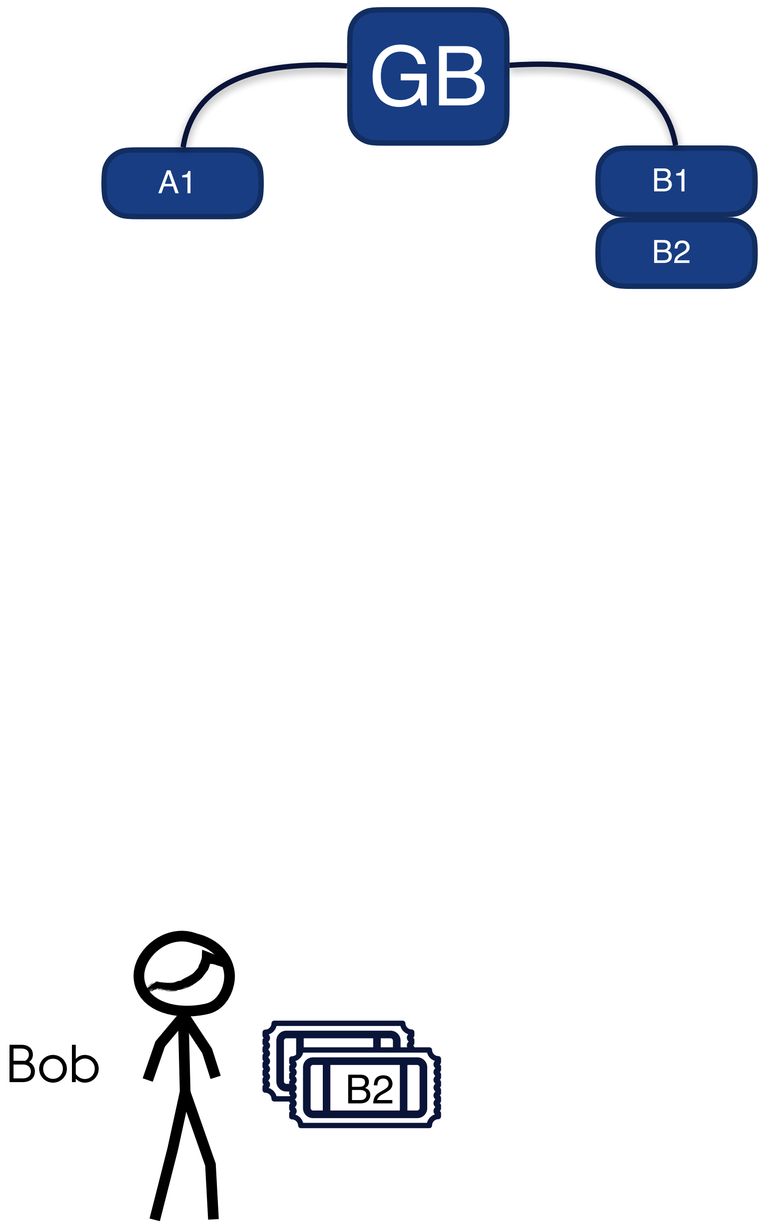

A1: 0.5,
B1: 0.5,

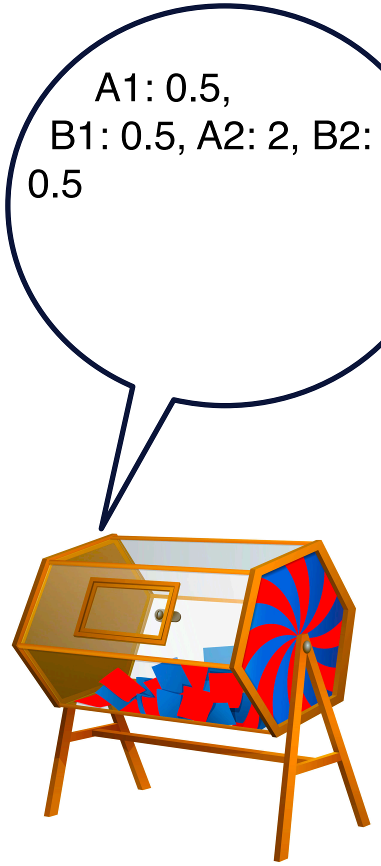

GB
A1
B1
Alice
A1

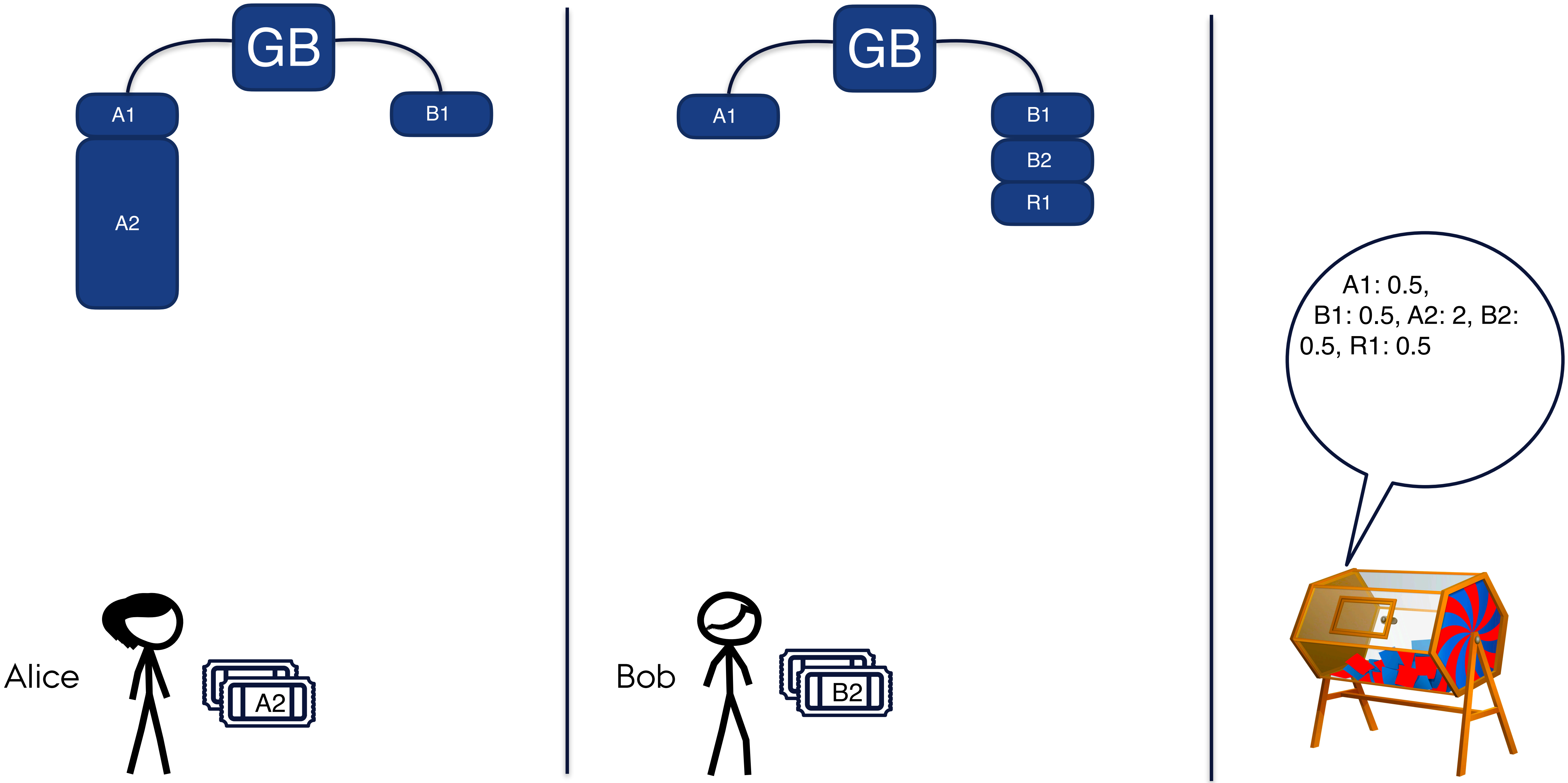

GB
A1
B1
Bob
B1

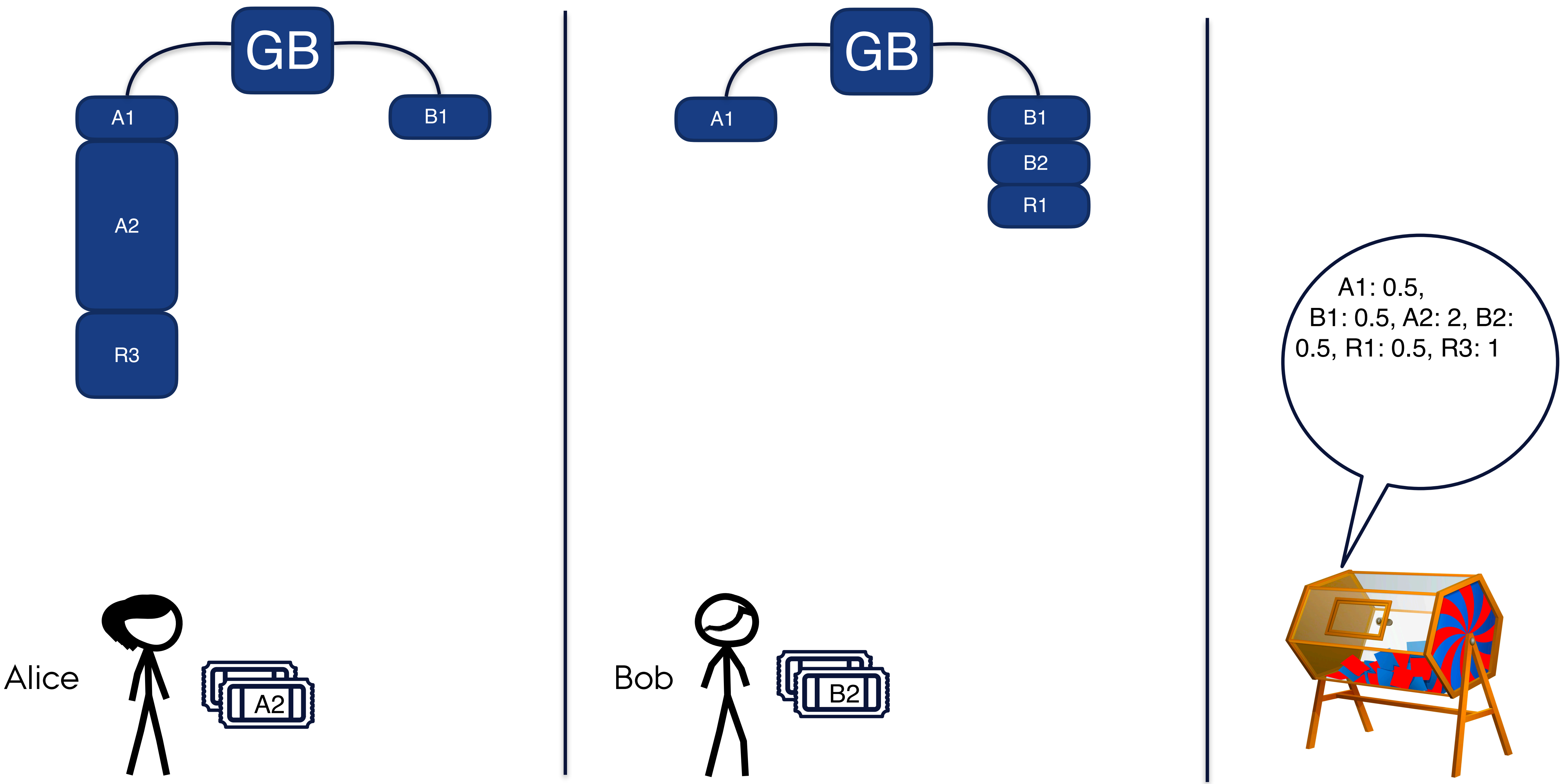

A1: 0.5,
B1: 0.5

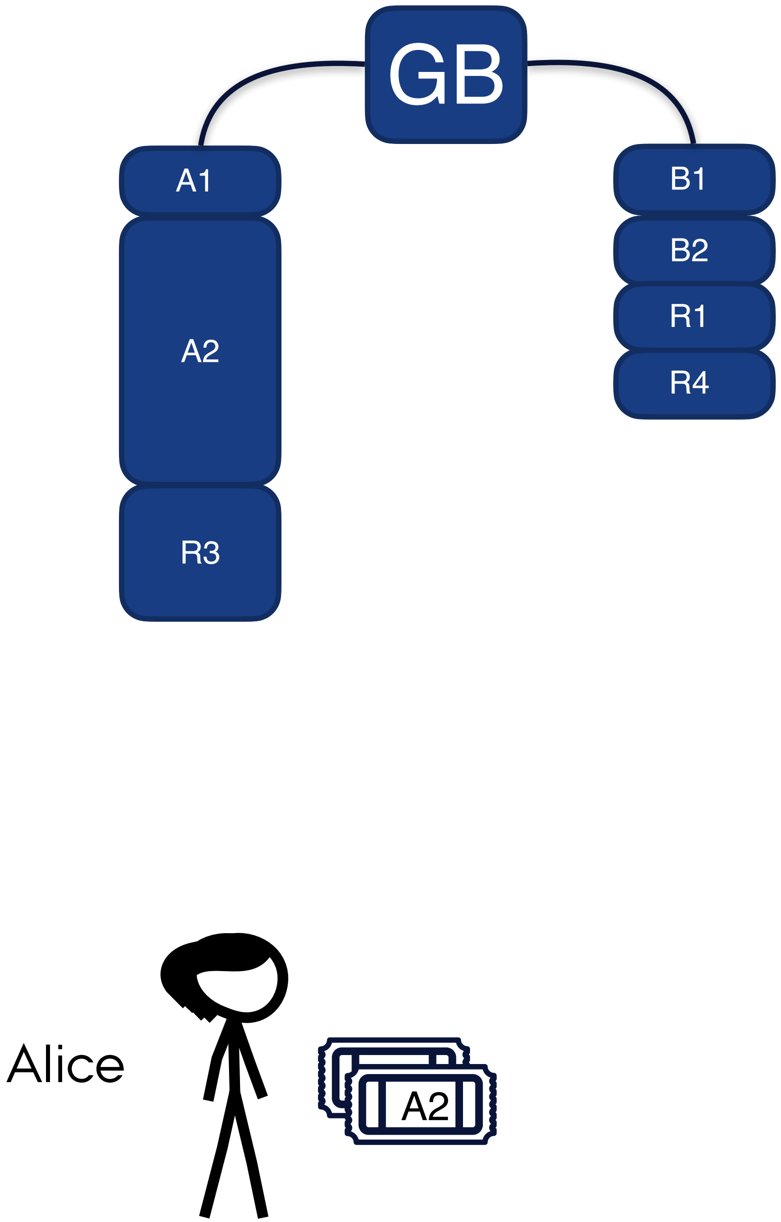

GB
A1
B1
A2
Alice
A2

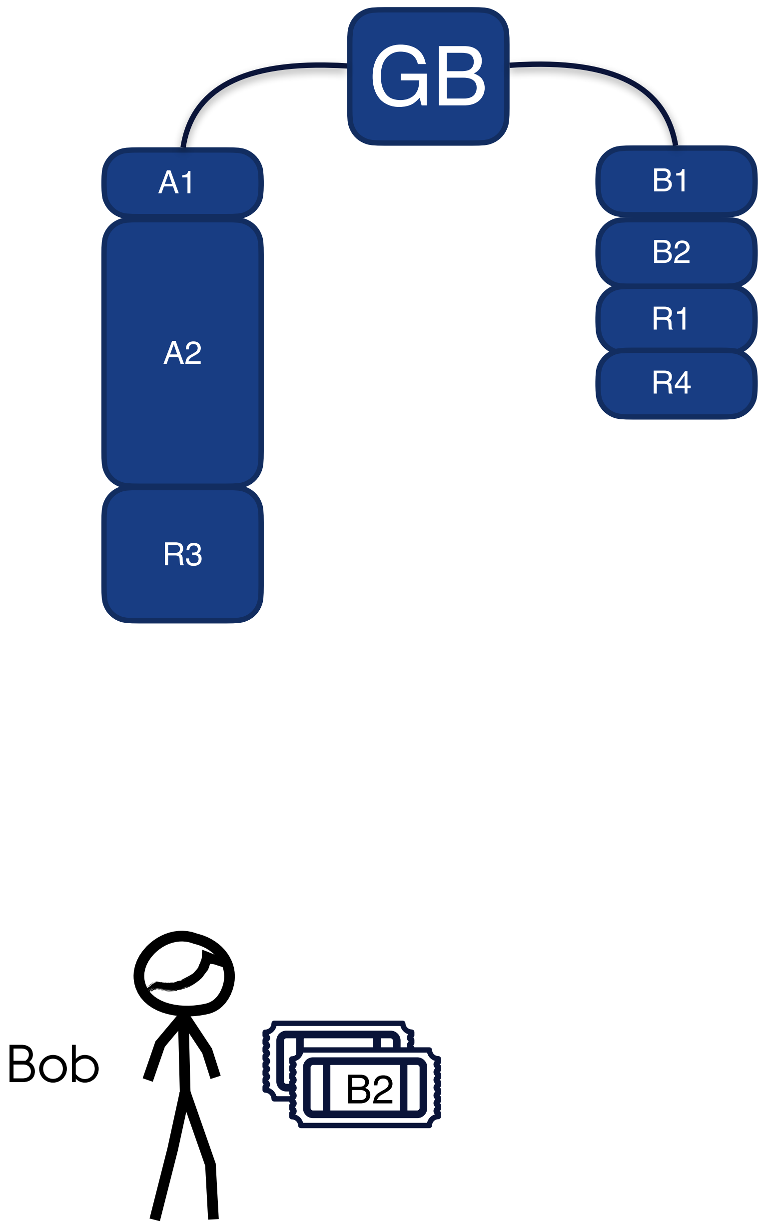

