PAC-Learning & Monitoring

How machine learning could help runtime verification.

Kaushik | Konstantin | Mahyar | Tom

A high-level overview.

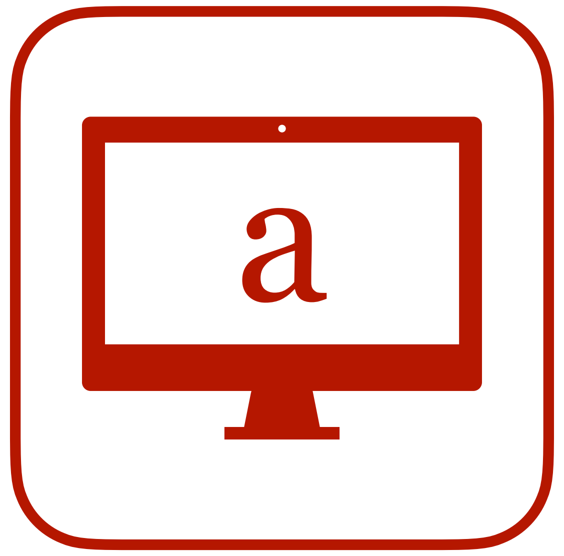
Focus on problems, not results.

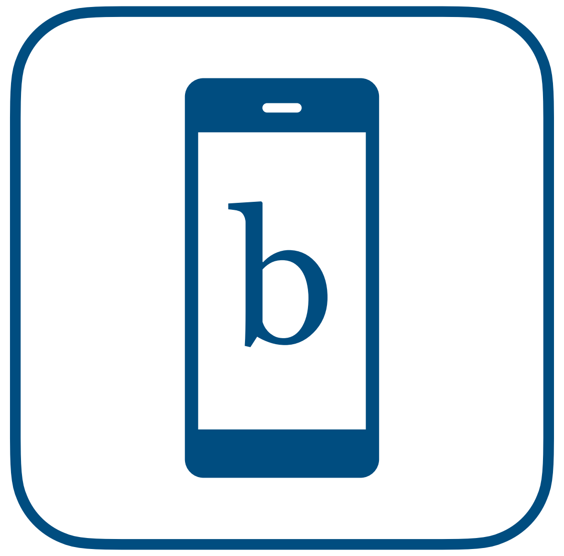
Formal Verification.

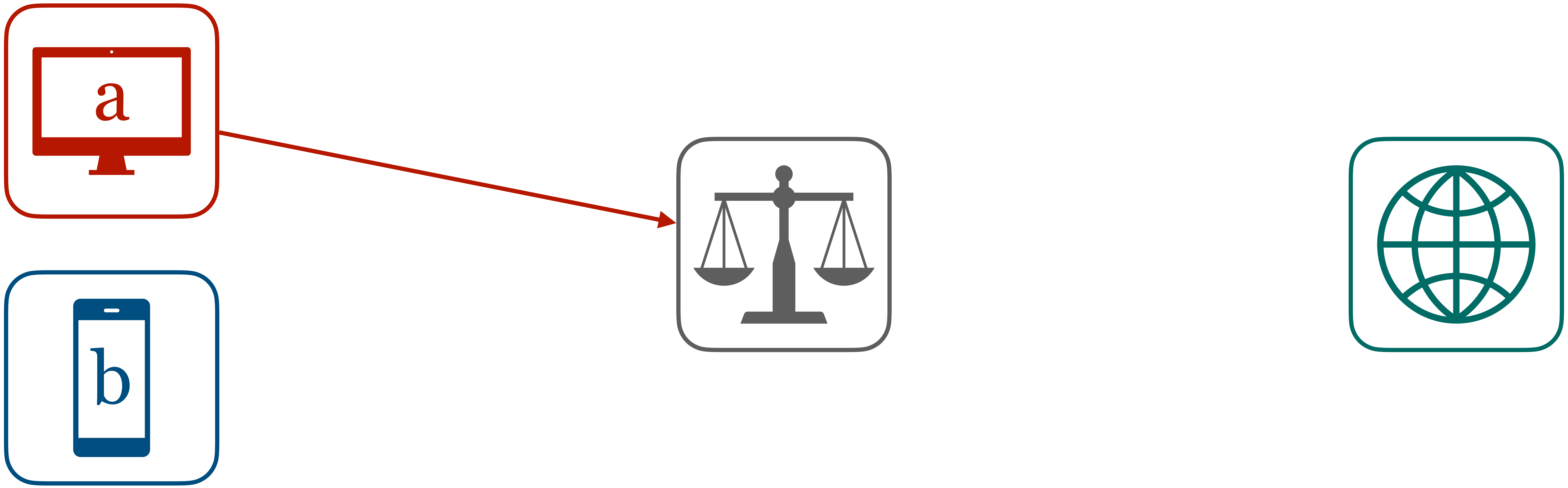
Proving the correctness of a system.

Monitoring.

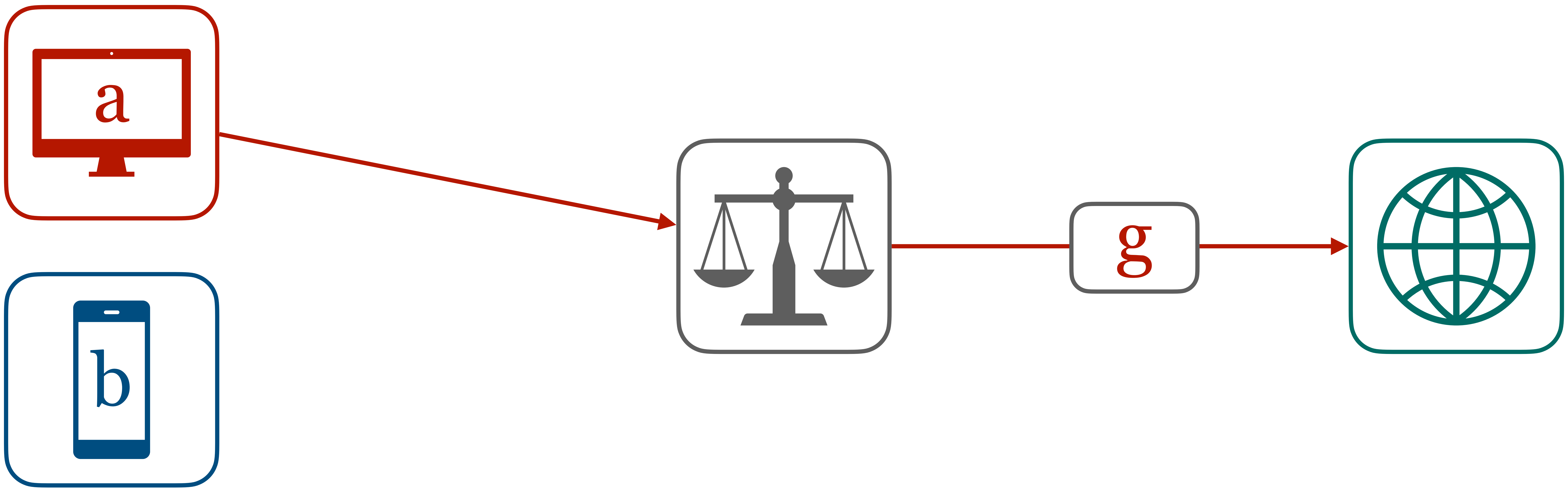
Proving the correctness of a system on a particular run at runtime.


