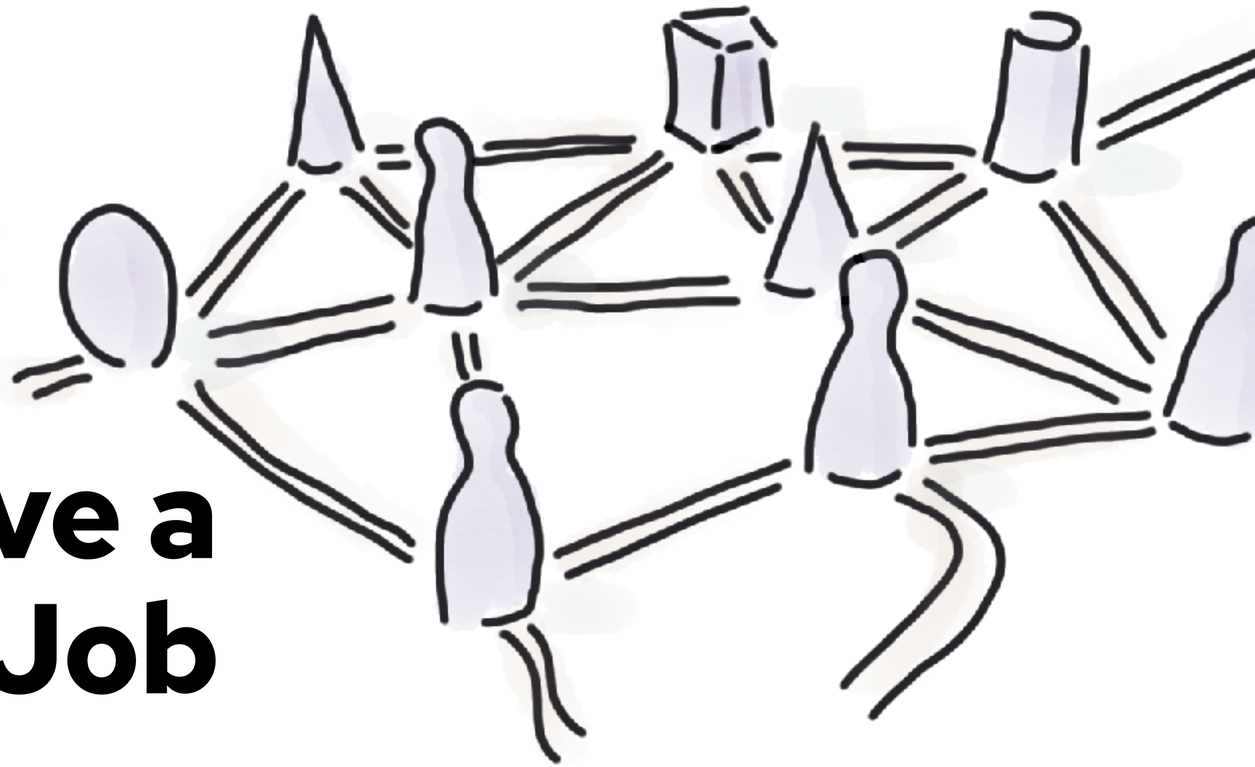
Things You Thought You Didn't Need To Care About That Have a Big Impact On Your Job



Holly Cummins

IBM

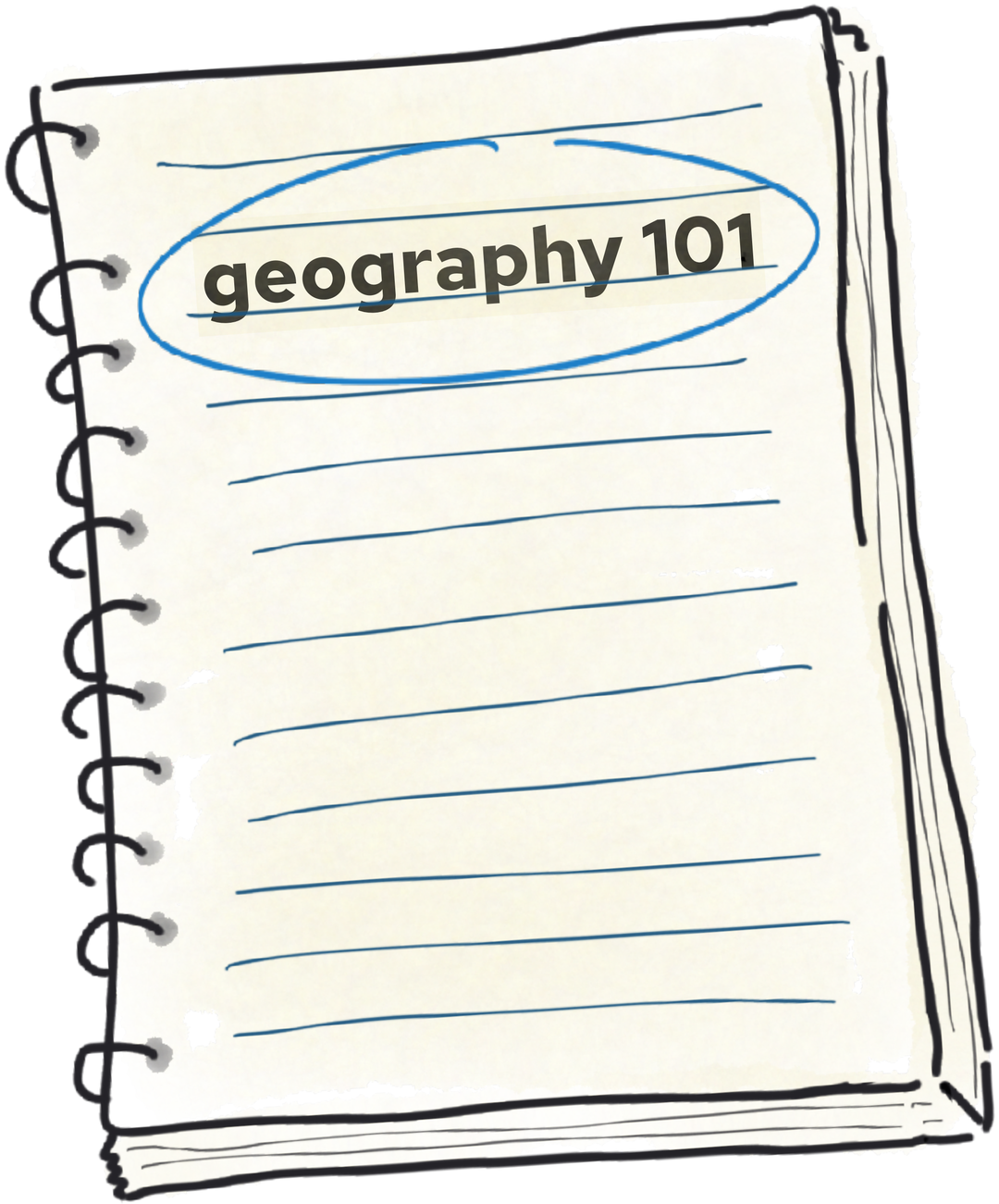
invisible forces shaping your job

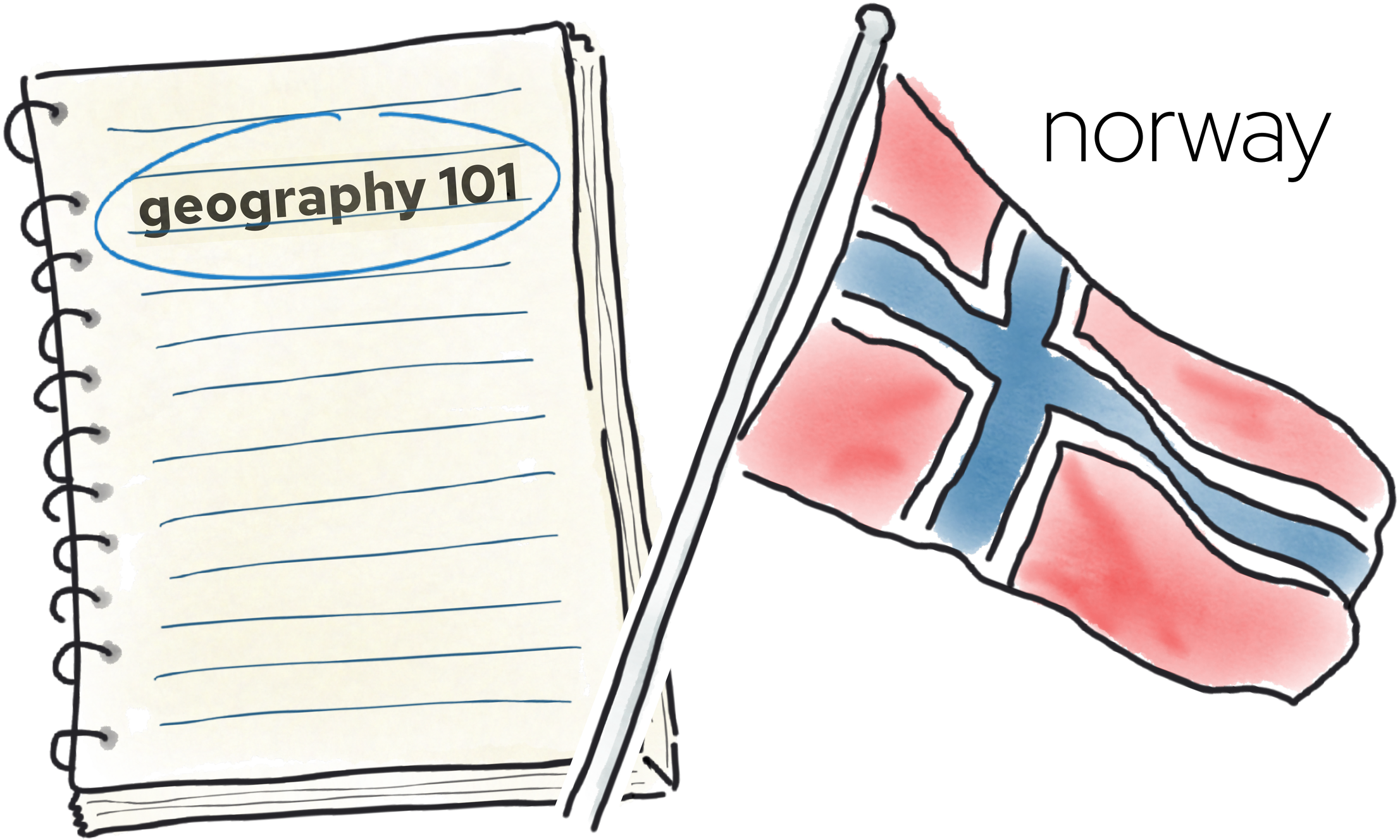


why is everything hard?



why are computers terrible?


geography 101


geography 101
norway

```
ski_regions:
```

```
ski_regions:
  - fr
```

```
ski_regions:
  - fr
  - ch
```

```
ski_regions:
  - fr
  - ch
  - se
```

```
ski_regions:
   - fr
   - ch
   - se
   - no
```

```
ski_regions:
  - fr
  - ch
  - se
  - no
```



```
ski_regions:
  - fr
  - ch
  - se
  - no
```

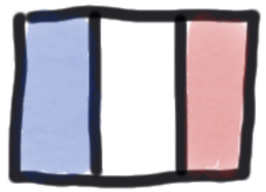


```
{"ski_regions": [    ,        ,       ,          ]}
```

```
ski_regions:
  - fr
  - ch
  - se
  - no
```

↓

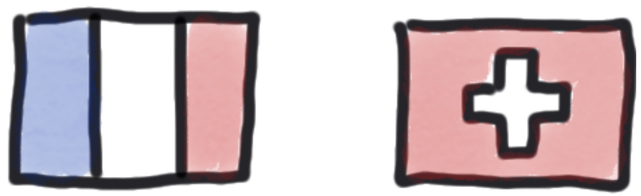
```
{"ski_regions": ["fr",      ,      ]}
```



```
ski_regions:
  - fr
  - ch
  - se
  - no
```



```
{"ski_regions": ["fr", "ch",      ,      ]}
```



```
ski_regions:
  - fr
  - ch
  - se
  - no
```

↓

```
{"ski_regions": ["fr", "ch", "se",      ]}
```



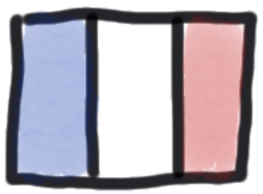
```
ski_regions:
  - fr
  - ch
  - se
  - no
```

↓

```
{"ski_regions": ["fr", "ch", "se", false]}
```



- no



false







sensible decision had
bad outcome



how can we know what outcomes our decisions will have?

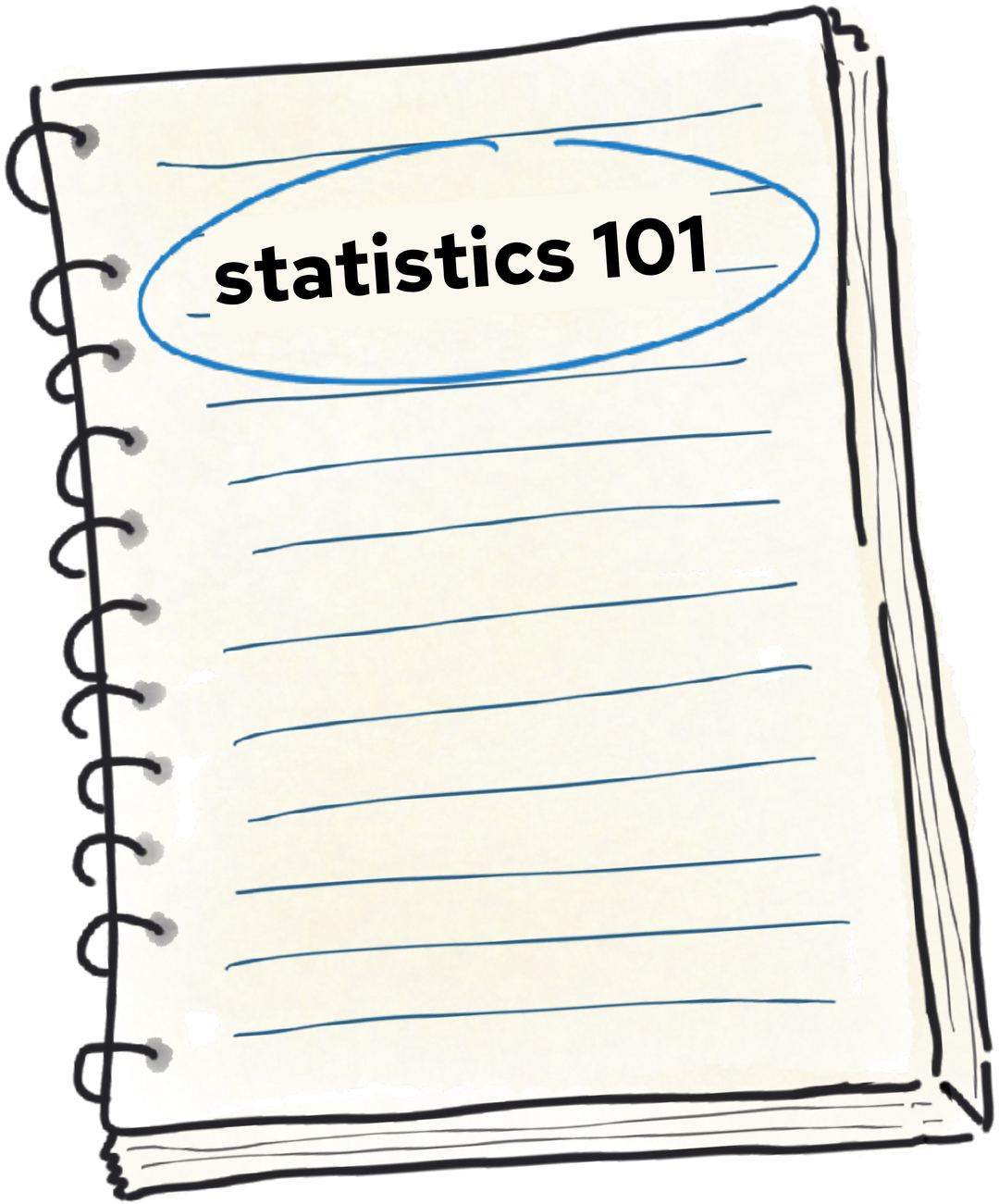


how can we make decisions in a complex world?

systems thinking



how can we make decisions in an uncertain world?


statistics 101

what do you call a
statistician who lives
in san francisco?




geography 201

what do you call a statistician who lives in san francisco?



what do you call a statistician who lives in san francisco?

a data scientist.

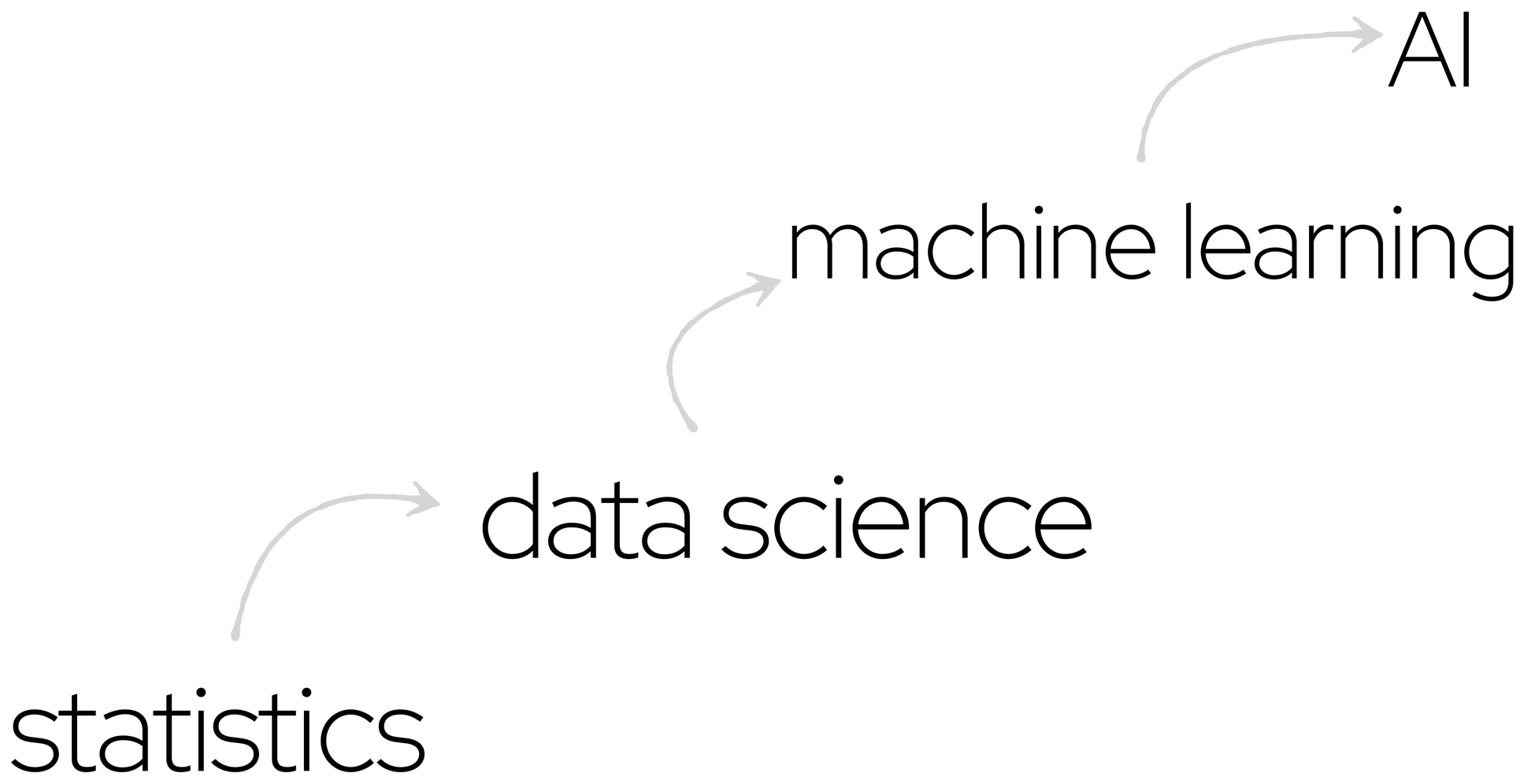


statistics

data science

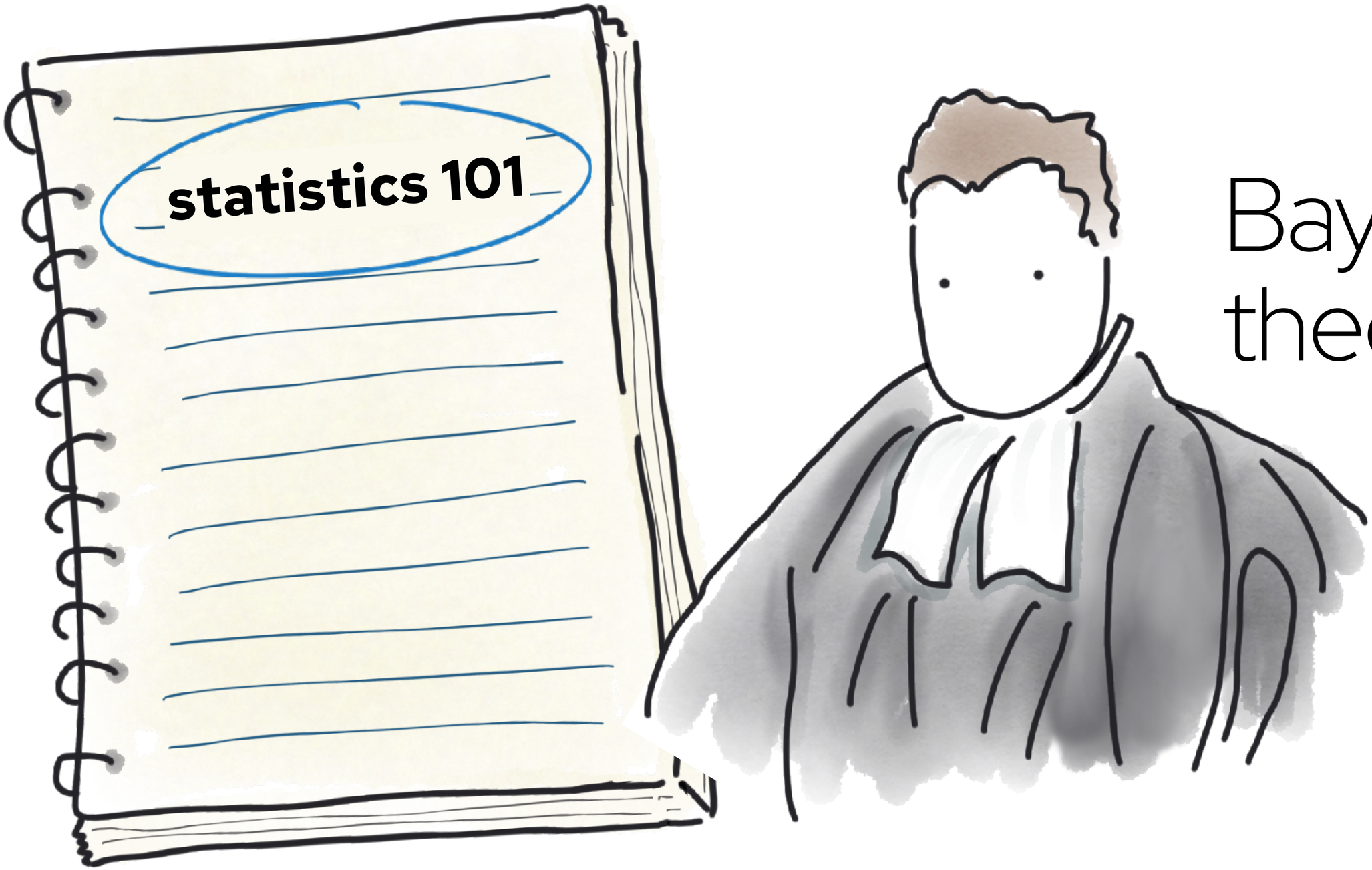
statistics


machine learning
data science
statistics


AI
machine learning
data science
statistics

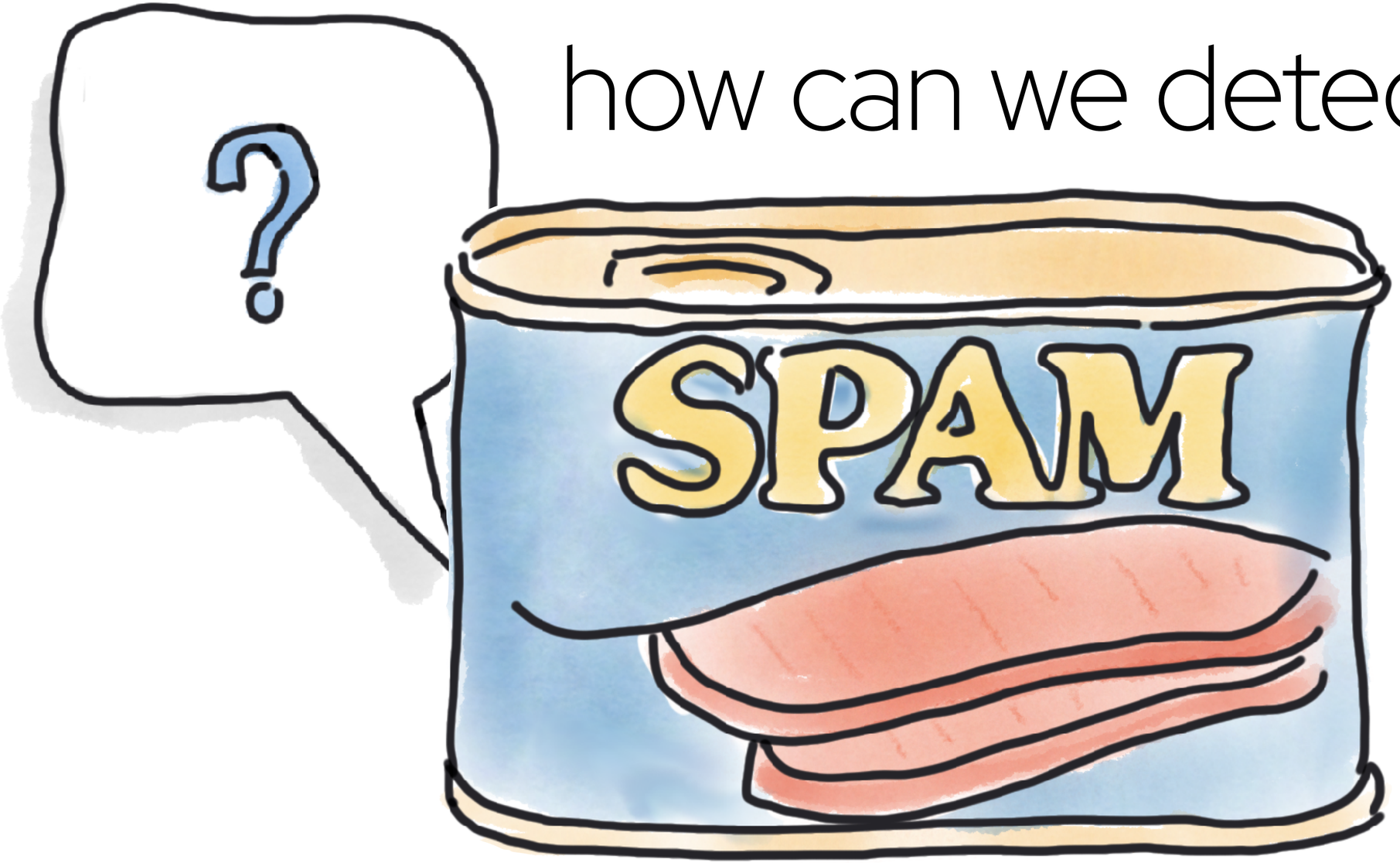


even if you're not doing AI,
statistics is important

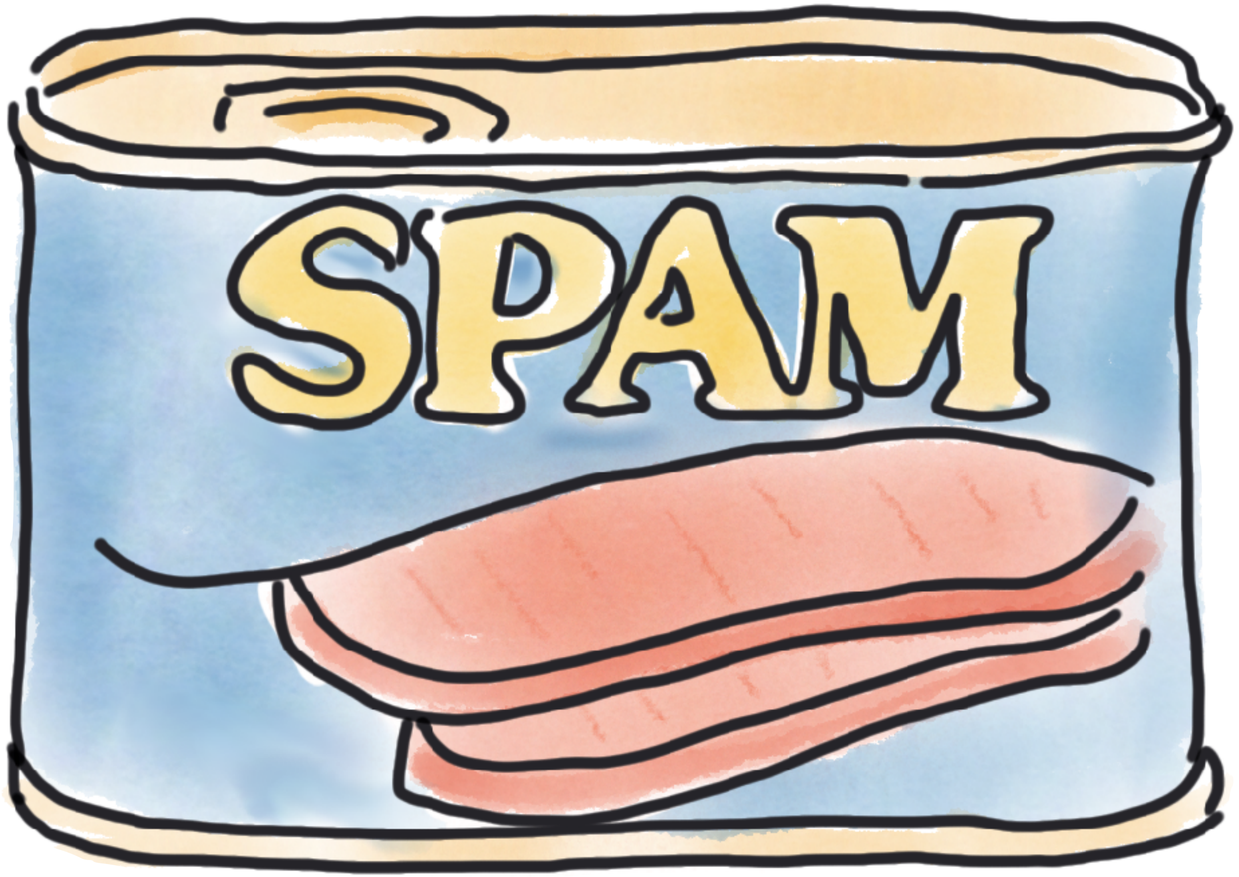


Bayes' theorem

how can we detect spam?



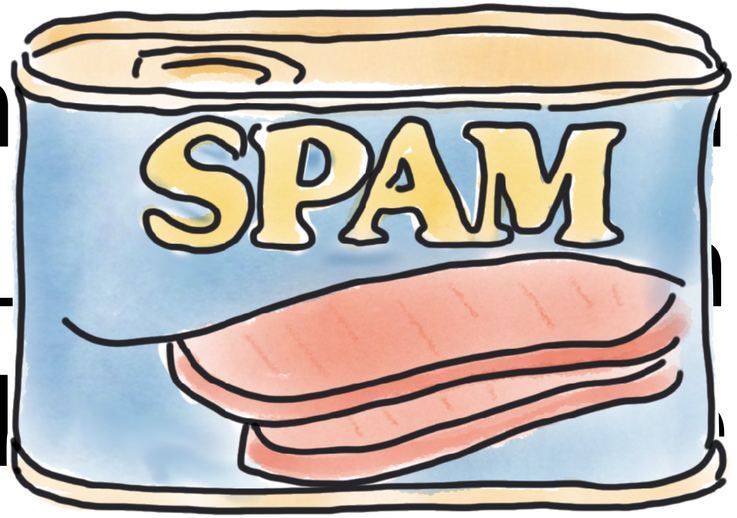
"spamicity"



Exciting offer just for you!
Deep discounts on Viagra.
Limited time offer, act now.

Exciting offer just for you!
Deep discounts on Viagra.
Limited time offer, act now.

Exciting offer just for you!
Deep discounts on Ozempic.
Limited time offer, act now.

Excitin 

st for you!
Deep di n Ozempic.
Limited r, act now.

banned-words:

```
banned-words:
  - Ozempic
```

```
banned-words:
  - Ozempic
```

```
banned-words:
  - Ozempic
```

Exciting offer just for you!
Deep discounts on Ozemp1c.
Limited time offer, act now.

Exciting offer just for you!
Deep discounts on 0zempic.
Limited time offer, act now.

Exciting offer just for you!
Deep discounts on Ozempick.
Limited time offer, act now.

```
banned-words:
```

```
banned-words:
  - Ozempic
```

```
banned-words:
  - Ozempic
  - Ozempick
```

```
banned-words:
  - Ozempic
  - Ozempick
  - Ozempik
```

```
banned-words:
  - Ozempic
  - Ozempick
  - Ozempik
  - 0zempic
```

```
banned-words:
  - Ozempic
  - Ozempick
  - Ozempik
  - 0zempic
  - Ozemp1c
```

```
banned-words:
  - Ozempic
  - Ozempick
  - Ozempik
  - 0zempic
  - Ozemp1c
  - Øzempic
```

```
banned-words:
  - Ozempic
  - Ozempick
  - Ozempik
  - 0zempic
  - Ozemp1c
  - Øzempic
  - 0zempick
```

```
banned-words:
  - Ozempic
  - Ozempick
  - Ozempik
  - 0zempic
  - Ozemp1c
  - Øzempic
  - 0zempick
  - …
```

```
banned-words:
  - Ozempic
  - Ozempick
  - Ozempik
  - 0zempic
  - Ozemp1c
  - Øzempic
  - 0zempick
  - …
```

Dear friend,
Exciting offer just for you! Deep discounts on Ozemp1c.
Limited time offer, act now.

Dear friend,
Exciting offer just for you! Deep discounts on Ozemp1c. Limited time offer, act now.

Hey Alice,
Are you still good for next week? We had drama yesterday because the dog threw up, on the clean dishes in the dishwasher! On the bright side, at least it was easy to clean. I started my Ozempic on Sunday, and so far so good. I can see my appetite is less already.

Dear friend,
Exciting offer just for you! Deep discounts on Ozemp1c.
Limited time offer, act now.