GB
A1
B1
B2
Bob
B2


A1: 0.5,
B1: 0.5, A2: 2, B2:
0.5

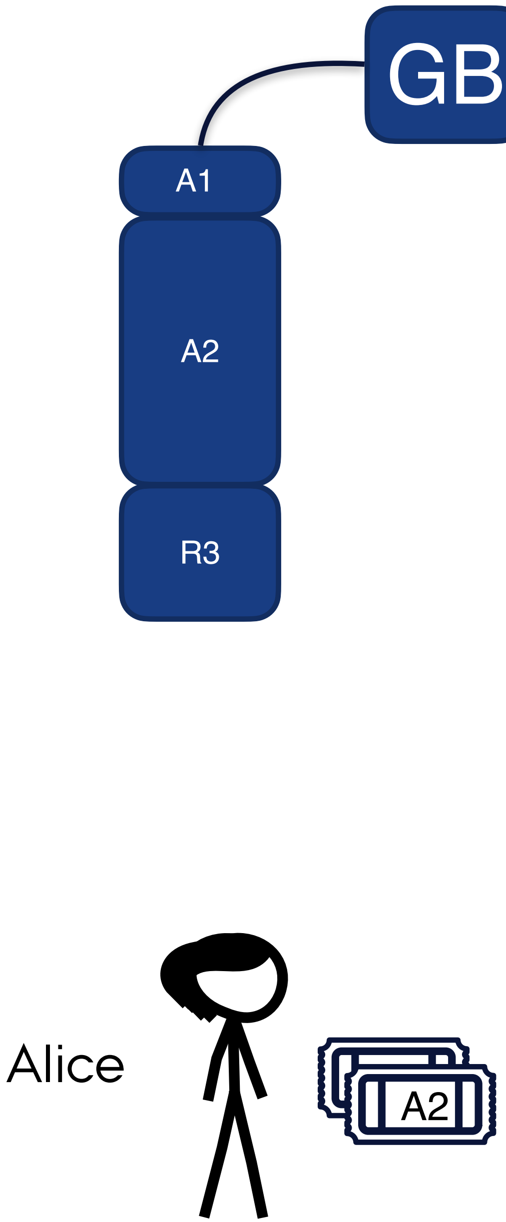

GB
A1
B1
A2
Alice
A2
GB
A1
B1
B2
R1
Bob
B2
A1: 0.5,
B1: 0.5, A2: 2, B2:
0.5, R1: 0.5

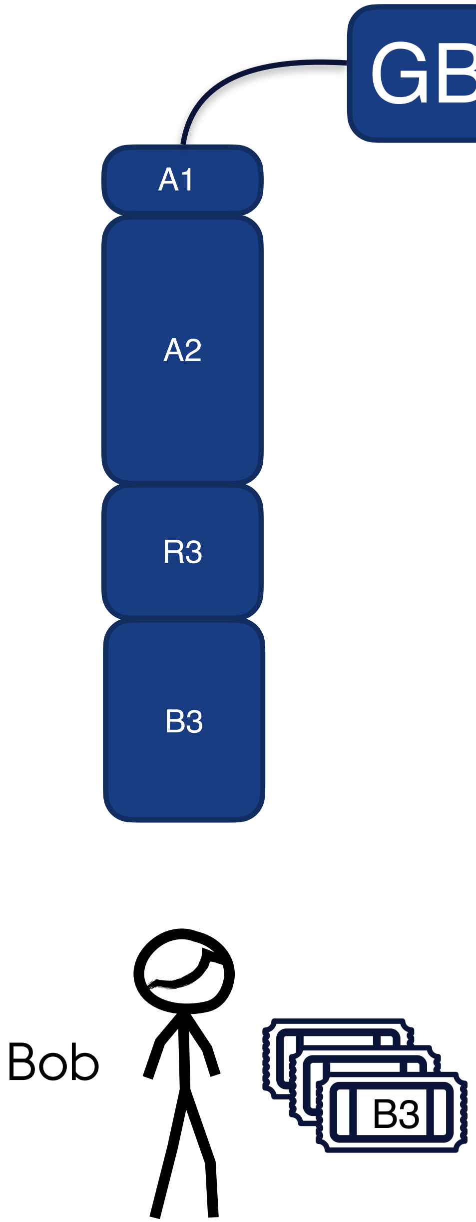

GB
A1
B1
A2
R3
Alice
A2
GB
A1
B1
B2
R1
Bob
B2
A1: 0.5,
B1: 0.5, A2: 2, B2:
0.5, R1: 0.5, R3: 1