a

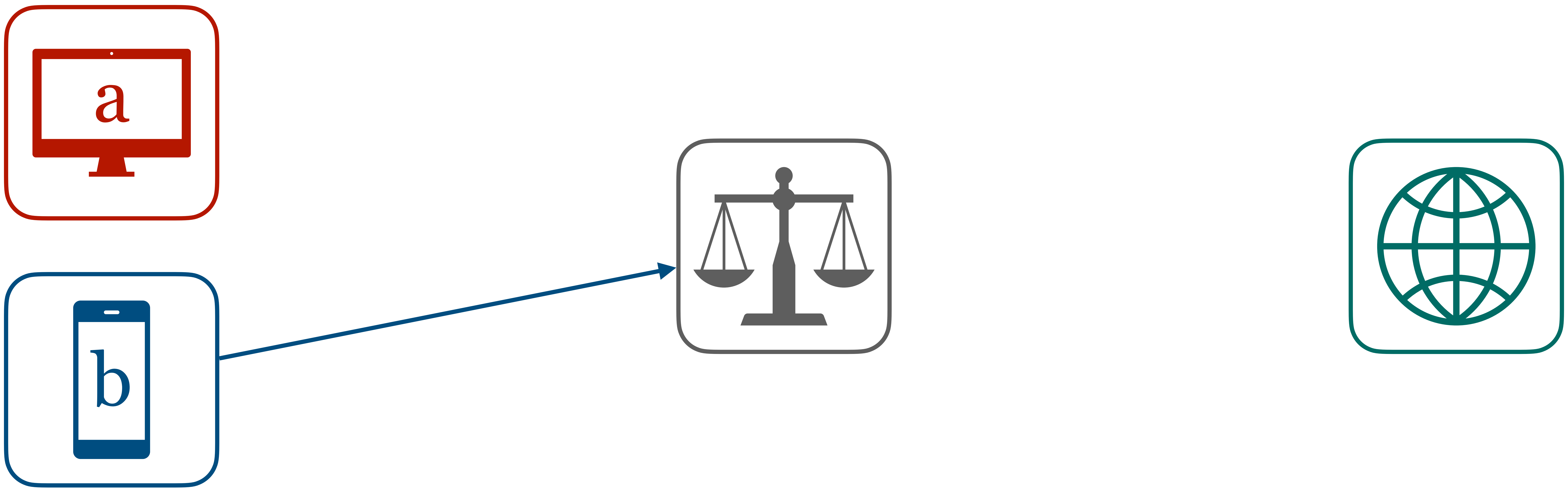

b



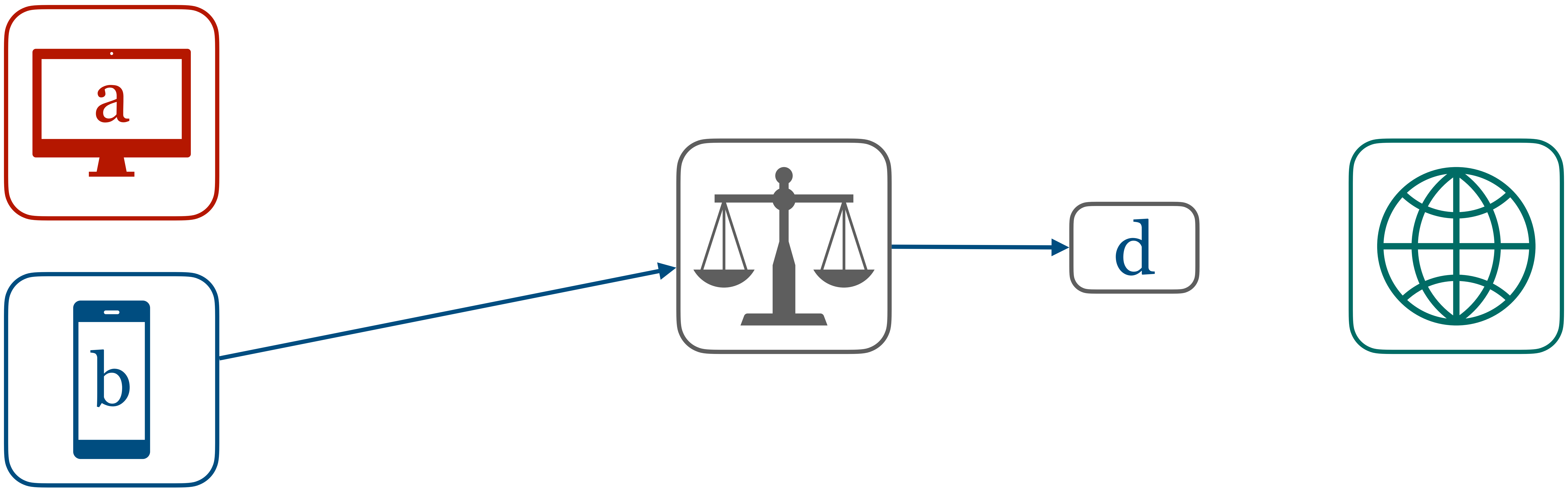
a



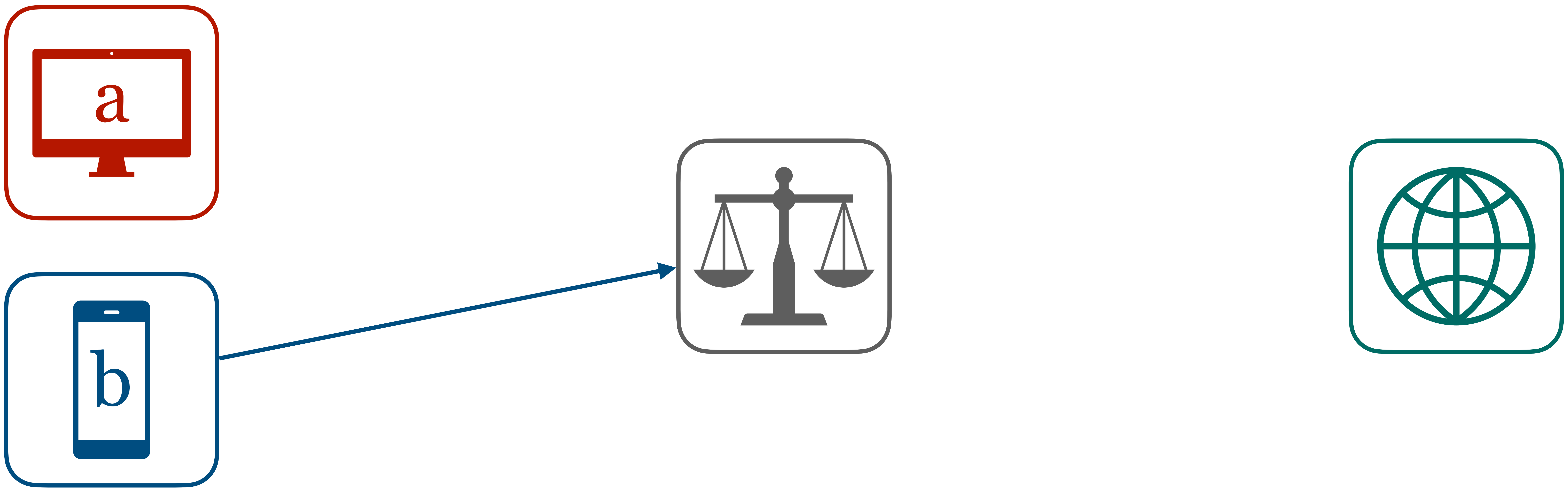
a g



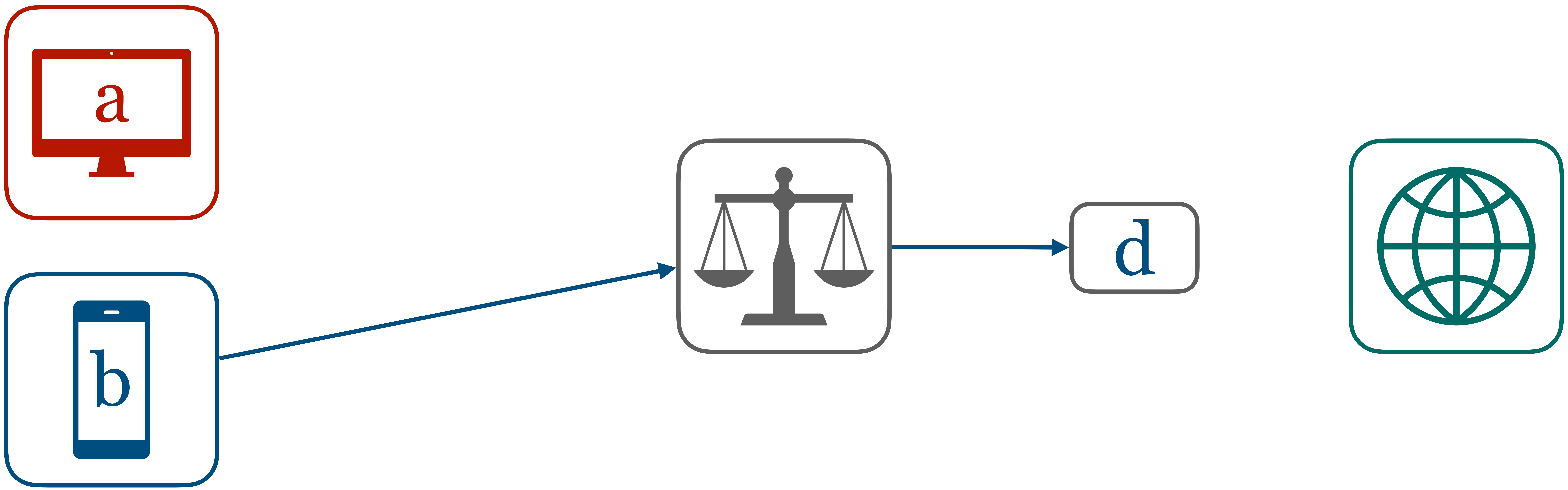
a g b



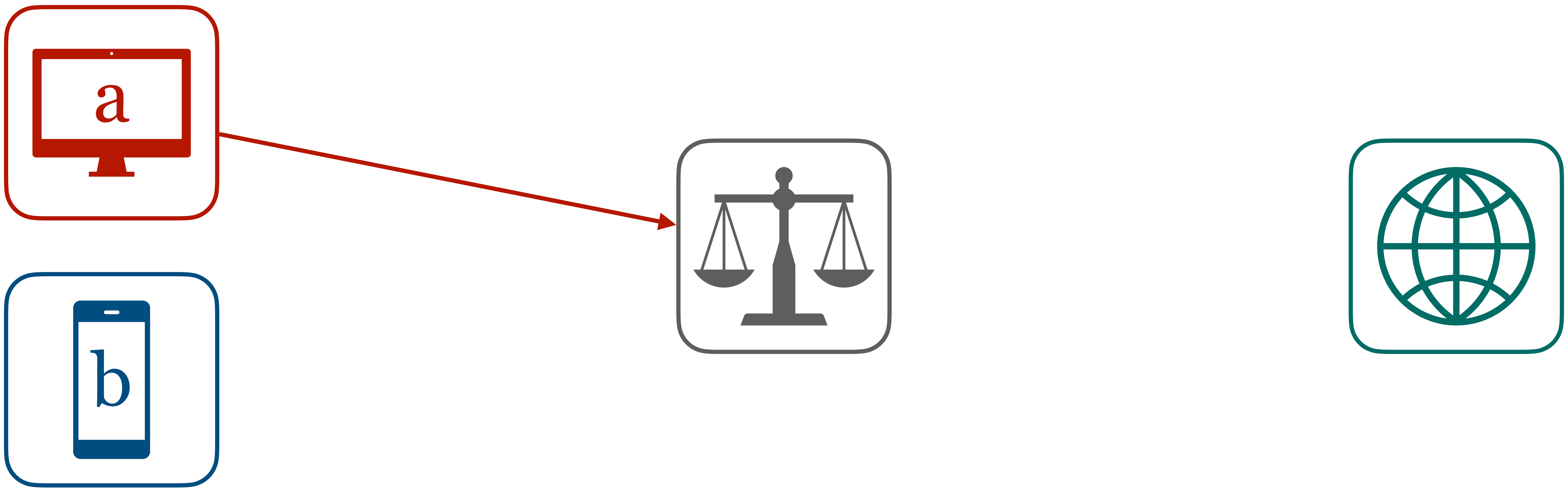
a g b d



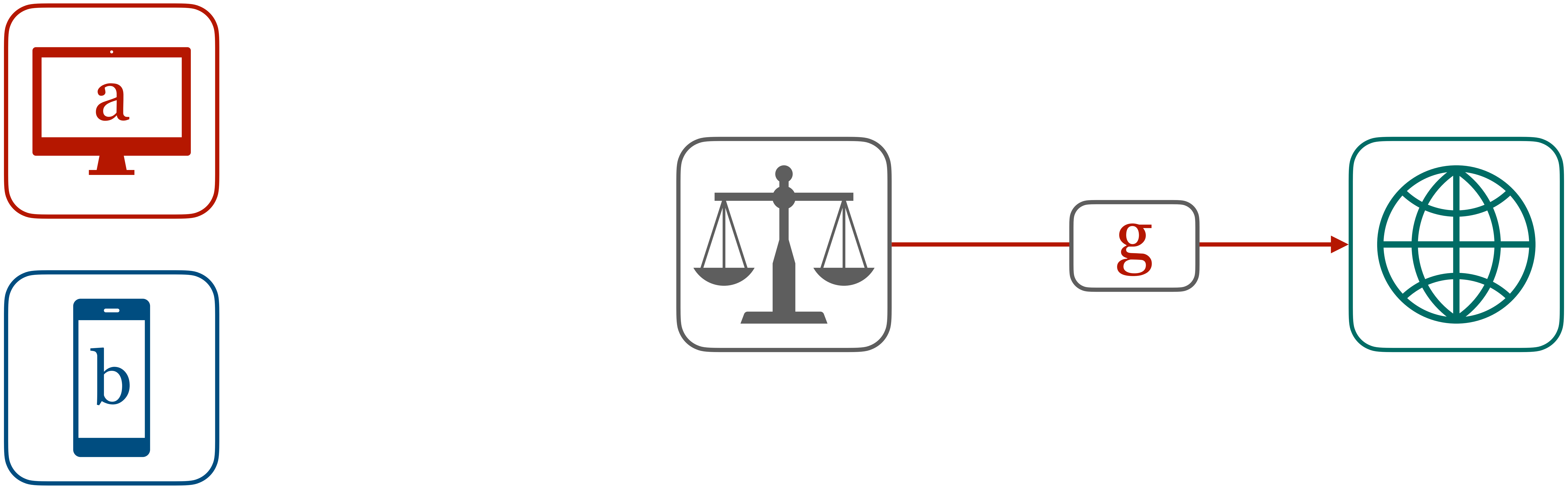
a g b d b



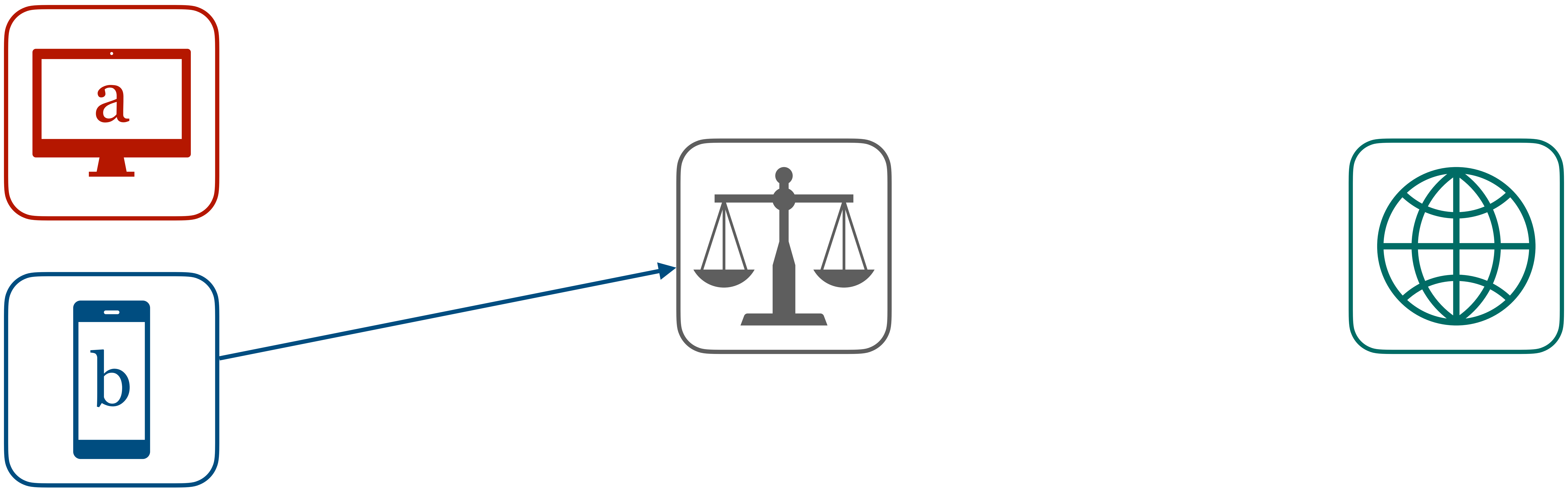
a g b d b d



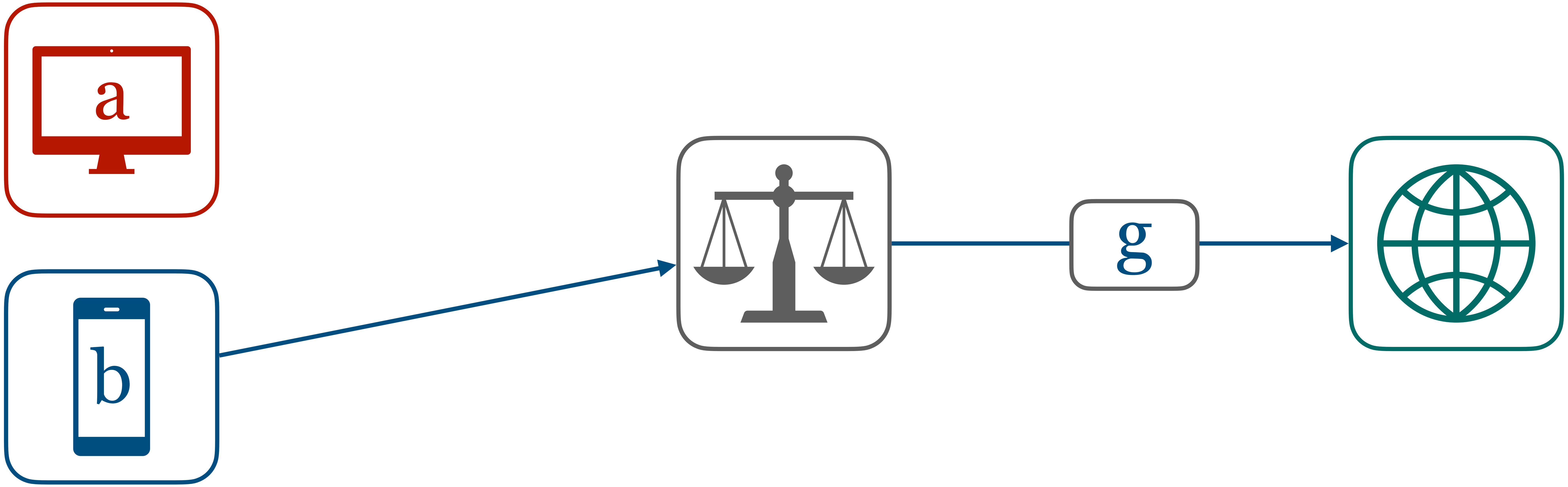
a g b d b d a



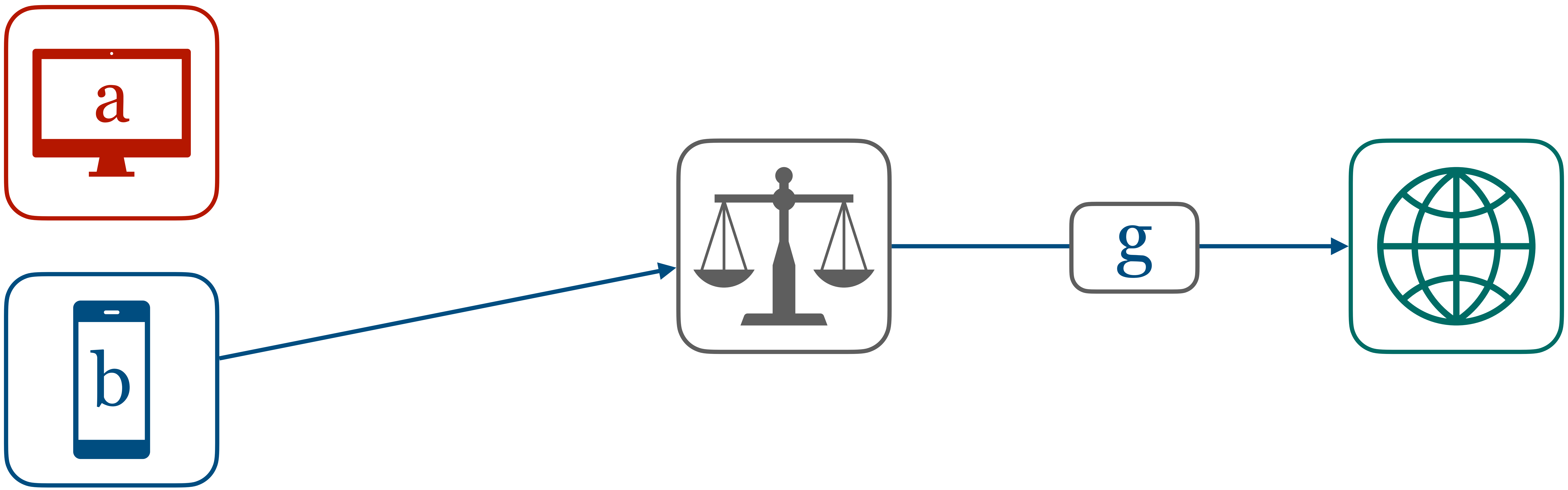
a g b d b d a g



a g b d b d a g b



a g b d b d a g b g



a g b d b d a g b g . . . . . .