Hey Alice,
Are you still good for next week? We had drama yesterday because the dog threw up, on the clean dishes in the dishwasher! On the bright side, at least it was easy to clean. I started my Ozempic on Sunday, and so far so good. I can see my appetite is less already.

Dear friend,
Exciting offer just for you! Deep discounts on Ozemp1c.
Limited time offer, act now.

Hey Alice,
Are you still good for next week? We had drama yesterday because the dog threw up, on the clean dishes in the dishwasher! On the bright side, at least it was easy to clean. I started my Ozempic on Sunday, and so far so good. I can see my appetite is less already.

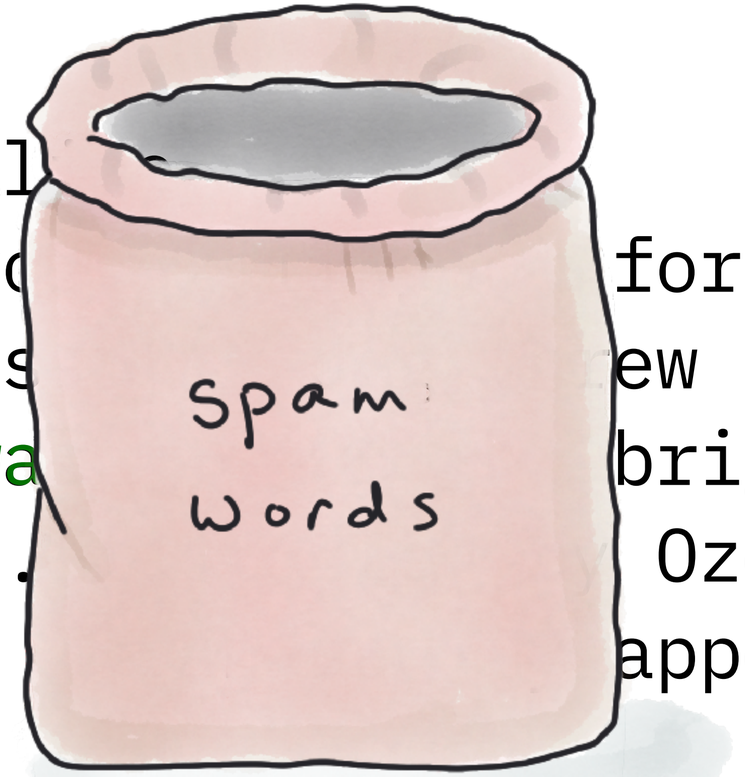
Dear friend,
Exciting offer just for you! Deep discounts on Ozemp1c.
Limited time offer, act now.

Hey Alice,
Are you still good for next week? We had drama yesterday because the dog threw up, on the clean dishes in the dishwasher! On the bright side, at least it was easy to clean. I started my Ozempic on Sunday, and so far so good. I can see my appetite is less already.

Dear friend,
Exciting offer just for you! Deep discounts on Ozemp1c.
Limited time offer, act now.

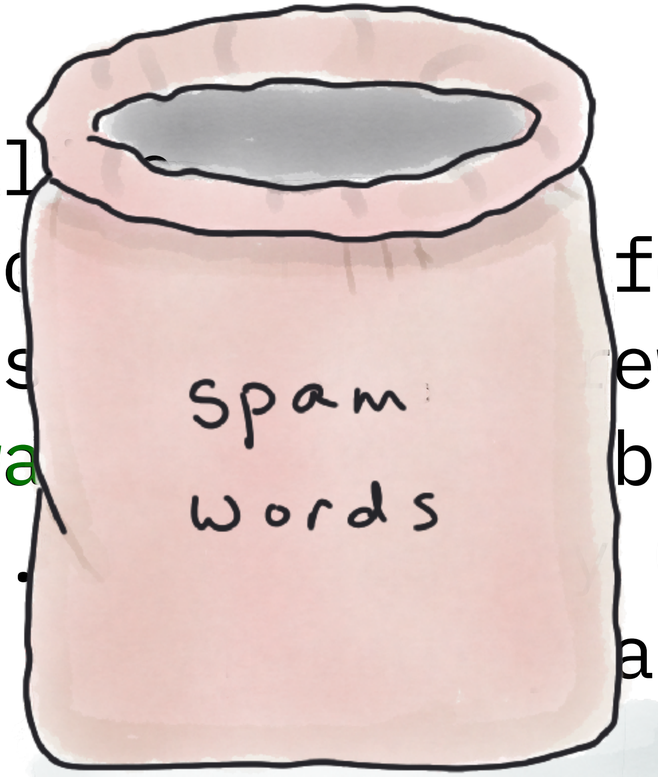
Hey Alice,
Are you still good for next week? We had drama yesterday because the dog threw up, on the clean dishes in the dishwasher! On the bright side, at least it was easy to clean. I started my Ozempic on Sunday, and so far so good. I can see my appetite is less already.

Dear friend,
Exciting offer just for you! Deep discounts on Ozemp1c.
Limited time offer, act now.



Hey Al
Are yo for next week? We had drama yesterday
becaus ew up, on the clean dishes in the
dishwa bright side, at least it was easy to
clean. Ozempic on Sunday, and so far so
good. appetite is less already.

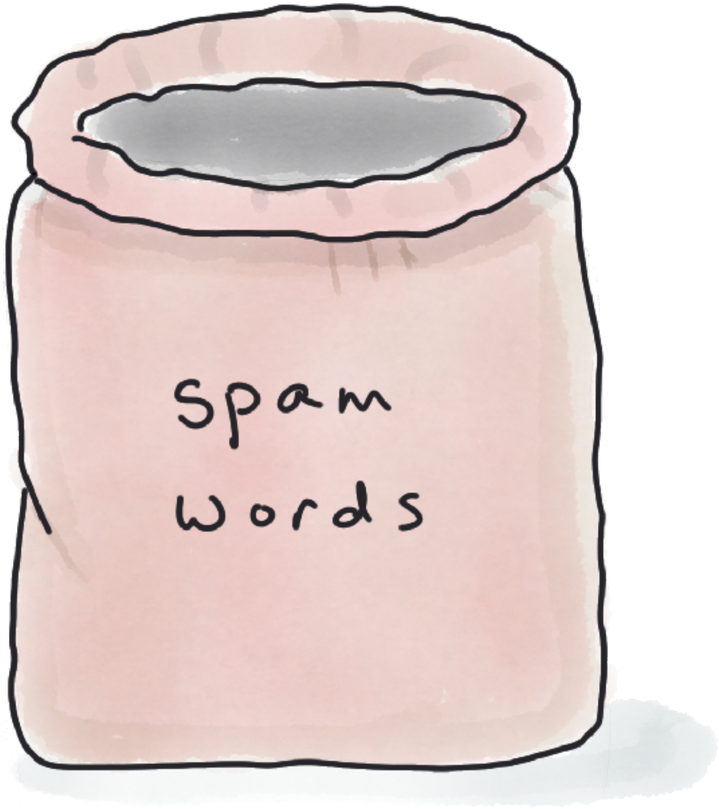
Dear friend,
Exciting offer just for you! Deep discounts on Ozemp1c.
Limited time offer, act now.



Hey Al
Are yo for next week? We h erday
becaus ew up, on the clean e
dishwa bright side, at lea y to
clean. Ozempic on Sunday, o
good. appetite is less al



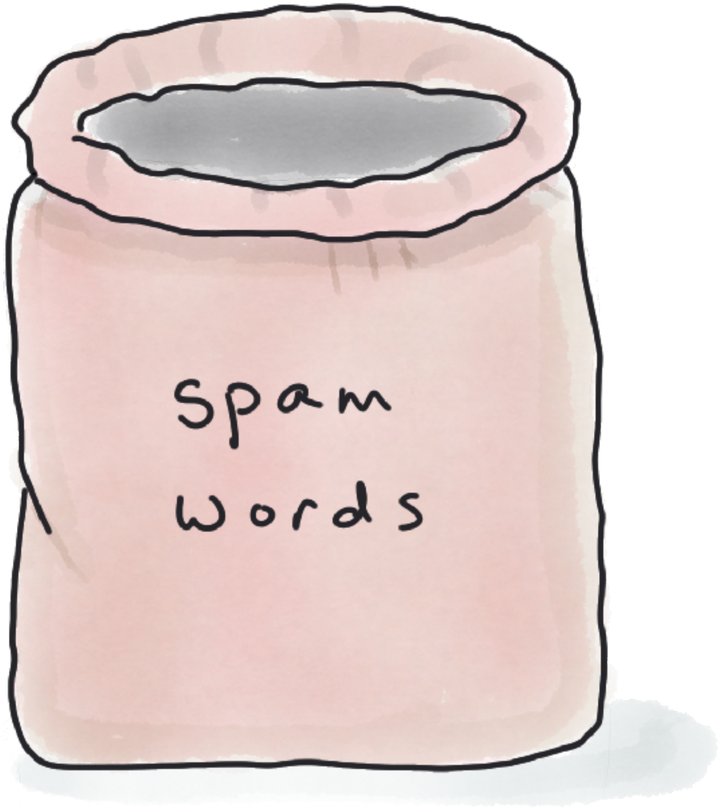
offer
act
discount
Ozemp1c



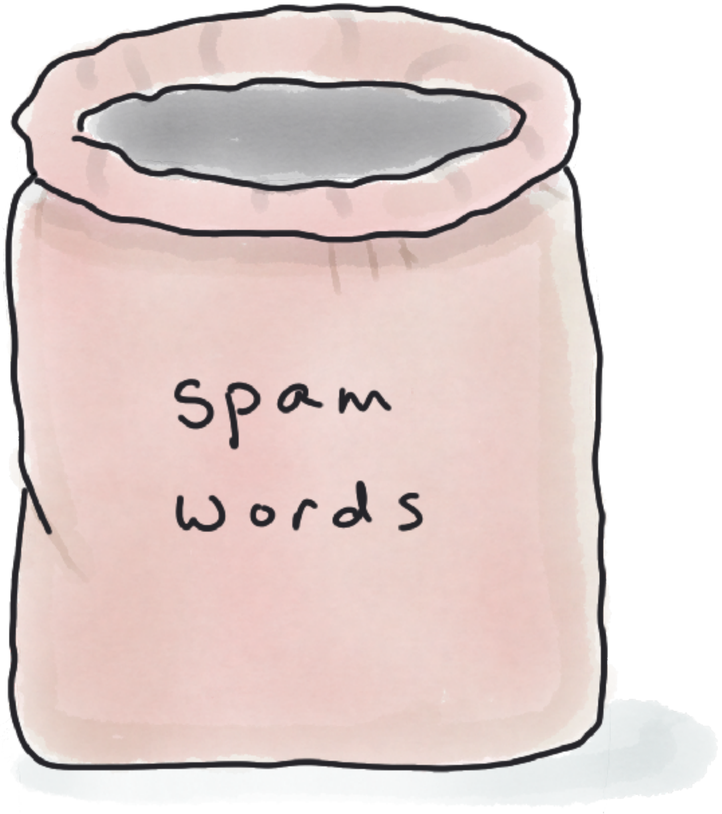
dog
dishwasher
yesterday
Ozempic



dog
dishwasher
yesterday
Ozempic






spam
words


ham
words

P(spam | 0zemp1c)

“probability of”

P(spam | 0zemp1c)

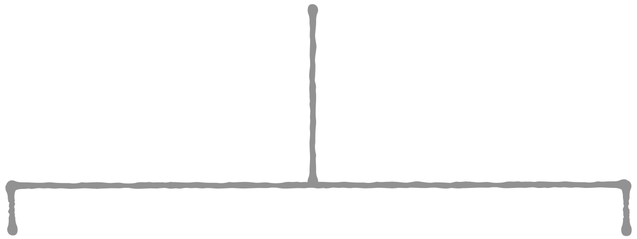
“probability of”

P(spam | 0zemp1c)

“given”

$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$$

probability of A, given B

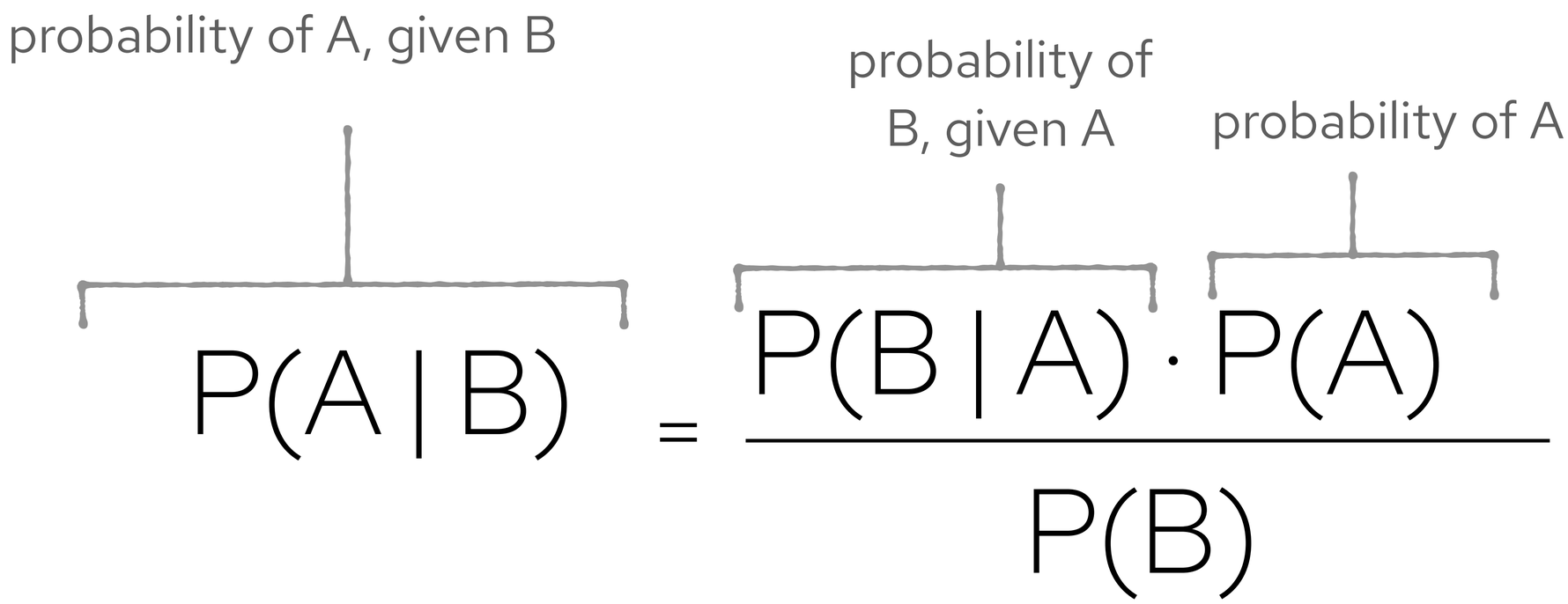


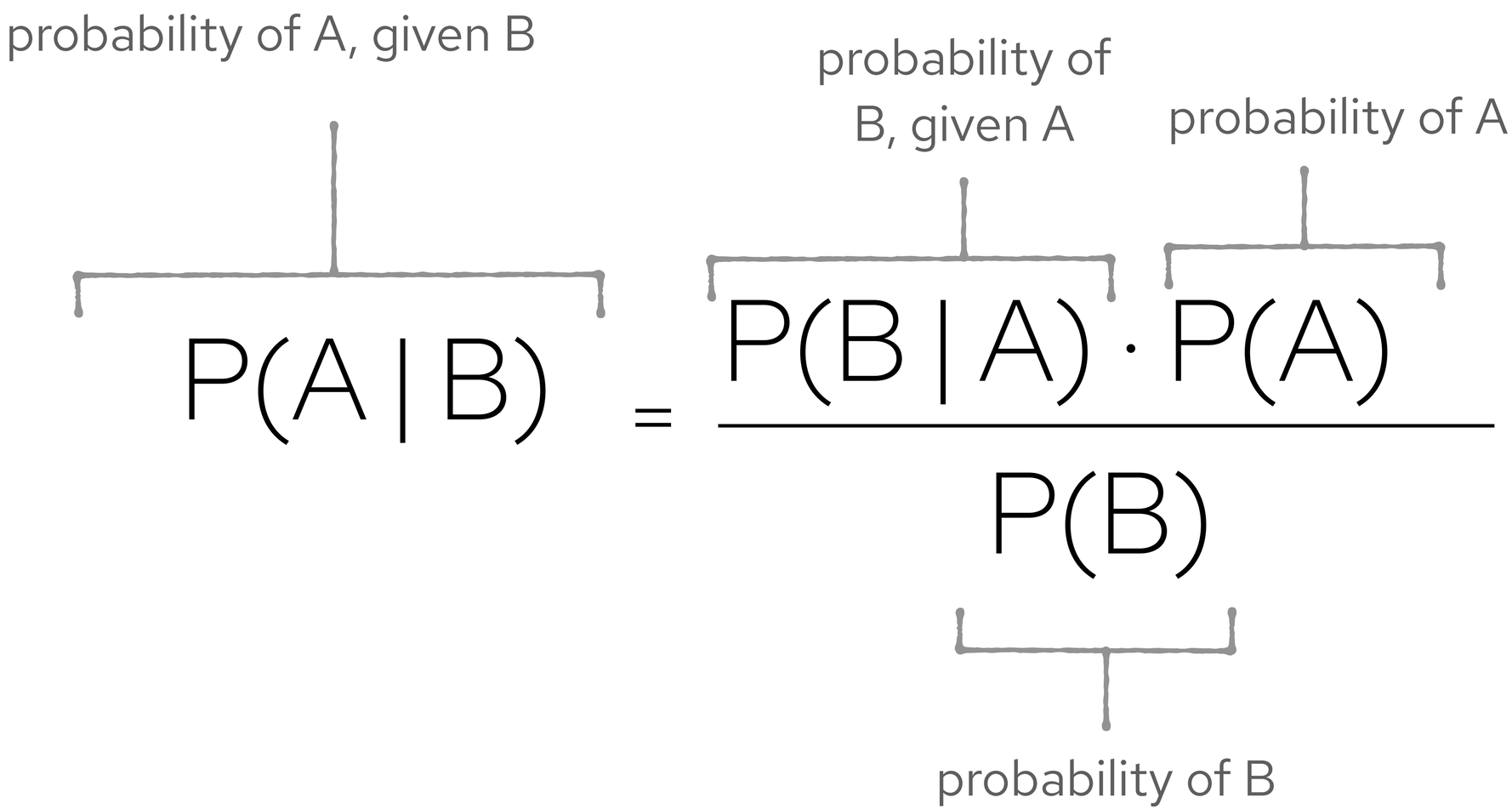
$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$$

probability of A, given B

probability of B, given A

$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$$


probability of A, given B
probability of B, given A
probability of A
P(A | B) = P(B | A) · P(A) / P(B)


probability of A, given B
probability of B, given A
probability of A
P(A | B) = P(B | A) · P(A) / P(B)
probability of B

guidance for a decision

probability of B, given A

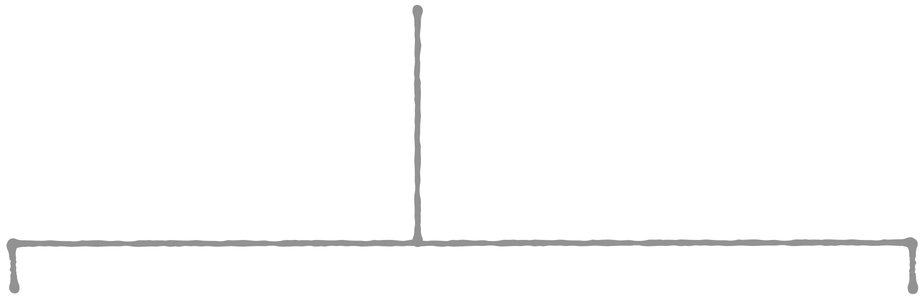
probability of A

$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$$

probability of B

$$P(\text{spam} \mid \text{Ozemp1c}) = \frac{P(\text{Ozemp1c} \mid \text{spam}) \cdot P(\text{spam})}{P(\text{Ozemp1c})}$$

is this email spam?



$$P(\text{spam} \mid \text{Ozemp1c}) = \frac{P(\text{Ozemp1c} \mid \text{spam}) \cdot P(\text{spam})}{P(\text{Ozemp1c})}$$

is this email spam?

what proportion of spam talks about Ozemp1c?

$$P(\text{spam} \mid \text{Ozemp1c}) = \frac{P(\text{Ozemp1c} \mid \text{spam}) \cdot P(\text{spam})}{P(\text{Ozemp1c})}$$

is this email spam?

what proportion of spam talks about Ozemp1c?

what proportion of emails are spam?

$$P(\text{spam} \mid \text{Ozemp1c}) = \frac{P(\text{Ozemp1c} \mid \text{spam}) \cdot P(\text{spam})}{P(\text{Ozemp1c})}$$

is this email spam?

what proportion of spam talks about Ozemp1c?

what proportion of emails are spam?

$$P(\text{spam} \mid \text{Ozemp1c}) = \frac{P(\text{Ozemp1c} \mid \text{spam}) \cdot P(\text{spam})}{P(\text{Ozemp1c})}$$

what proportion of all emails mention Ozemp1c?

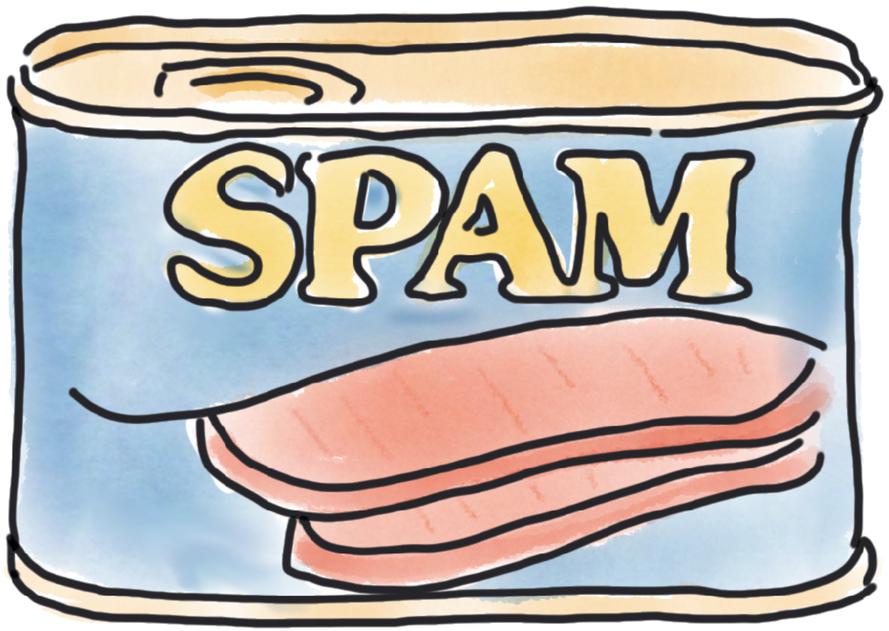
$$P(\text{spam} \mid \text{Ozemp1c}) = \frac{P(\text{Ozemp1c} \mid \text{spam}) \cdot P(\text{spam})}{P(\text{Ozemp1c})}$$

$$P(\text{spam} \mid \text{Ozemp1c}) = \frac{1\% \cdot P(\text{spam})}{P(\text{Ozemp1c})}$$

$$P(\text{spam} \mid \text{Ozemp1c}) = \frac{1\% \cdot P(\text{spam})}{0.001\%}$$

$$P(\text{spam} \mid \text{Ozemp1c}) = \frac{1\% \cdot 6\%}{0.001\%}$$

P(spam | Ozemp1c) = 60%



$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$$

what if I don’t know any of these numbers??

$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$$

what if I don't know any of these numbers??

$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$$

or this one?

what if I don't know any of these numbers??

$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$$

or this one?

most **useless** formula ever?

$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$$

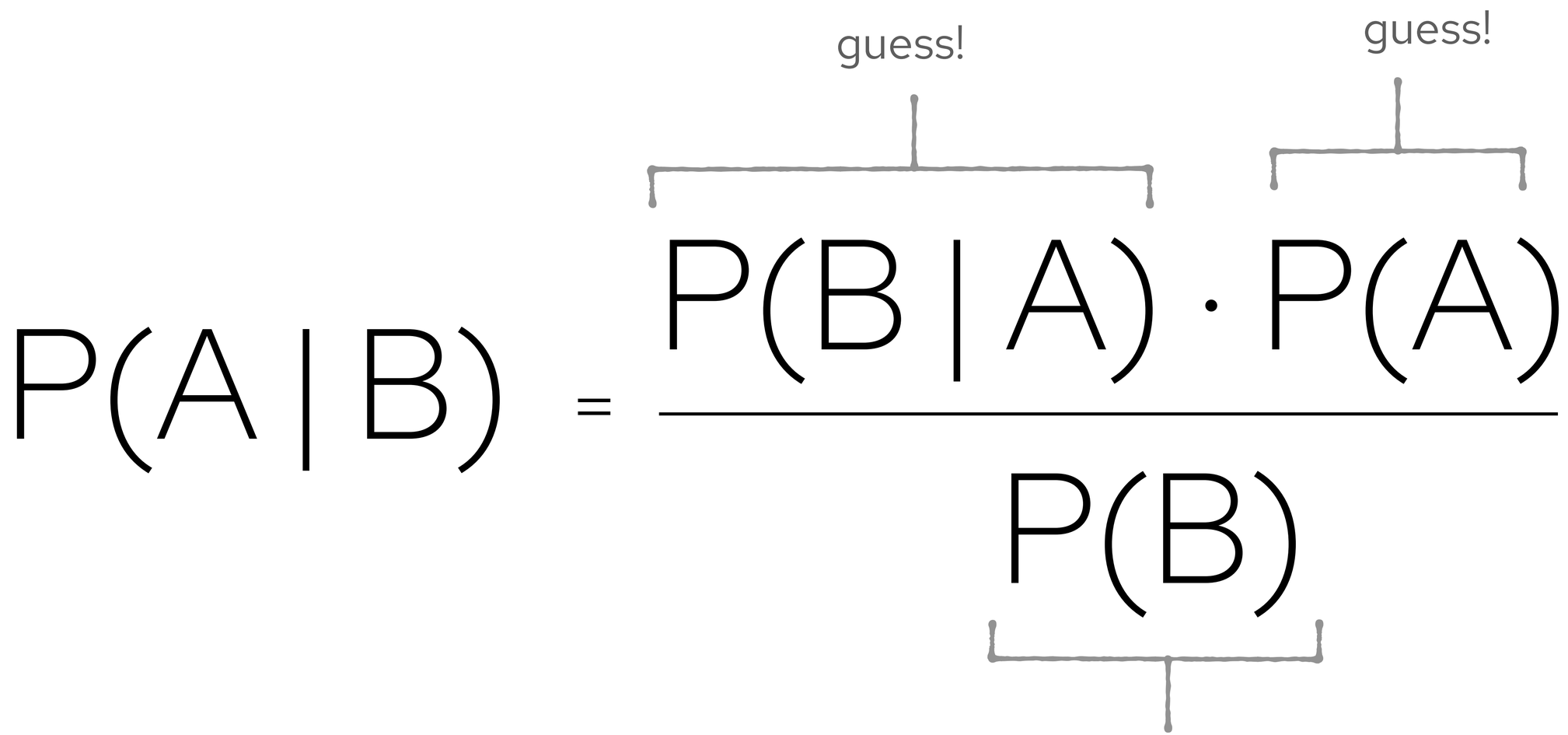
guess!

$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$$

guess!

guess!

$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$$


guess!
guess!
P(A | B) = P(B | A) · P(A) / P(B)
guess!
or ignore, because it's a normalizing factor

$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$$

$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$$

recursion

$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$$

recursion (cheating)

$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$$

recursion (iteration)

$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$$

"ignorance... coined into science."

"ignorance... coined into science."

“founded upon an error, and must be wholly rejected”

"ignorance... coined into science."

“founded upon an error, and
must be wholly rejected”

“perhaps the only error to which
the mathematical world has so
deeply committed itself”

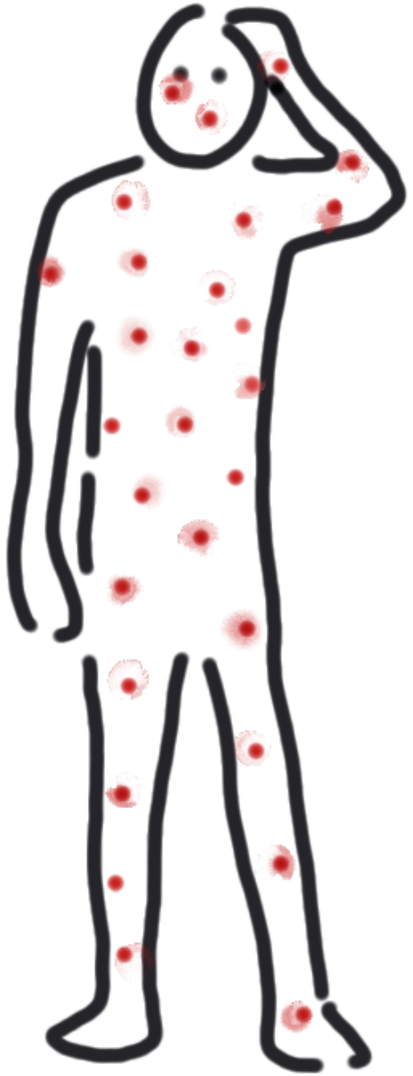
"ignorance... coined into science."

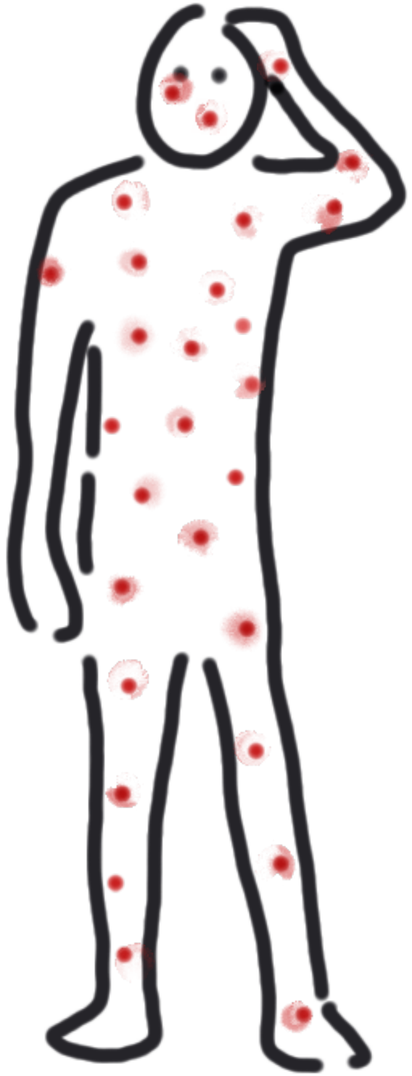
“founded upon an error, and
must be wholly rejected”

“perhaps the only error to which
the mathematical world has so
deeply committed itself”

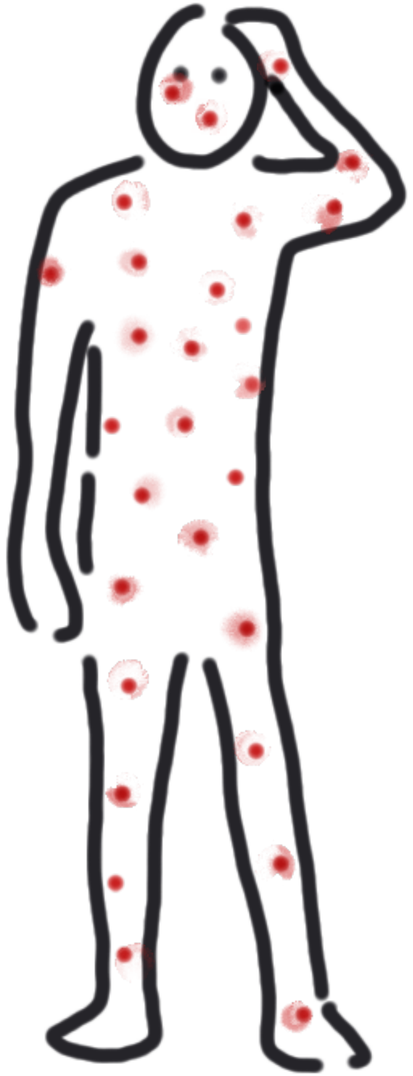
“a staggering falsity”







cowpox?

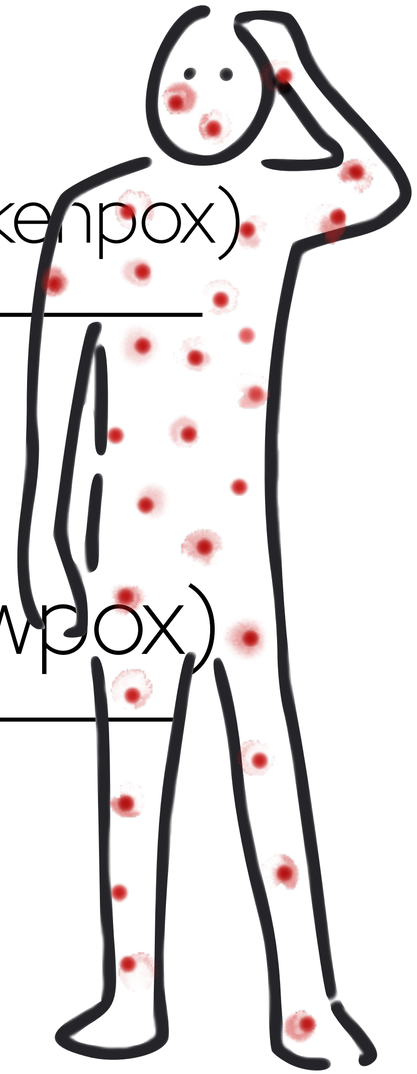


cowpox?

chickenpox?