GB
A1
A2
R3
B1
B2
R1
R4
Alice
A2


GB
A1
A2
R3
B1
B2
R1
R4
Bob
B2

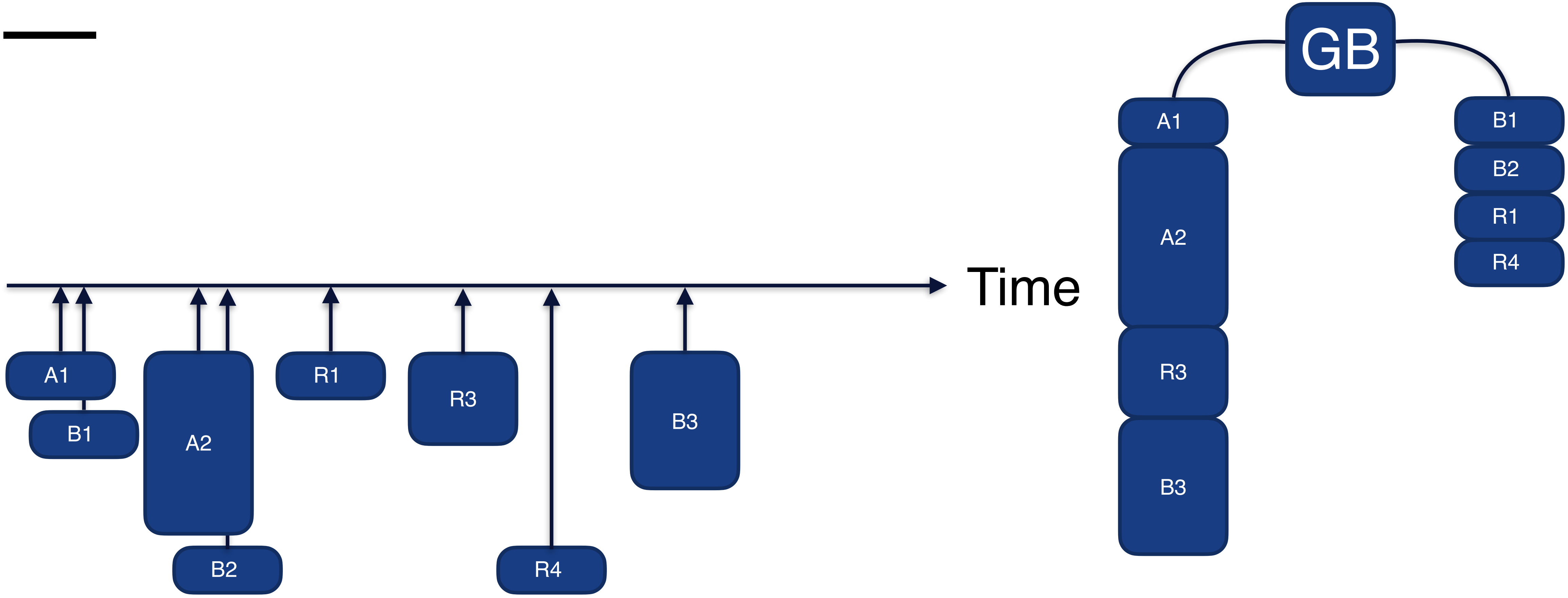

A1: 0.5,
B1: 0.5, A2: 2, B2:
0.5, R1: 0.5, R3: 1,
R4: 0.5,


GB
A1
A2
R3
B1
B2
R1
R4
Alice
A2


GB
A1
A2
R3
B3
B1
B2
R1
R4
Bob
B3

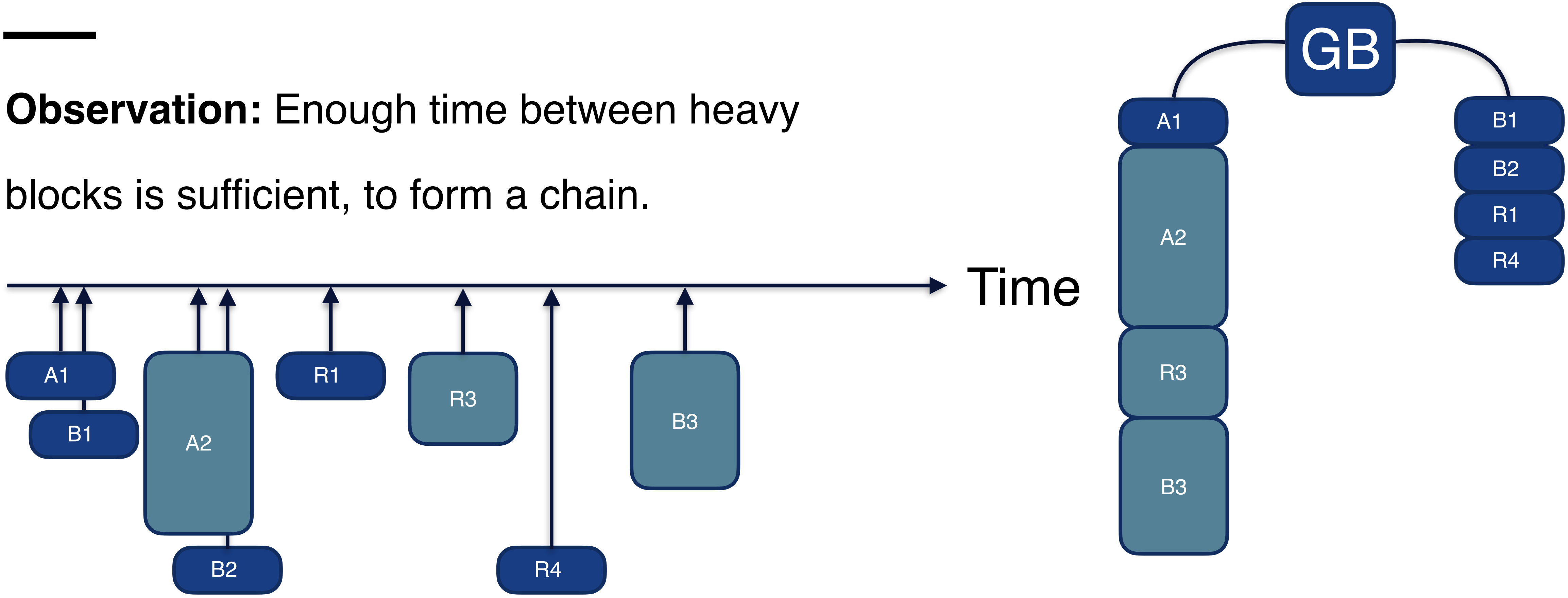

A1: 0.5,
B1: 0.5, A2: 2, B2:
0.5, R1: 0.5, R3: 1,
R4: 0.5, B3: 1.5

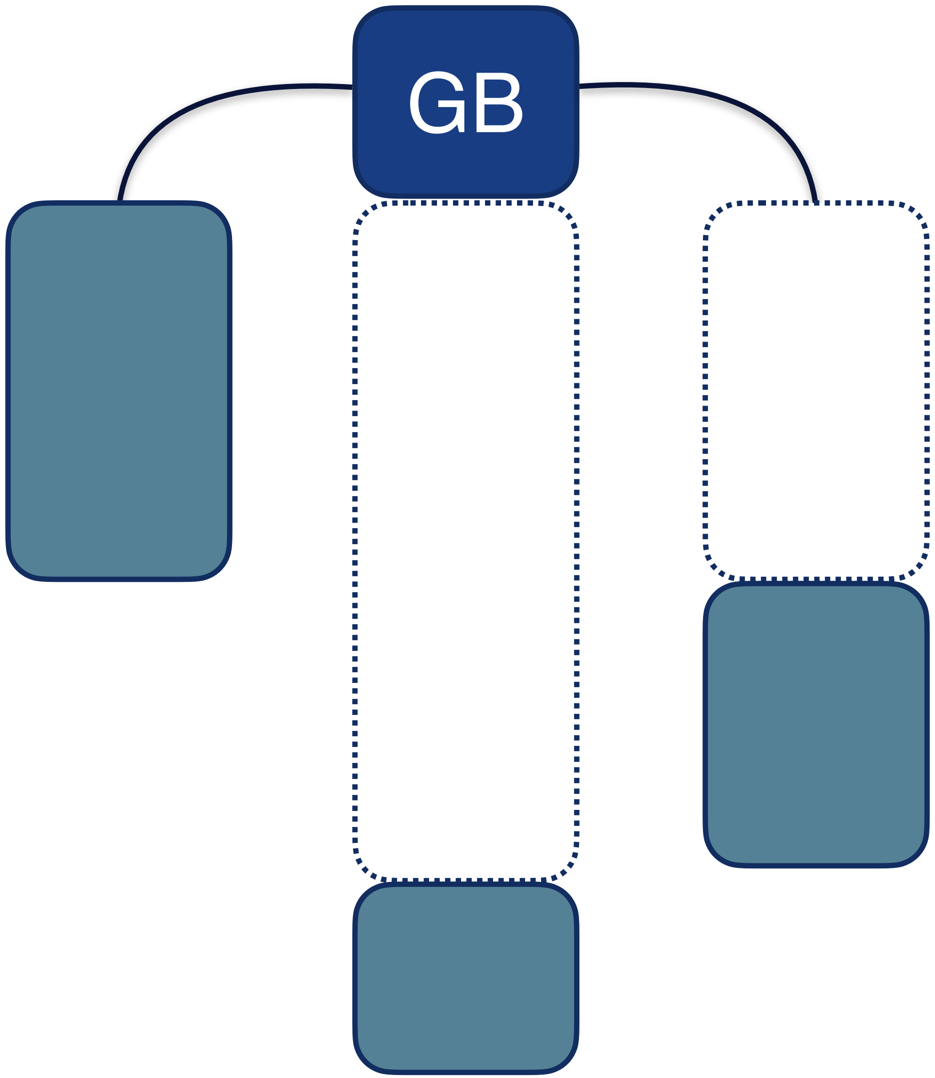
ANALYSIS

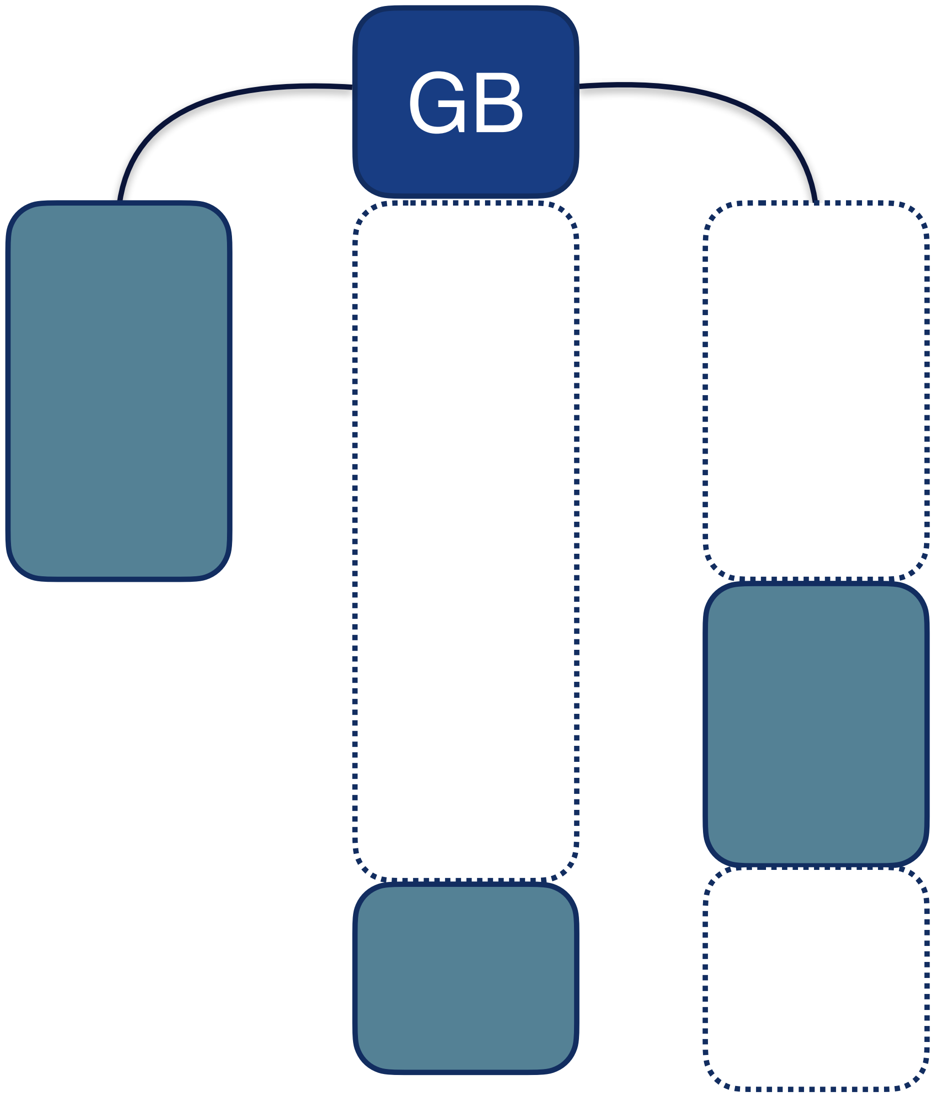


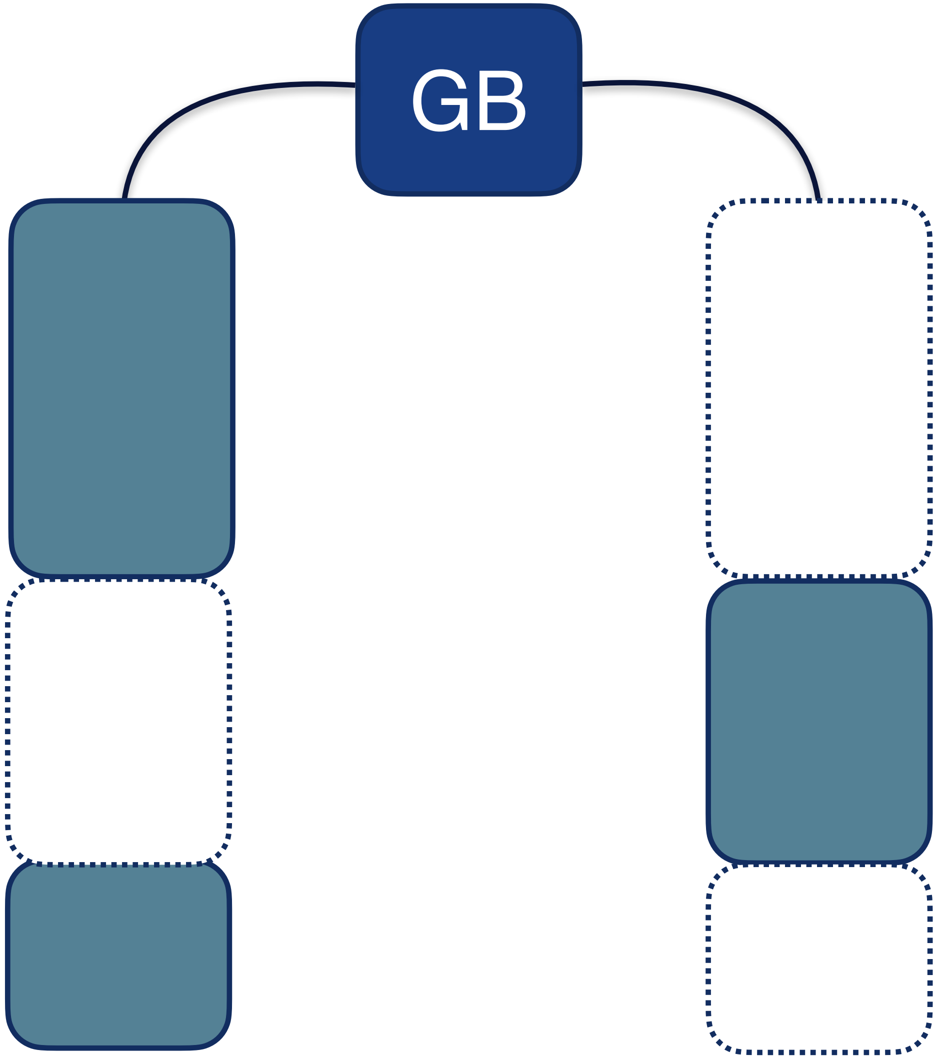
ANALYSIS

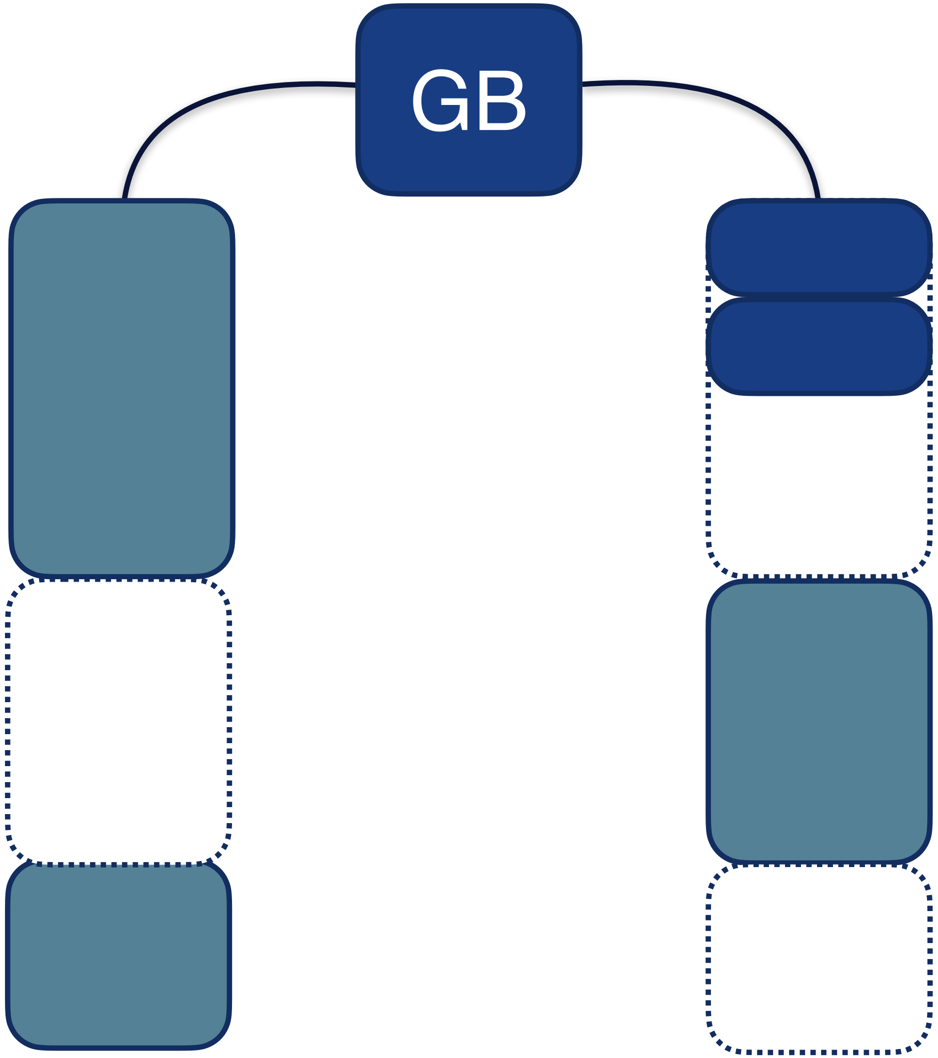
Observation: Enough time between heavy blocks is sufficient, to form a chain.