Property

$\varphi \subseteq \Sigma^\omega$

a g b d b d a g b g . . . . . .

Property

$\varphi \subseteq \Sigma^\omega$

Monitor

$\mathscr{A} : \Sigma^* \to \{0,1,?\}$

a g b d b d a g b g . . . . . .

Property

$\varphi \subseteq \Sigma^\omega$

Monitor

$\mathscr{A} : \Sigma^* \to \{0,1,?\}$

$w \in \Sigma^\omega, u \prec w :$

a g b d b d a g b g . . . . . .

Property

$$\varphi \subseteq \Sigma^\omega$$

Monitor

$$\mathscr{A} : \Sigma^* \to \{0,1,?\}$$

$$w \in \Sigma^\omega, u \prec w:$$

$$\mathscr{A}(u) = 0 \Rightarrow w \notin \varphi$$

a g b d b d a g b g . . . . . .

Property

$\varphi \subseteq \Sigma^\omega$

Monitor

$\mathscr{A} : \Sigma^* \to \{0,1,?\}$

$w \in \Sigma^\omega, u \prec w:$

$\mathscr{A}(u) = 0 \Rightarrow w \notin \varphi$

$\mathscr{A}(u) = 1 \Rightarrow w \in \varphi$

a g b d b d a g b g . . . . . .

Monitorability.

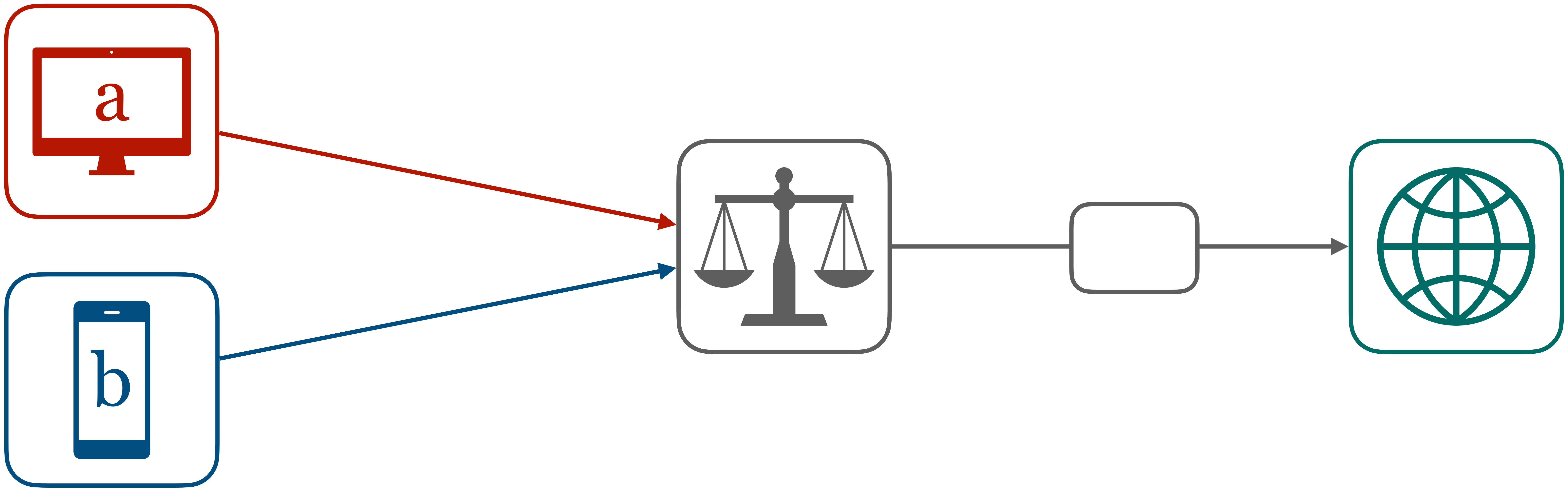
If every infinite string has a point, where the monitor can stop watching.

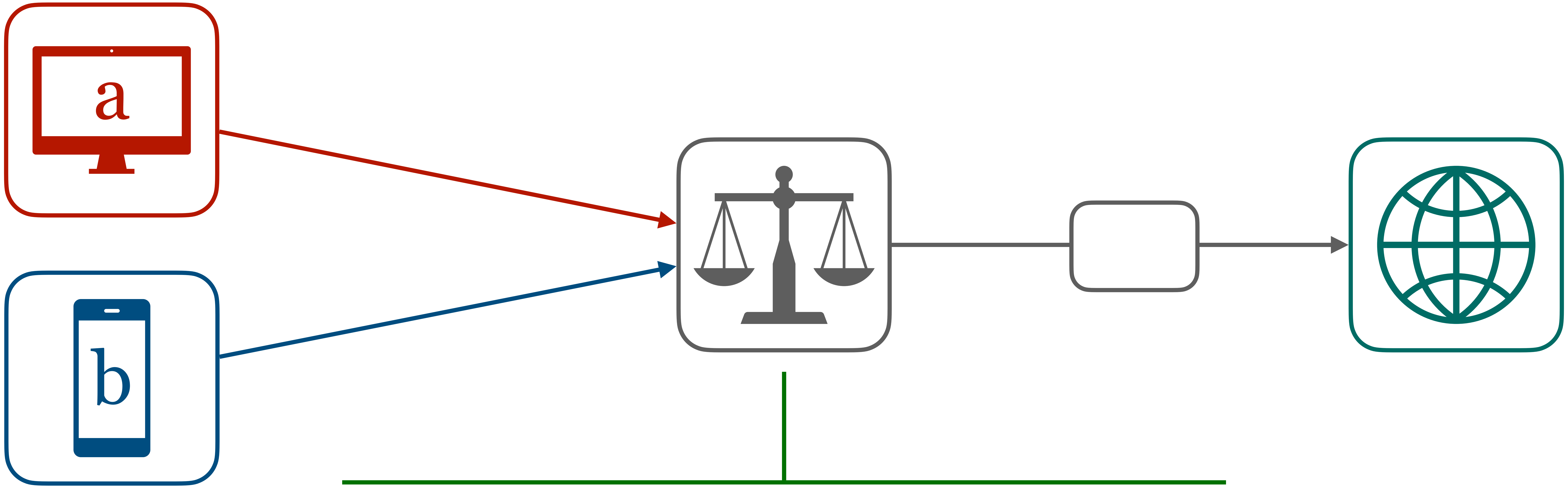
Fairness Properties

From formal methods to machine learning.