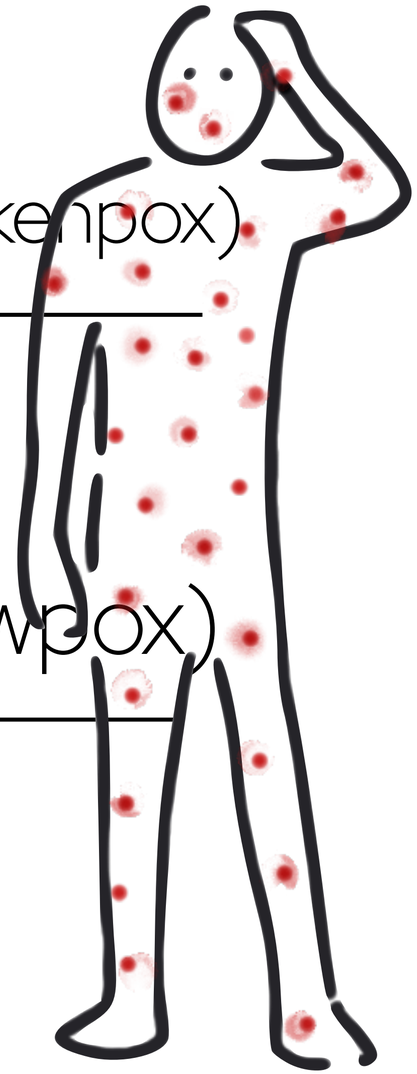
$$P(\text{chickenpox} \mid \text{spots}) = \frac{P(\text{spots} \mid \text{chickenpox}) \cdot P(\text{chickenpox})}{P(\text{spots})}$$

$$P(\text{cowpox} \mid \text{spots}) = \frac{P(\text{spots} \mid \text{cowpox}) \cdot P(\text{cowpox})}{P(\text{spots})}$$



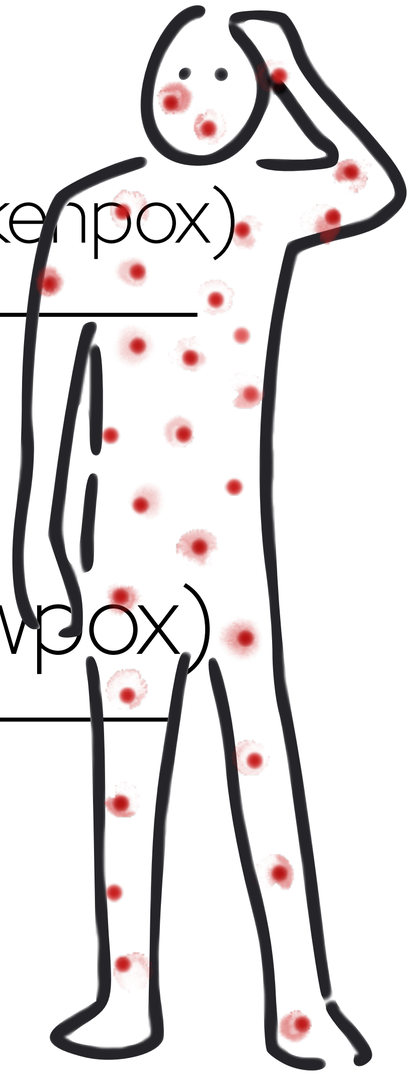
$$P(\text{chickenpox} \mid \text{spots}) = \frac{P(\text{spots} \mid \text{chickenpox}) \cdot P(\text{chickenpox})}{}$$

$$P(\text{cowpox} \mid \text{spots}) = \frac{P(\text{spots} \mid \text{cowpox}) \cdot P(\text{cowpox})}{}$$



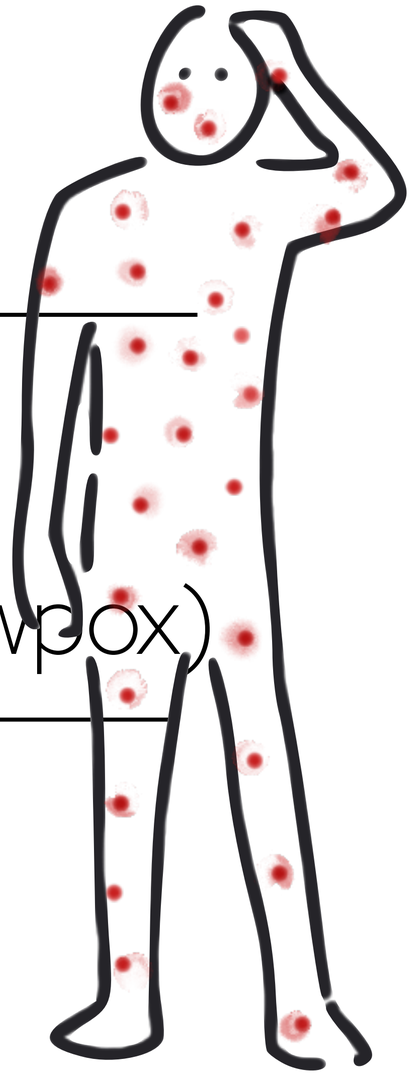
$$P(\text{chickenpox} \mid \text{spots}) = \frac{85\% \cdot P(\text{chickenpox})}{}$$

$$P(\text{cowpox} \mid \text{spots}) = \frac{P(\text{spots} \mid \text{cowpox}) \cdot P(\text{cowpox})}{}$$



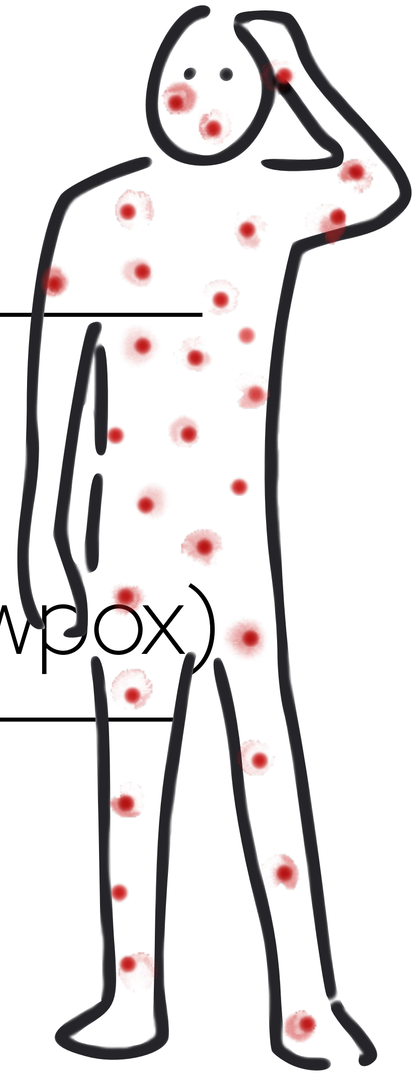
$$P(\text{chickenpox} \mid \text{spots}) = \frac{85\% \cdot 1\%}{\qquad\qquad}$$

$$P(\text{cowpox} \mid \text{spots}) = \frac{P(\text{spots} \mid \text{cowpox}) \cdot P(\text{cowpox})}{\qquad\qquad}$$



$$P(\text{chickenpox} \mid \text{spots}) = \frac{85\% \cdot 1\%}{\quad}$$

$$P(\text{cowpox} \mid \text{spots}) = \frac{90\% \cdot P(\text{cowpox})}{\quad}$$



$$P(\text{chickenpox} \mid \text{spots}) = \frac{85\% \cdot 1\%}{\qquad\qquad}$$

$$P(\text{cowpox} \mid \text{spots}) = \frac{90\% \cdot 0.0001\%}{\qquad\qquad}$$



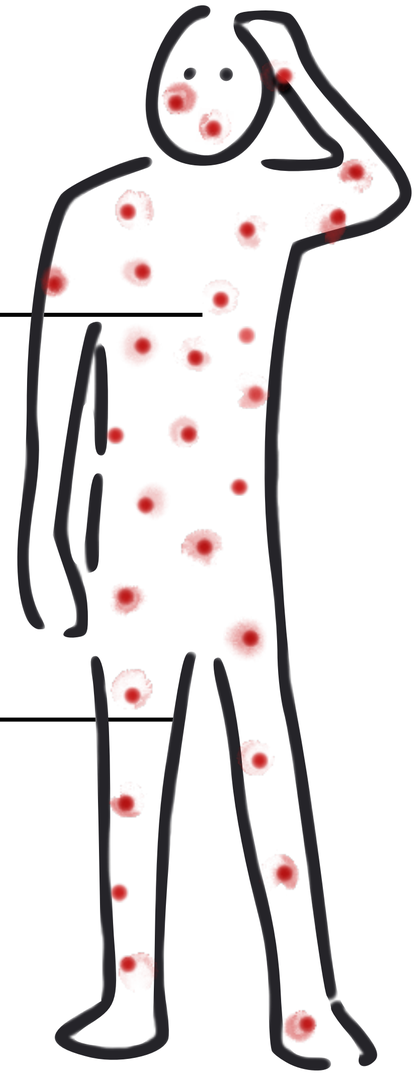
$$P(\text{chickenpox} \mid \text{spots}) = \frac{0.85\%}{\qquad\qquad}$$

$$P(\text{cowpox} \mid \text{spots}) = \frac{90\% \cdot 0.0001\%}{\qquad\qquad}$$



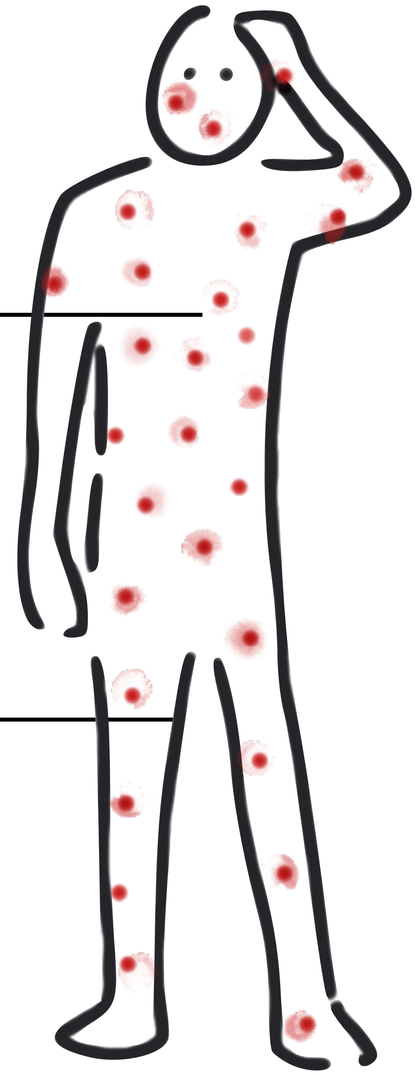
$$P(\text{chickenpox} \mid \text{spots}) = \frac{0.85\%}{}$$

$$P(\text{cowpox} \mid \text{spots}) = \frac{0.0009\%}{}$$

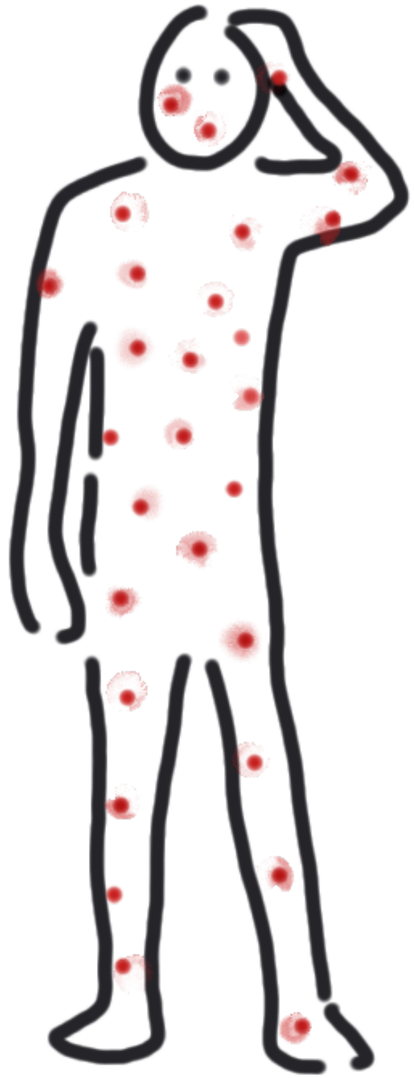


$$P(\text{chickenpox} \mid \text{spots}) = \frac{0.85\%}{}$$

$$= \frac{0.0009\%}{}$$

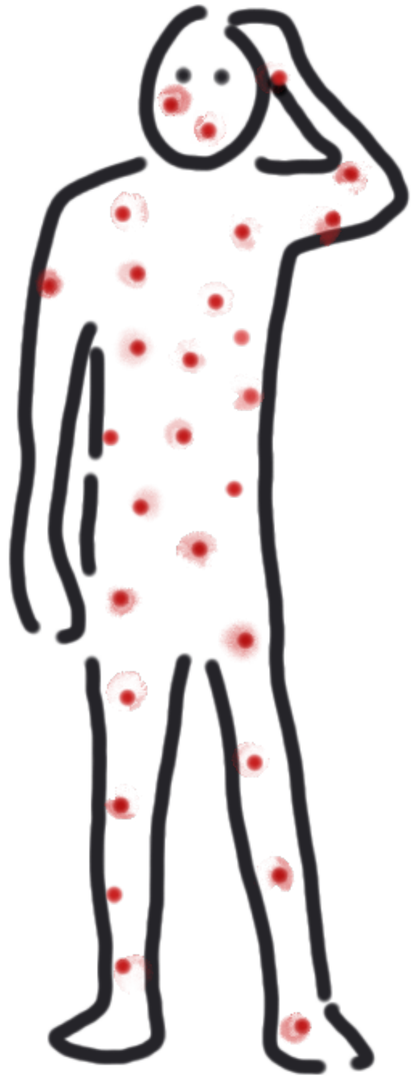


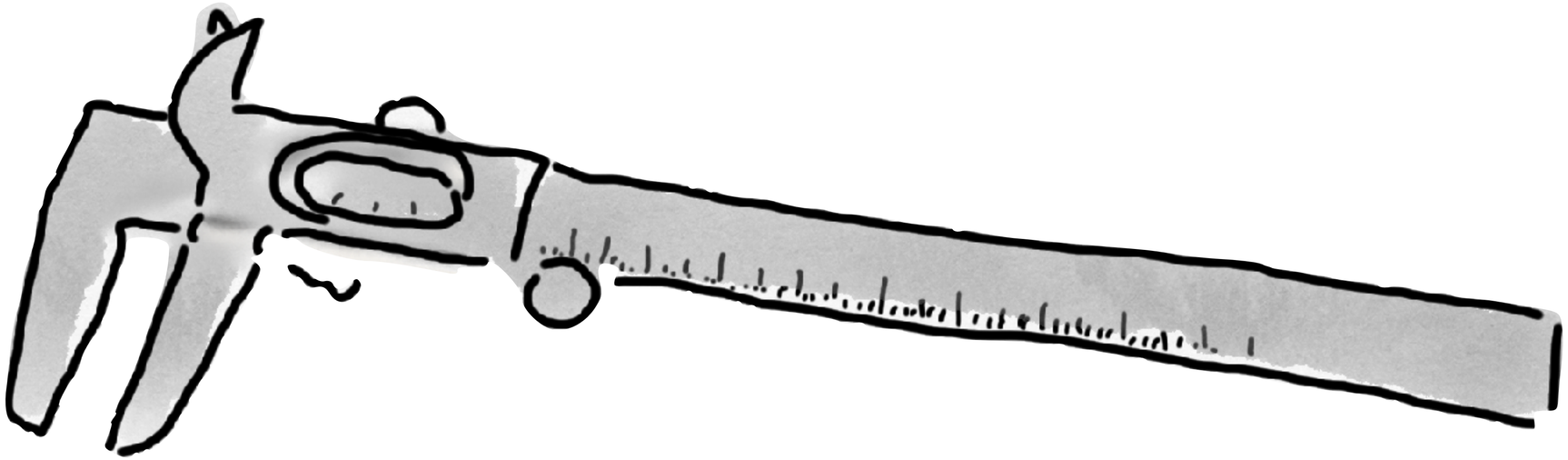
it's chickenpox



it's chickenpox

common sense





magic static analysis tool

99% accurate

✓ code is clean ☺

✓ code is clean ☺

what's the chance the code is clean?

$$P(\text{clean code} \mid \text{clean report}) = \frac{P(\text{clean report} \mid \text{clean code}) \cdot P(\text{clean code})}{P(\text{clean report})}$$

$$P(\text{clean code} \mid \text{clean report}) = \frac{99\% \cdot P(\text{clean code})}{P(\text{clean report})}$$

$$P(\text{clean code} \mid \text{clean report}) = \frac{99\% \cdot P(\text{clean code})}{1.98\%}$$

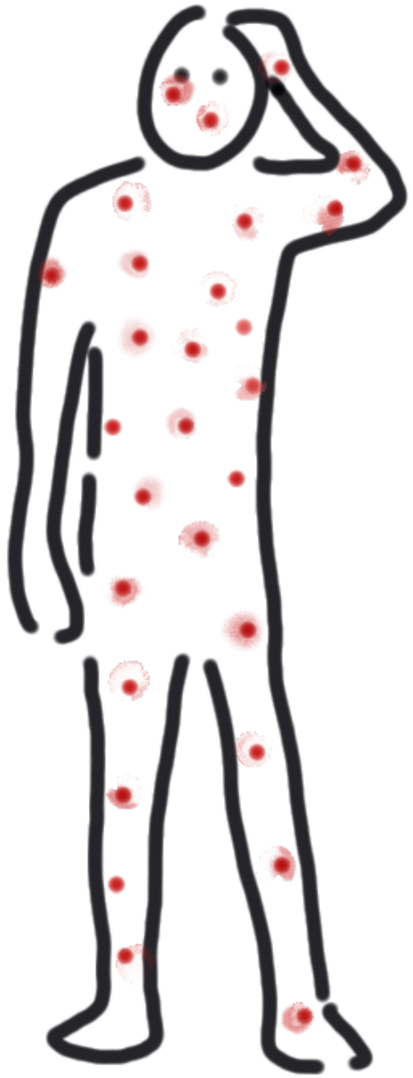
$$P(\text{clean code} \mid \text{clean report}) = \frac{99\% \cdot 1\%}{1.98\%}$$

P(clean code | clean report) = 50% .

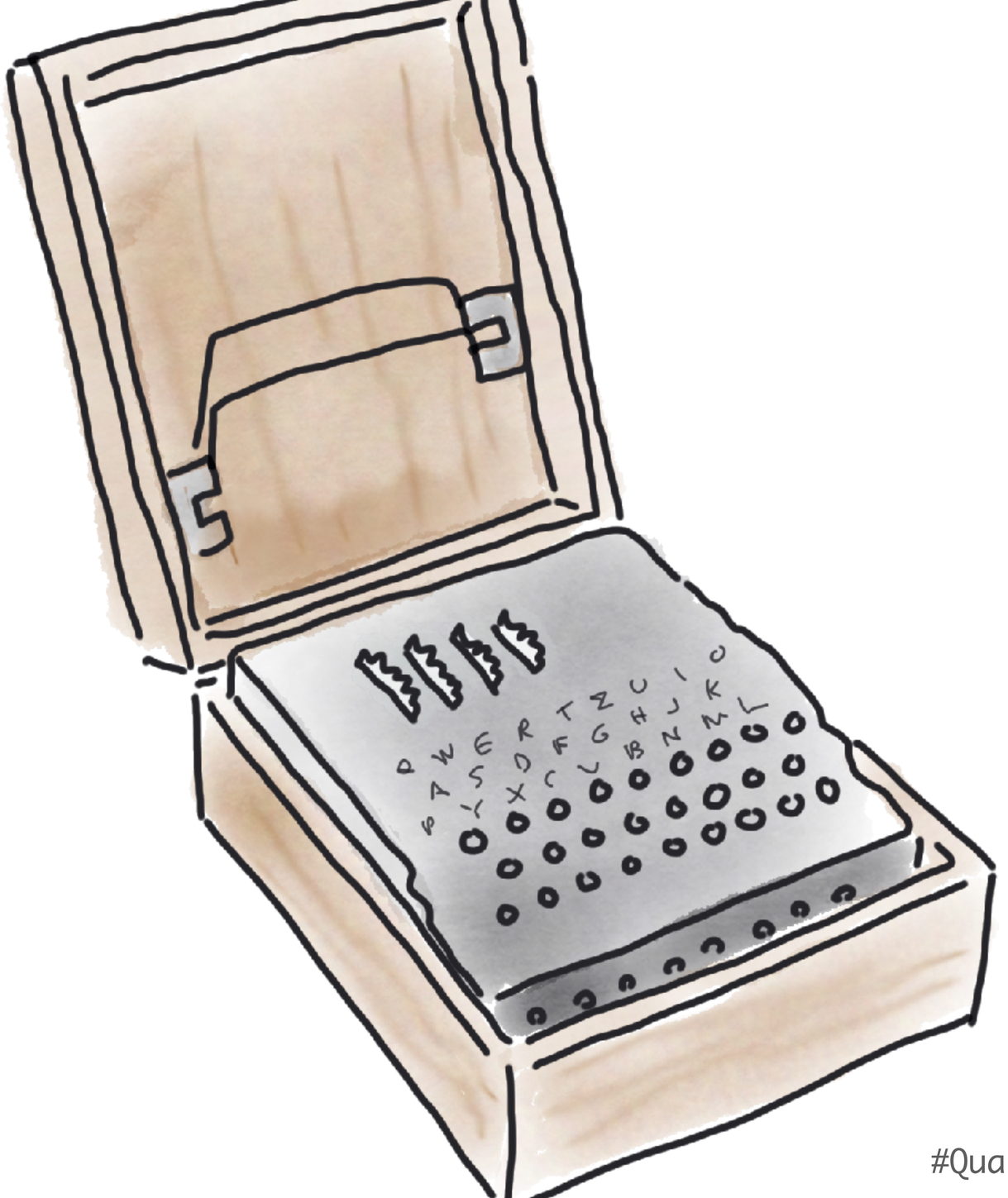
not common-sense

bayes is **everywhere**


artificial intelligence



medicine



336 combinations



336 combinations

4 days



ein

jxf

W-E-T-T-E-R-F-U-R



brute force 336 combinations

bayes-ed

18 combinations

top tip

tired: “we have no idea”

wired: “we are adopting bayesian thinking”



why does concurrency make my head hurt?

$$P(\text{concurrency} \mid \text{headache}) = \frac{P(\text{headache} \mid \text{concurrency}) \cdot P(\text{concurrency})}{P(\text{headache})}$$

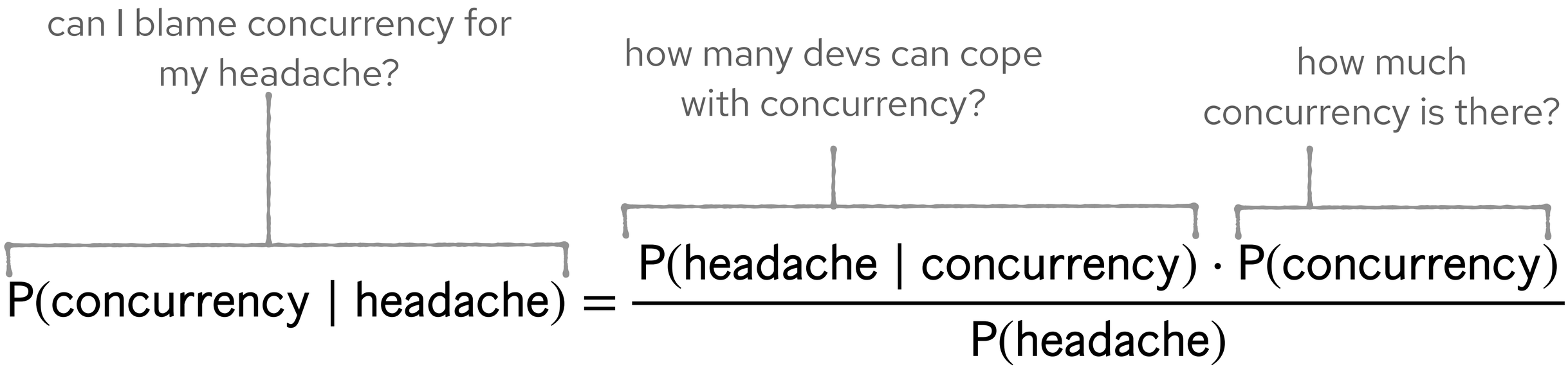
can I blame concurrency for my headache?

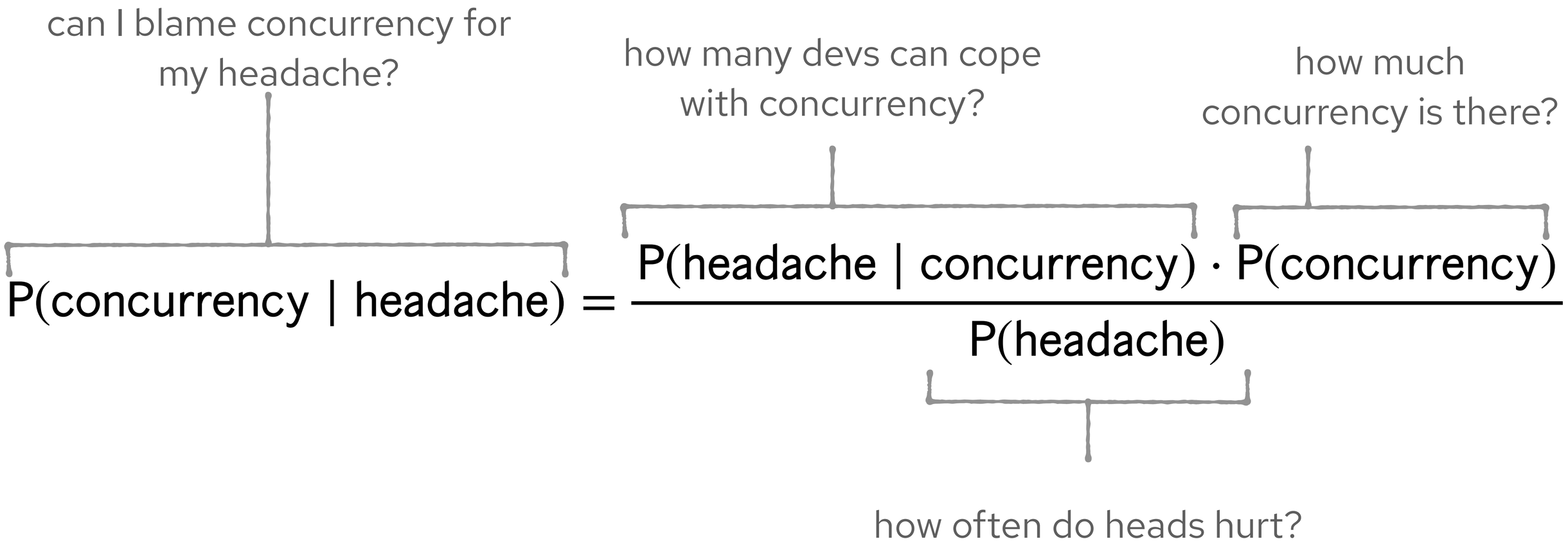
$$P(\text{concurrency} \mid \text{headache}) = \frac{P(\text{headache} \mid \text{concurrency}) \cdot P(\text{concurrency})}{P(\text{headache})}$$

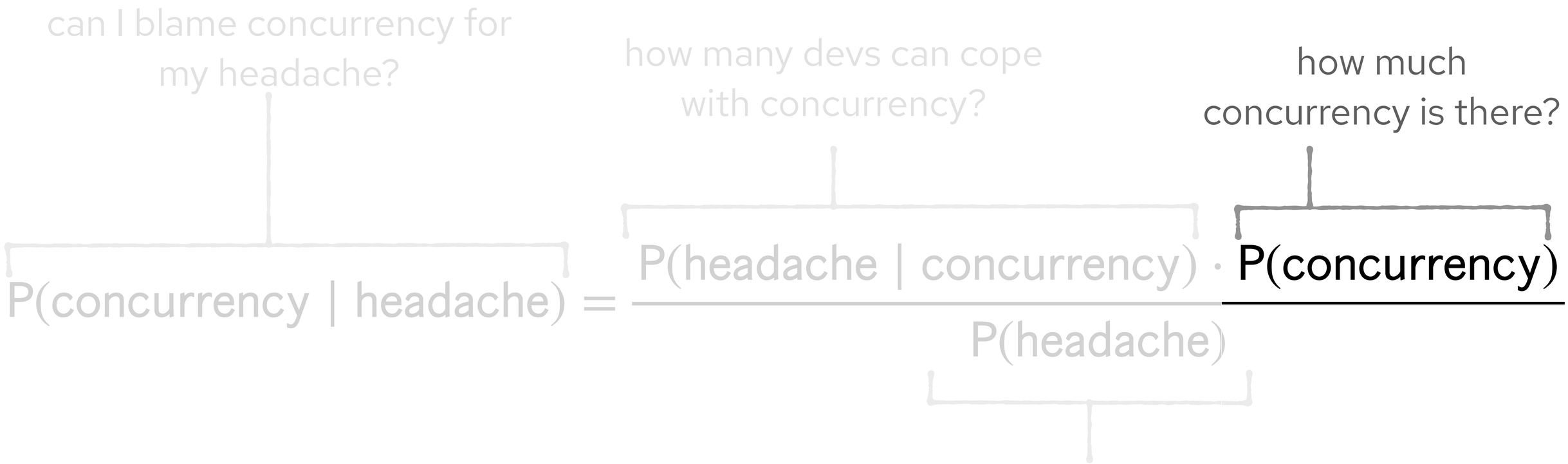
can I blame concurrency for my headache?

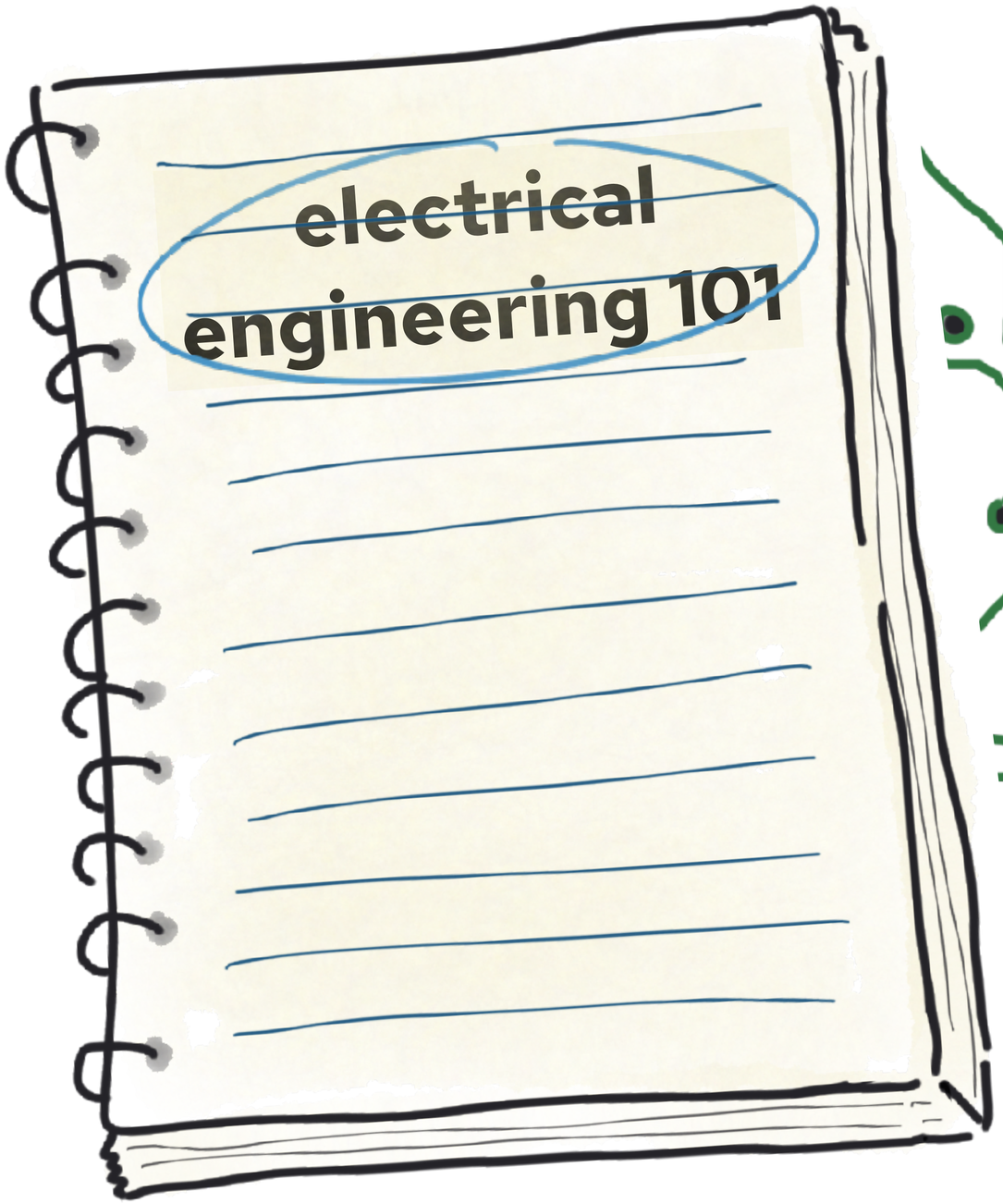
how many devs can cope with concurrency?

$$P(\text{concurrency} \mid \text{headache}) = \frac{P(\text{headache} \mid \text{concurrency}) \cdot P(\text{concurrency})}{P(\text{headache})}$$


can I blame concurrency for my headache?
how many devs can cope with concurrency?
how much concurrency is there?
P(concurrency | headache) = P(headache | concurrency) · P(concurrency) / P(headache)


can I blame concurrency for my headache?
how many devs can cope with concurrency?
how much concurrency is there?
P(concurrency | headache) = P(headache | concurrency) · P(concurrency) / P(headache)
how often do heads hurt?


can I blame concurrency for my headache?
how many devs can cope with concurrency?
how much concurrency is there?
P(concurrency | headache) = P(headache | concurrency) · P(concurrency) / P(headache)
how often do heads hurt?