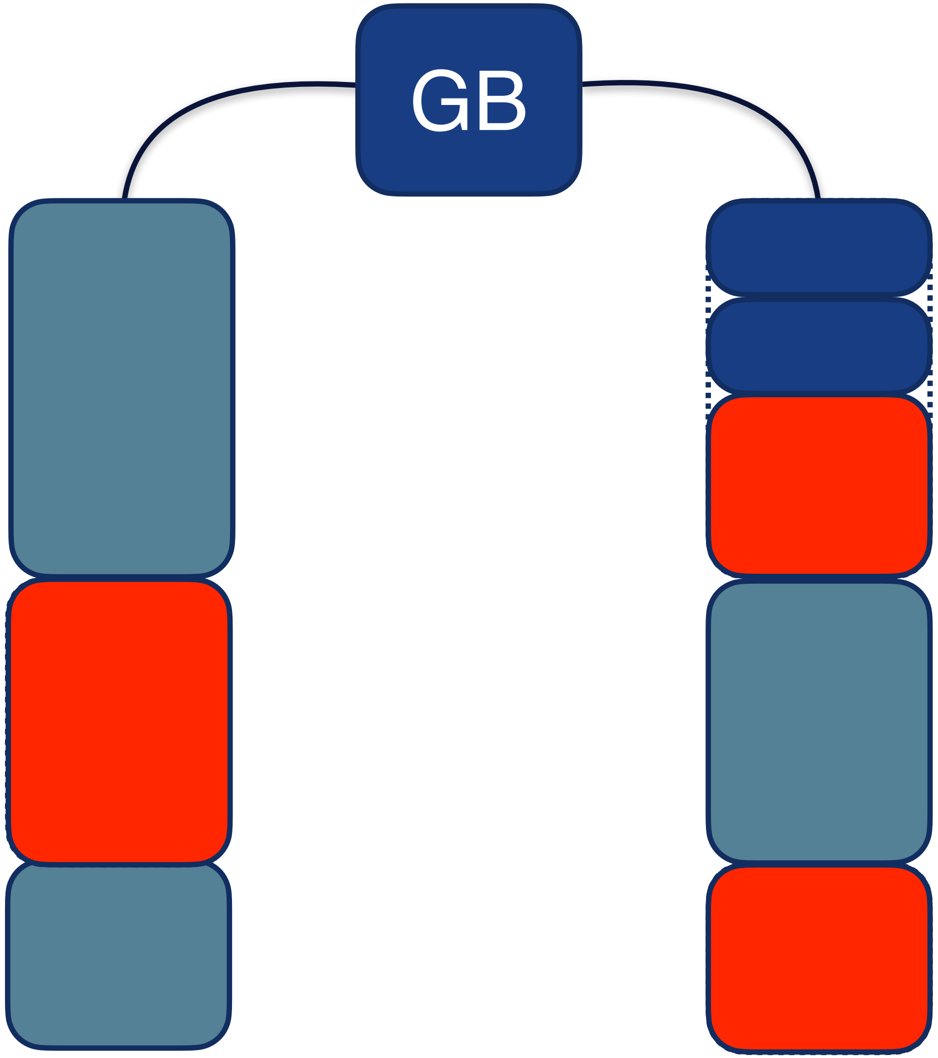



GB

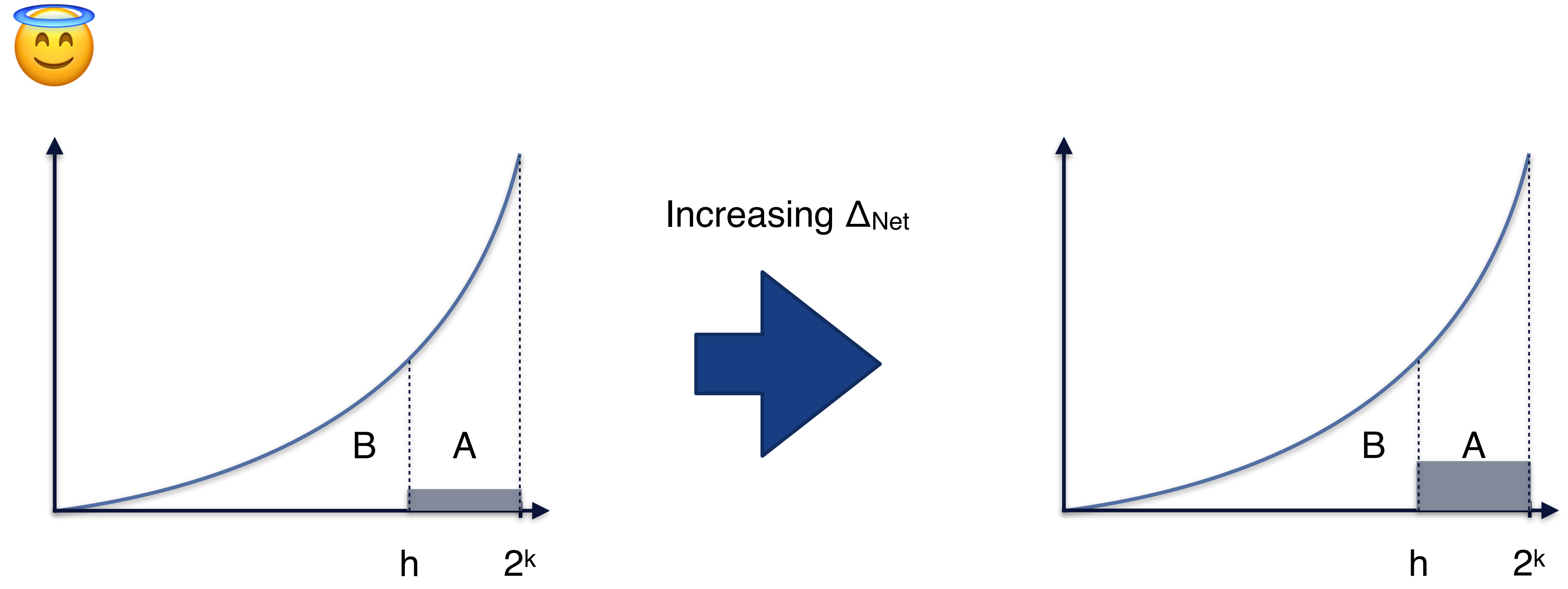

GB


GB


GB

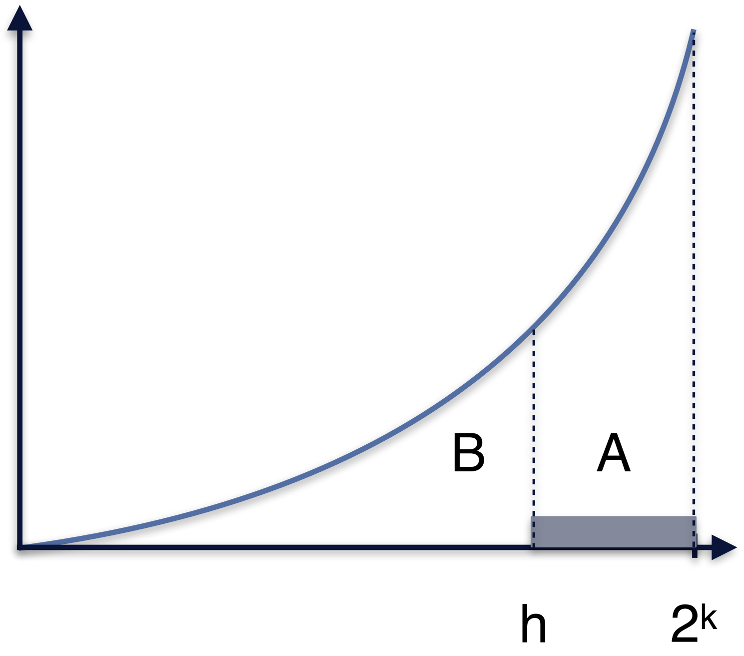

GB

WHAT SHOULD A “HEAVY” BLOCK BE?

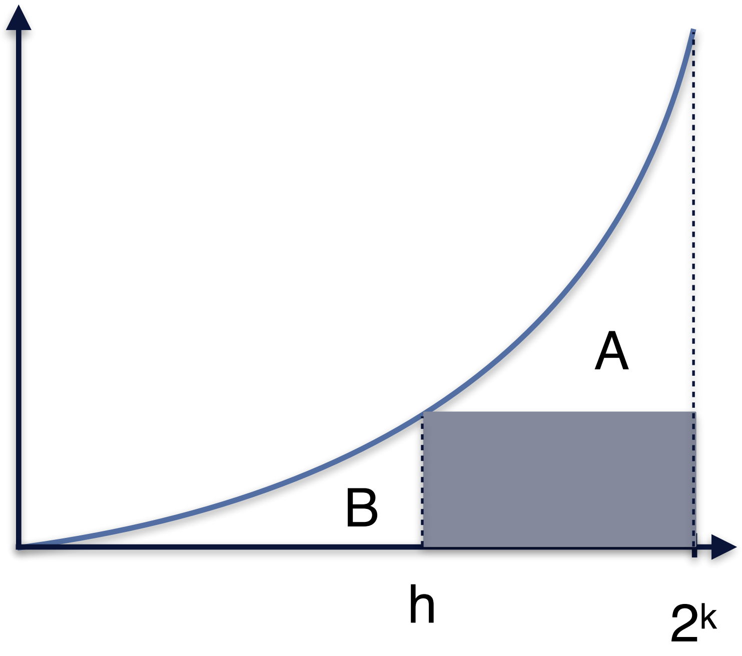


WHAT SHOULD A “HEAVY” BLOCK BE?

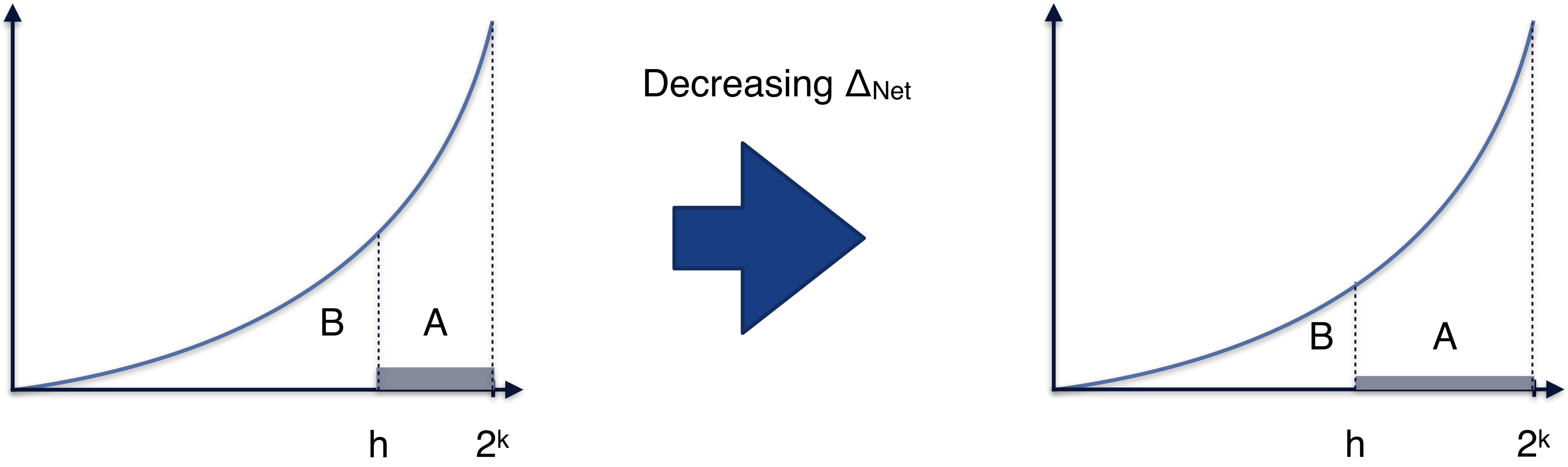
😇



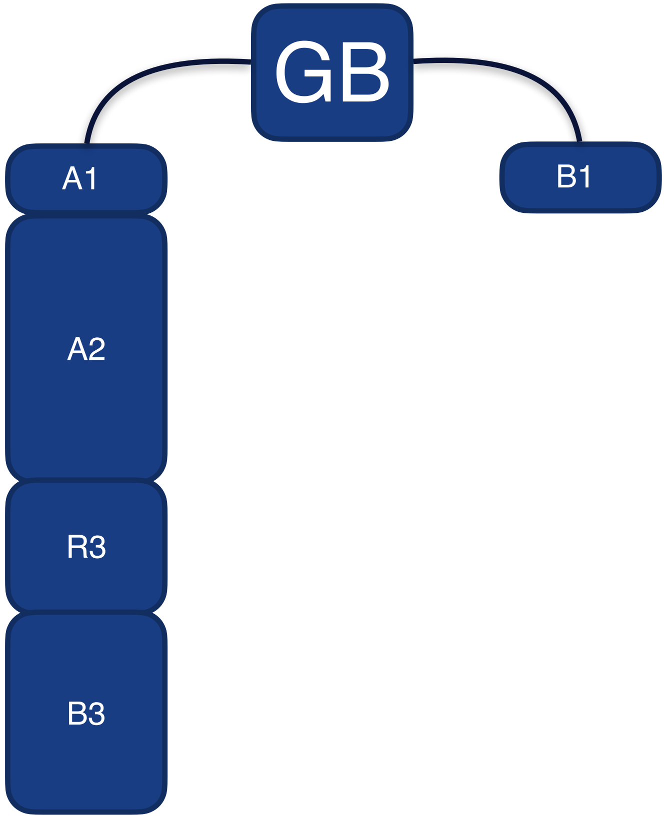
Moving h to the left

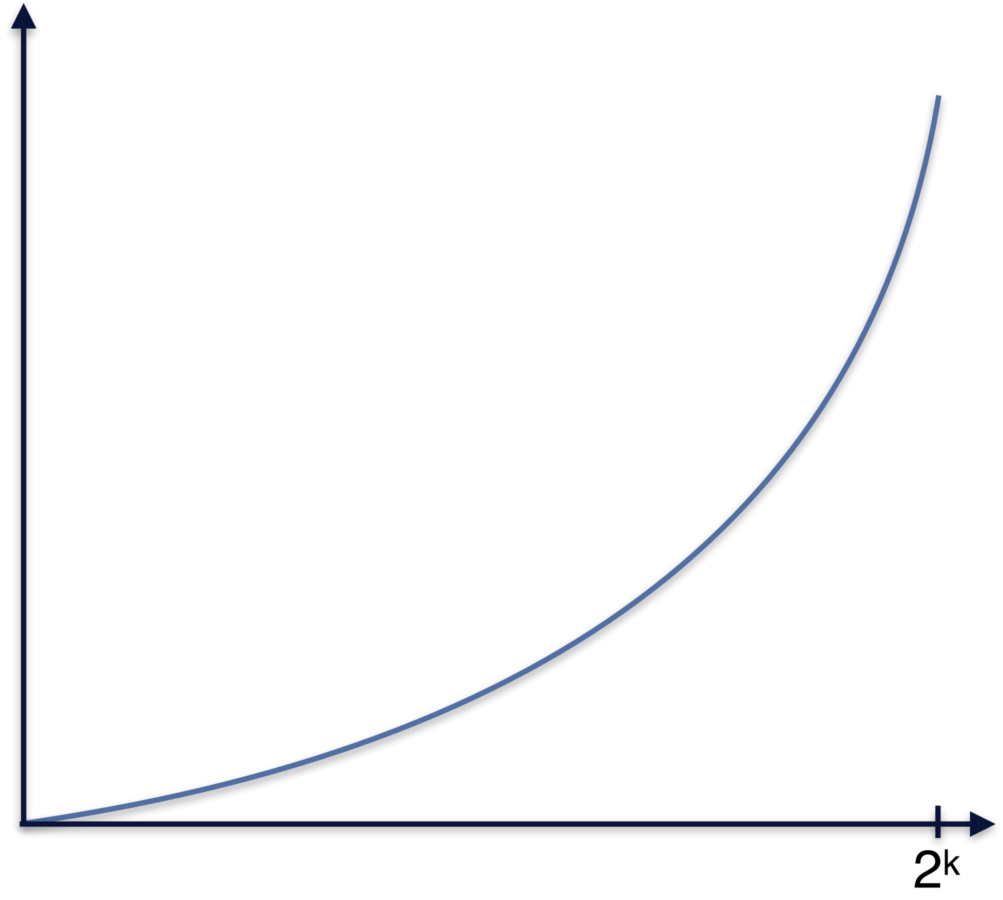


WHAT SHOULD A “HEAVY” BLOCK BE?