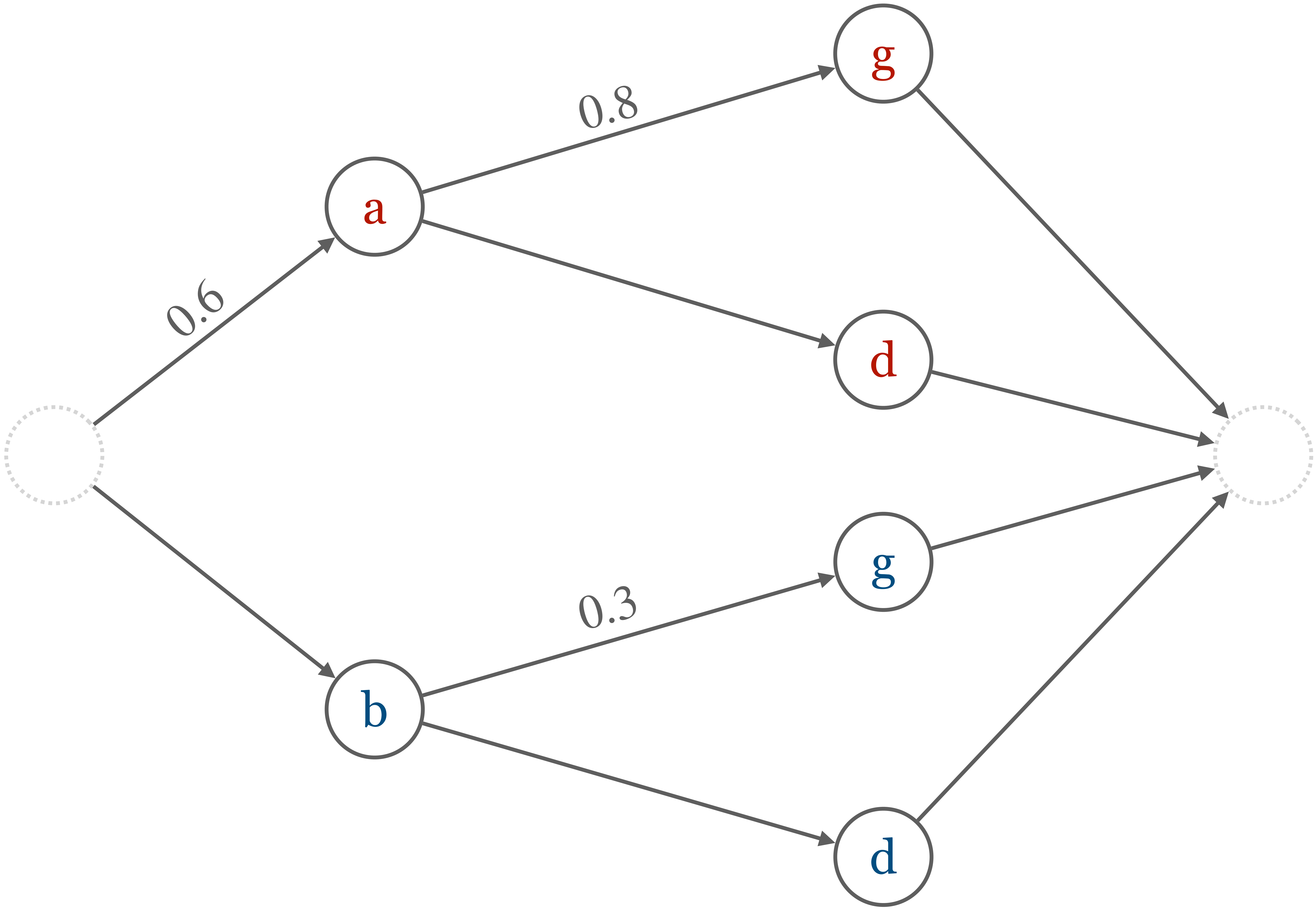
$$(\Box\Diamond a \rightarrow \Box\Diamond g) \land (\Box\Diamond b \rightarrow \Box\Diamond g)$$

Fairness in Formal Methods


a
b



Memoryless & Probabilistic


0.8
0.6
0.3
g
a
d
g
b
d

$$(\Box\Diamond a \rightarrow \Box\Diamond g) \wedge (\Box\Diamond b \rightarrow \Box\Diamond g)$$

$$(\Box\Diamond a \to \Box\Diamond g) \land (\Box\Diamond b \to \Box\Diamond g)$$

$$\downarrow$$

$$\mathbb{P}(g \mid a) > 0 \land \mathbb{P}(g \mid b) > 0$$

$$(\Box\Diamond a \to \Box\Diamond g) \wedge (\Box\Diamond b \to \Box\Diamond g)$$

$$\downarrow$$

$$\mathbb{P}(g \mid a) > 0 \wedge \mathbb{P}(g \mid b) > 0$$

$$\downarrow$$

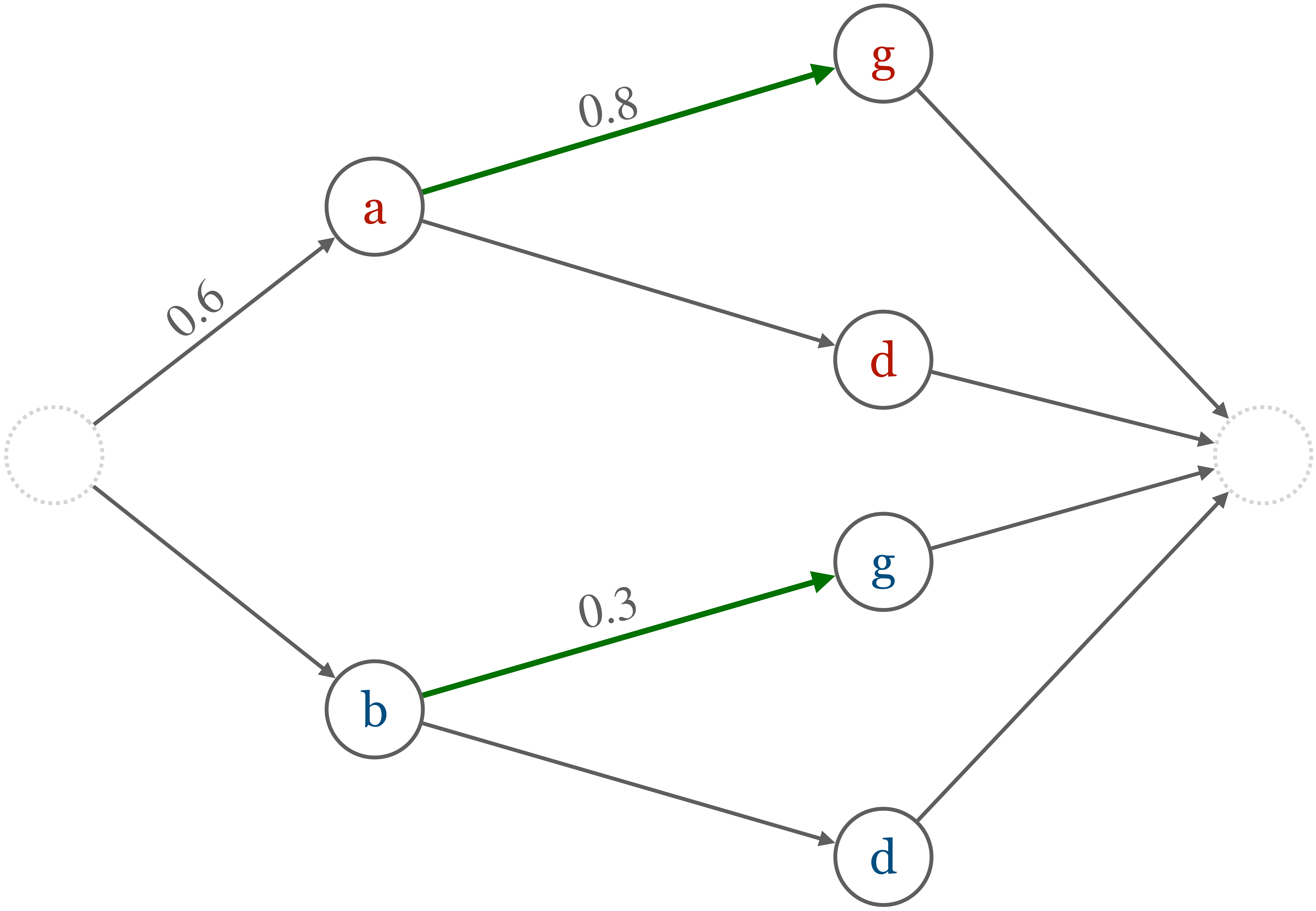
$$\mathbb{P}(g \mid a) - \mathbb{P}(g \mid b)$$

$$\mathbb{P}(g \mid a) - \mathbb{P}(g \mid b)$$

Fairness in Machine Learning

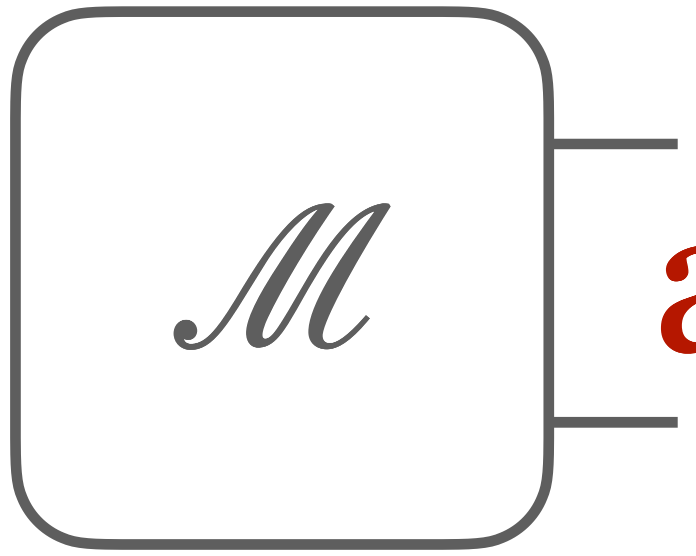
Monitorability.

Can we estimate the property from observations?