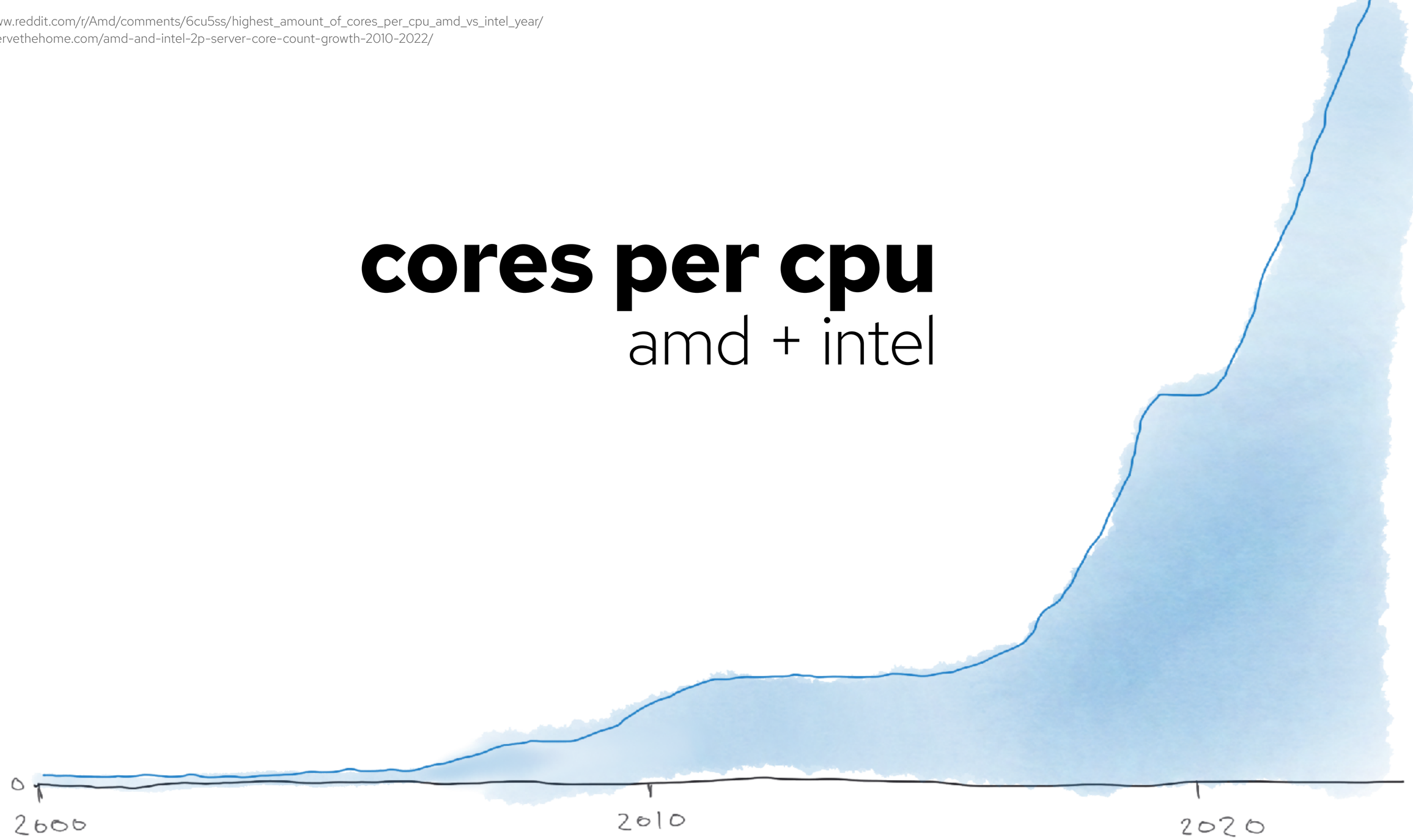


chip design

sources: https://www.reddit.com/r/Amd/comments/6cu5ss/highest_amount_of_cores_per_cpu_amd_vs_intel_year/
and https://www.servethehome.com/amd-and-intel-2p-server-core-count-growth-2010-2022/

cores per cpu

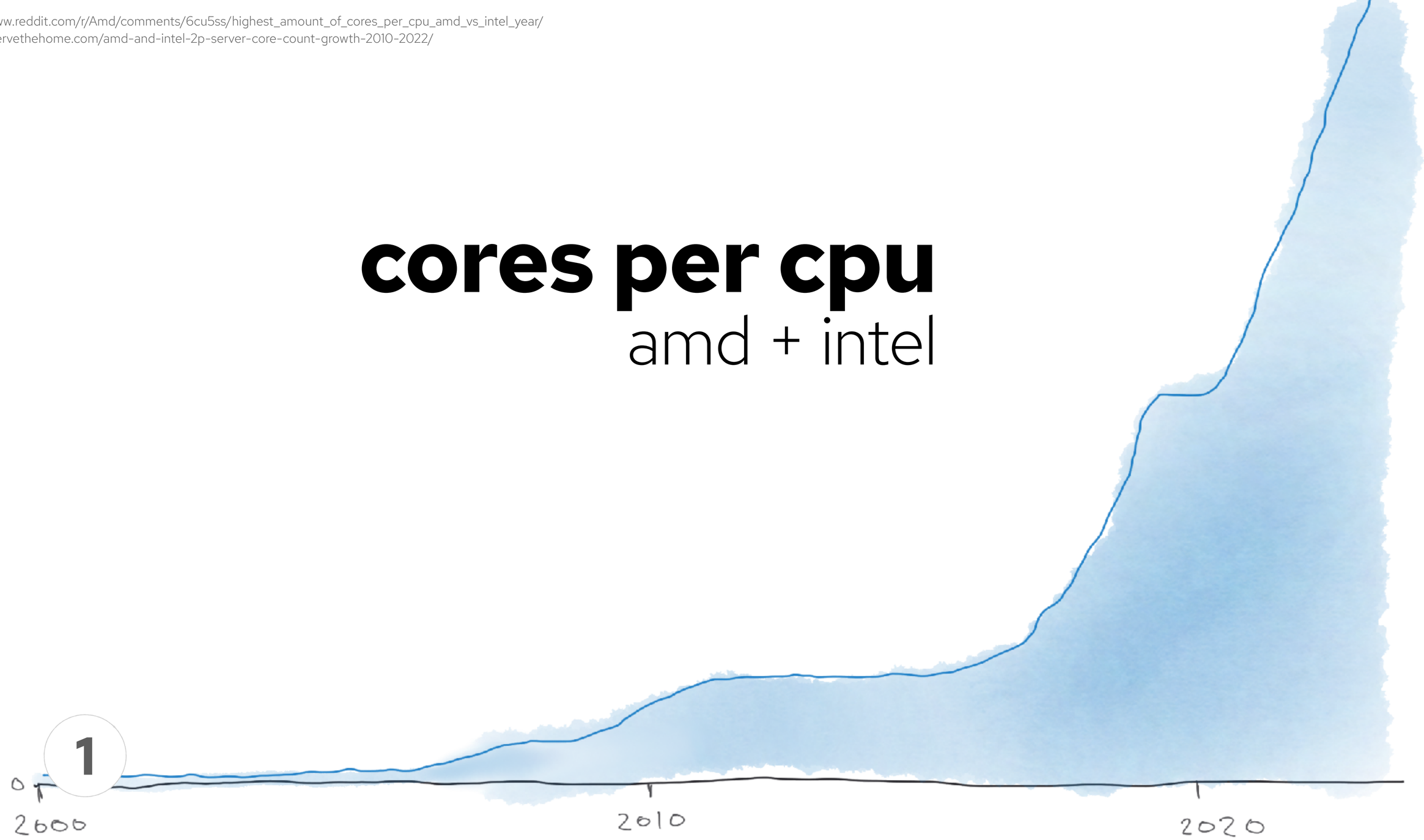
amd + intel



sources: https://www.reddit.com/r/Amd/comments/6cu5ss/highest_amount_of_cores_per_cpu_amd_vs_intel_year/
and https://www.servethehome.com/amd-and-intel-2p-server-core-count-growth-2010-2022/

cores per cpu

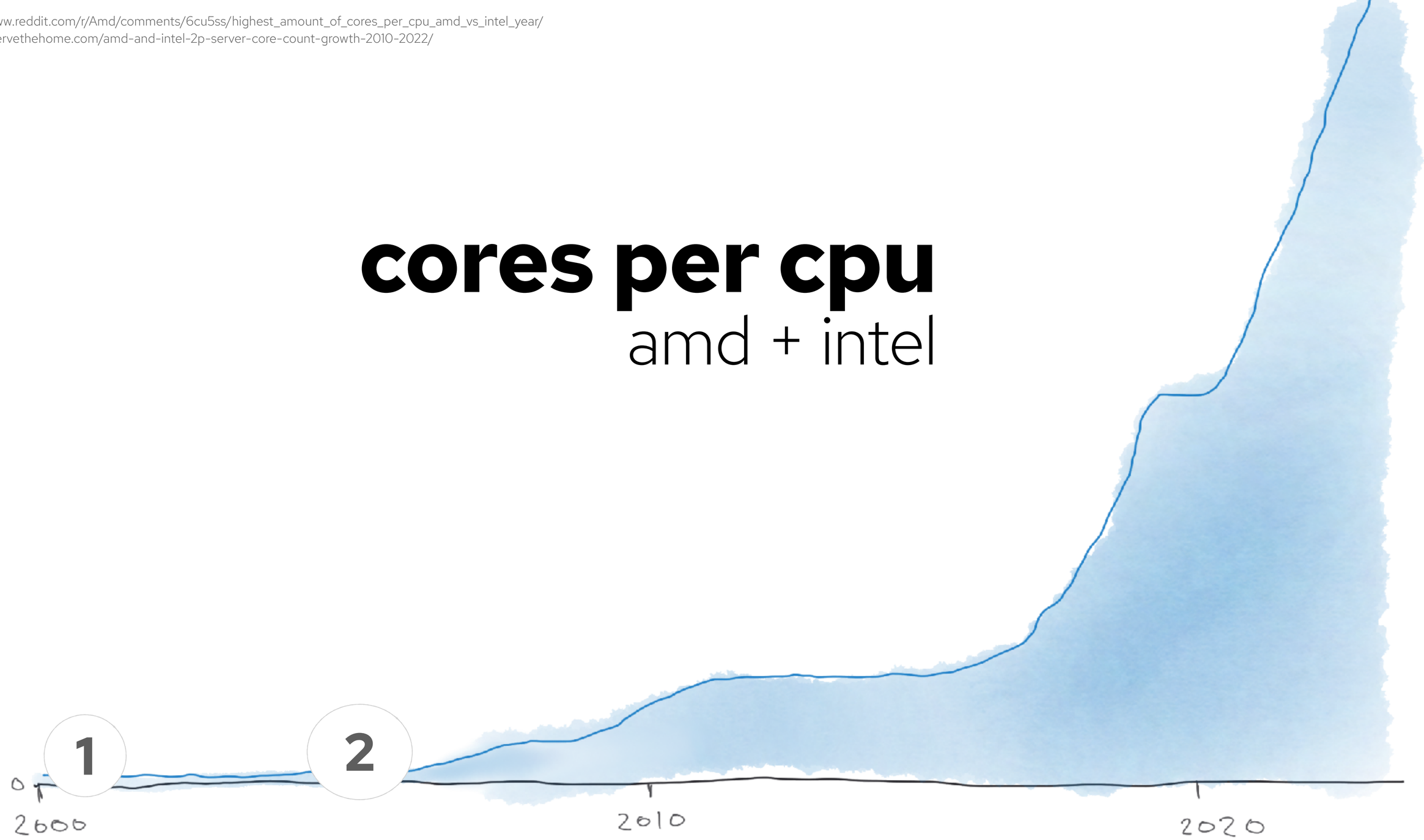
amd + intel



sources: https://www.reddit.com/r/Amd/comments/6cu5ss/highest_amount_of_cores_per_cpu_amd_vs_intel_year/
and https://www.servethehome.com/amd-and-intel-2p-server-core-count-growth-2010-2022/

cores per cpu

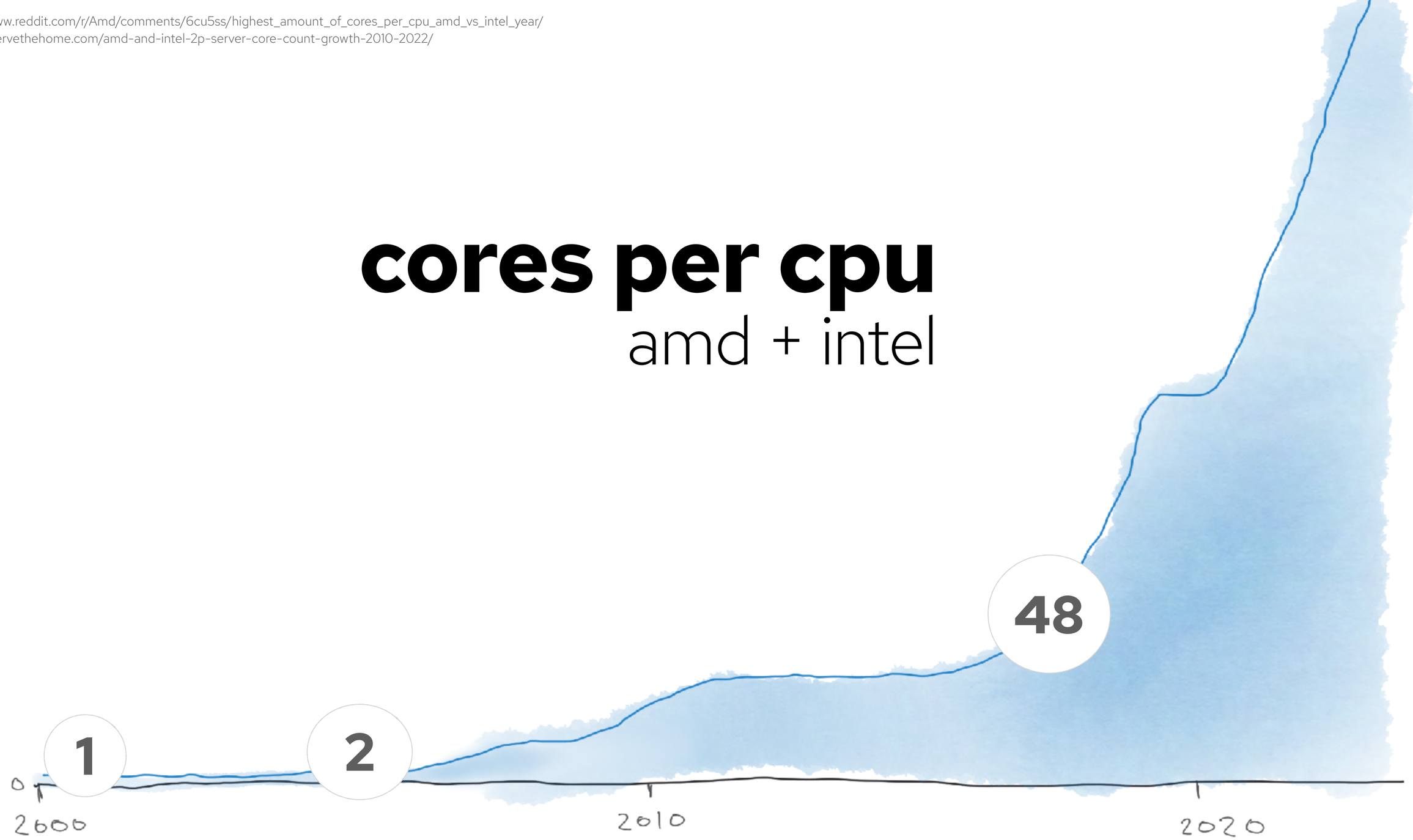
amd + intel



sources: https://www.reddit.com/r/Amd/comments/6cu5ss/highest_amount_of_cores_per_cpu_amd_vs_intel_year/
and https://www.servethehome.com/amd-and-intel-2p-server-core-count-growth-2010-2022/

cores per cpu

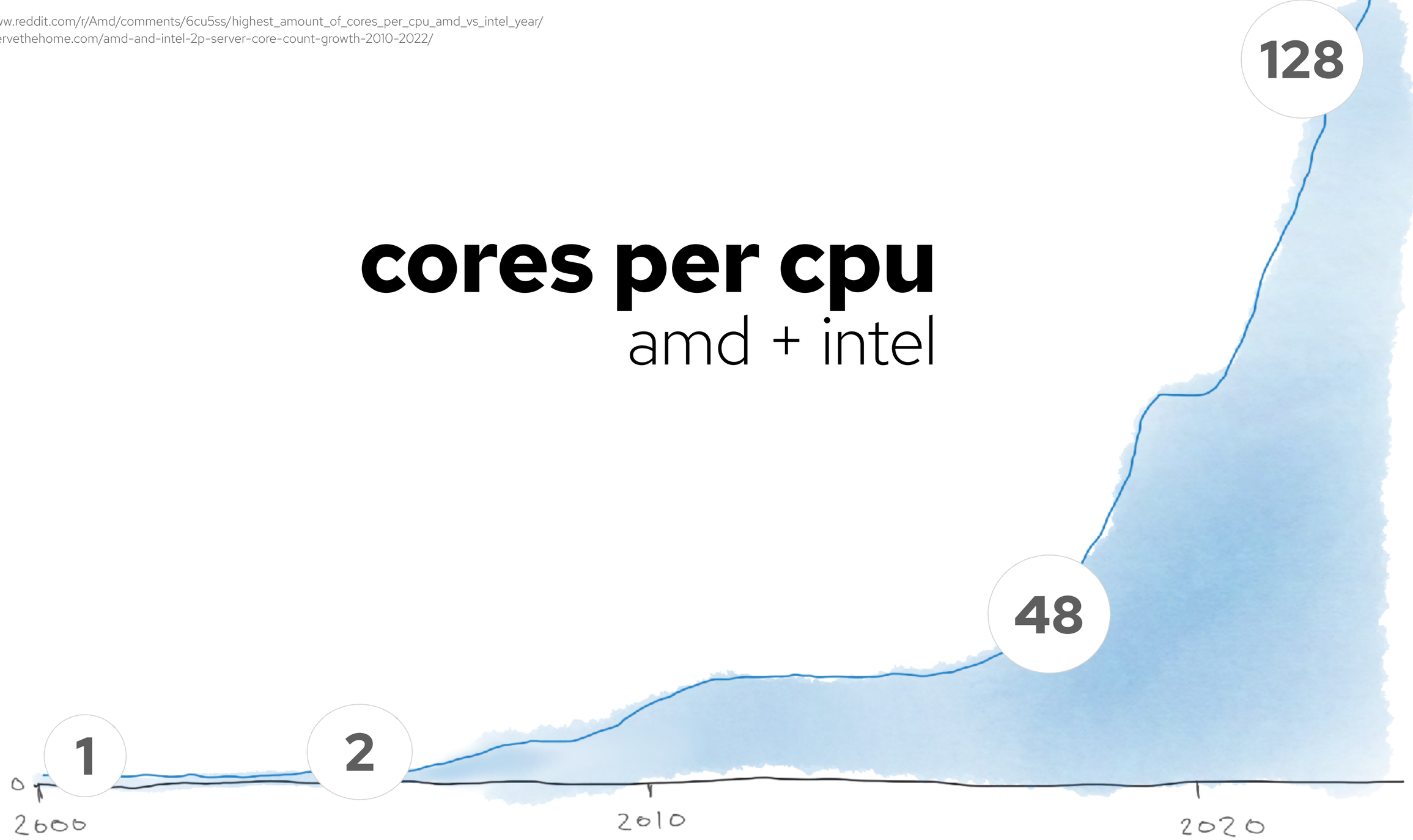
amd + intel



sources: https://www.reddit.com/r/Amd/comments/6cu5ss/highest_amount_of_cores_per_cpu_amd_vs_intel_year/
and https://www.servethehome.com/amd-and-intel-2p-server-core-count-growth-2010-2022/

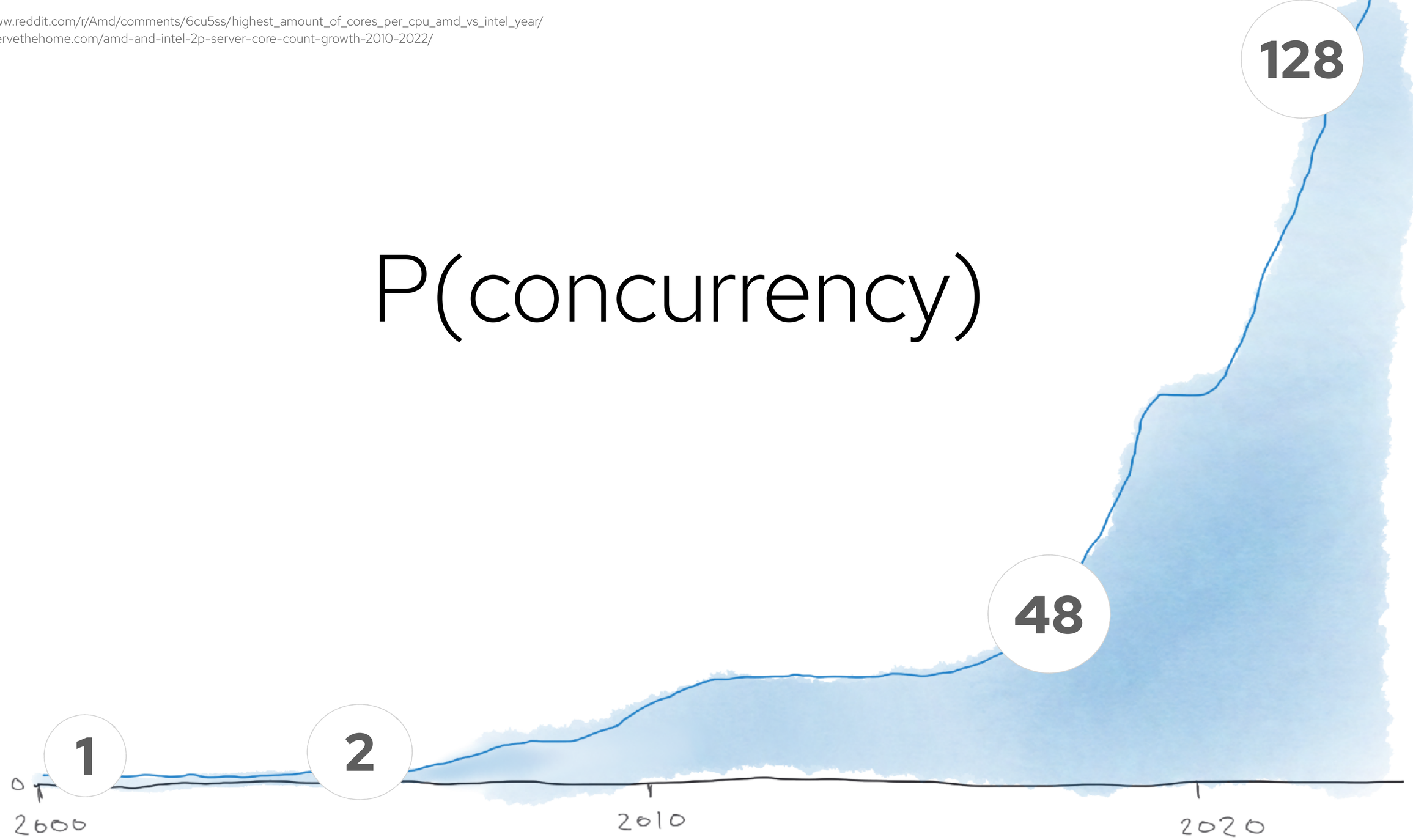
cores per cpu

amd + intel



sources: https://www.reddit.com/r/Amd/comments/6cu5ss/highest_amount_of_cores_per_cpu_amd_vs_intel_year/
and https://www.servethehome.com/amd-and-intel-2p-server-core-count-growth-2010-2022/

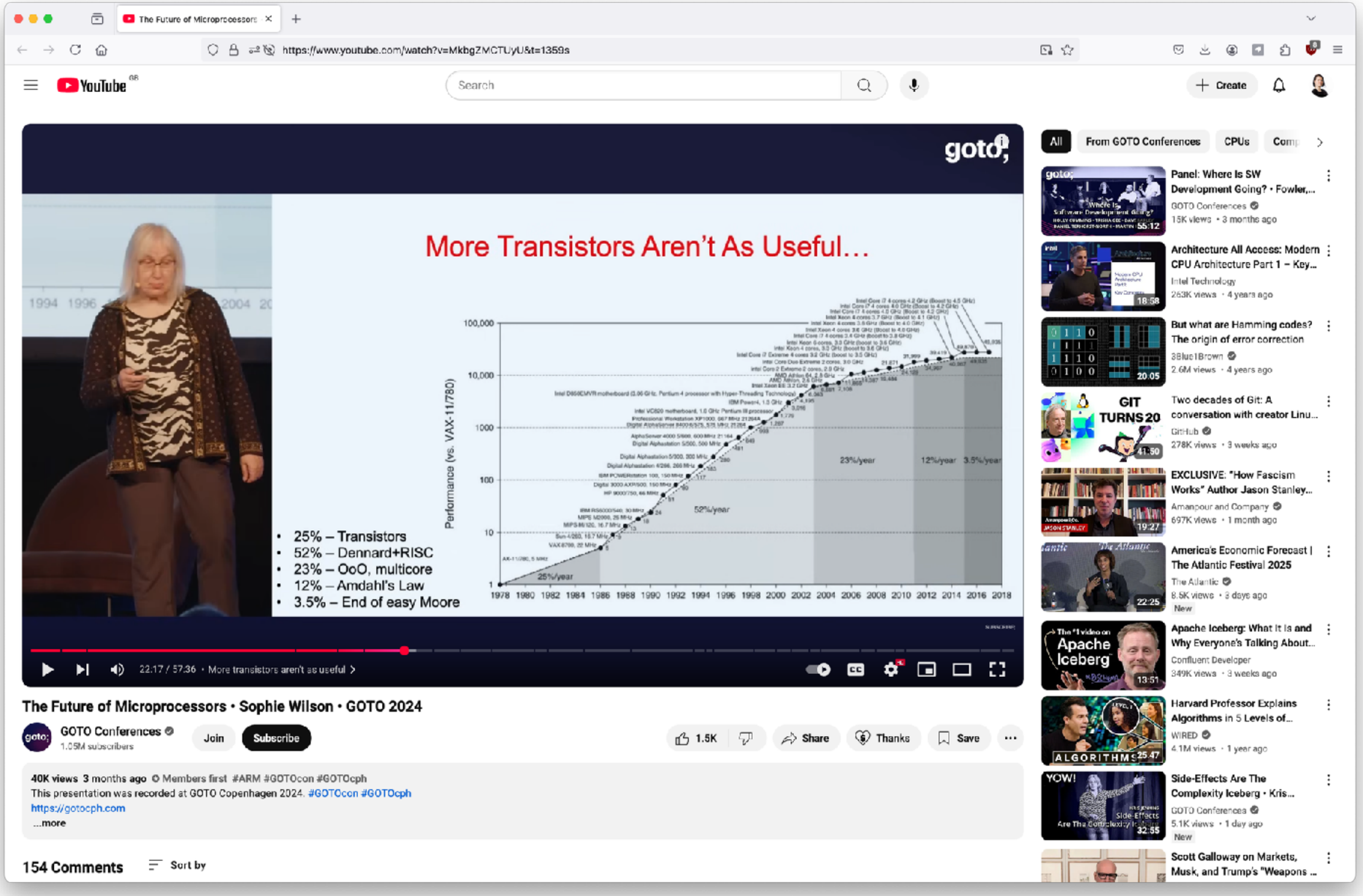
P(concurrency)



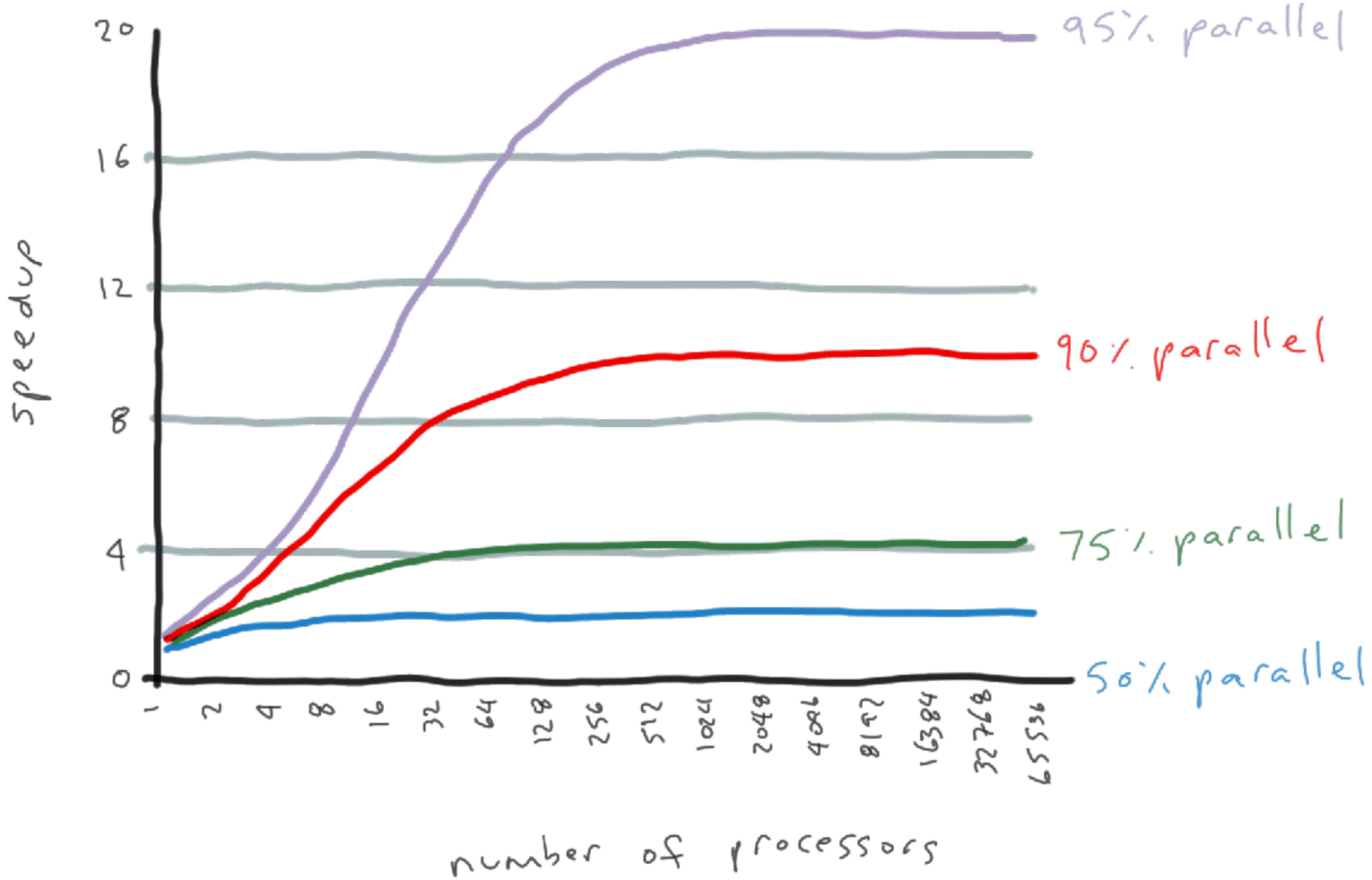
why?

why?

single-processor performance has **plateaued**

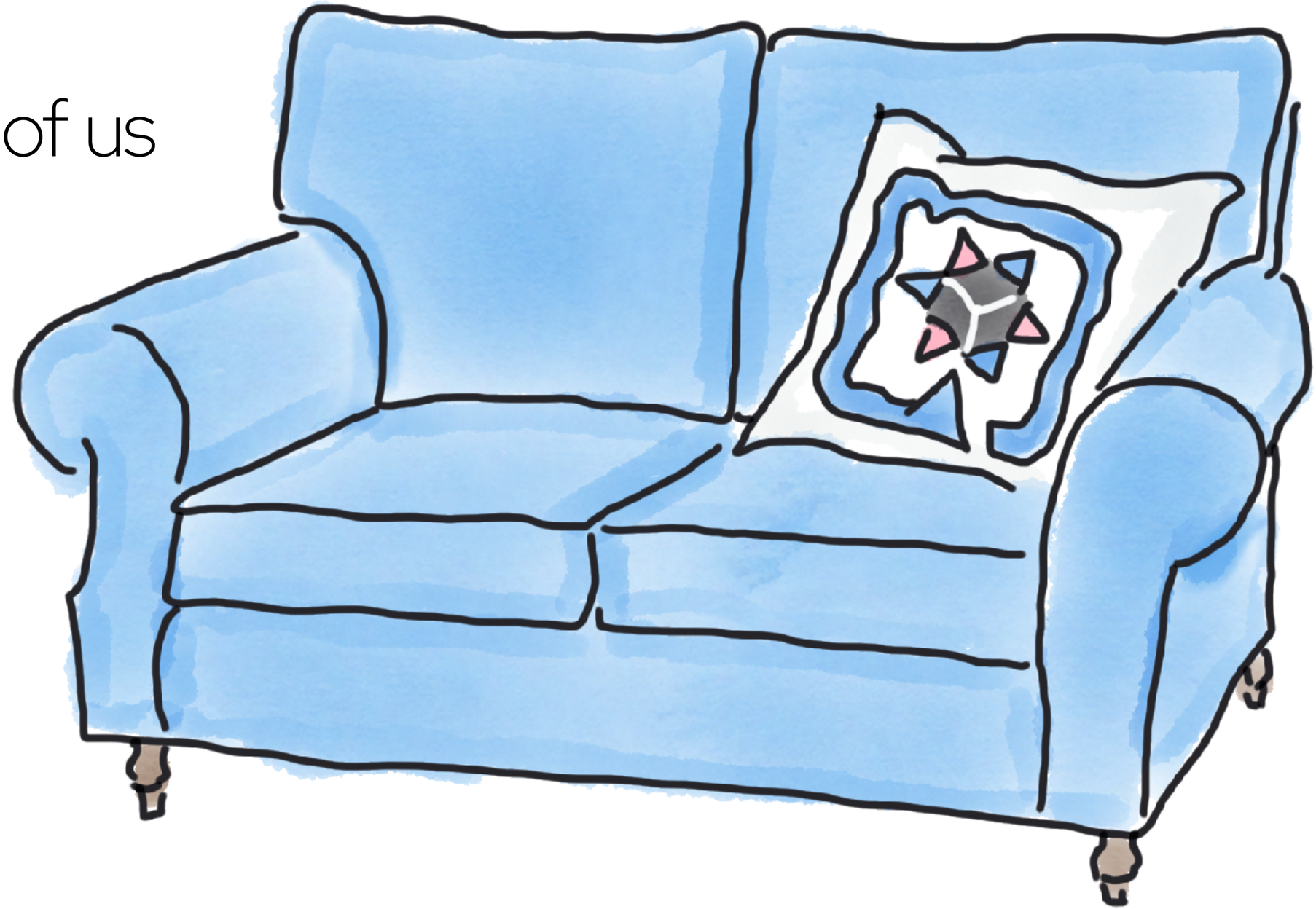

The Future of Microprocessors
https://www.youtube.com/watch?v=MkbgZMCTUyU&t=1359s
YouTube
Search
Create
More Transistors Aren't As Useful…
Performance (vs. VAX-11/780)
25%/year
52%/year
23%/year
12%/year
3.5%/year
25% – Transistors
52% – Dennard+RISC
23% – OoO, multicore
12% – Amdahl's Law
3.5% – End of easy Moore
22:17 / 57:36 • More transistors aren't as useful
The Future of Microprocessors • Sophie Wilson • GOTO 2024
GOTO Conferences
1.05M subscribers
Join
Subscribe
1.5K
Share
Thanks
Save
40K views 3 months ago Members first #ARM #GOTOcon #GOTOcph
This presentation was recorded at GOTO Copenhagen 2024. #GOTOcon #GOTOcph
https://gotocph.com
...more
154 Comments
Sort by
All
From GOTO Conferences
CPUs
Panel: Where Is SW Development Going? • Fowler,...
GOTO Conferences
15K views • 3 months ago
Architecture All Access: Modern CPU Architecture Part 1 – Key...
Intel Technology
263K views • 4 years ago
But what are Hamming codes? The origin of error correction
3Blue1Brown
2.6M views • 4 years ago
Two decades of Git: A conversation with creator Linu...
GitHub
278K views • 3 weeks ago
EXCLUSIVE: "How Fascism Works" Author Jason Stanley...
Amanpour and Company
697K views • 1 month ago
America's Economic Forecast | The Atlantic Festival 2025
The Atlantic
8.5K views • 3 days ago
New
Apache Iceberg: What It Is and Why Everyone's Talking About...
Confluent Developer
349K views • 3 weeks ago
Harvard Professor Explains Algorithms in 5 Levels of...
WIRED
4.1M views • 1 year ago
Side-Effects Are The Complexity Iceberg • Kris...
GOTO Conferences
5.1K views • 1 day ago
New
Scott Galloway on Markets, Musk, and Trump's "Weapons ...