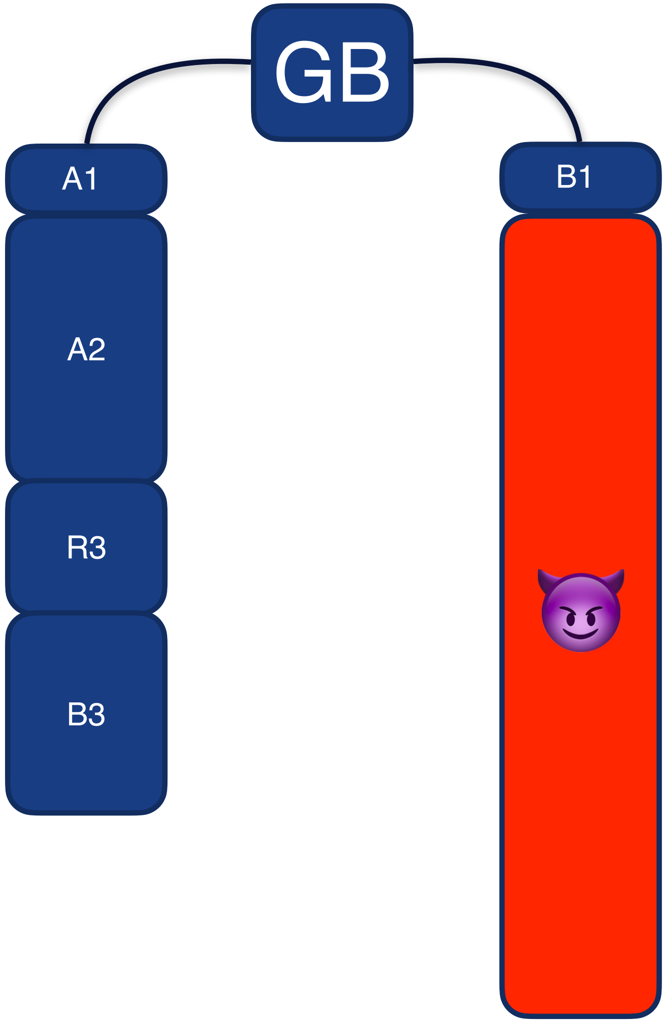


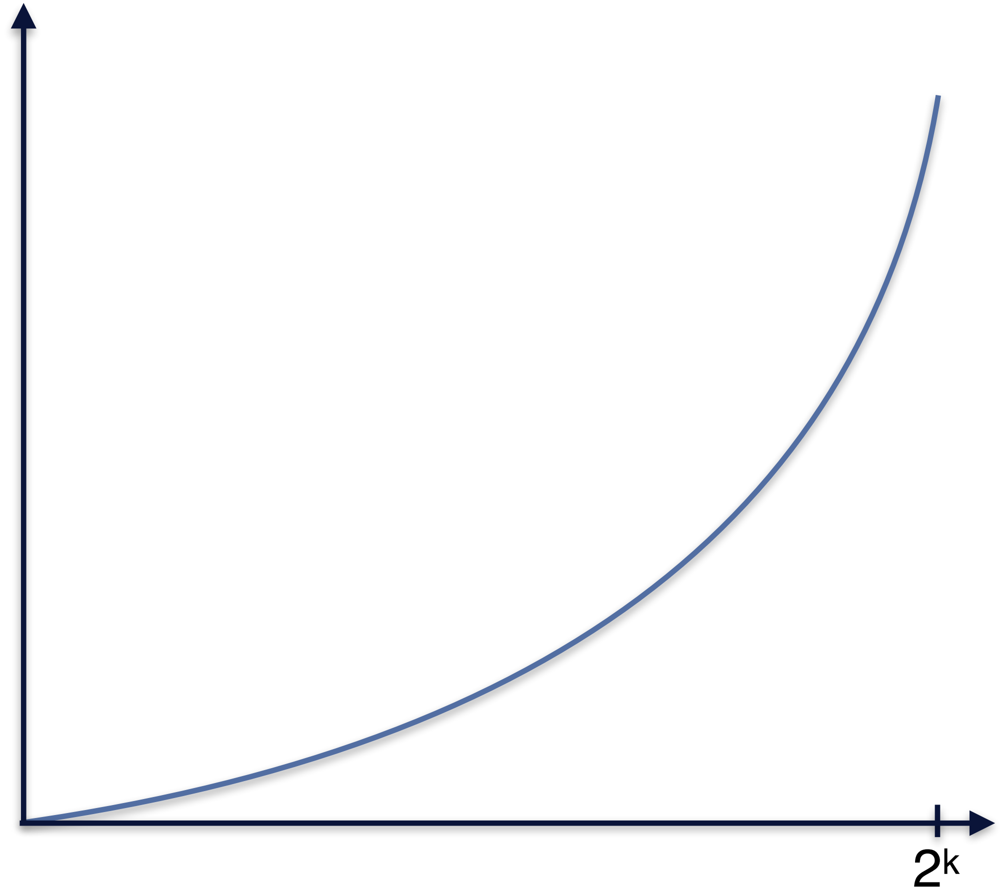
WHAT DOES A NICE WEIGHT FUNCTION LOOK LIKE?



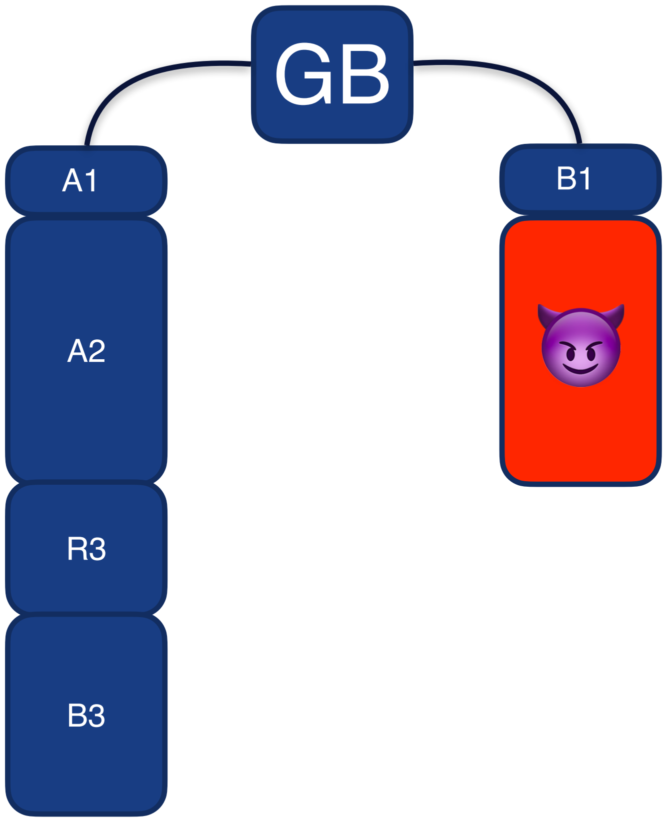


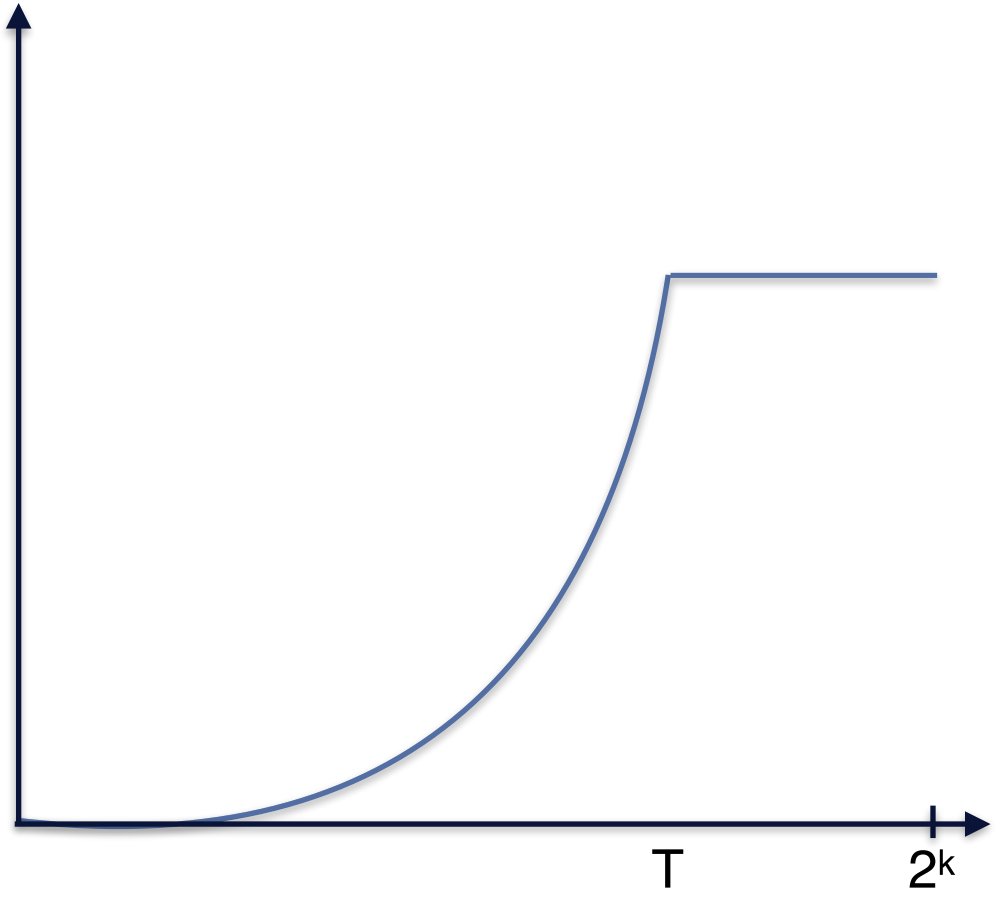
WHAT DOES A NICE WEIGHT FUNCTION LOOK LIKE?