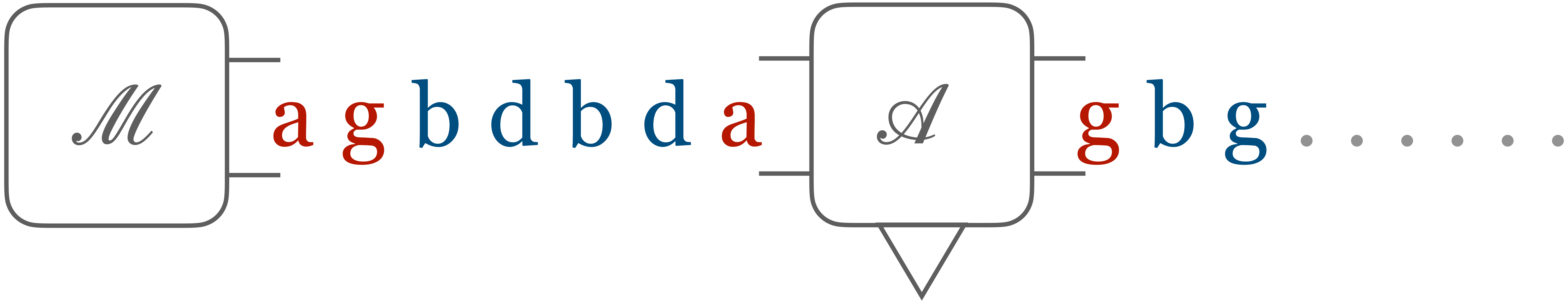

0.8
0.6
0.3
g
a
d
g
b
d

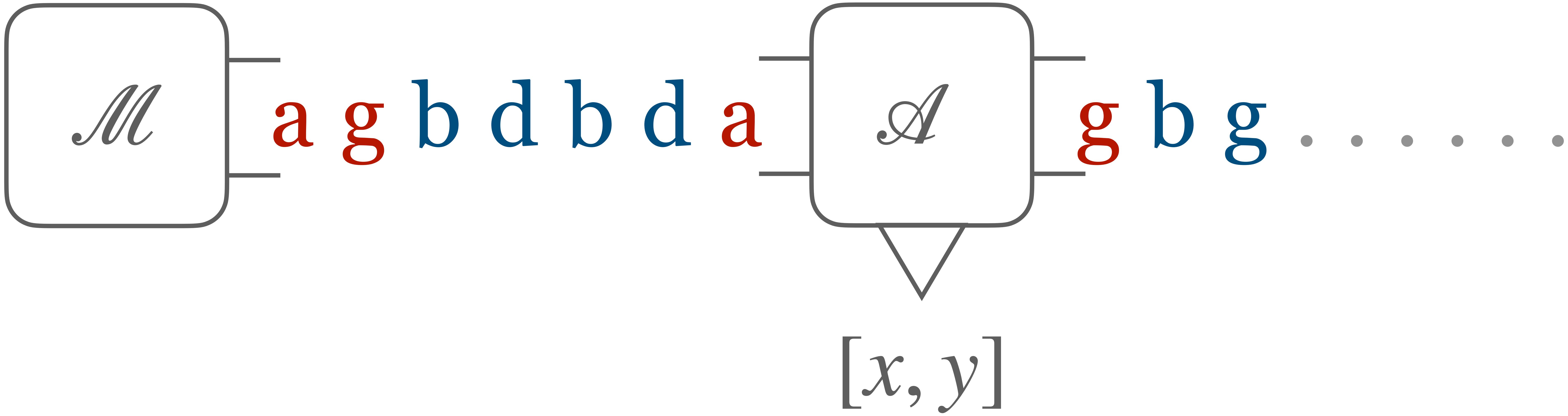
General Idea.

We observe a Markov chain and at every time step the monitor provides PAC-style guarantees.



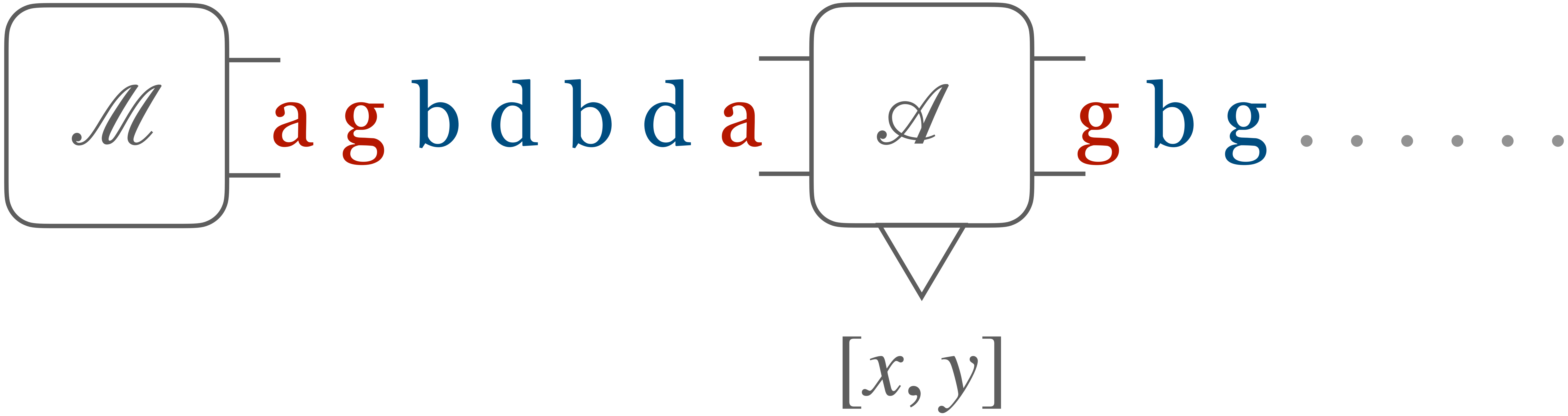
a g b d b d a g b g . . . . . .


$\mathscr{M}$
a g b d b d a
$\mathscr{A}$
g b g



$\mathscr{M}$
a g b d b d a
$\mathscr{A}$
g b g . . . . . .
$[x, y]$

$$\mathbb{P}(g \mid a) - \mathbb{P}(g \mid b) \in [x, y] \text{ with probability } 1 - \delta$$



Problem Statement

Let's be slightly more general.

Let $M \in \Delta(N-1)^N$,

Let $M \in \Delta(N-1)^N$, $W \sim (M, q_0)$

Let $M \in \Delta(N-1)^N$, $W \sim (M, q_0)$ and $U \prec W$.

Let $M \in \Delta(N-1)^N$, $W \sim (M, q_0)$ and $U \prec W$. Given a function $f : \Delta(N-1)^N \to \mathbb{R}$, Let $M \in \Delta(N-1)^N$, $W \sim (M, q_0)$ and $U \prec W$. Given a function $f : \Delta(N-1)^N \to \mathbb{R}$, find a monitor $\mathscr{A} : [N]^* \to \mathbb{R}^2$ such that:

Let $M \in \Delta(N-1)^N$, $W \sim (M, q_0)$ and $U \prec W$. Given a function $f : \Delta(N-1)^N \to \mathbb{R}$, find a monitor $\mathscr{A} : [N]^* \to \mathbb{R}^2$ such that:

$$\mathbb{P}(f(M) \in \mathscr{A}(U)) \geq 1 - \delta$$

(Obviously we want the bounds to be as tight as possible.)

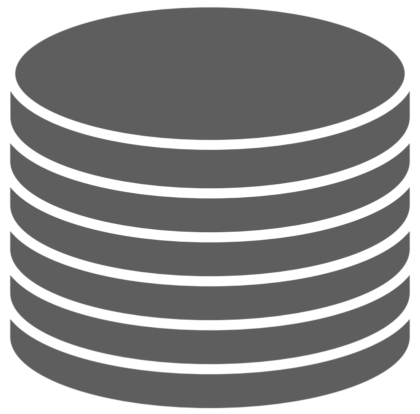
Tradeoffs.

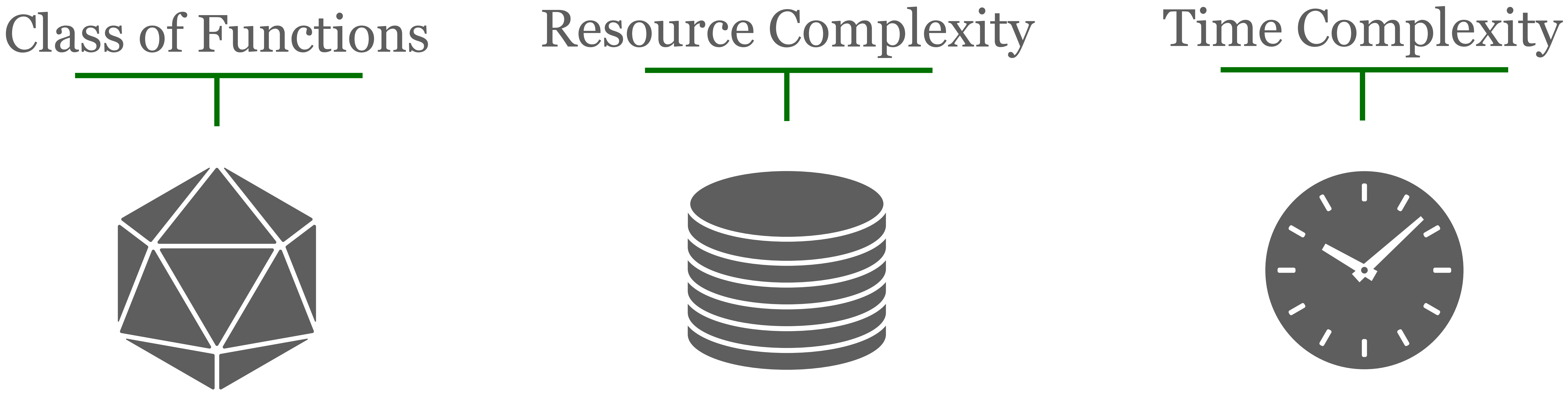
We want to map the problem across four dimensions