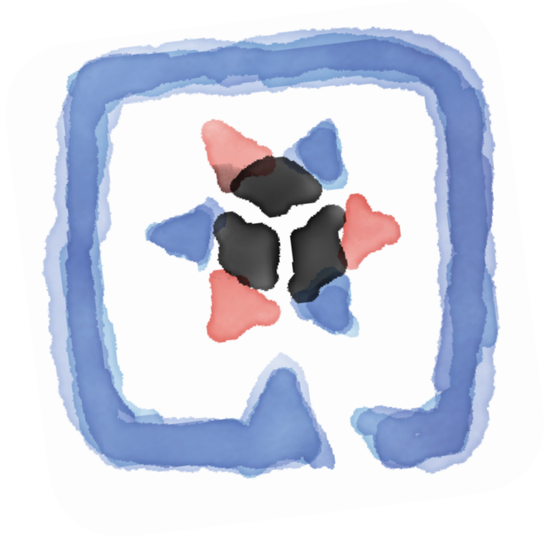
amdahl's law


speedup
20
16
12
8
4
0
1
2
4
8
16
32
64
128
256
512
1024
2048
4096
8192
16384
32768
65536
number of processors
95% parallel
90% parallel
75% parallel
50% parallel

we **have** to get good
at concurrency

but not all of us
have to :)

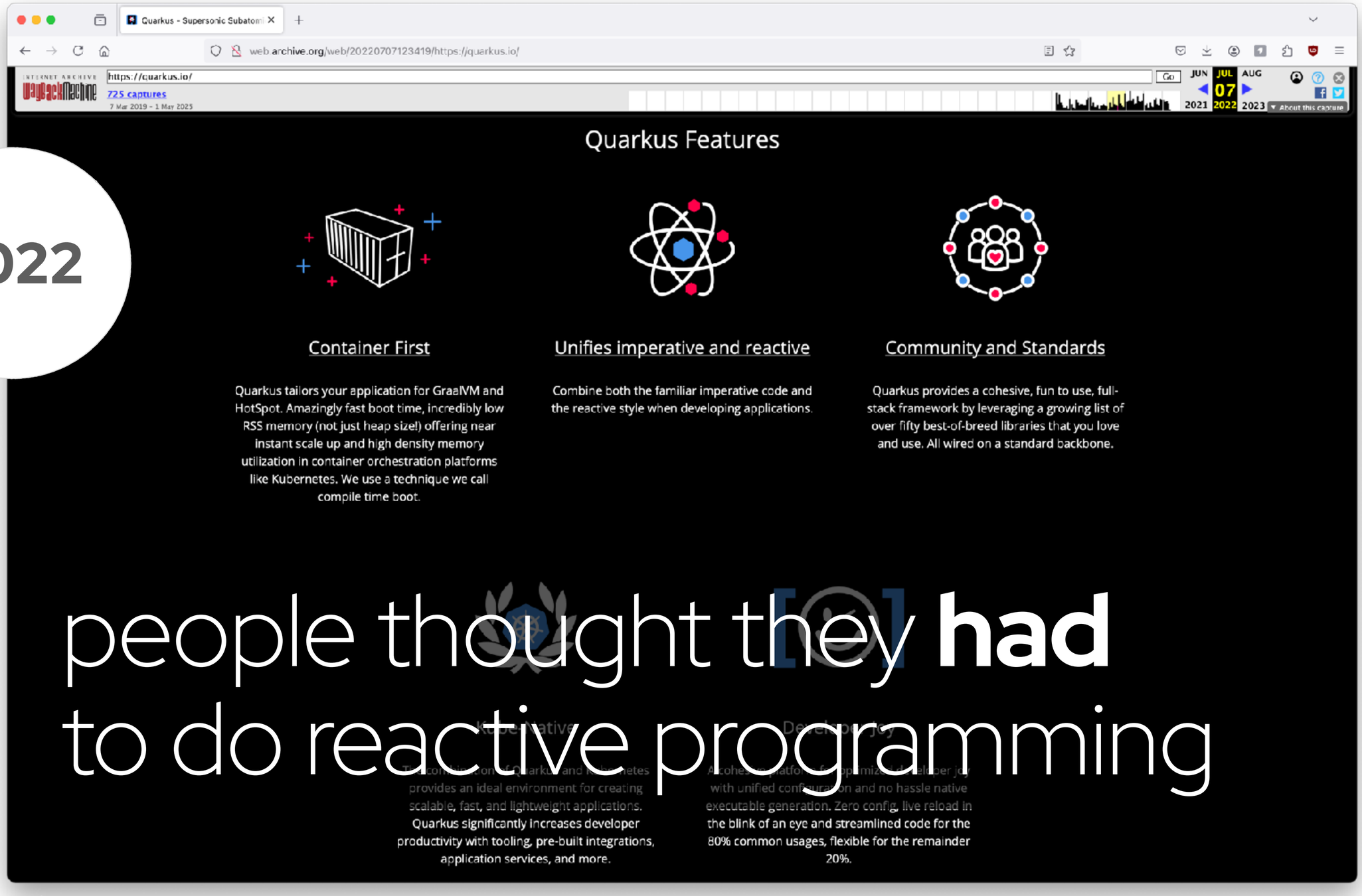




the quarkus team:

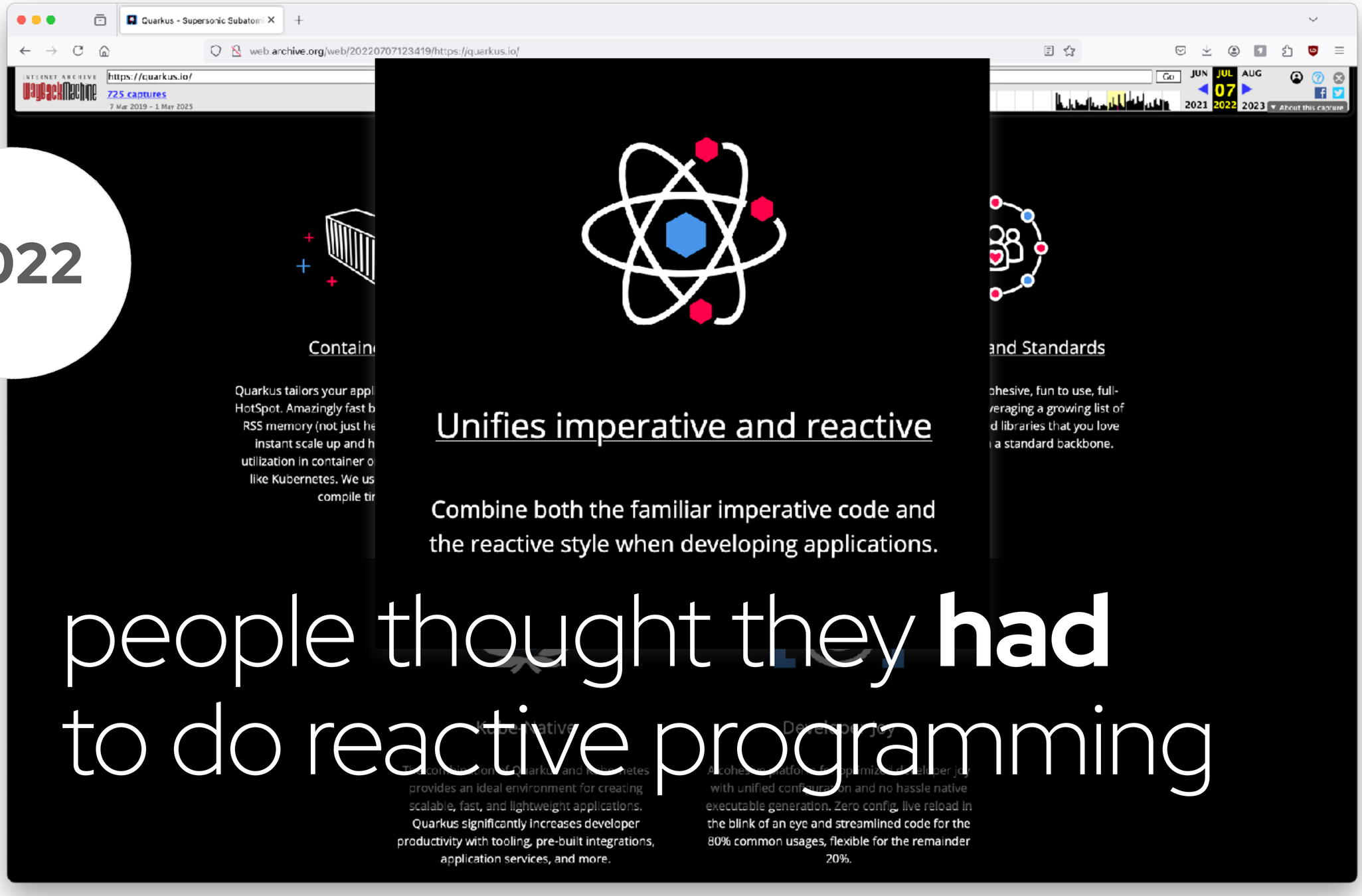
P(headache | concurrency) < 0.10

2022



people thought they **had** to do reactive programming

2022



people thought they **had** to do reactive programming

2025

Quarkus - Supersonic Subatomi

https://quarkus.io

80%

Quarkus Benefits

Developer Joy

A cohesive platform for optimized developer joy with unified configuration and no hassle native executable generation. Zero config, live reload in the blink of an eye and streamlined code for the 80% common usages, flexible for the remainder 20%.

Performance

Quarkus streamlines framework optimizations in the build phase to reduce runtime dependencies and improve efficiency. By precomputing metadata and optimizing class loading, it ensures fast startup times for JVM and native binary deployments, cutting down on memory usage.

Kube-Native

The combination of Quarkus and Kubernetes provides an ideal environment for creating scalable, fast, and lightweight applications. Quarkus significantly increases developer productivity with tooling, pre-built integrations, application services, and more.

Community and Standar

Quarkus provides a cohesive, fun to use, full stac
leveraging a growing list of over fifty best-of-breed
love and use. All wired on a standard bac

Reactive Core

Built on a robust reactive core, Quarkus ensures fast and efficient performance, supporting the development of a wide variety of modern applications.

Container First

our application for GraalVM and HotSpot.
ime, incredibly low RSS memory (not just heap
r instant scale up and high density memory
er orchestration platforms like Kubernetes. We
hnique we call compile time boot.

Lufthansa Technik

ADOPTIUM

framework

framework

fast reactive core
… if it’s quarkus :)

user code

framework

fast reactive core
... if it's quarkus :)

reactive programming model

user code

framework

fast reactive core
... if it's quarkus :)

reactive programming model

virtual threads

user code

framework

fast reactive core

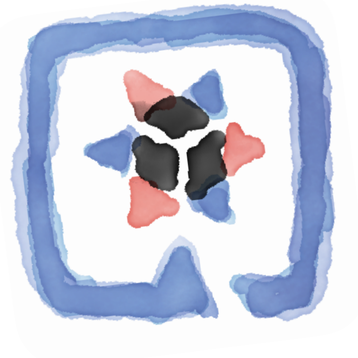
... if it's quarkus :)

user code

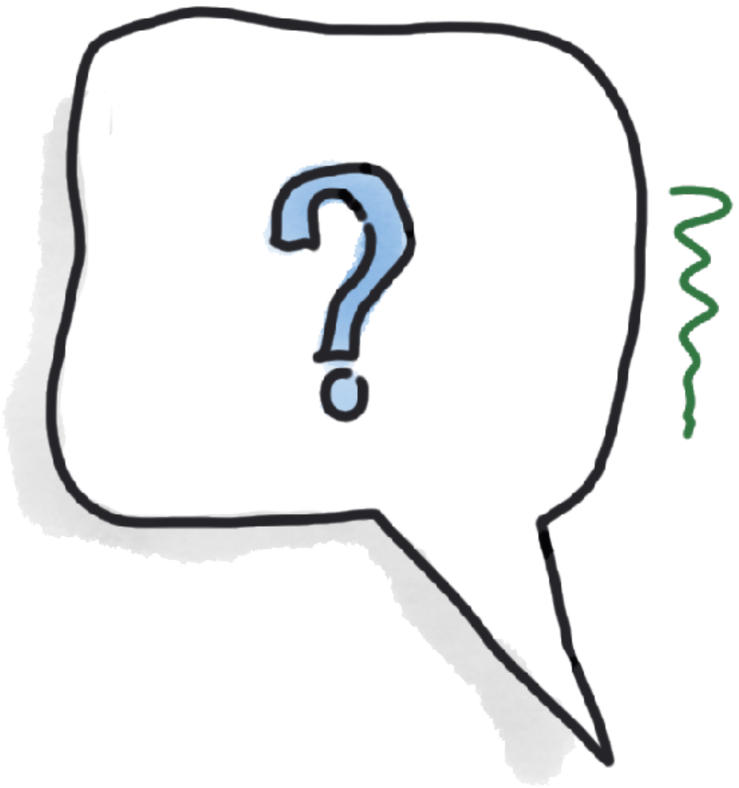
reactive programming model
virtual threads
structured concurrency

framework

fast reactive core
... if it's quarkus :)



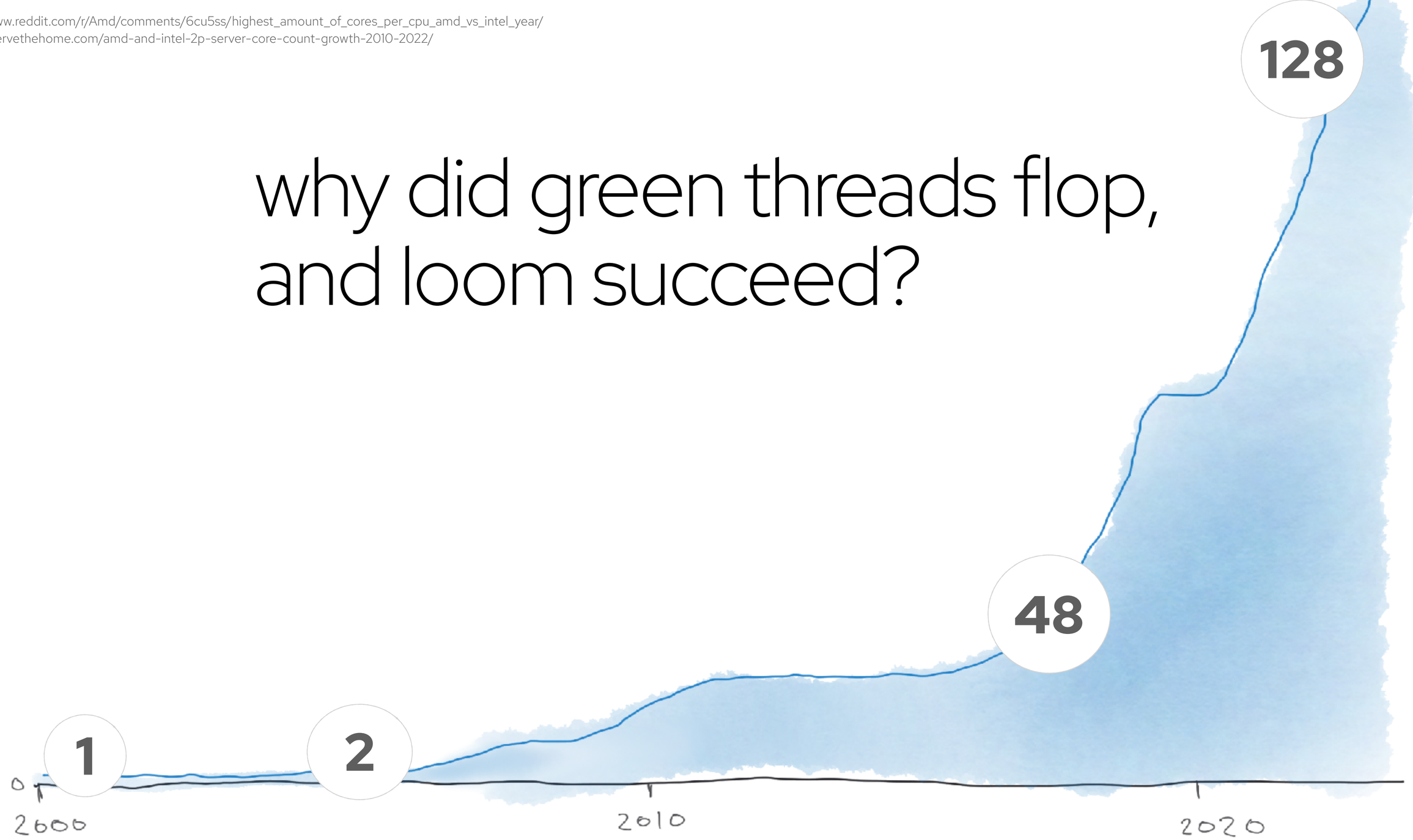
@RunOnVirtualThread



why did green threads flop,
and loom succeed?

sources: https://www.reddit.com/r/Amd/comments/6cu5ss/highest_amount_of_cores_per_cpu_amd_vs_intel_year/
and https://www.servethehome.com/amd-and-intel-2p-server-core-count-growth-2010-2022/

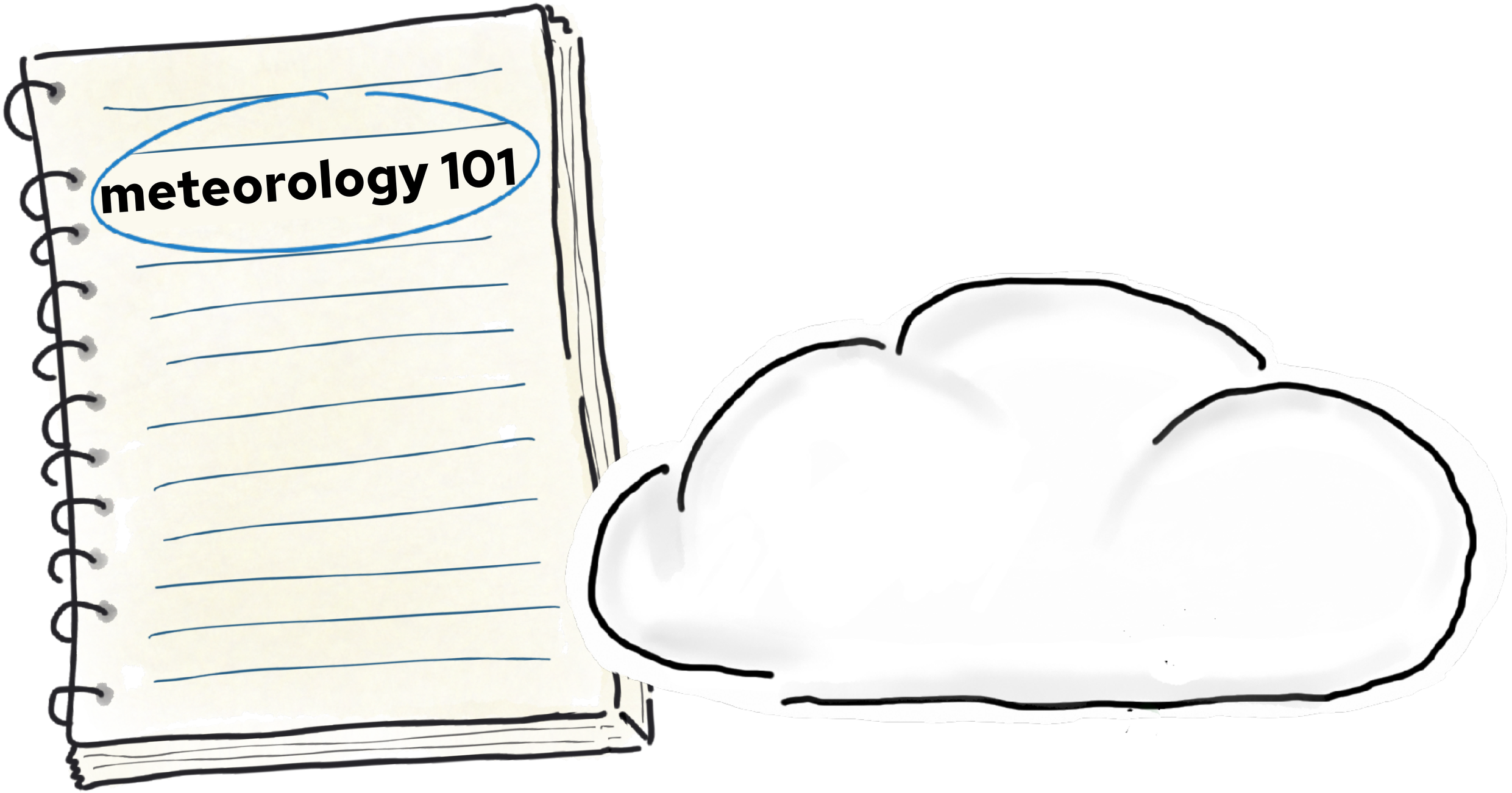
why did green threads flop, and loom succeed?

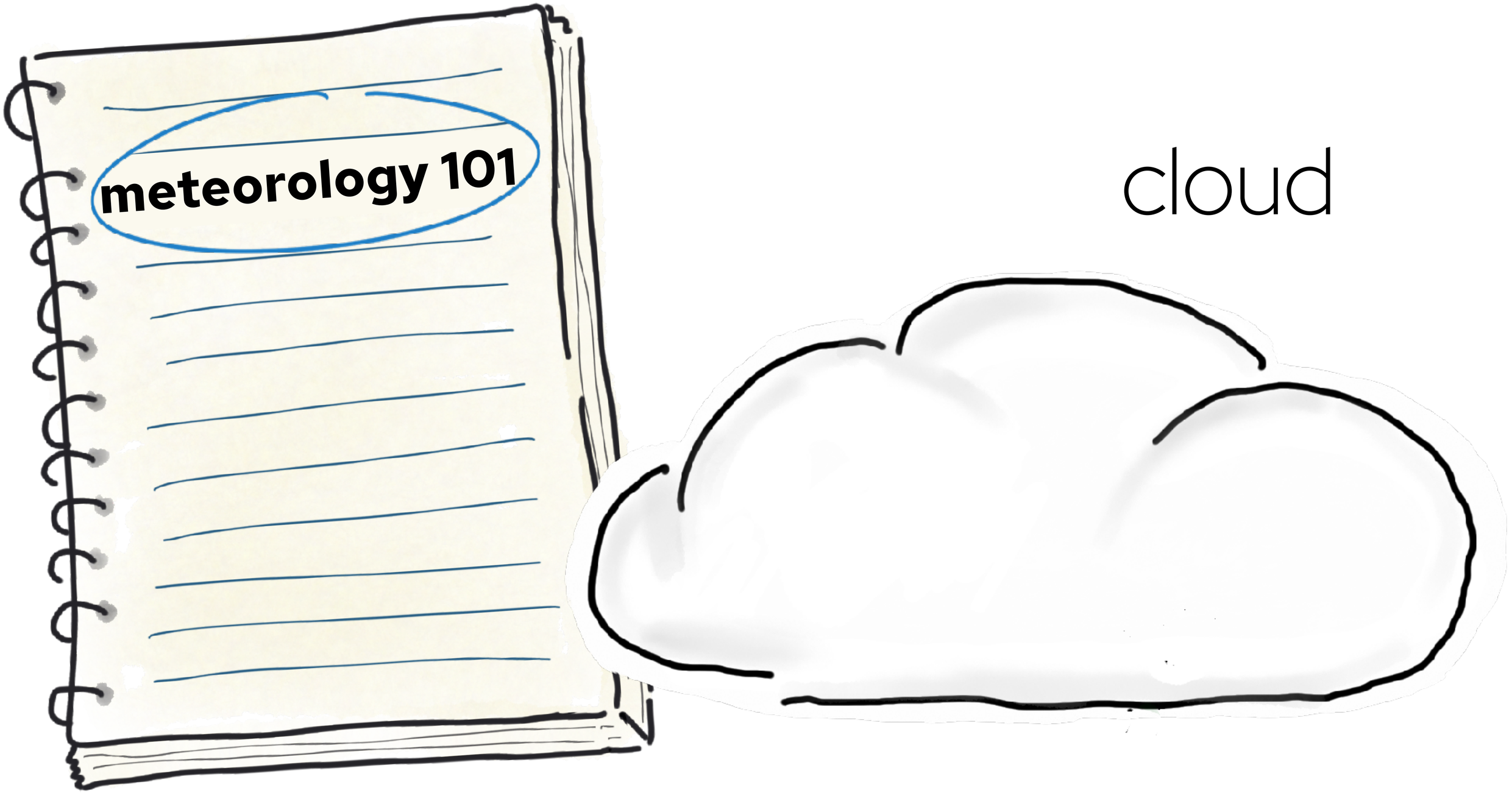




why was AOT a bad idea,
but GraalVM is a good one?

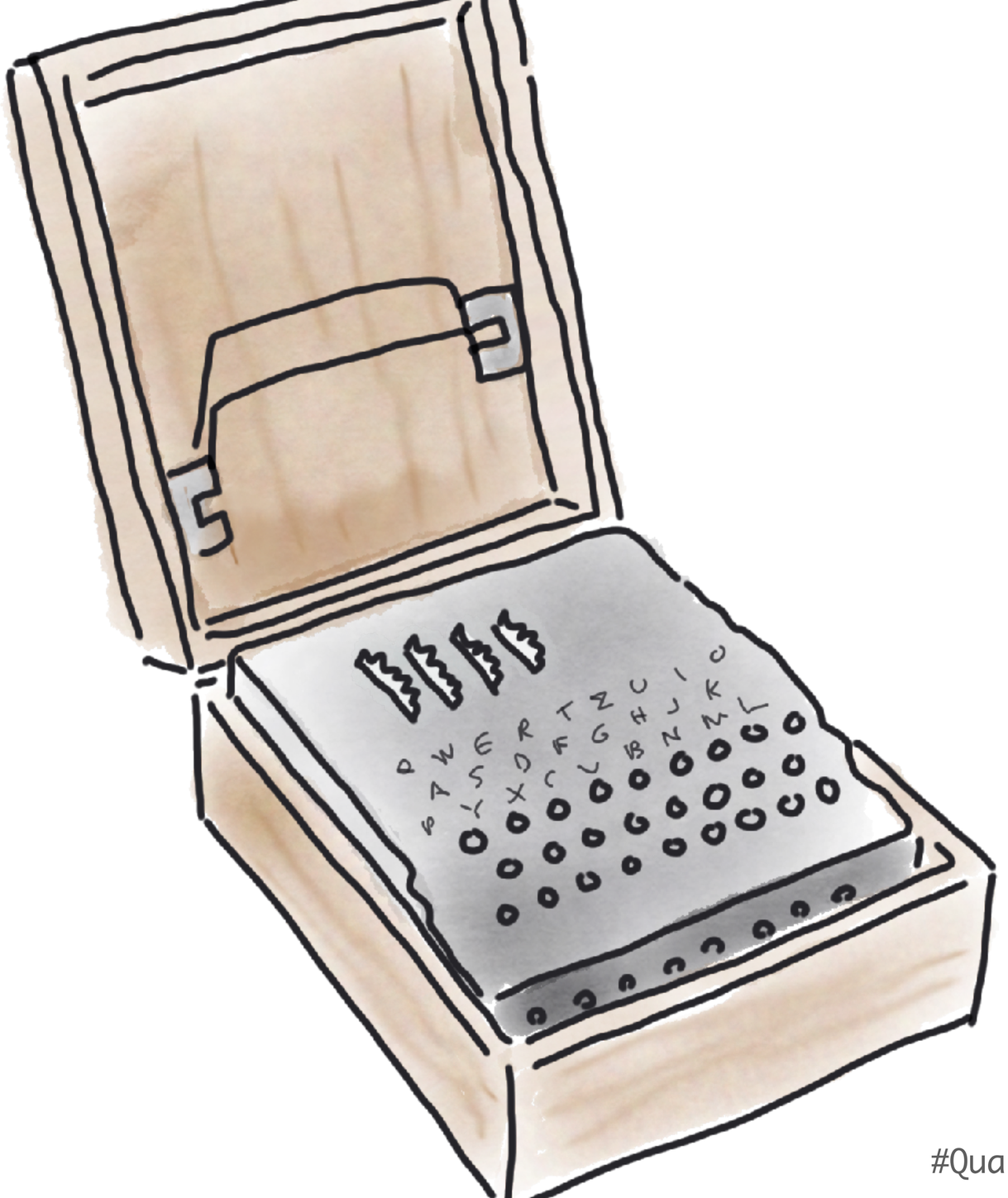

meteorology 101

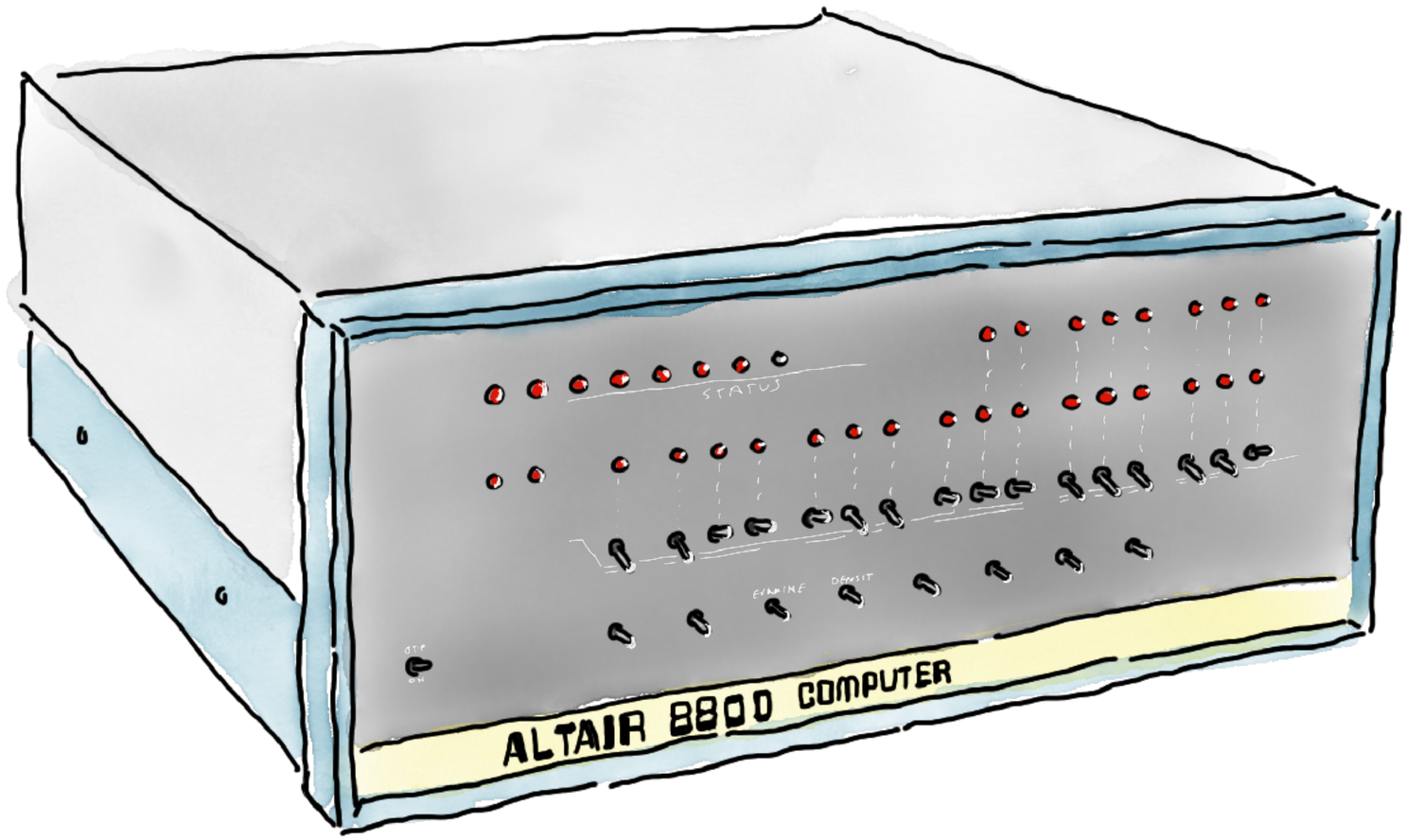

meteorology 101

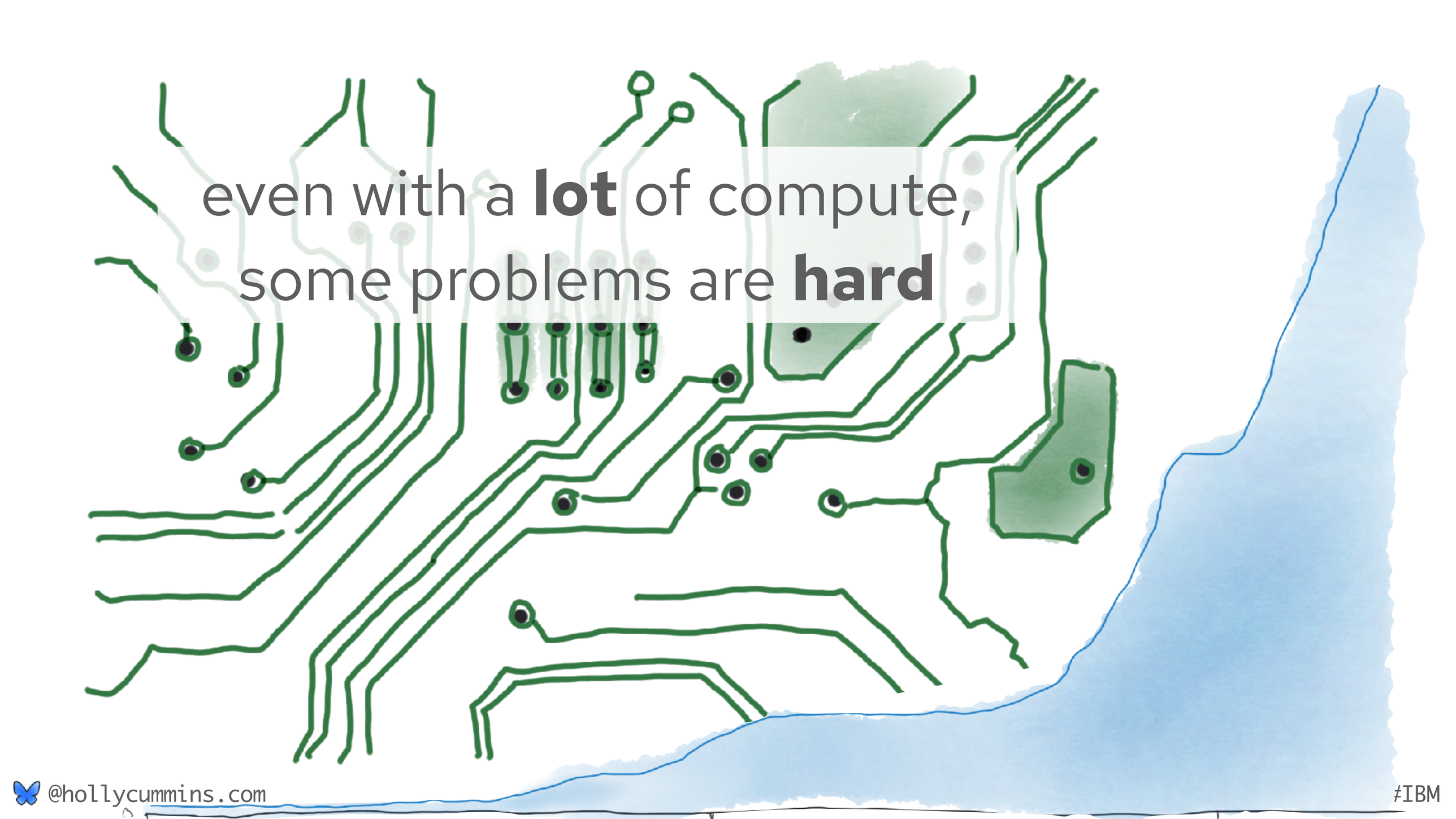

meteorology 101
cloud



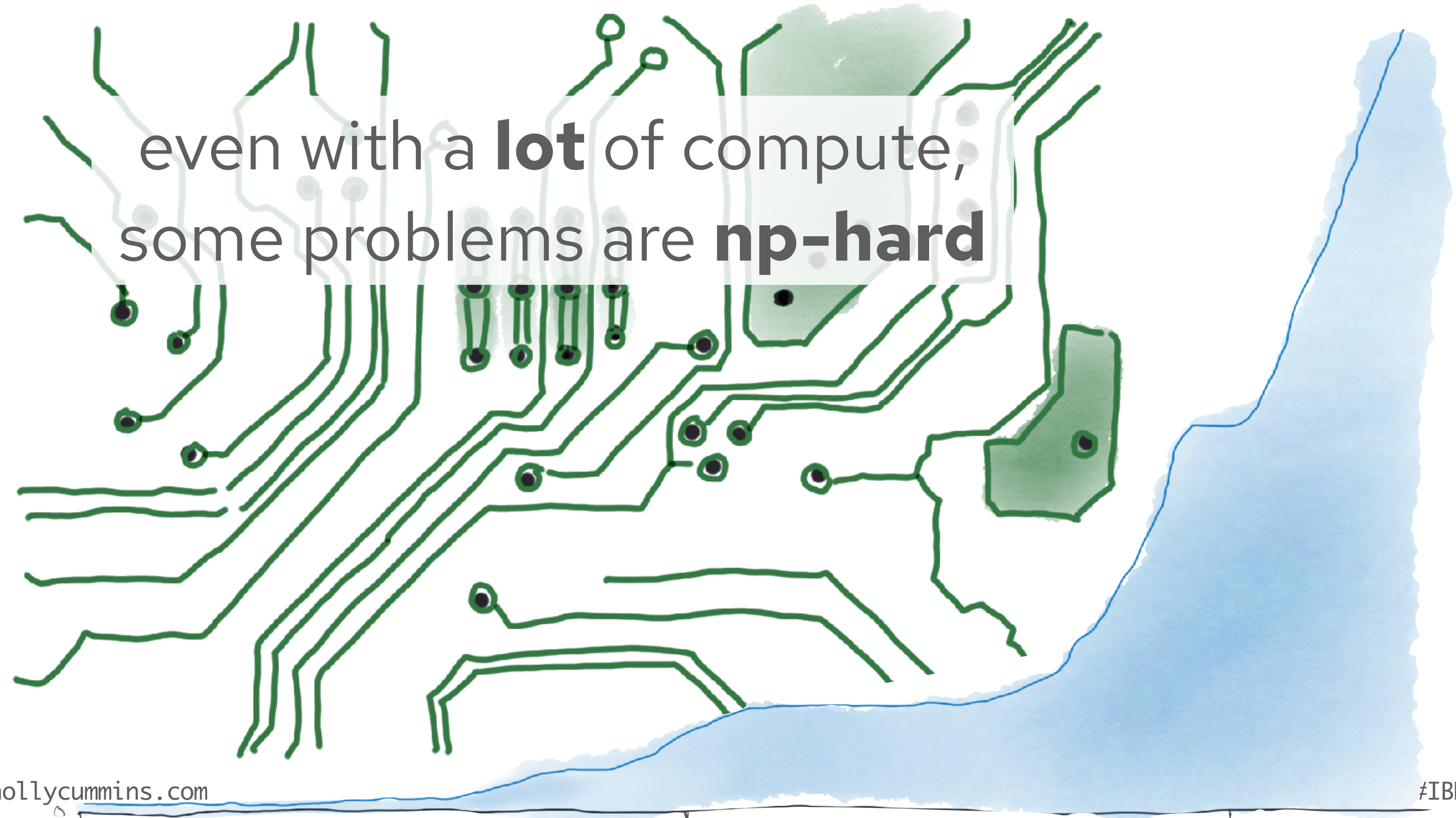
is my encrypted data safe?