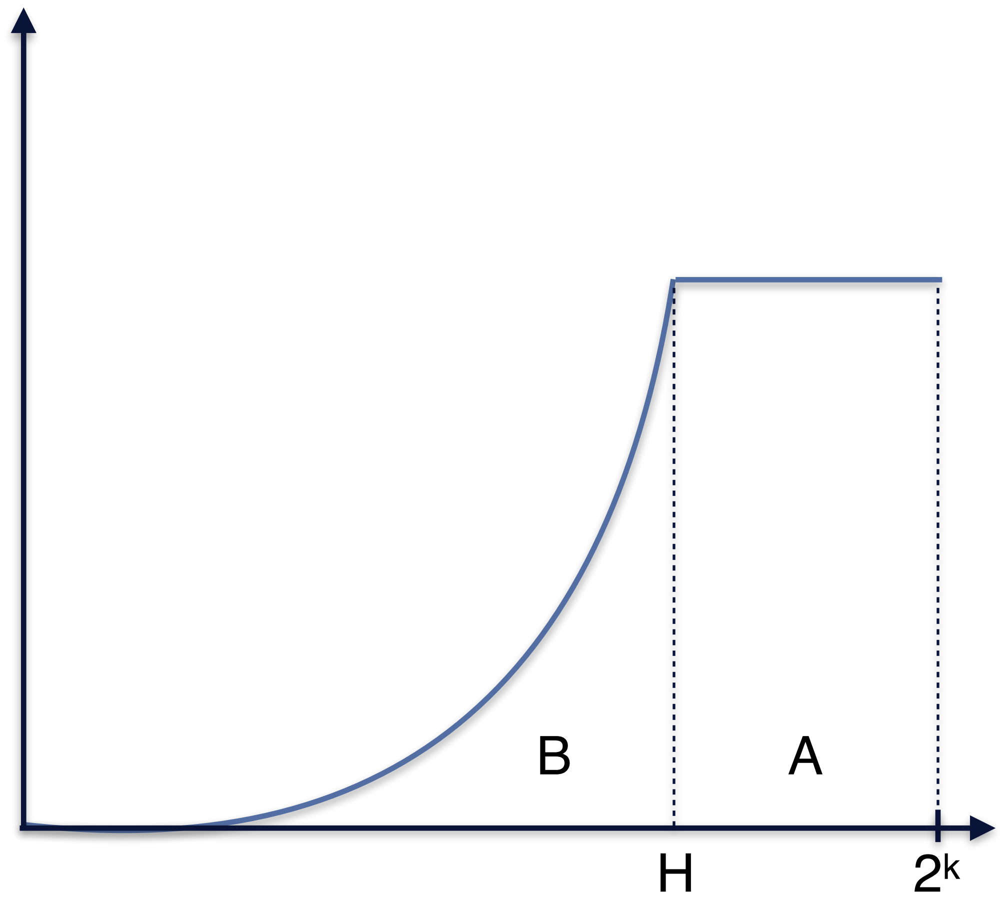
WHAT DOES A NICE WEIGHT FUNCTION LOOK LIKE?





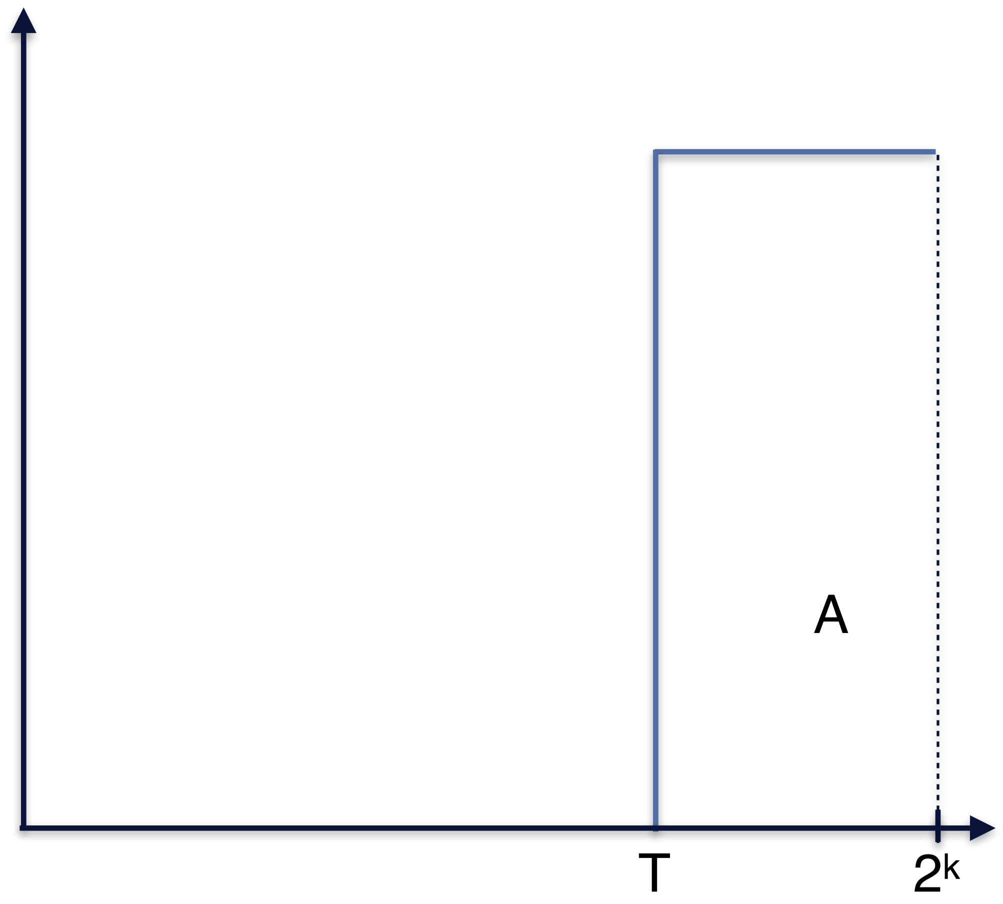
WHAT DOES A NICE WEIGHT FUNCTION LOOK LIKE?

- Low variance
- A >> B



A SUGGESTION: ₿

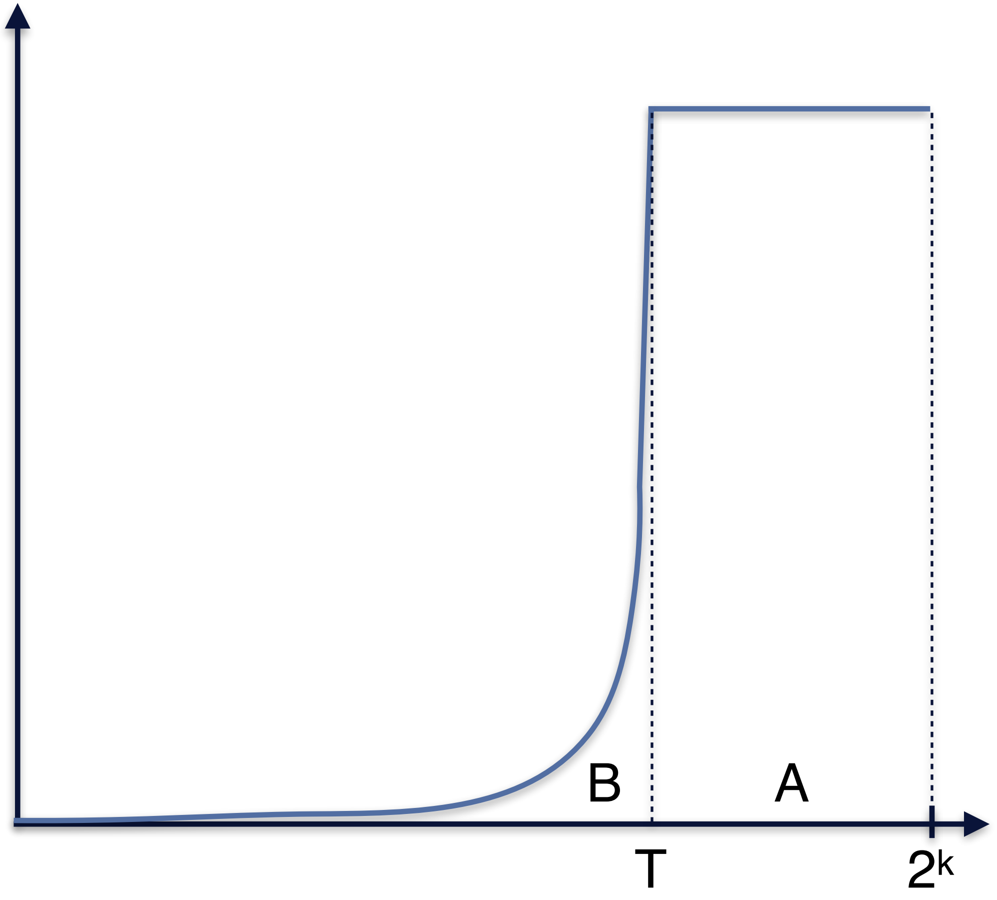
- Low variance: ✅
- A >> B: ✅
- Worst case (under attack): ✅
- Best case: 🐌