Class of Functions

Class of Functions

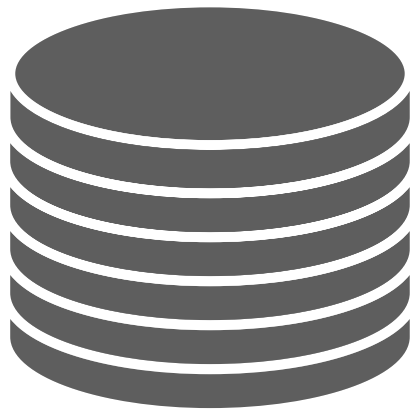
Resource Complexity




Class of Functions
Resource Complexity
Time Complexity

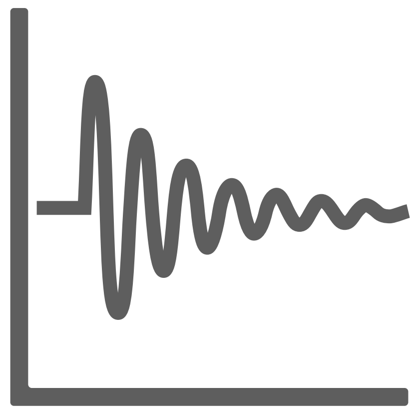
Class of Functions

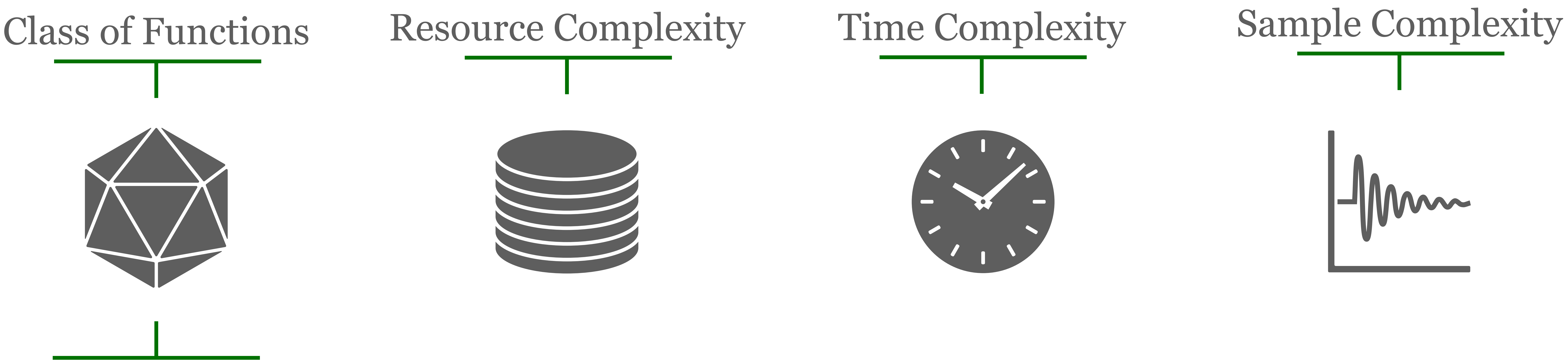
Resource Complexity



Time Complexity

Sample Complexity

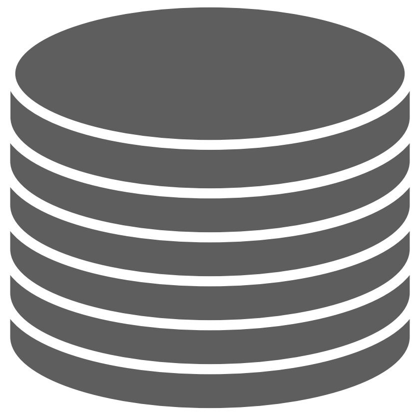




How does the class of functions influence
the complexities, e.g. (in)dependent sums over M,
polynomials over M (and/or the eigenvector of M).

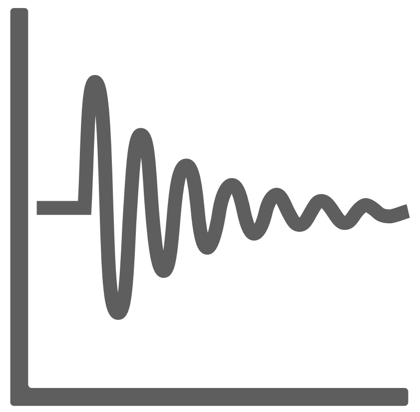
Class of Functions

Resource Complexity



Time Complexity

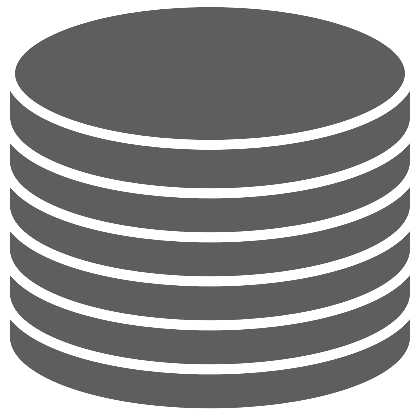
Sample Complexity



What is the minimal number of registers?
(w.r.t. time/sample complexity)

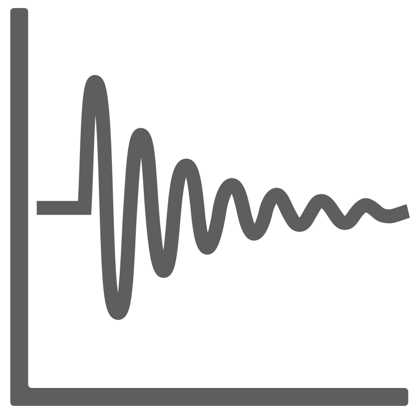
Class of Functions

Resource Complexity



Time Complexity

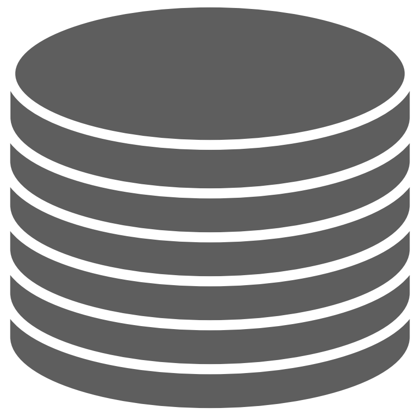
Sample Complexity



What is the minimal computation time?
(w.r.t. resource/sample complexity)