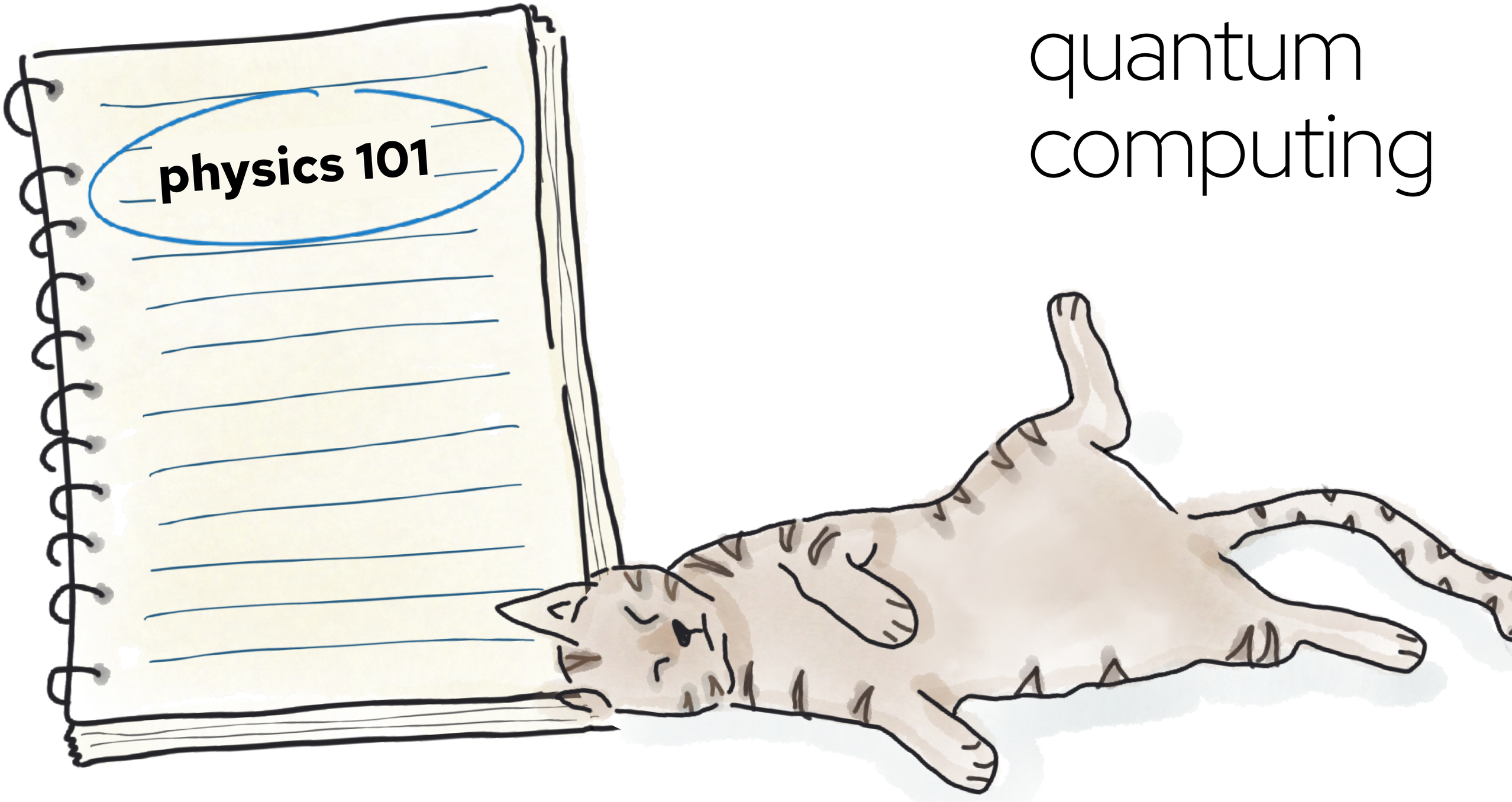



STATUS
EXAMINE
DEPOSIT
ALTAIR 8800 COMPUTER


even with a **lot** of compute,
some problems are **hard**

even with a **lot** of compute,
some problems are **np-hard**

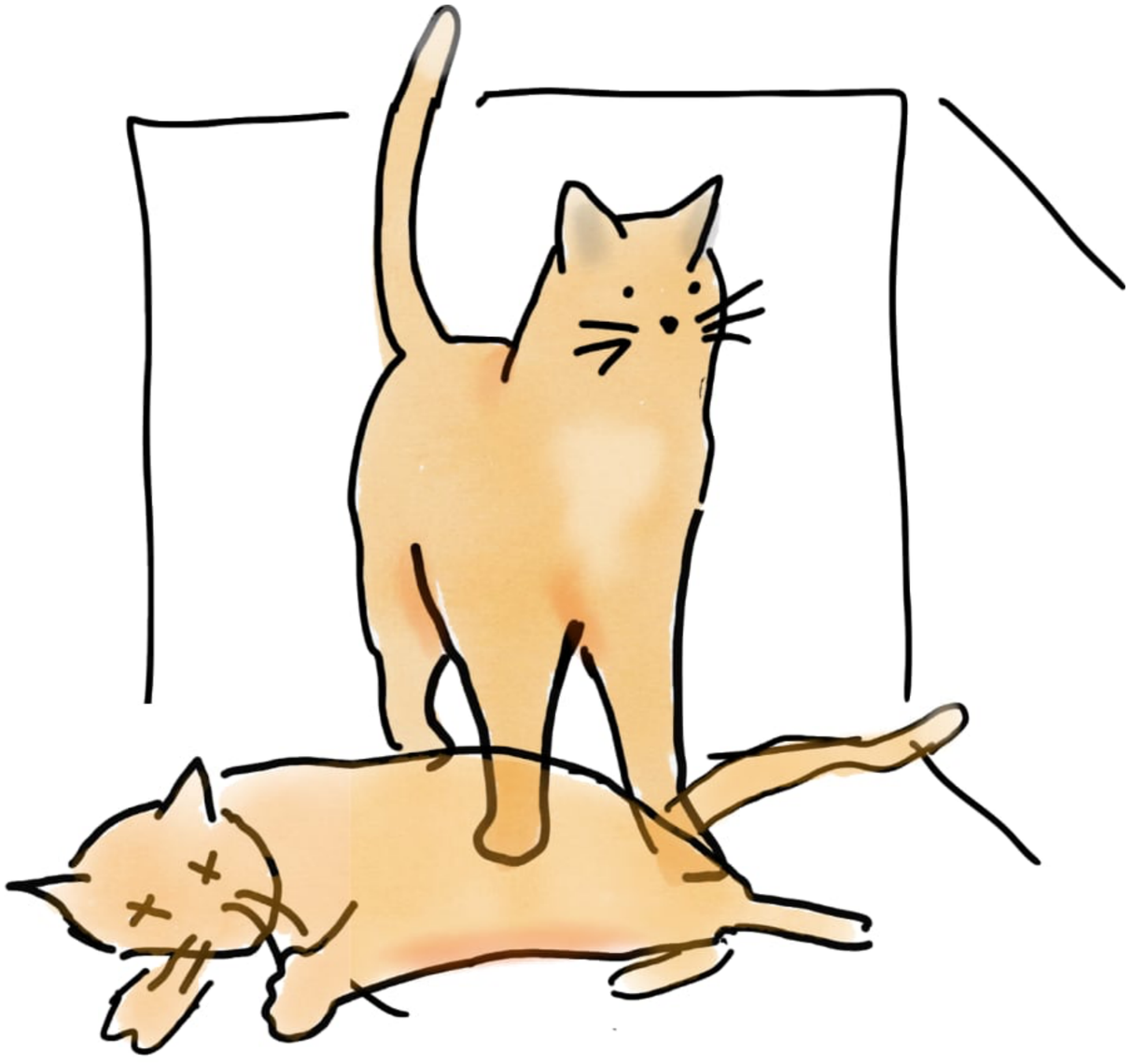




quantum
computing

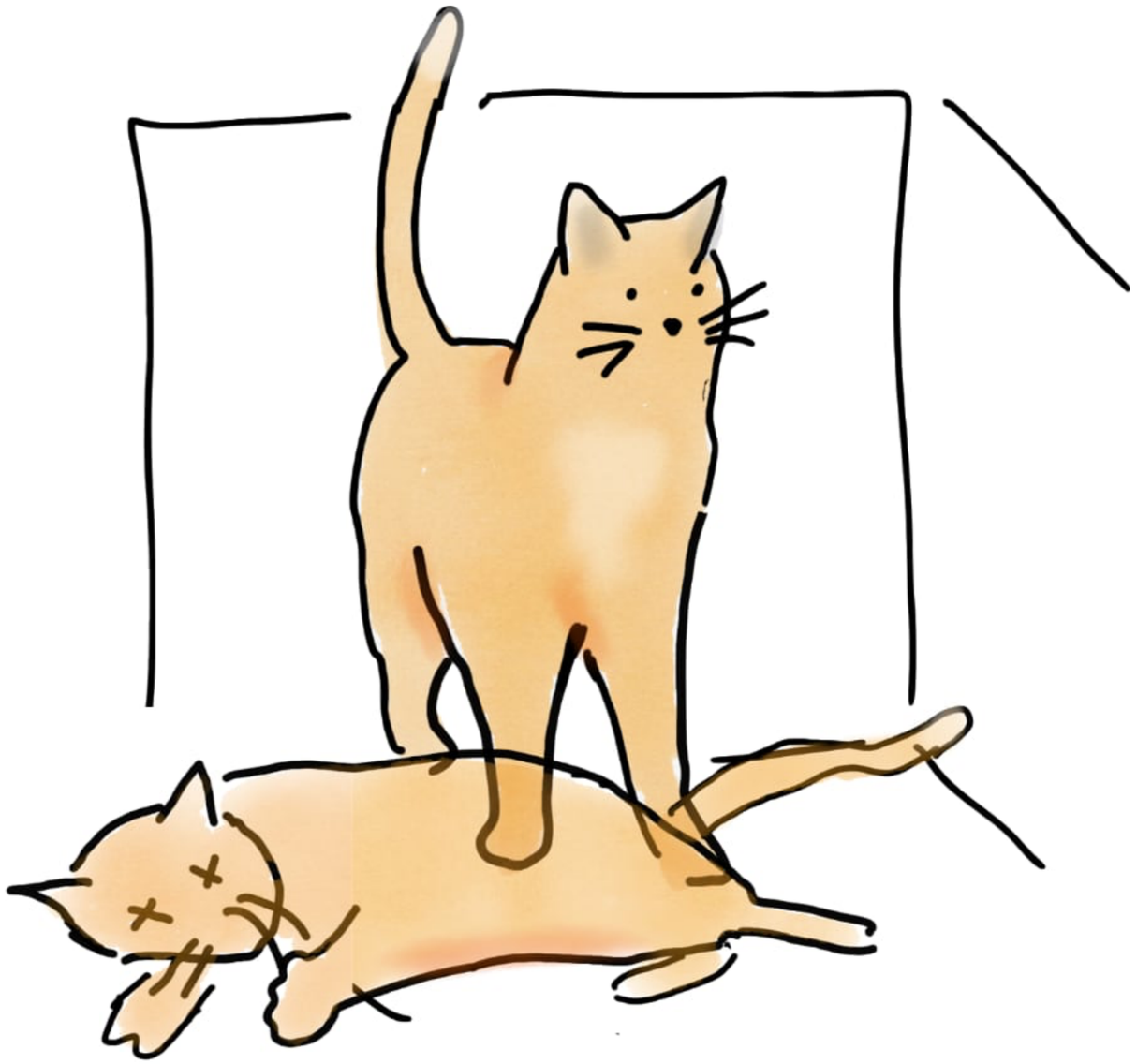
0

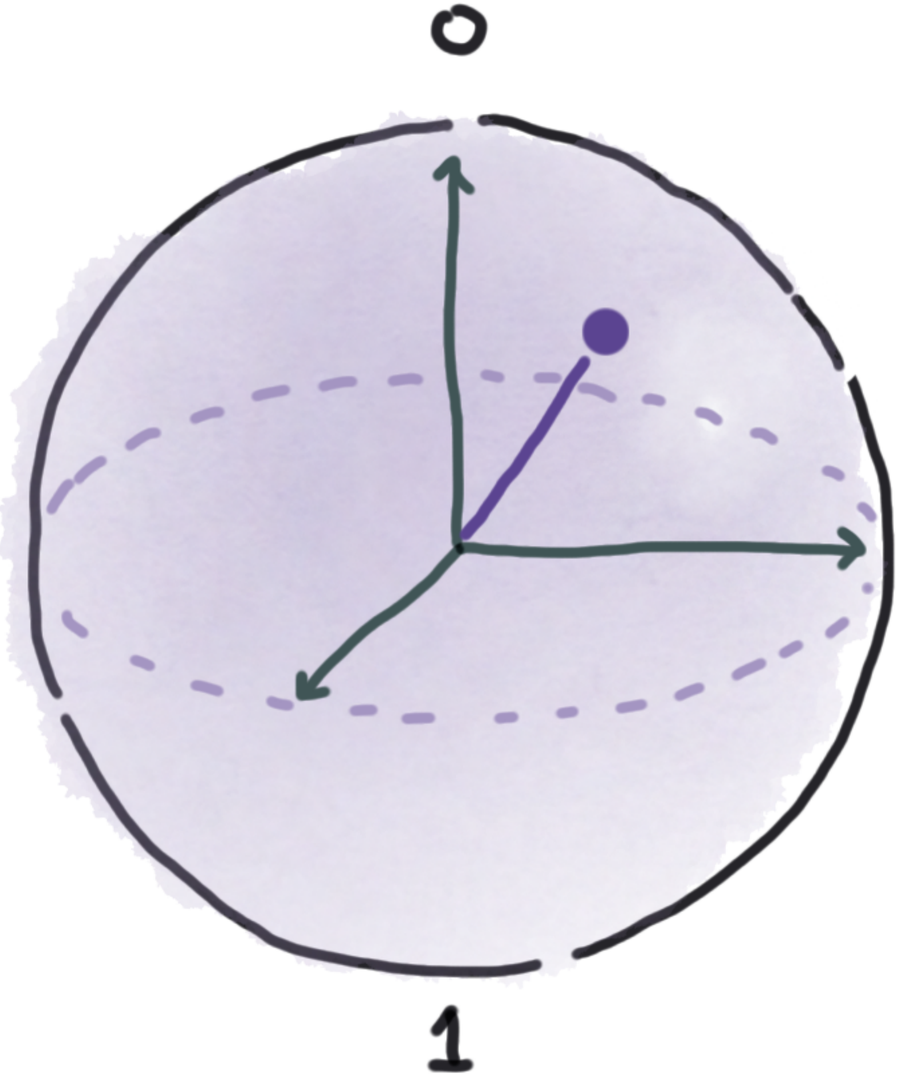
1



qubit

both 0 and 1




0
1

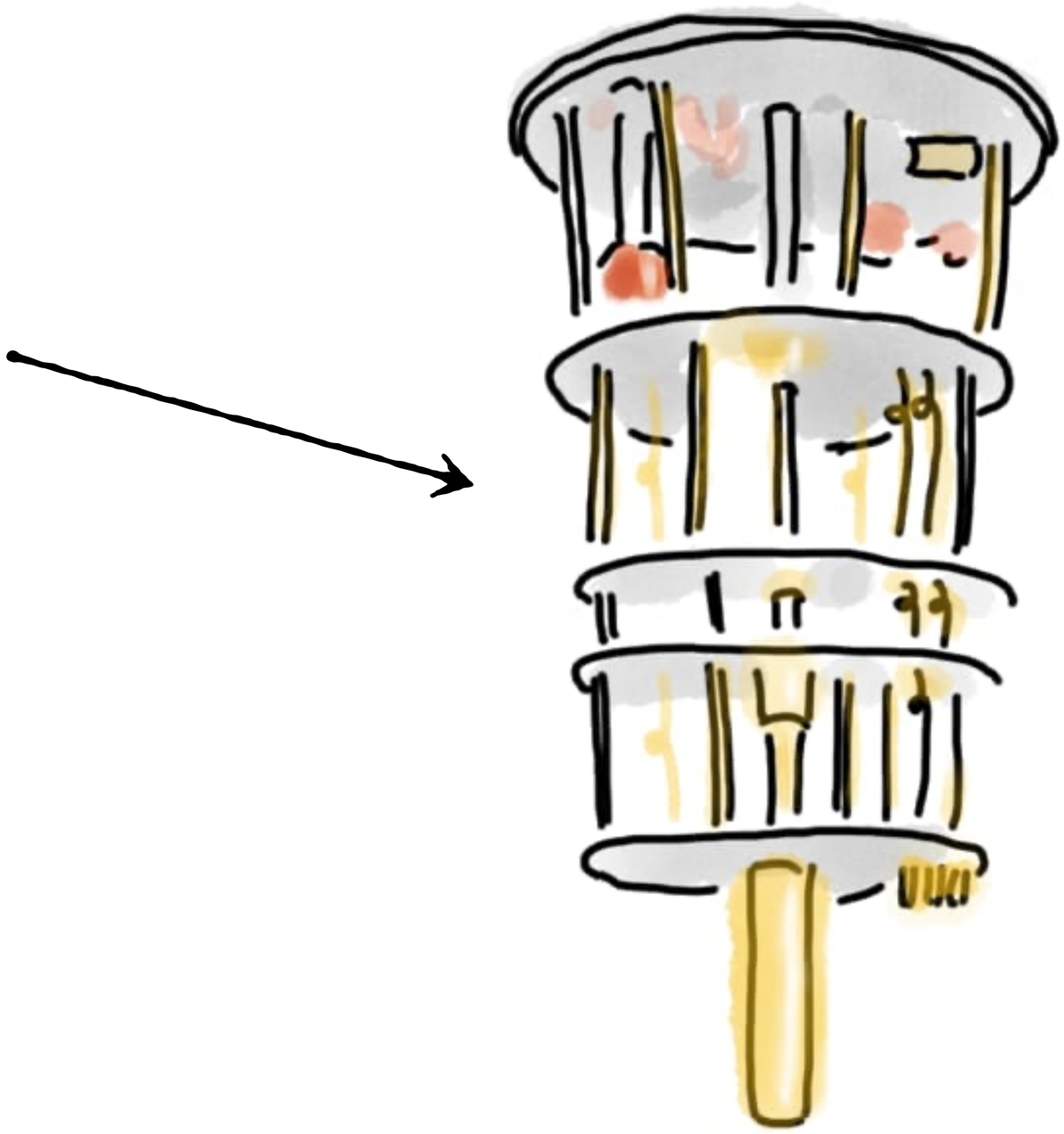
quantum computers
are becoming **real**





fridge

colder than the space
between the stars



fridge

colder than the space between the stars



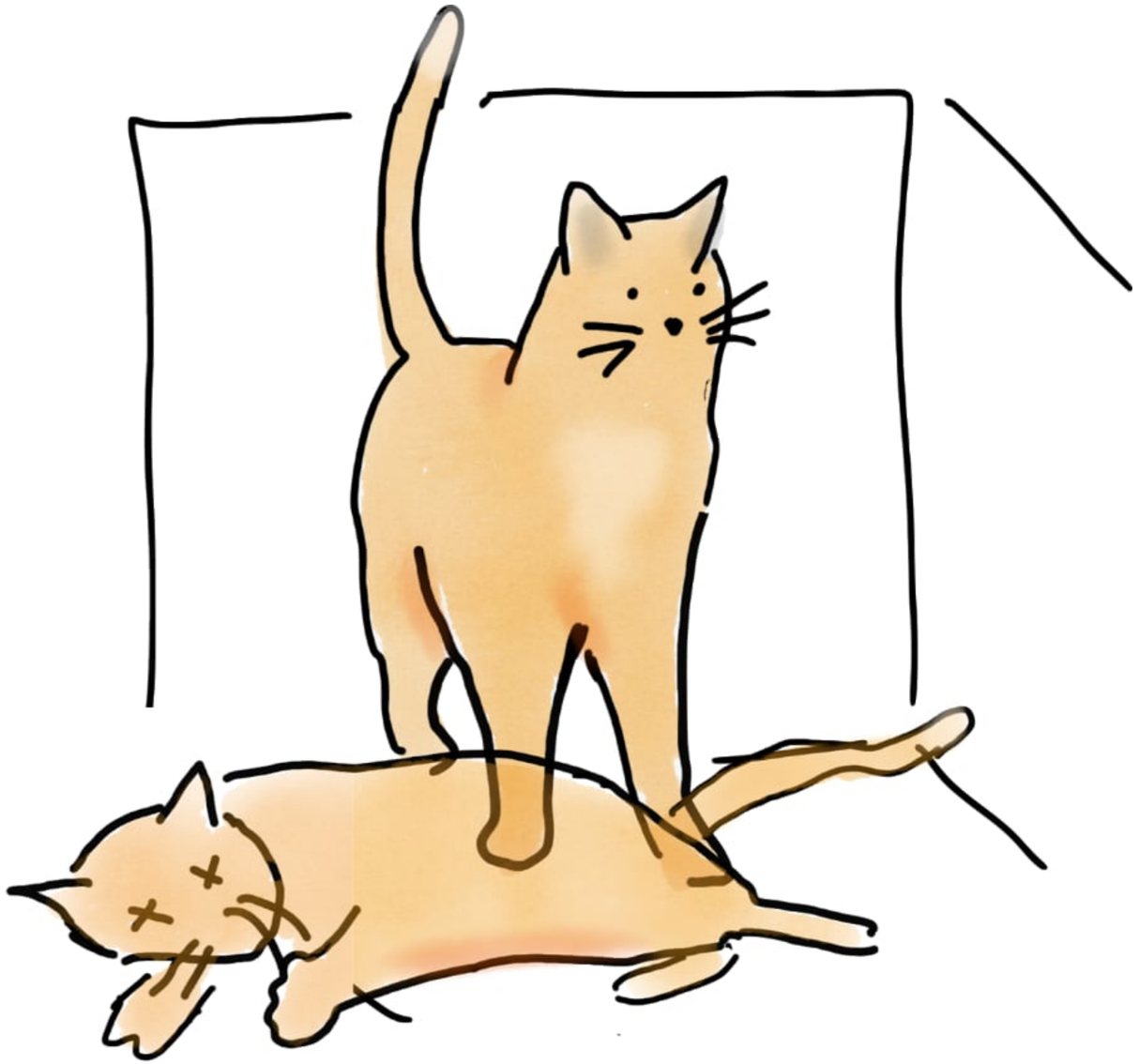
actual quantum chip

quantum computers would crack most public-key cryptography

quantum computers would crack most public-key cryptography

... but big enough ones don't exist yet

schrodinger's cryptography

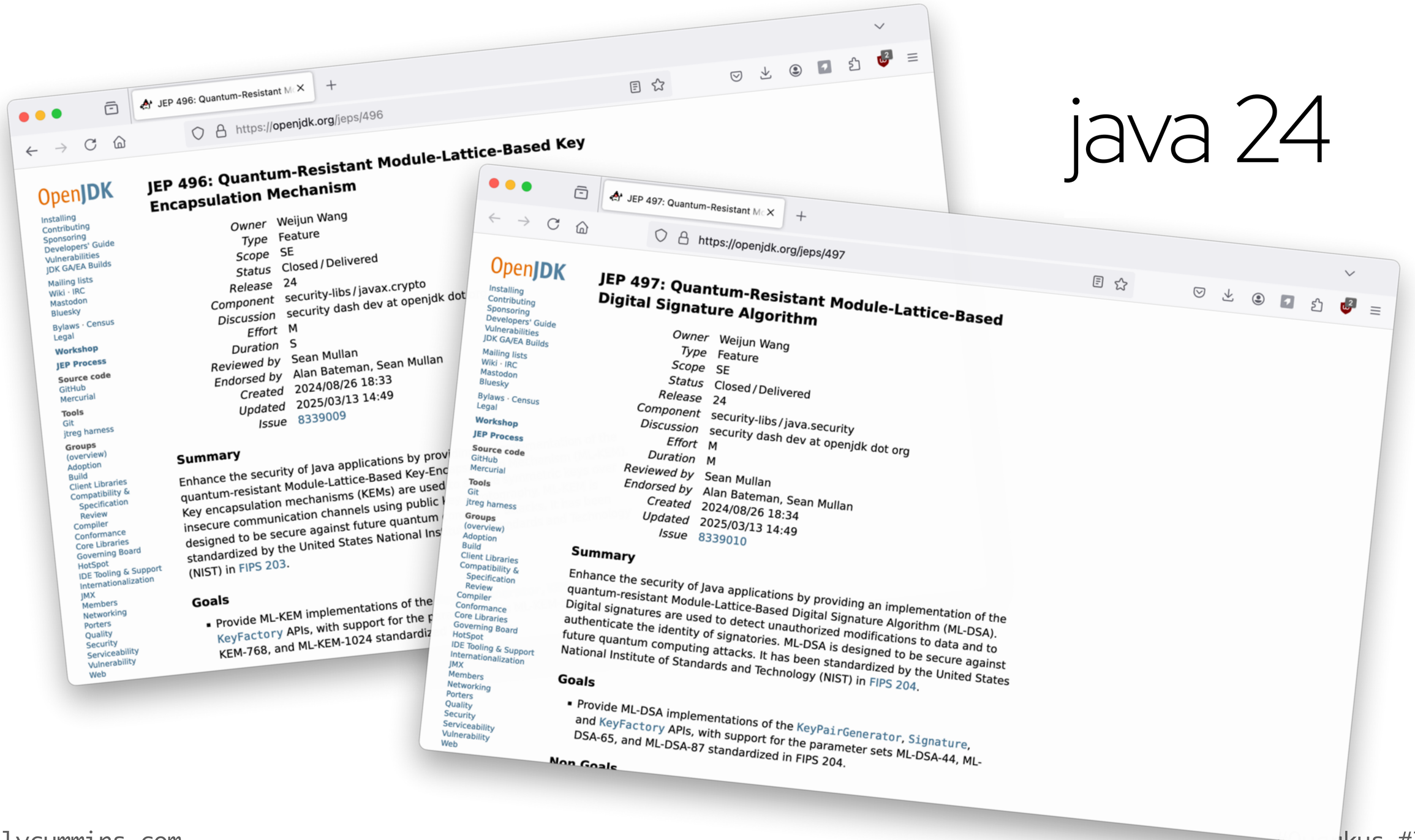


quantum computers would crack most public-key cryptography

quantum computers would crack most public-key cryptography

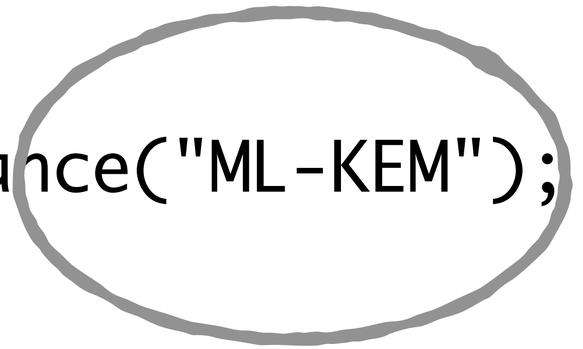
... but not **all** public-key cryptography

java 24


JEP 496: Quantum-Resistant
https://openjdk.org/jeps/496
OpenJDK
JEP 496: Quantum-Resistant Module-Lattice-Based Key Encapsulation Mechanism
Owner Weijun Wang
Type Feature
Scope SE
Status Closed / Delivered
Release 24
Component security-libs / javax.crypto
Discussion security dash dev at openjdk dot
Effort M
Duration S
Reviewed by Sean Mullan
Endorsed by Alan Bateman, Sean Mullan
Created 2024/08/26 18:33
Updated 2025/03/13 14:49
Issue 8339009
Summary
Goals
JEP 497: Quantum-Resistant
https://openjdk.org/jeps/497
OpenJDK
JEP 497: Quantum-Resistant Module-Lattice-Based Digital Signature Algorithm
Owner Weijun Wang
Type Feature
Scope SE
Status Closed / Delivered
Release 24
Component security-libs / java.security
Discussion security dash dev at openjdk dot org
Effort M
Duration M
Reviewed by Sean Mullan
Endorsed by Alan Bateman, Sean Mullan
Created 2024/08/26 18:34
Updated 2025/03/13 14:49
Issue 8339010
Summary
Enhance the security of Java applications by providing an implementation of the quantum-resistant Module-Lattice-Based Digital Signature Algorithm (ML-DSA). Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of signatories. ML-DSA is designed to be secure against future quantum computing attacks. It has been standardized by the United States National Institute of Standards and Technology (NIST) in FIPS 204.
Goals
Provide ML-DSA implementations of the KeyPairGenerator, Signature, and KeyFactory APIs, with support for the parameter sets ML-DSA-44, ML-DSA-65, and ML-DSA-87 standardized in FIPS 204.
Non-Goals