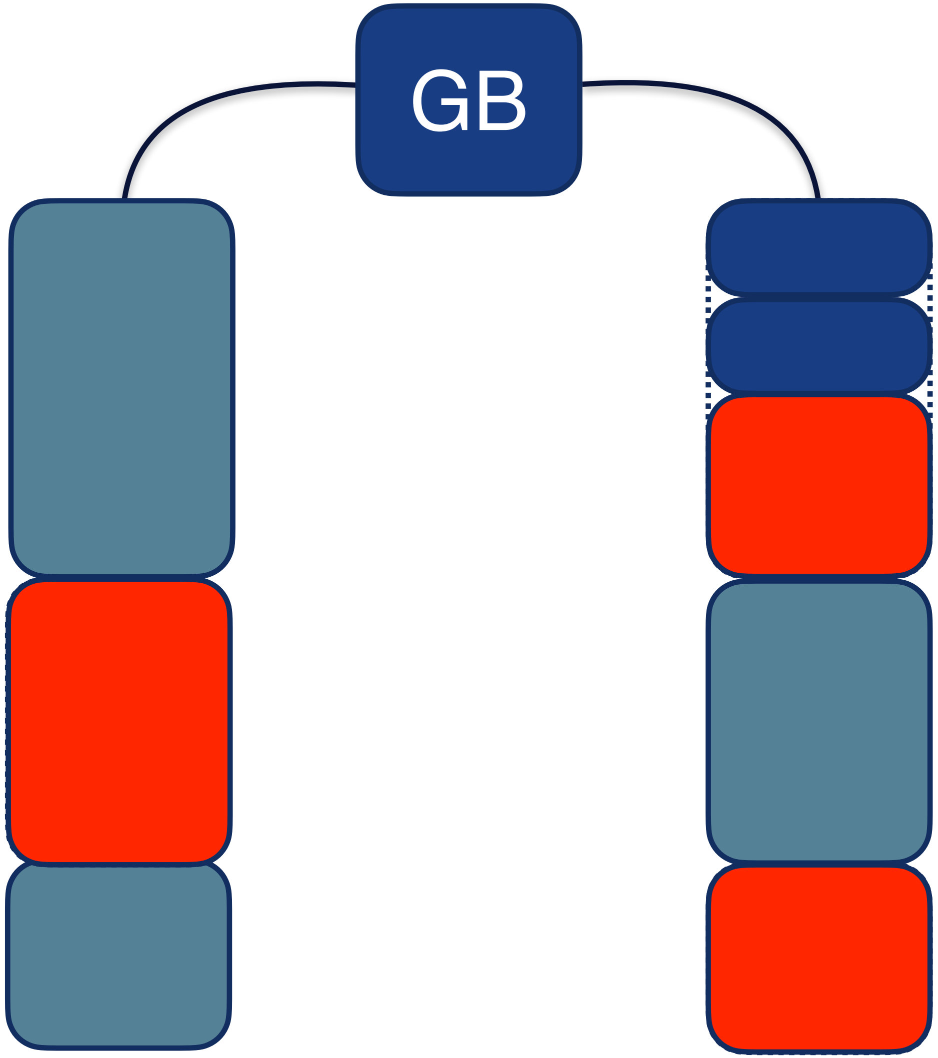


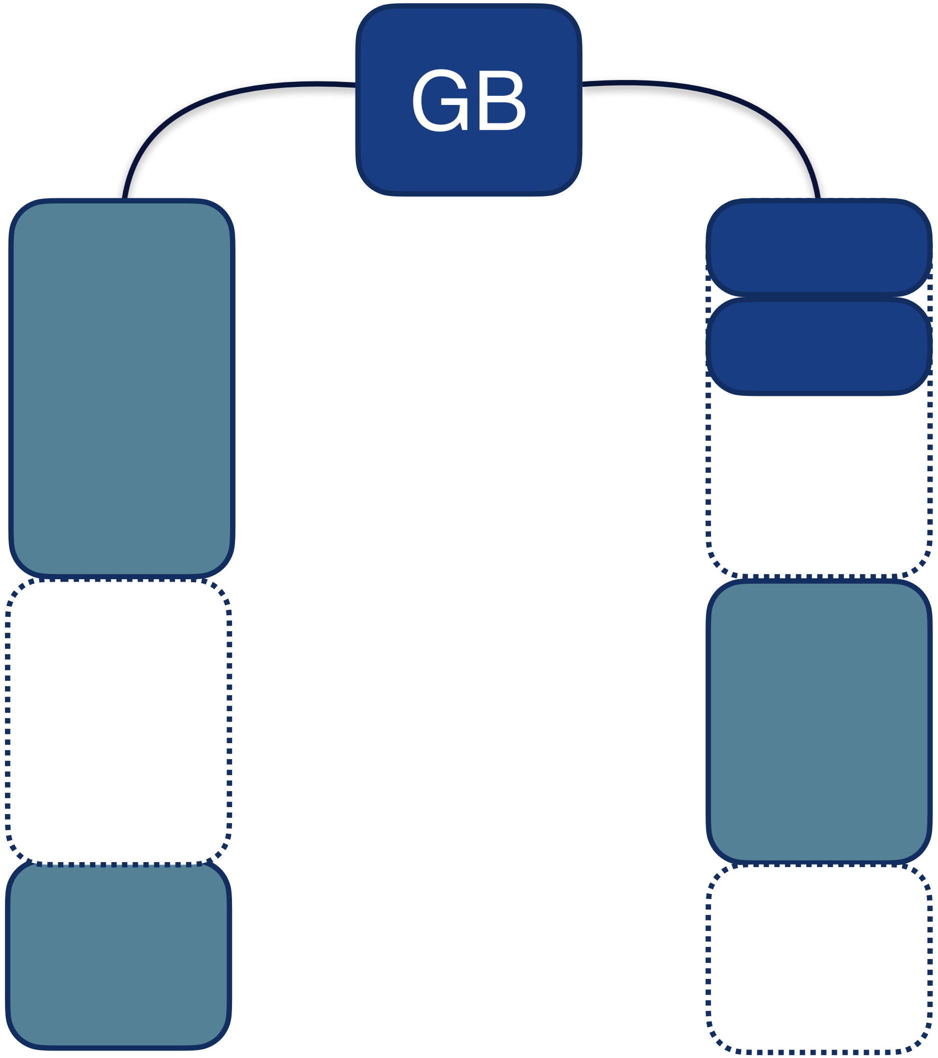
ANOTHER SUGGESTION:

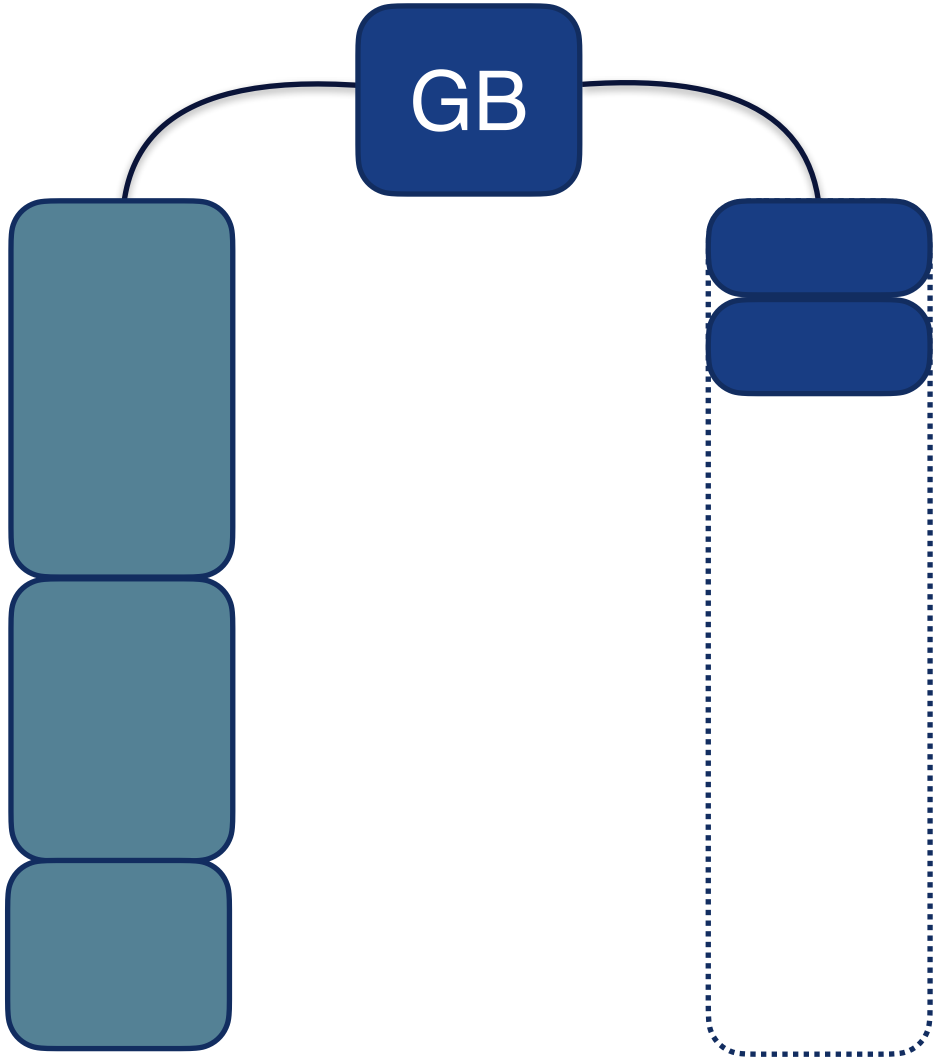
$$w(h) = \begin{cases} e^{hc}, & \text{if } h \leq T \\ e^{Tc}, & \text{else} \end{cases}$$

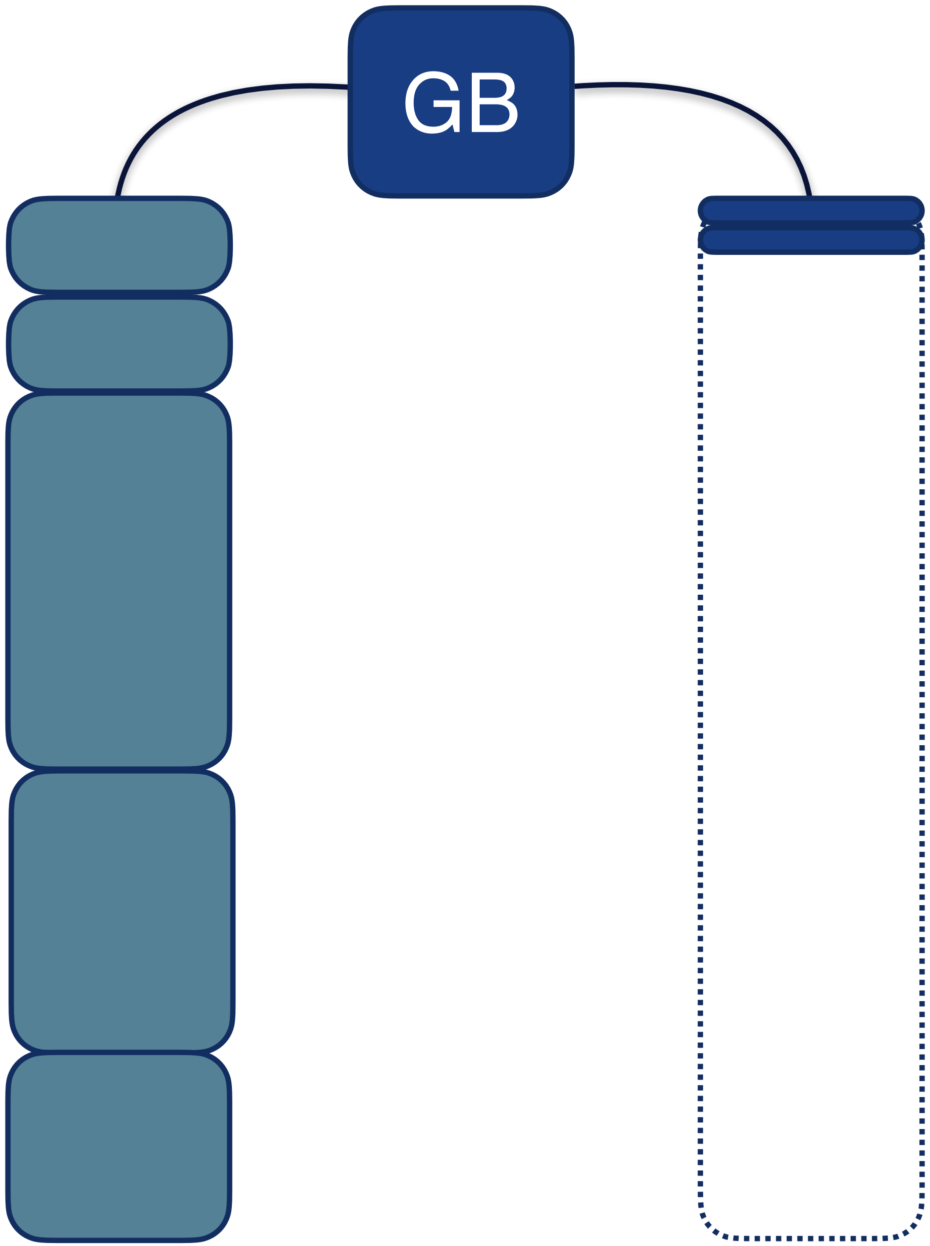
- Low variance: ✅
- A >> B: ✅
- Worst case (under attack): ✅
- Best case: 🏃💨

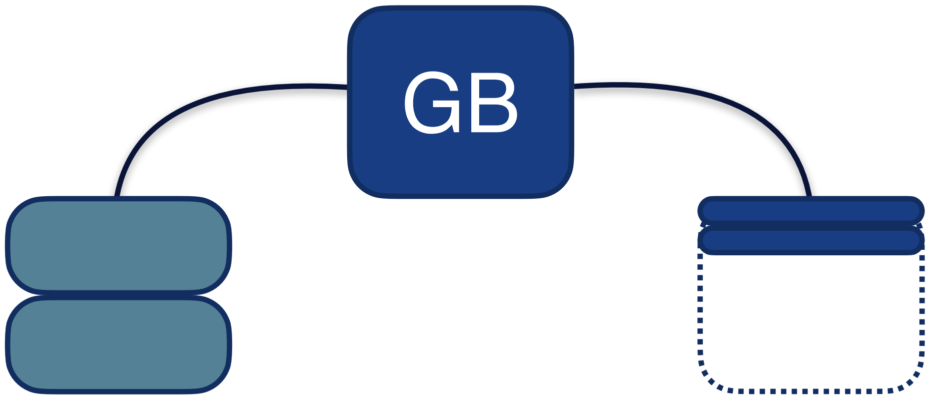



GB


GB


GB


GB


GB

SUMMING UP

- We present a general framework capable of analysing weight-functions, and show that there are advantages of using different weights in the lottery.
- The paper is available: https://eprint.iacr.org/2020/328
- Thank you for your attention!

CONCORDIUM