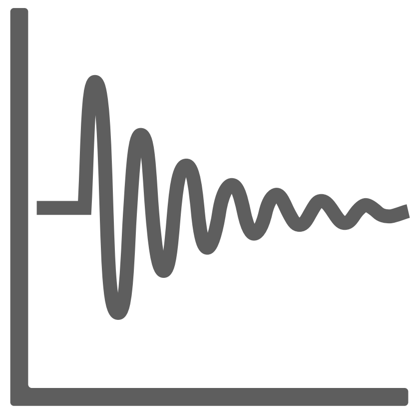
Class of Functions

Resource Complexity



Time Complexity

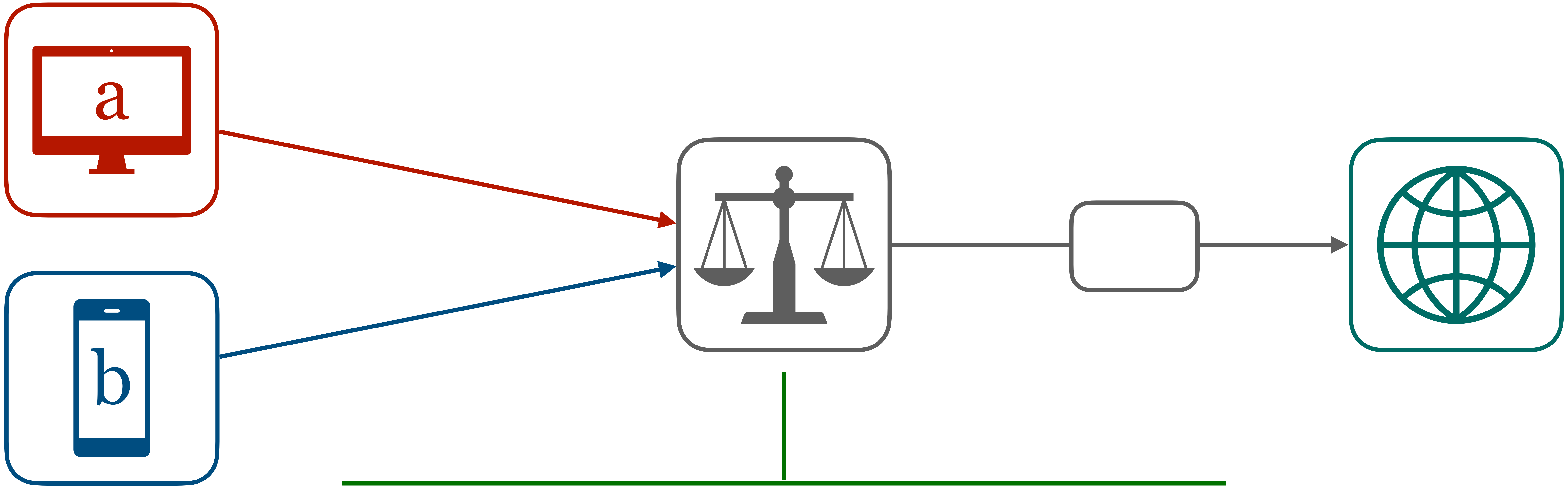
Sample Complexity



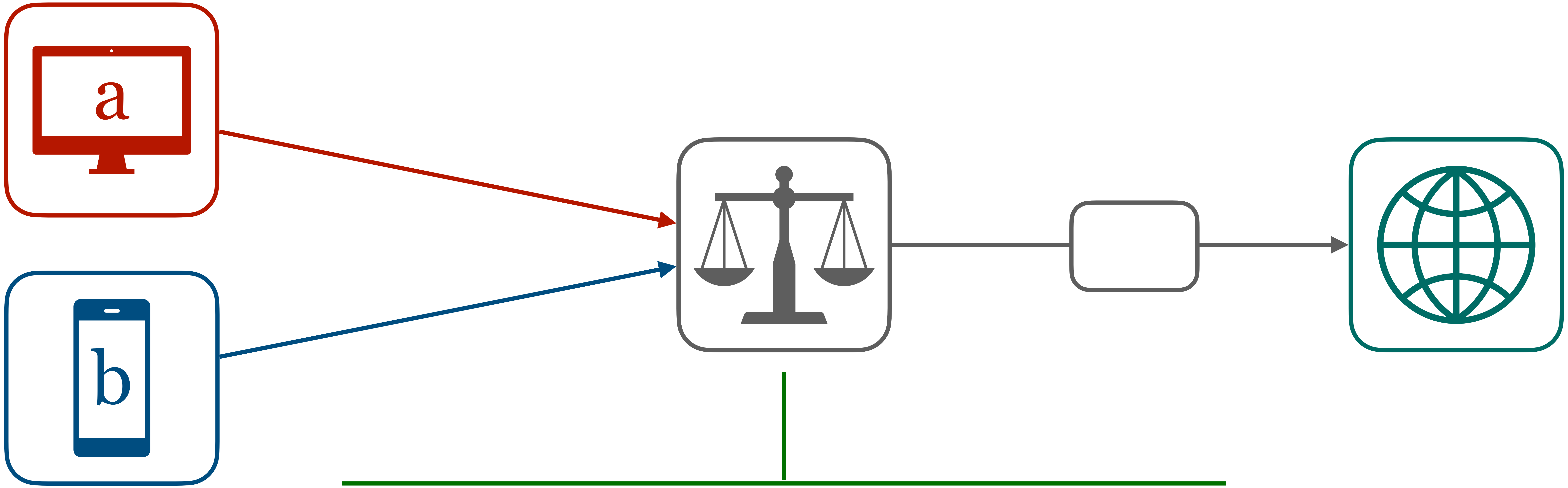
What is the rate at which the interval shrinks?
(w.r.t. resource/time complexity)

But wait, there is more.

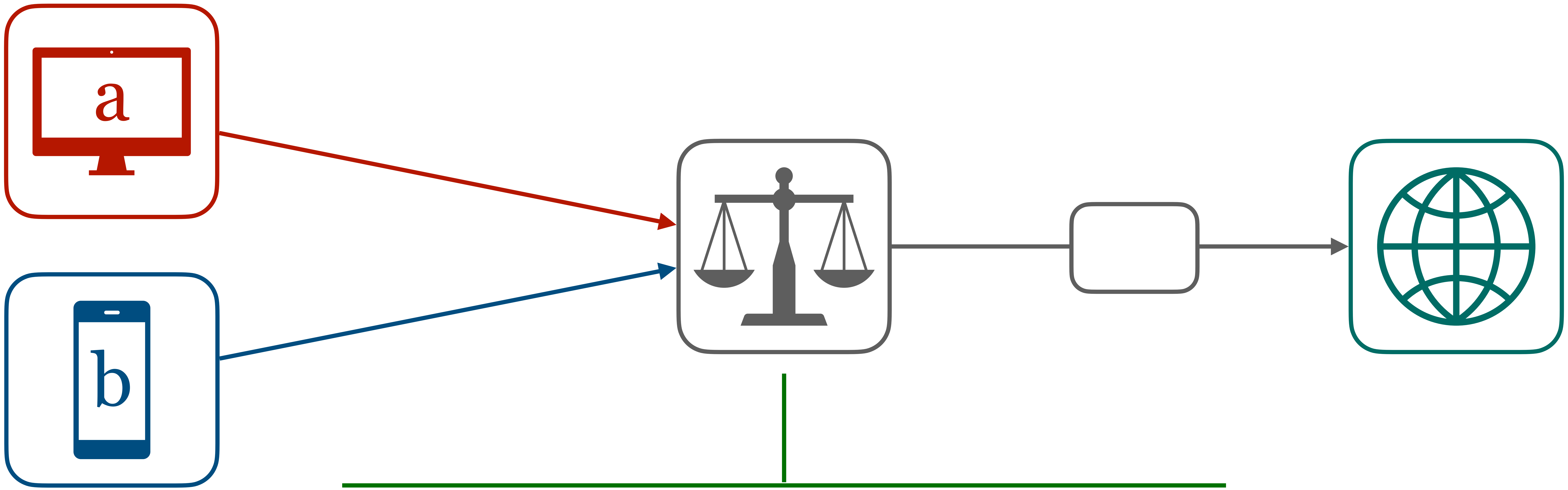
What if the system is more complex?



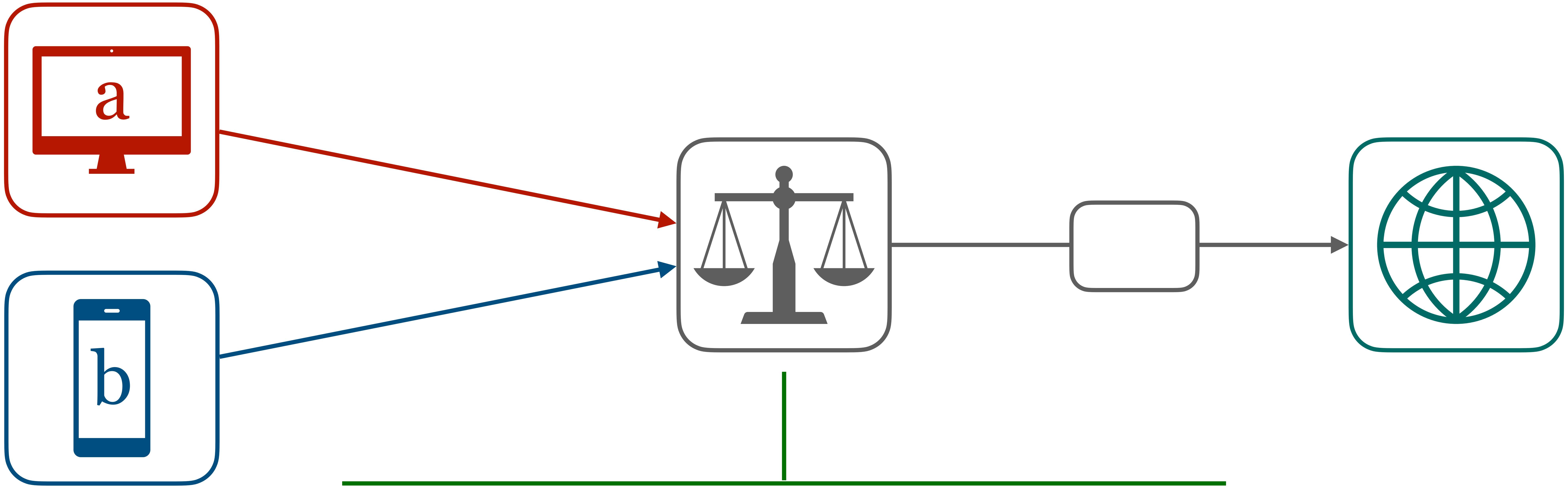
Remembers the last k-decisions.



Remembers some arbitrary
k-decisions.



The policy changes at each time step,
in a deterministic or probabilistic manner.



The decisions are corrupted
or partially hidden.

And many more.

From our perspective there is a lot we don't know.
It seems closely related to the concentration of functions over random variables with various dependencies.

What we did …

… so far.

(Almost) arbitrary *arithmetic expressions* over *transition probabilities* of Markov chains.

(Almost) arbitrary *arithmetic expressions* over *transition probabilities* of Markov chains.

Efficient computation of *expectation* of arbitrary *polynomials* over *transition probabilities* of Markov chains in a *Bayesian* setting using a Dirichlet prior.

(Almost) arbitrary *arithmetic expressions* over *transition probabilities* of Markov chains.

Efficient computation of *expectation* of arbitrary *polynomials* over *transition probabilities* of Markov chains in a *Bayesian* setting using a Dirichlet prior.

Weighted sums over *transition probabilities* of *time-inhomogeneous* Markov chains with *linear* and *observed change* in transition probabilities.

Is this interesting to you?

Let us know! (^_^)