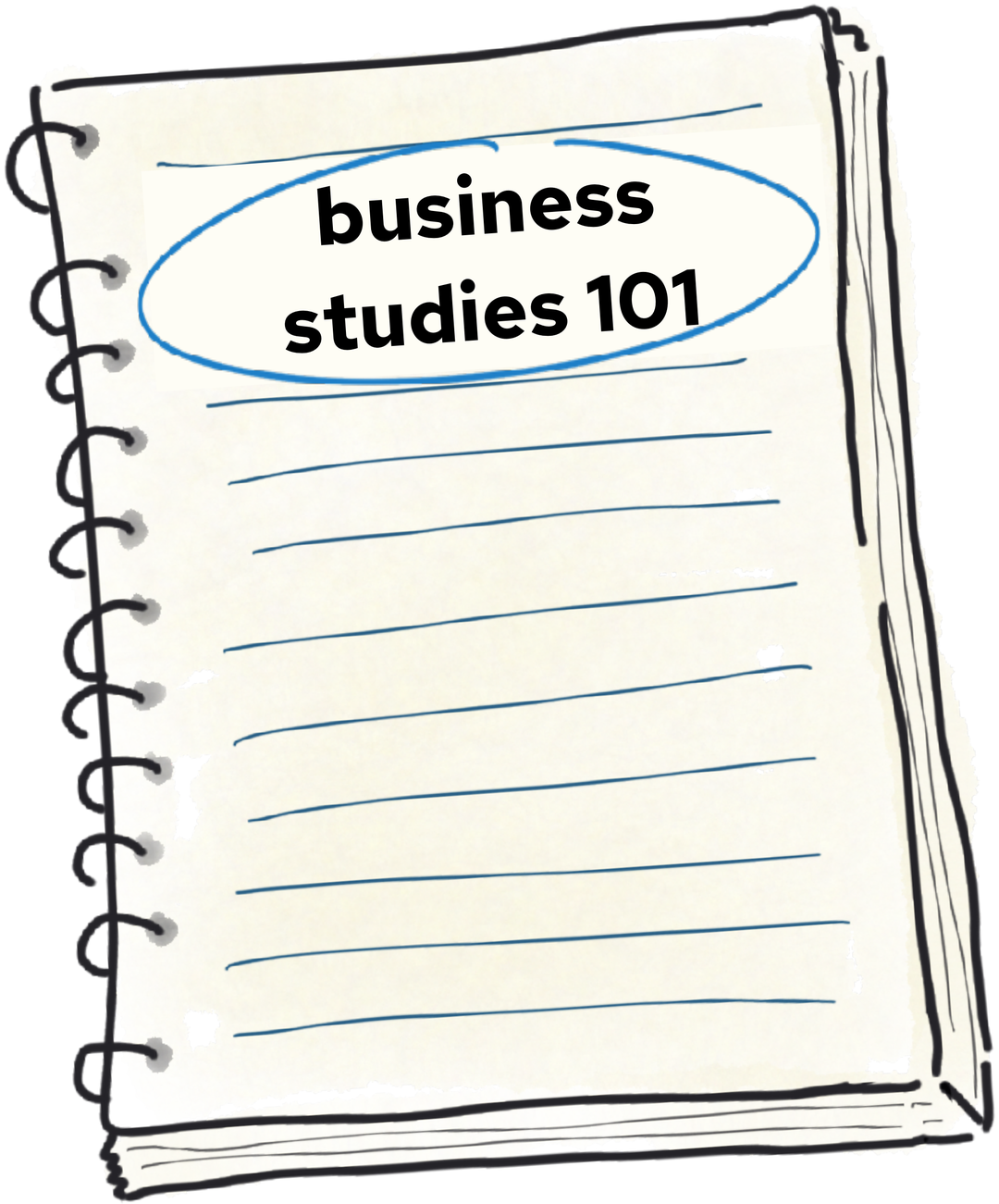
```
KeyPairGenerator g = KeyPairGenerator.getInstance("ML-KEM");
```

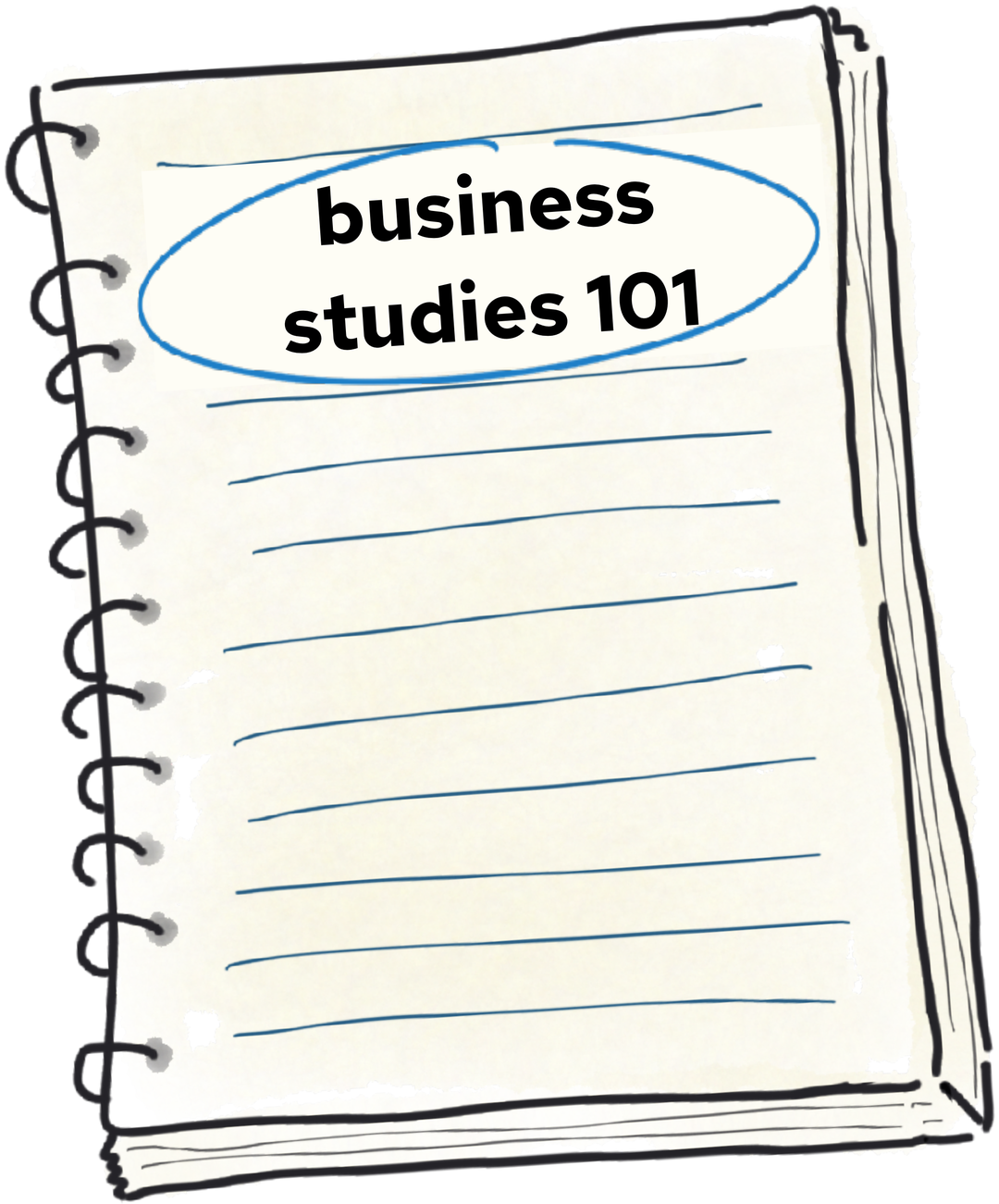
```
KeyPairGenerator g = KeyPairGenerator.getInstance("ML-KEM");
```



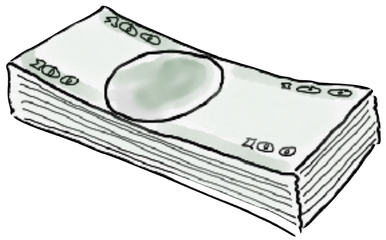


why is there all this hype, always?


business
studies 101

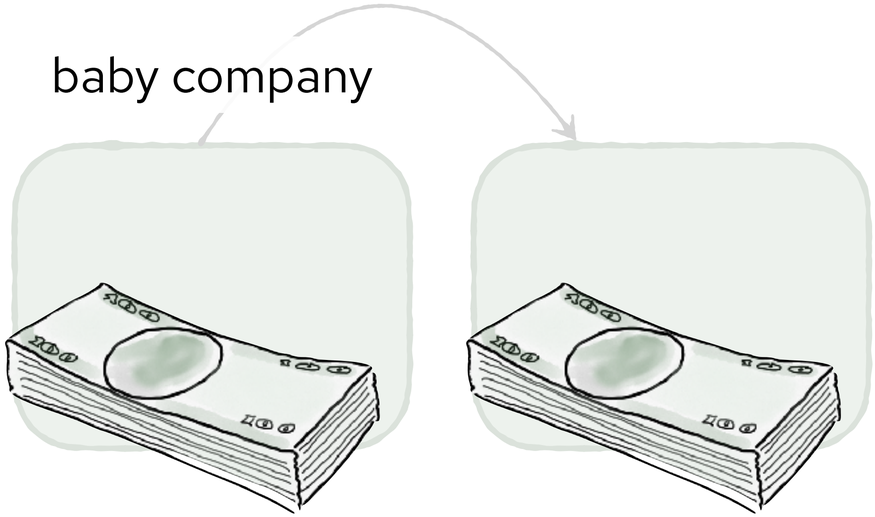


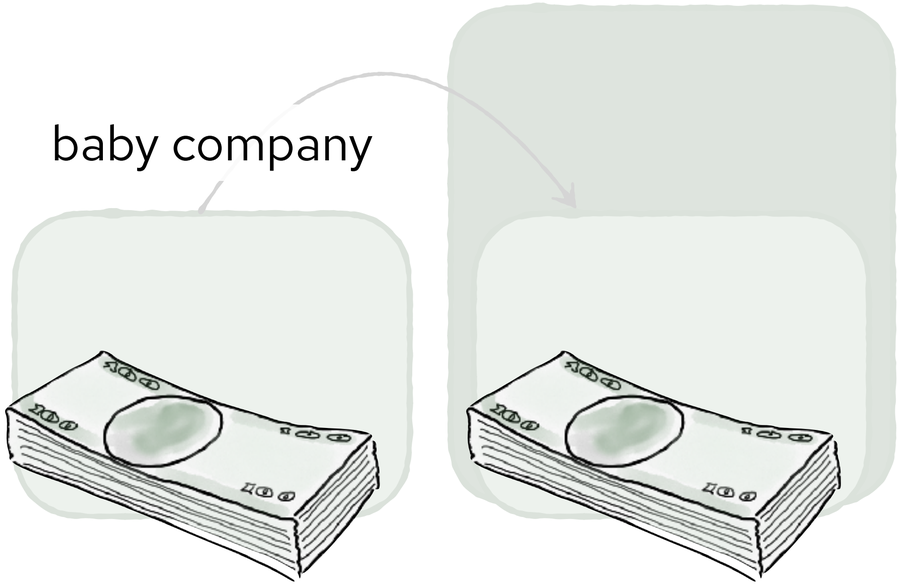
venture capital



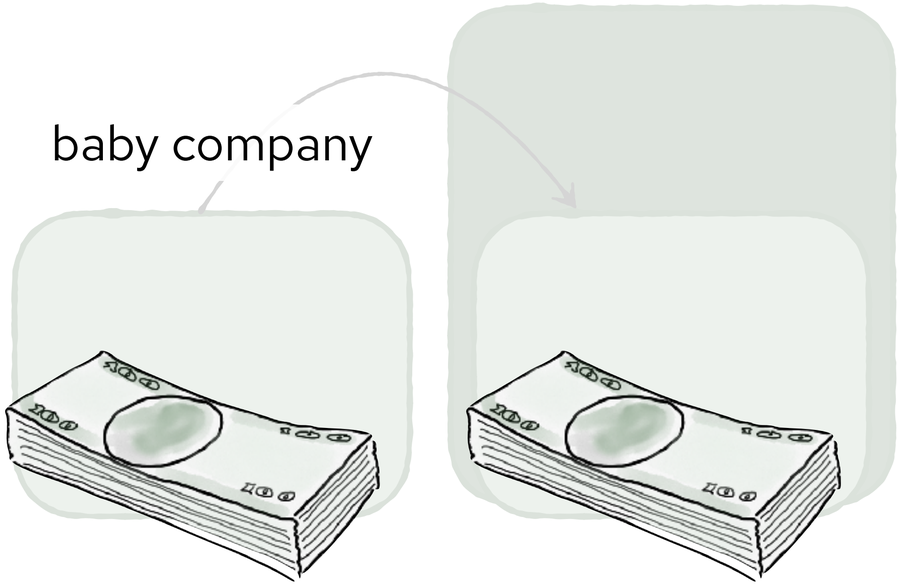
baby company




baby company


baby company

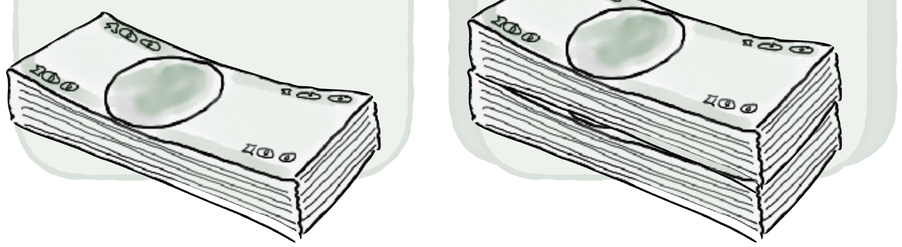
funding rounds



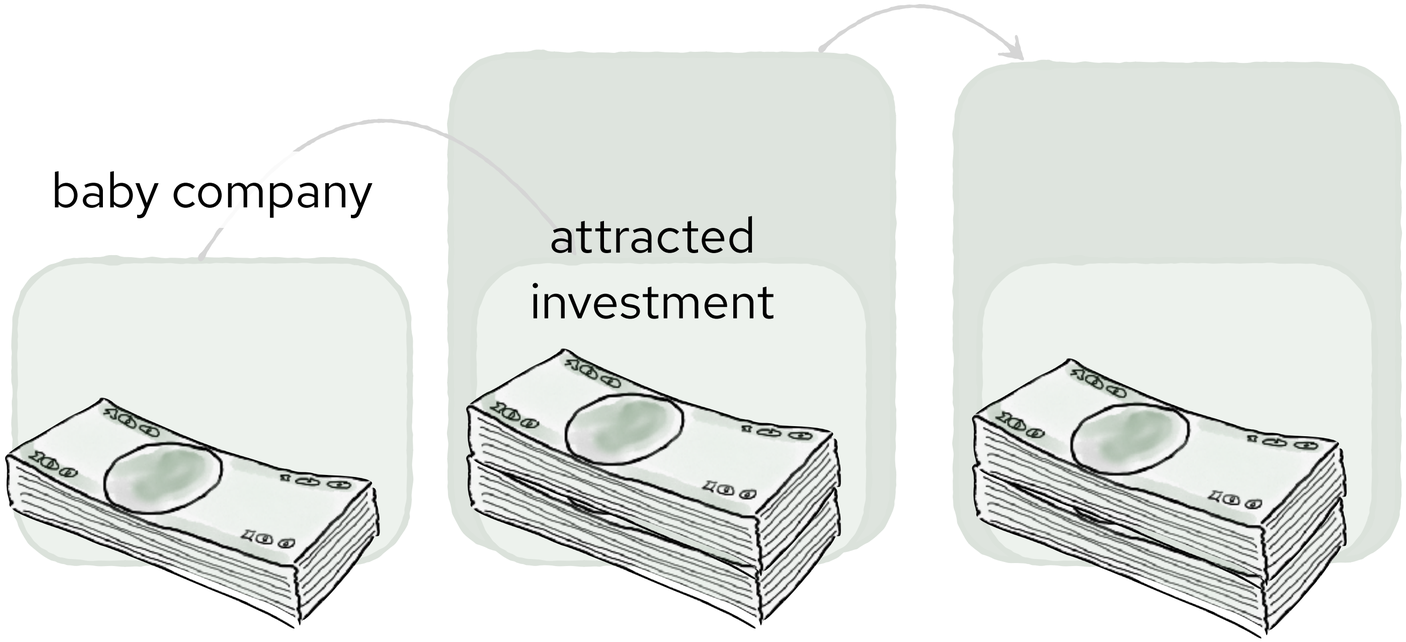
funding rounds

baby company

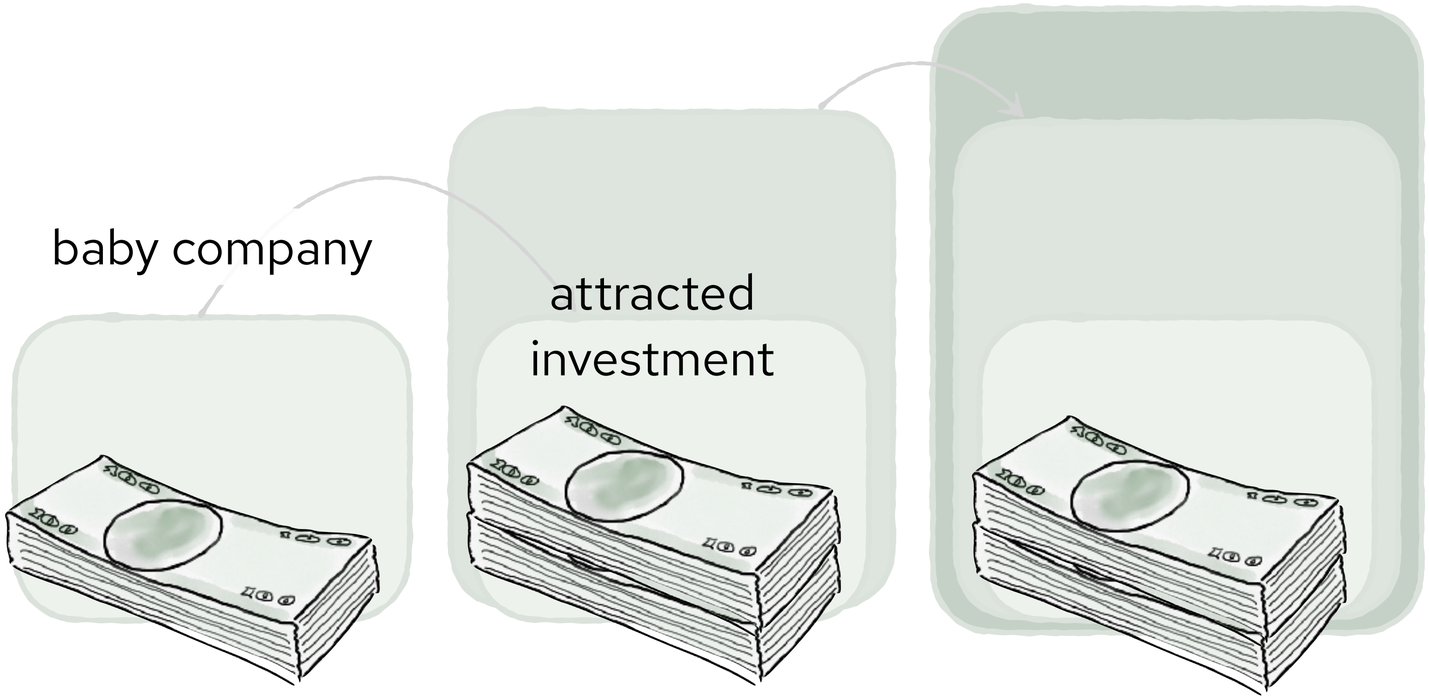
attracted investment



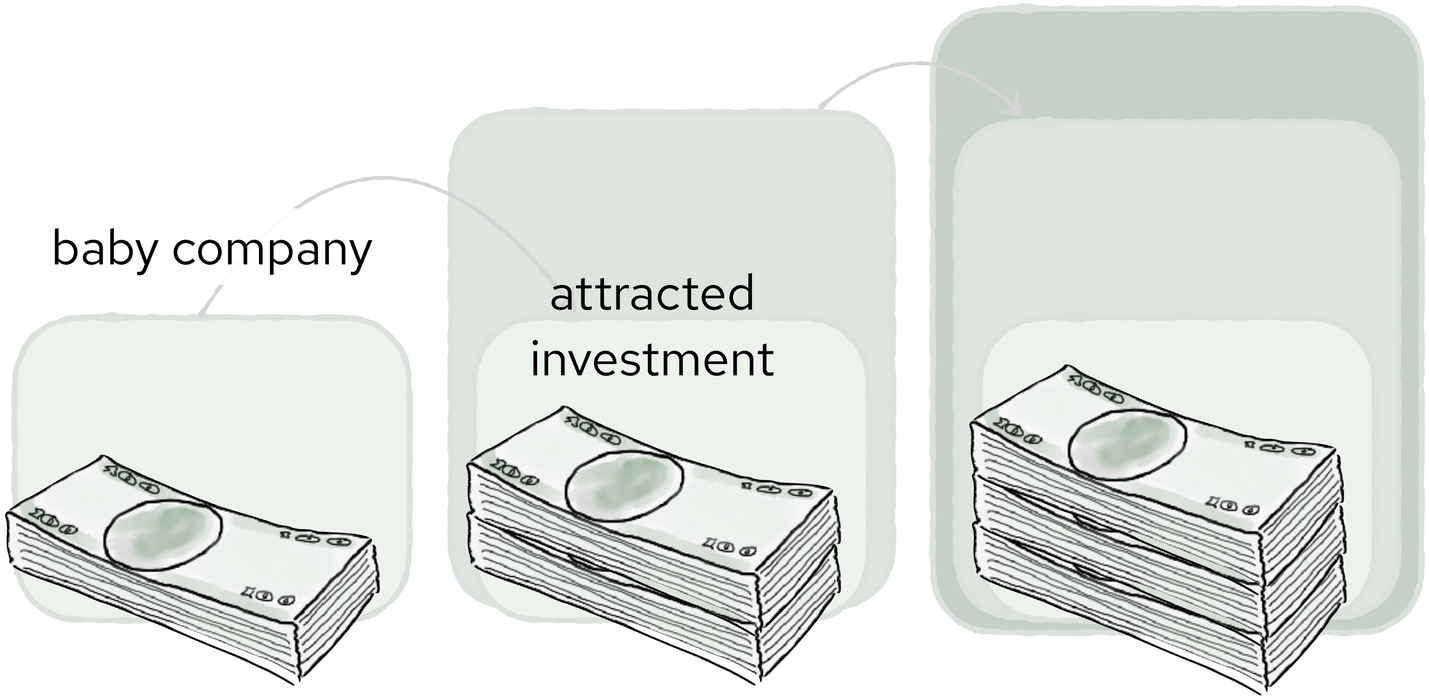
funding rounds



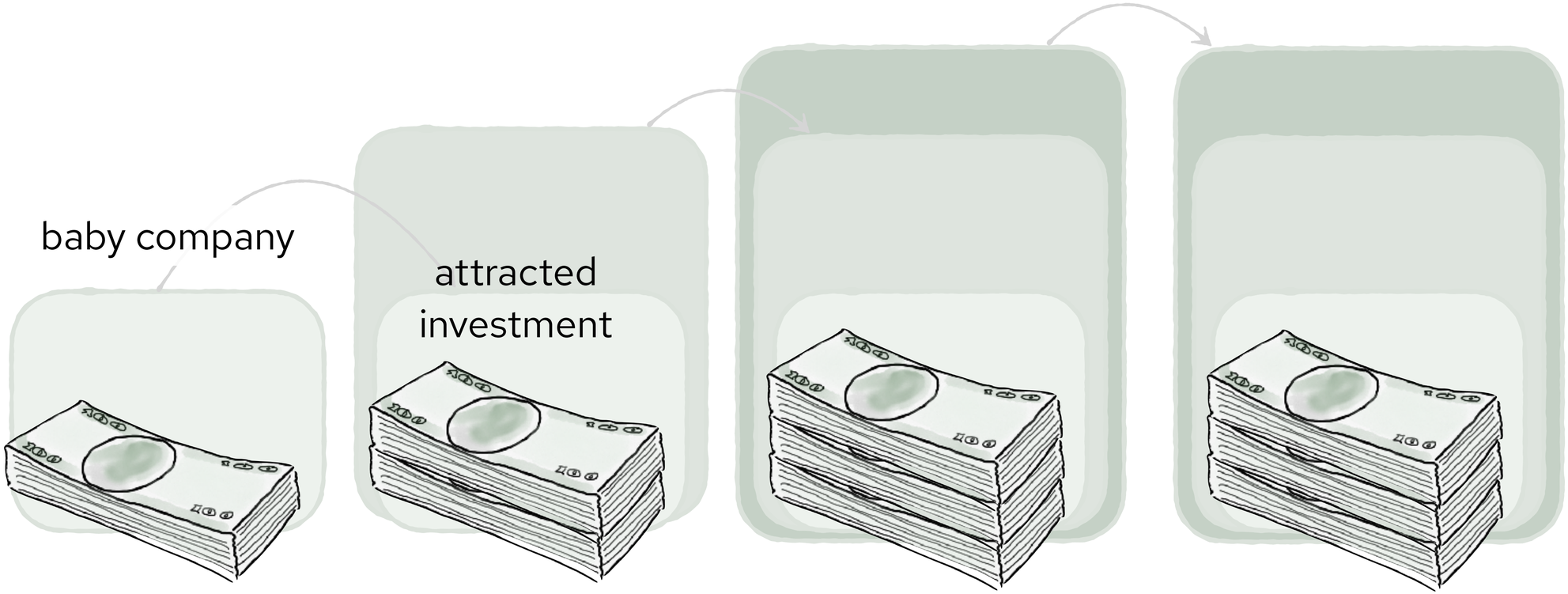
funding rounds

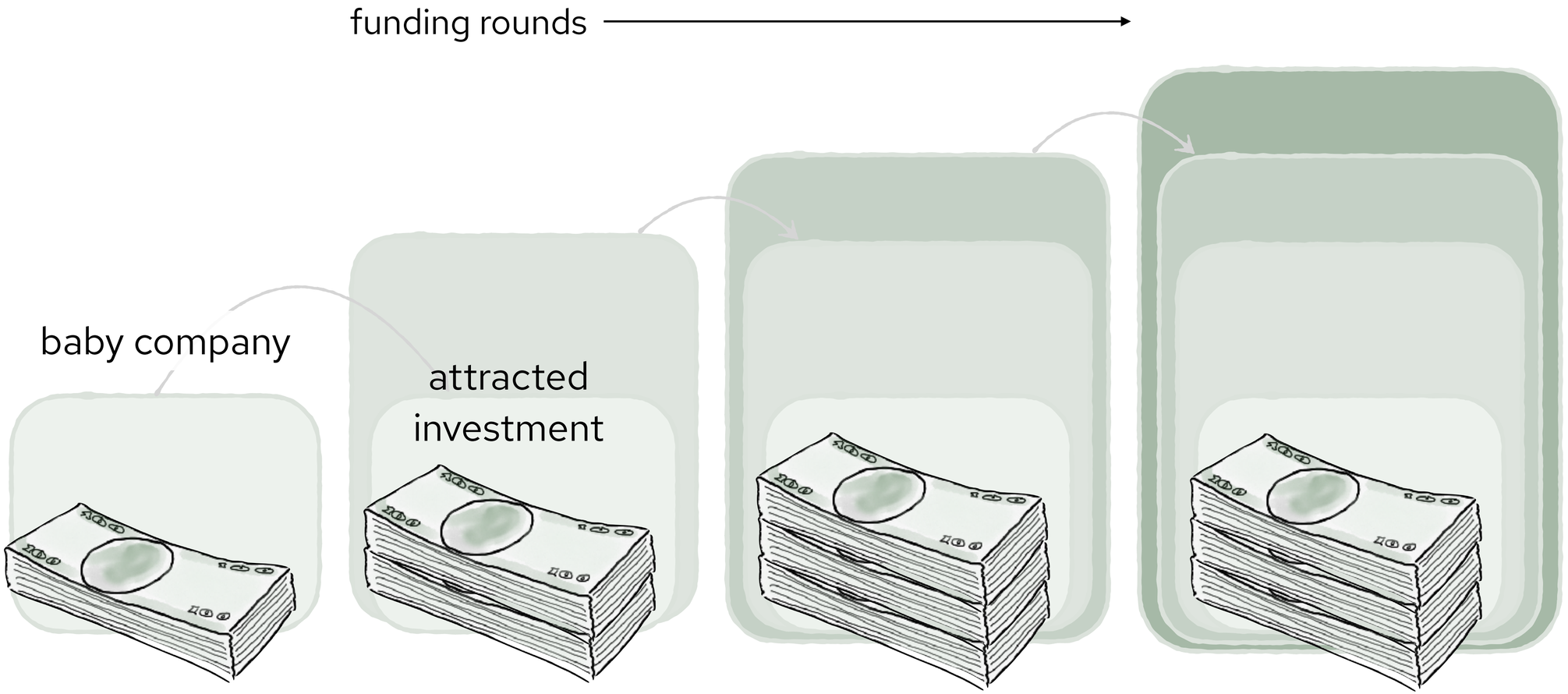


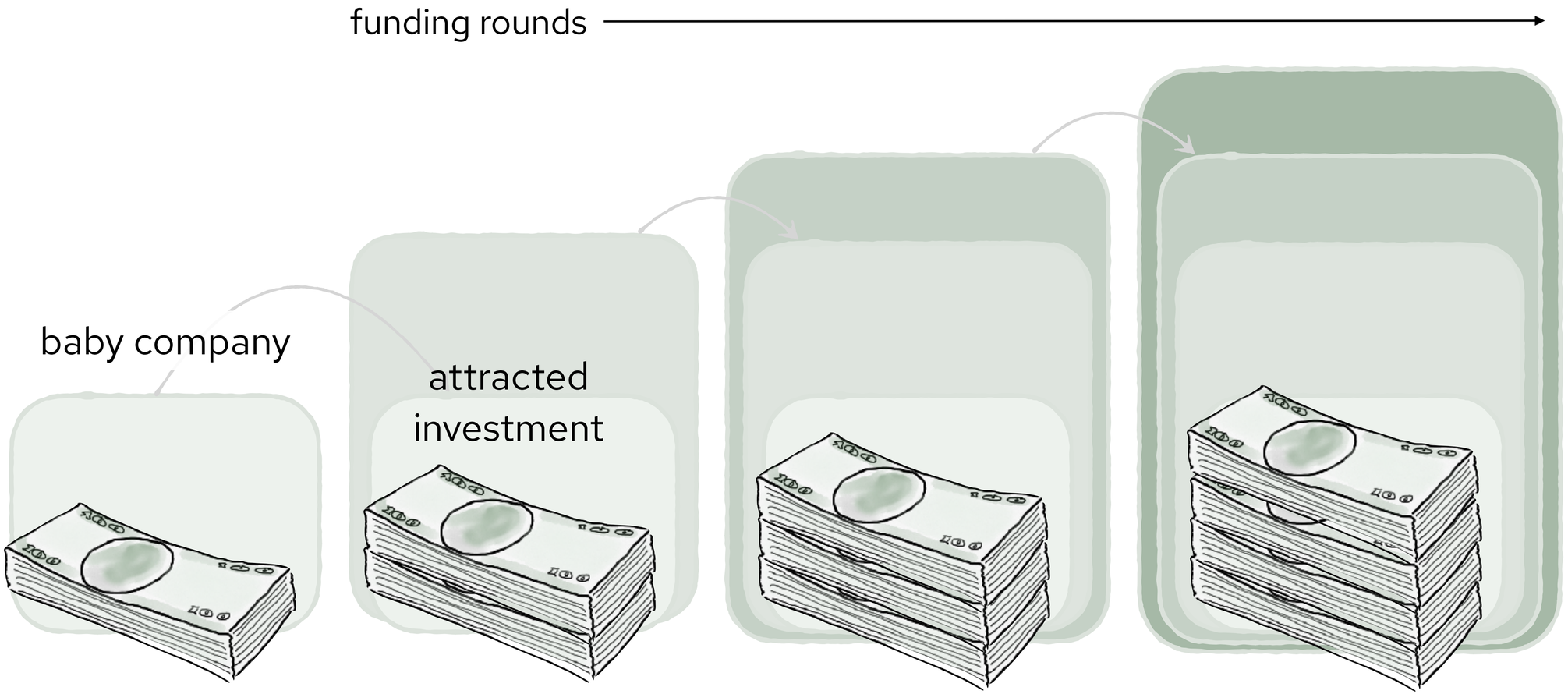
funding rounds

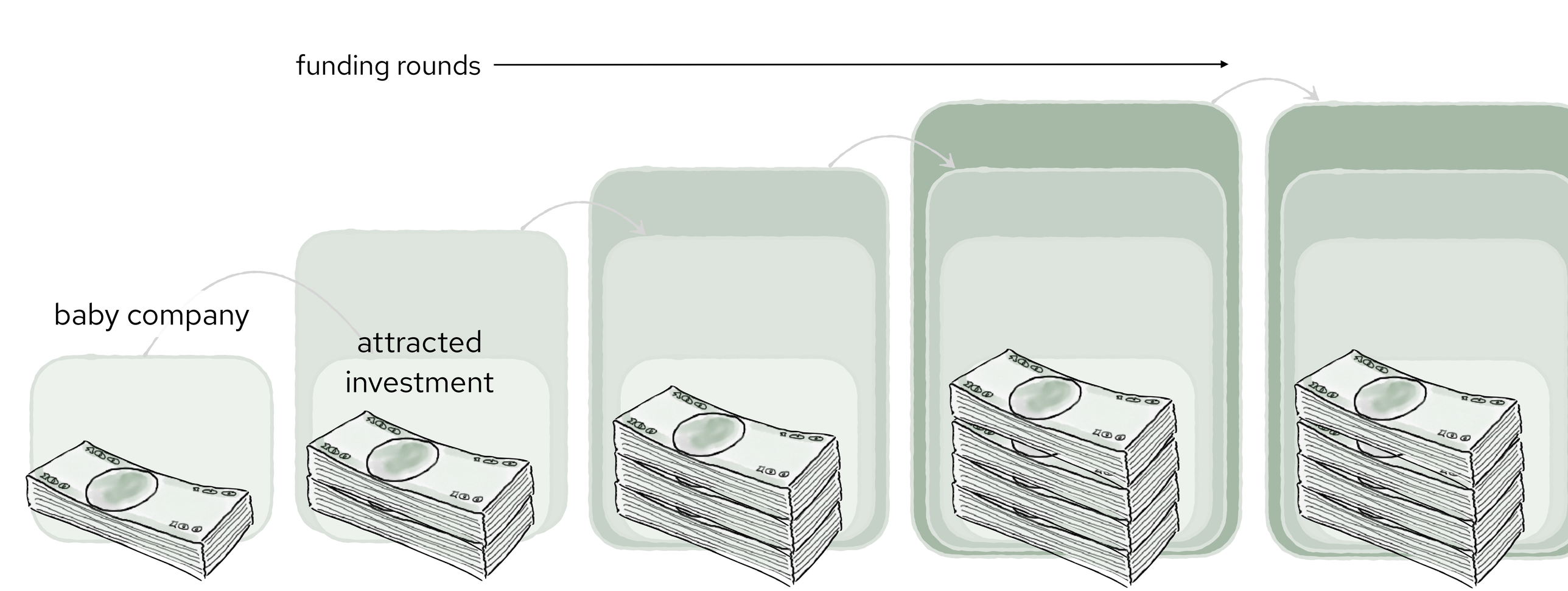


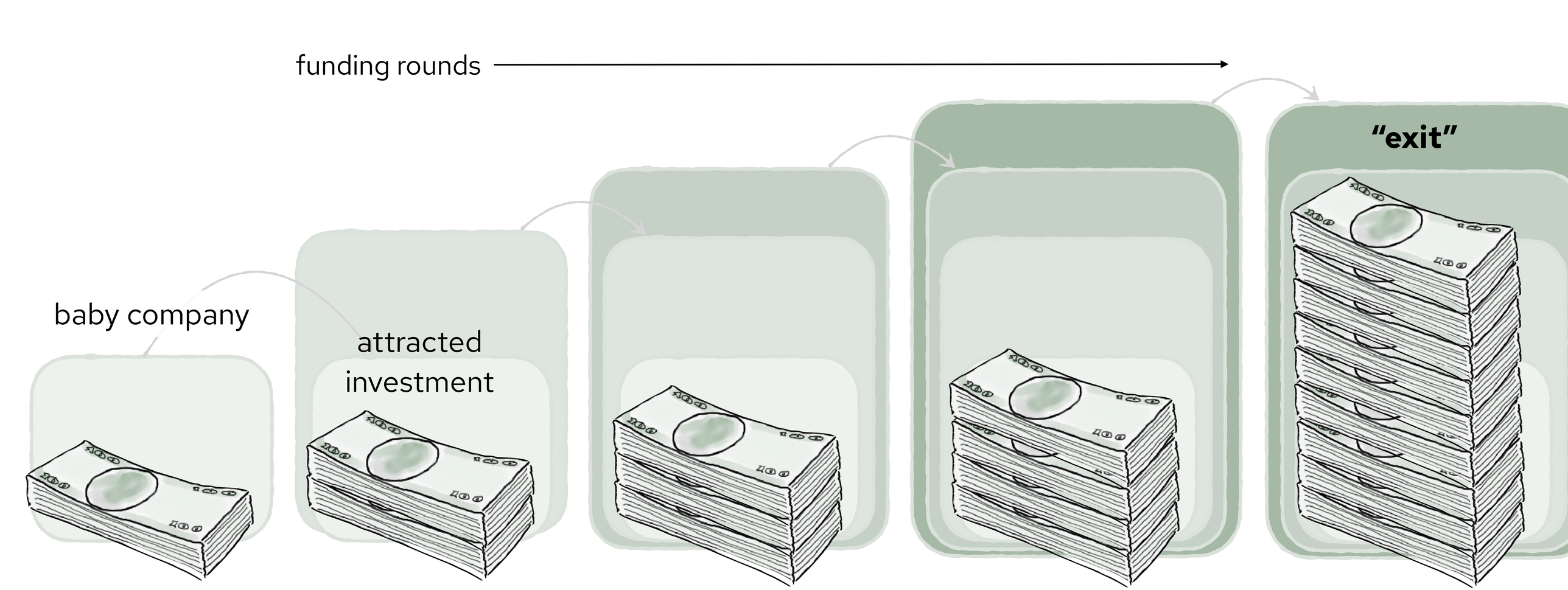
funding rounds

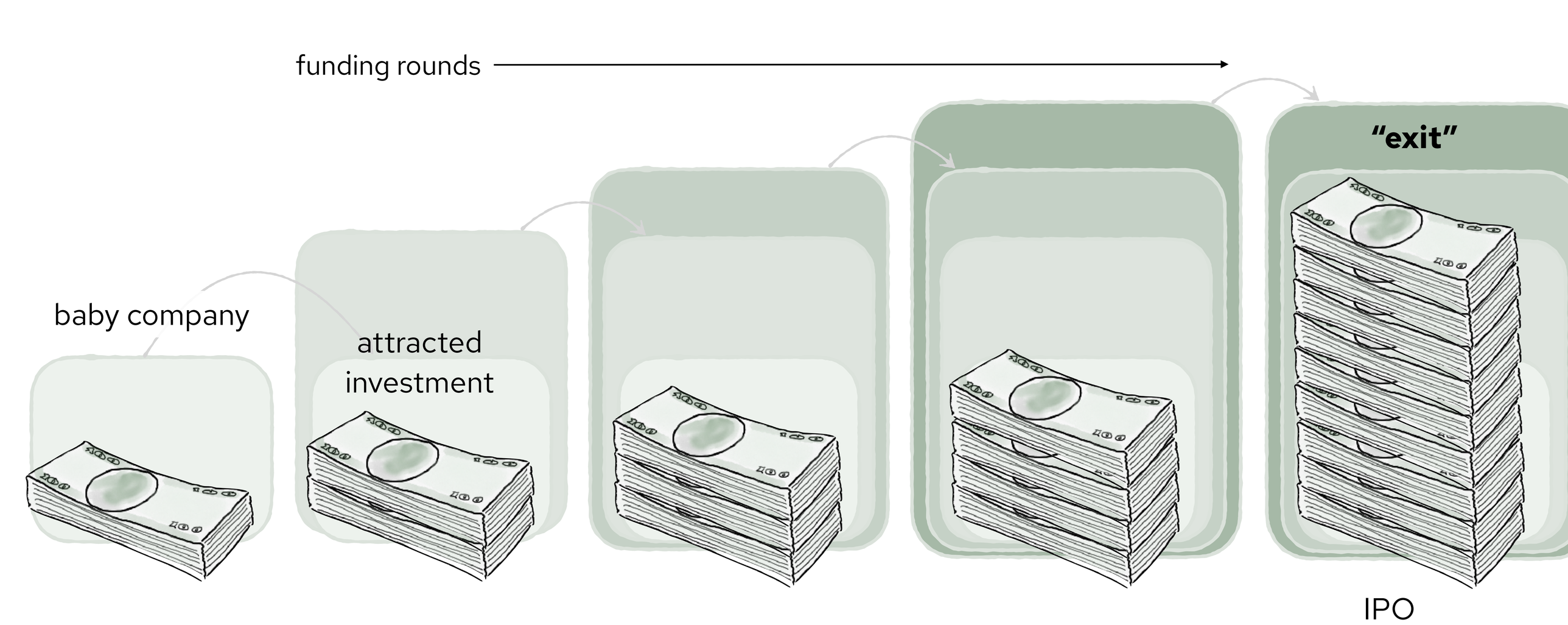


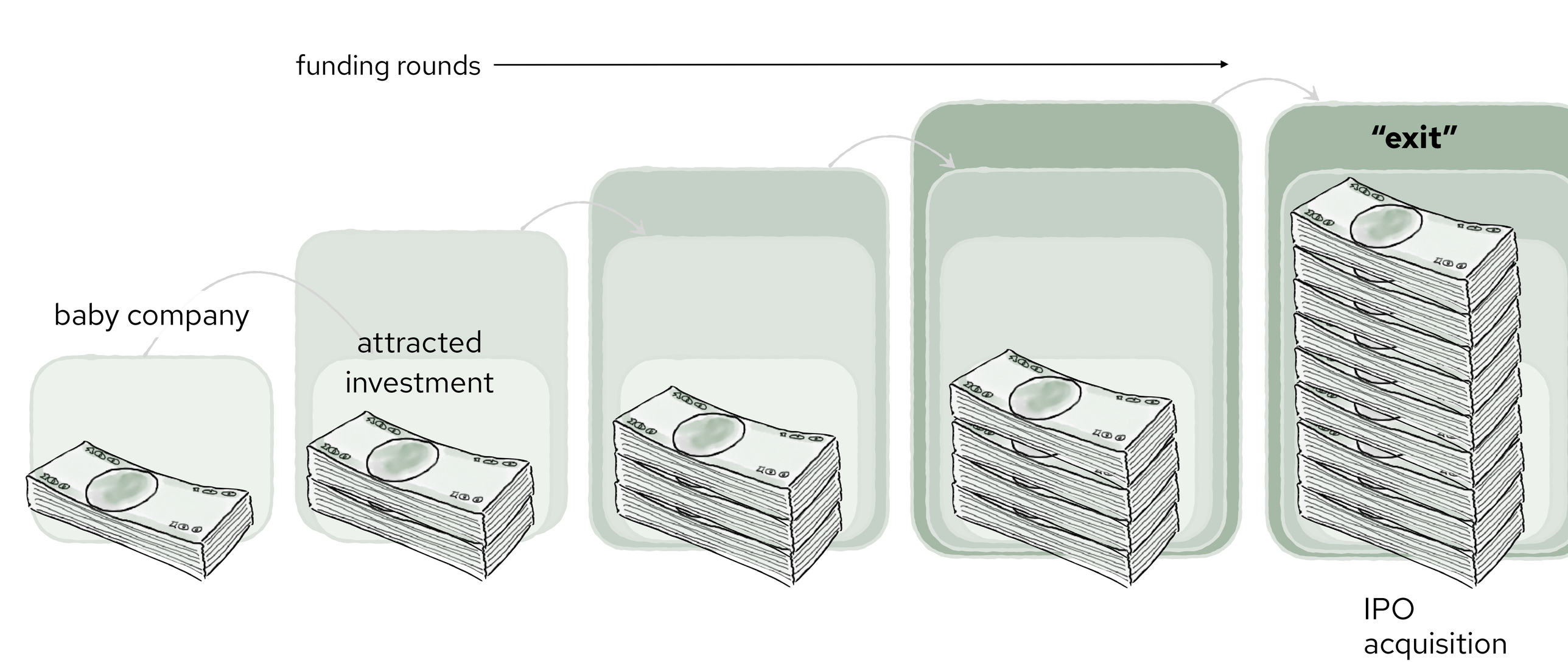

funding rounds
baby company
attracted
investment

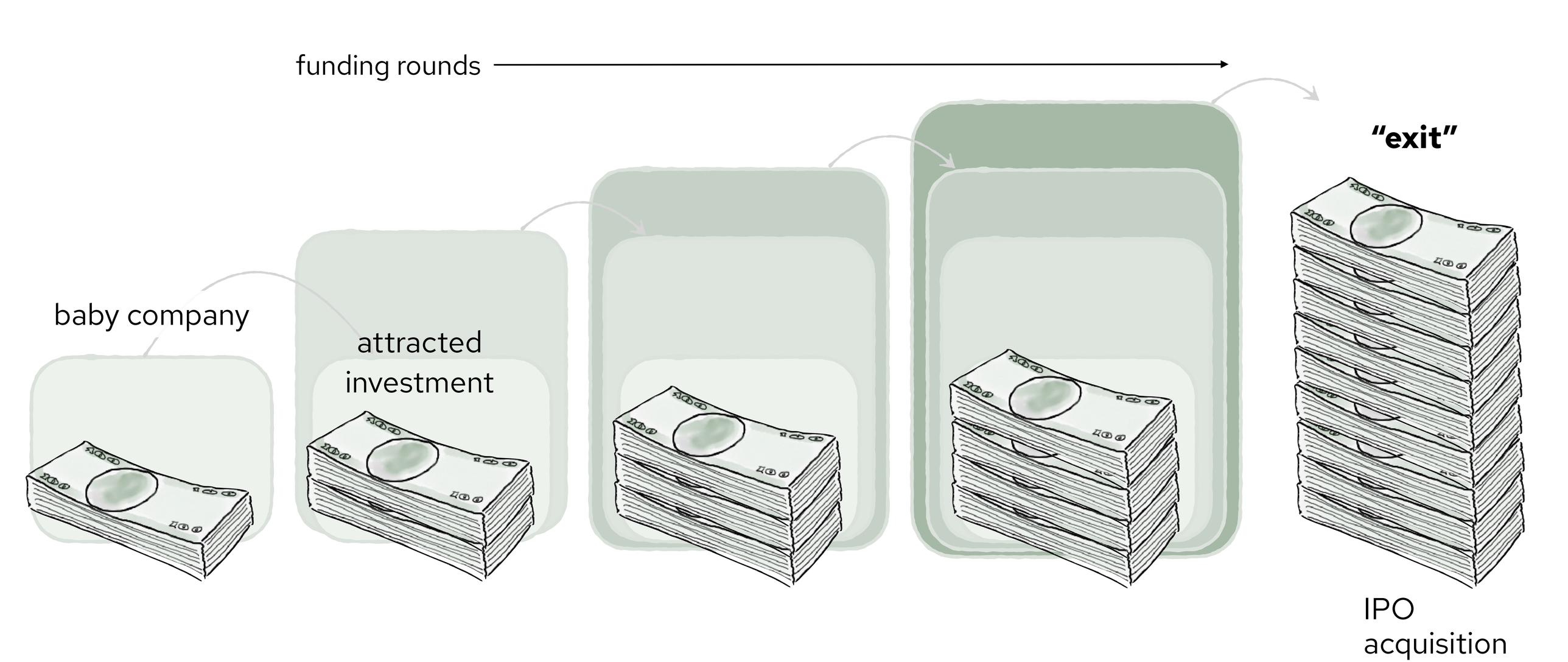

funding rounds
baby company
attracted
investment


funding rounds
baby company
attracted investment

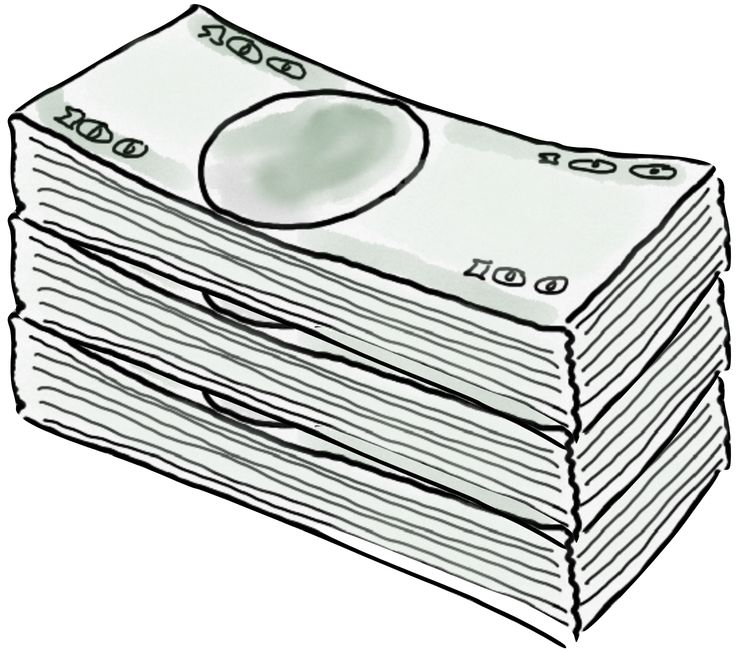

funding rounds
baby company
attracted investment
“exit”


funding rounds
baby company
attracted investment
“exit”
IPO


funding rounds
baby company
attracted investment
"exit"
IPO
acquisition

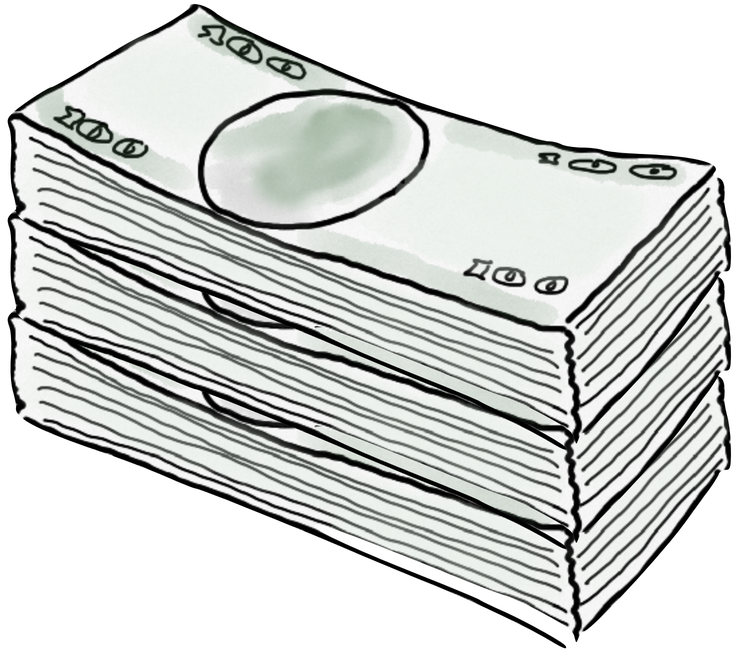

funding rounds
baby company
attracted investment
“exit”
IPO
acquisition

what attracts investment?



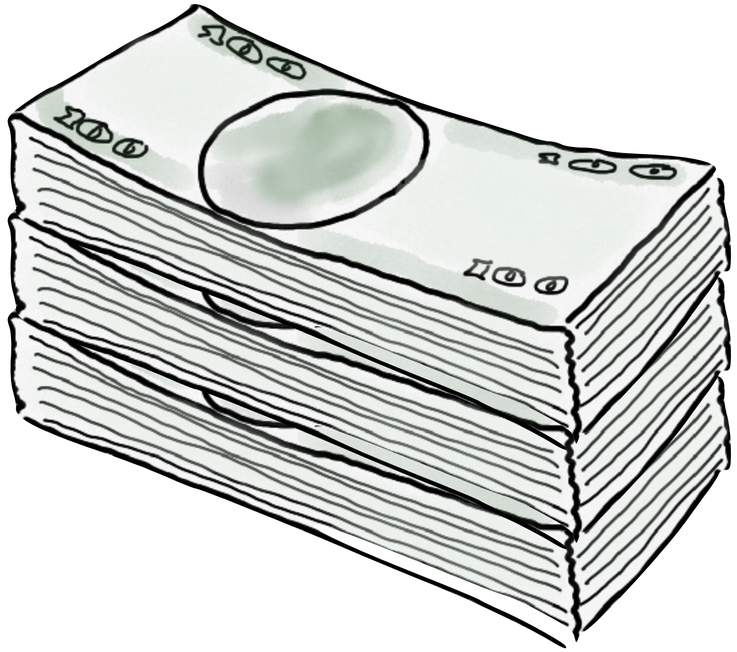
what attracts investment?

stability?

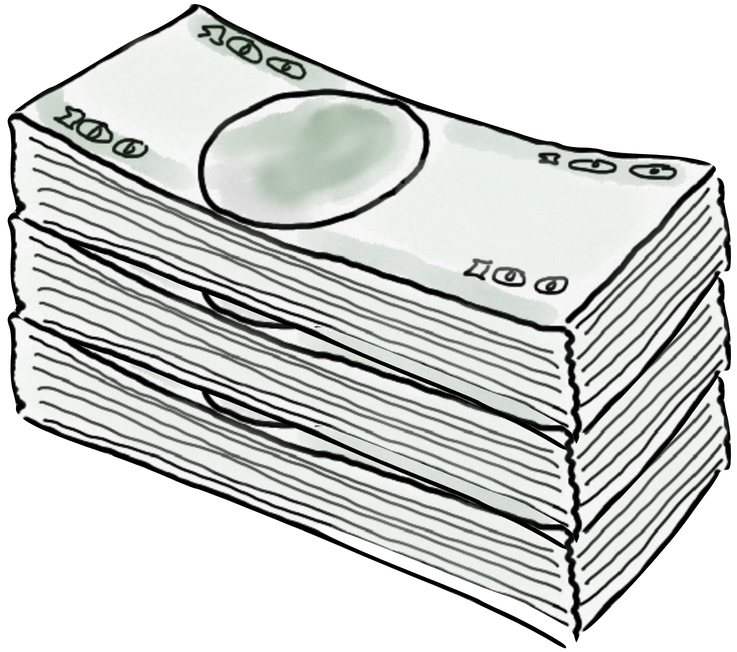


what attracts investment?

stability?
profitability?

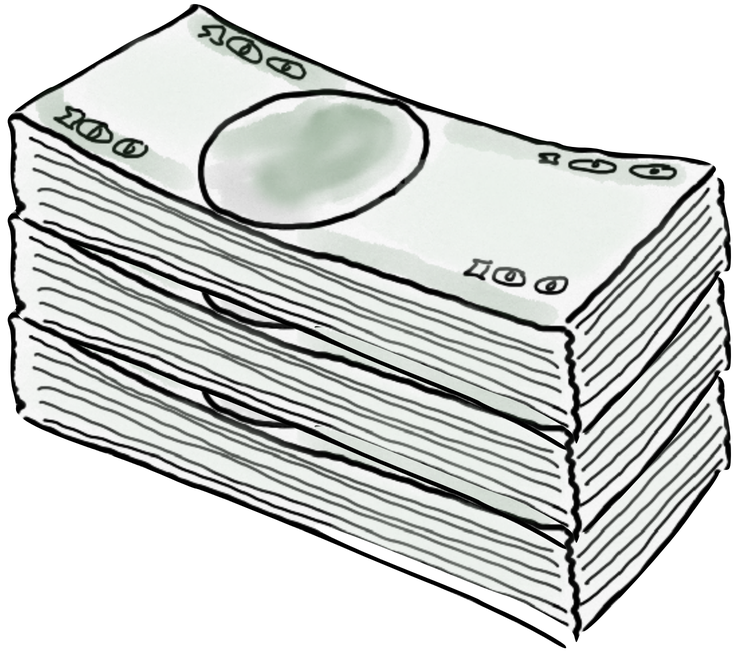


what attracts investment?



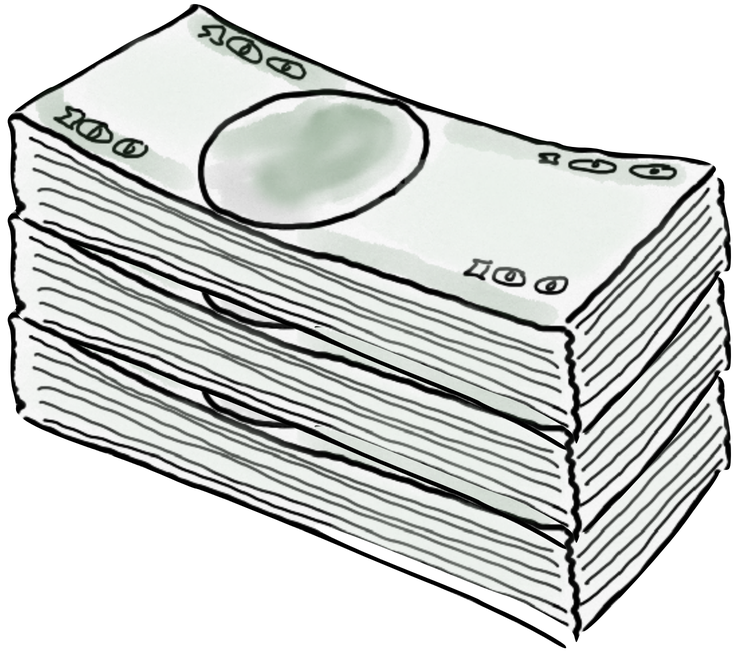
stability?
profitability?
revenue?

what attracts investment?



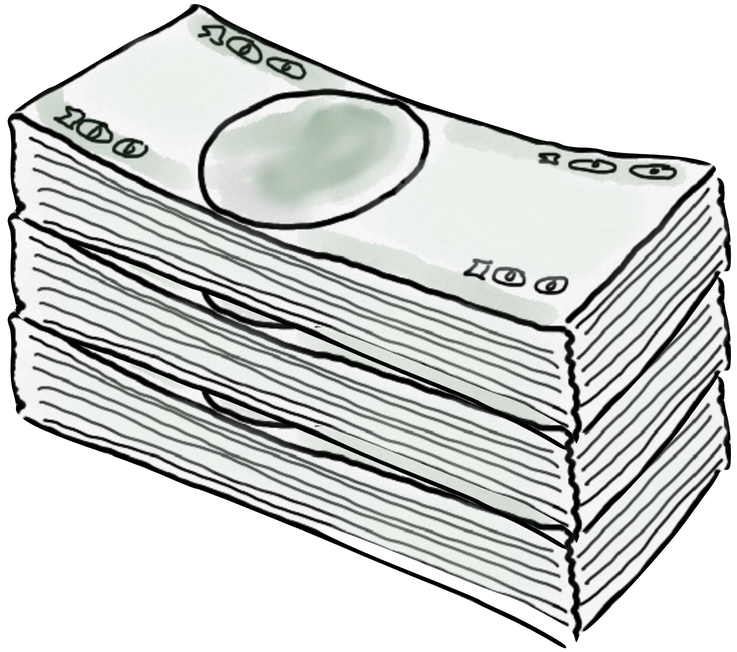
stability?
profitability?
revenue?
growth

what attracts investment?



stability?
profitability?
revenue?
growth
excitement

what attracts investment?



likelihood of selling stake at a profit

- growth
- excitement

“It’s not simply that one piece of technology is overhyped, it’s that hype is a necessary ingredient of the current business ecosystem of the tech industry.”

– Meredith Whittaker

“It’s not simply that one piece of technology is overhyped, it’s that hype is a necessary ingredient of the current business ecosystem of the tech industry.”

– Meredith Whittaker 

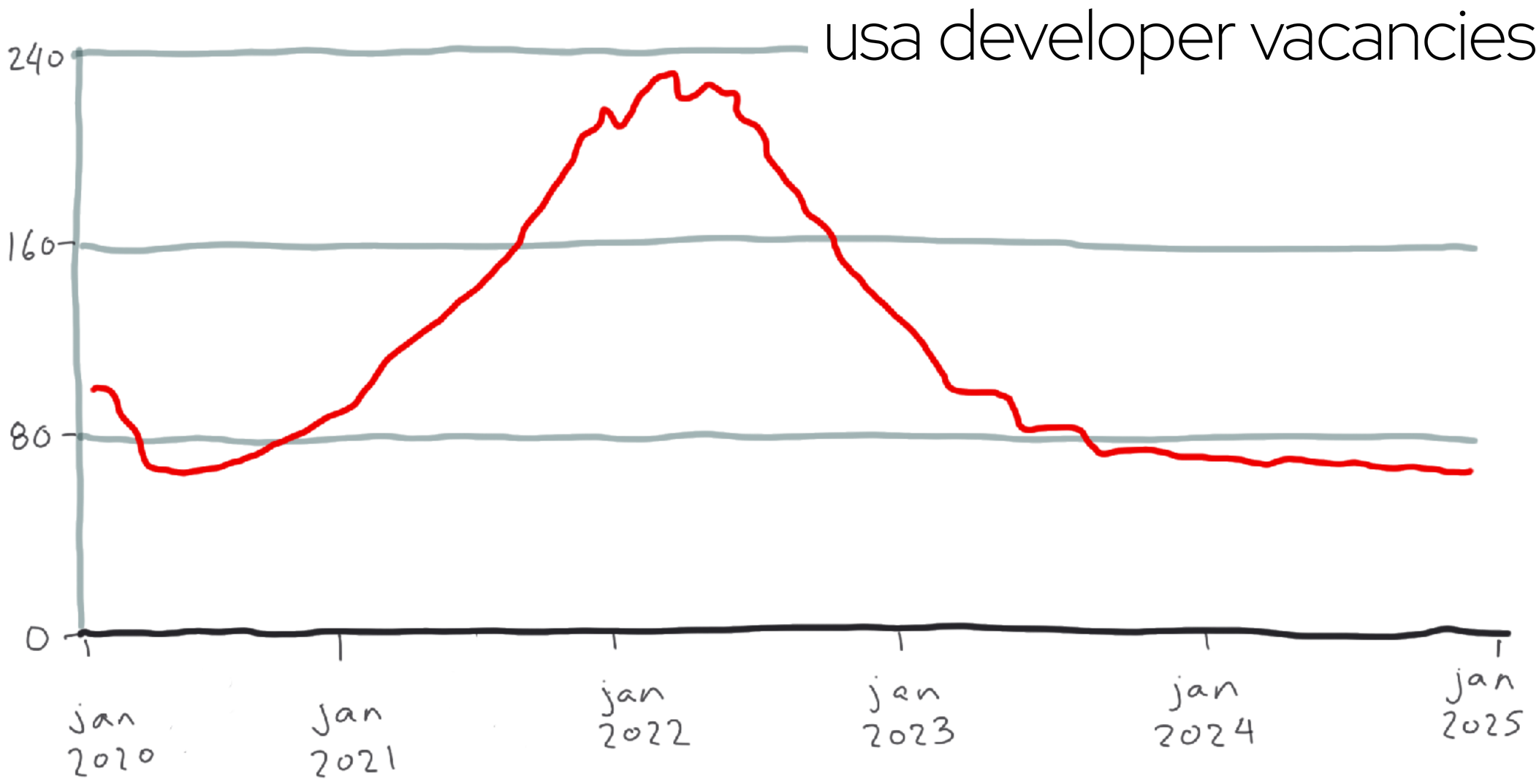


why can’t I find a job?



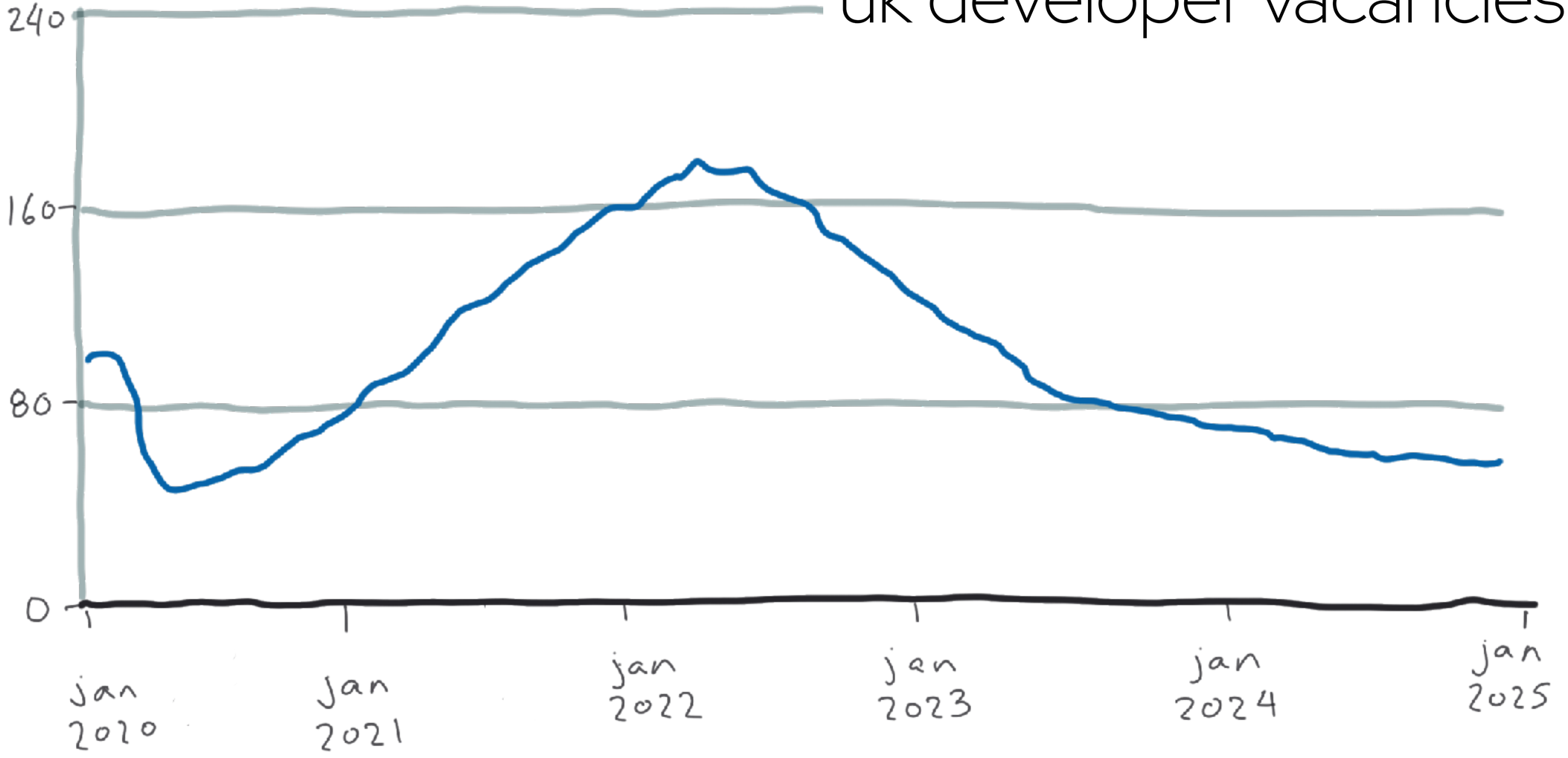
why can’t I find a new job?

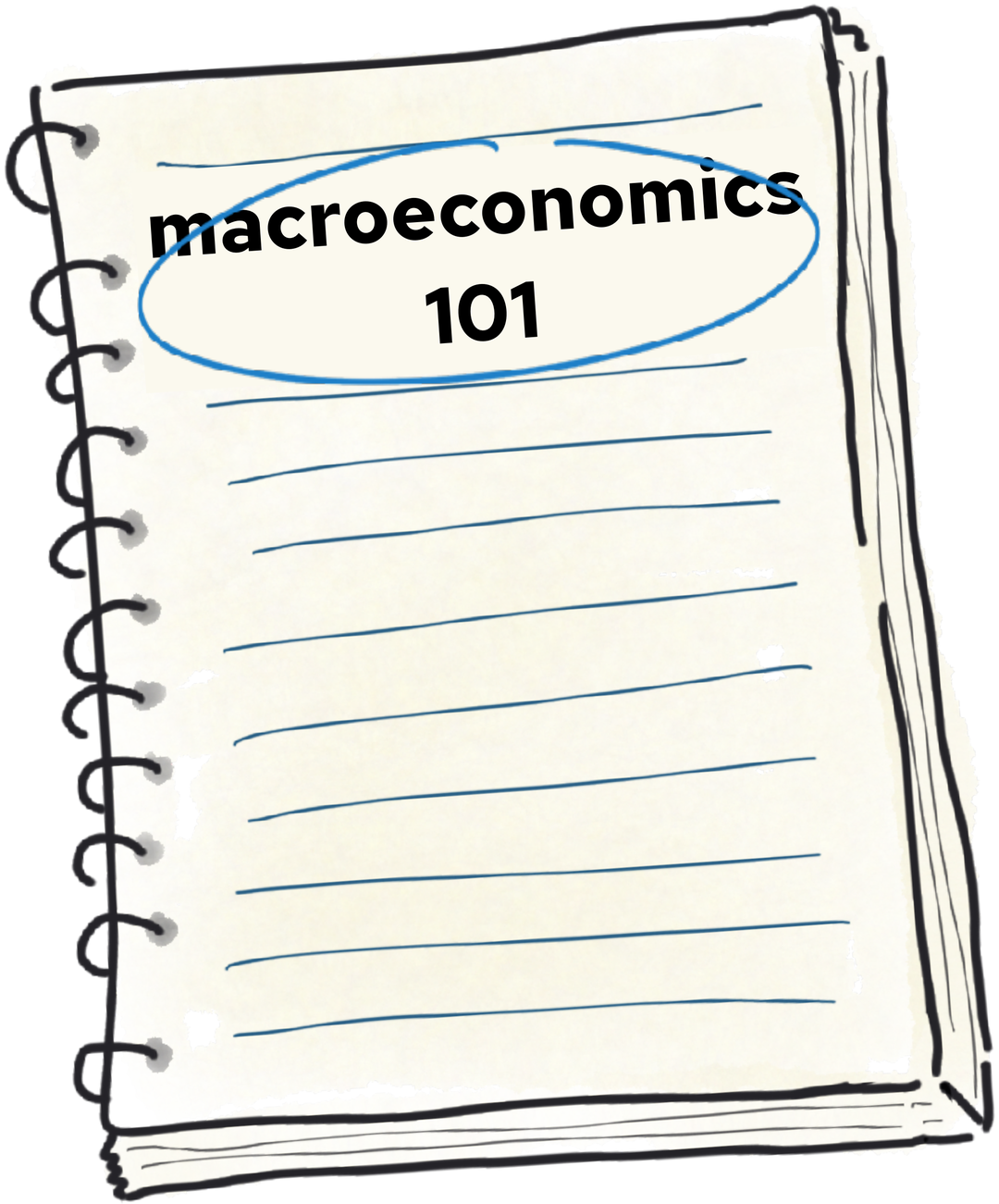
Source: indeed.com via https://newsletter.pragmaticengineer.com/p/software-engineering-job-openings?publication_id=458709



Source: indeed.com via https://newsletter.pragmaticengineer.com/p/software-engineering-job-openings?publication_id=458709

uk developer vacancies





interest rates

ZIRP

ZIRP

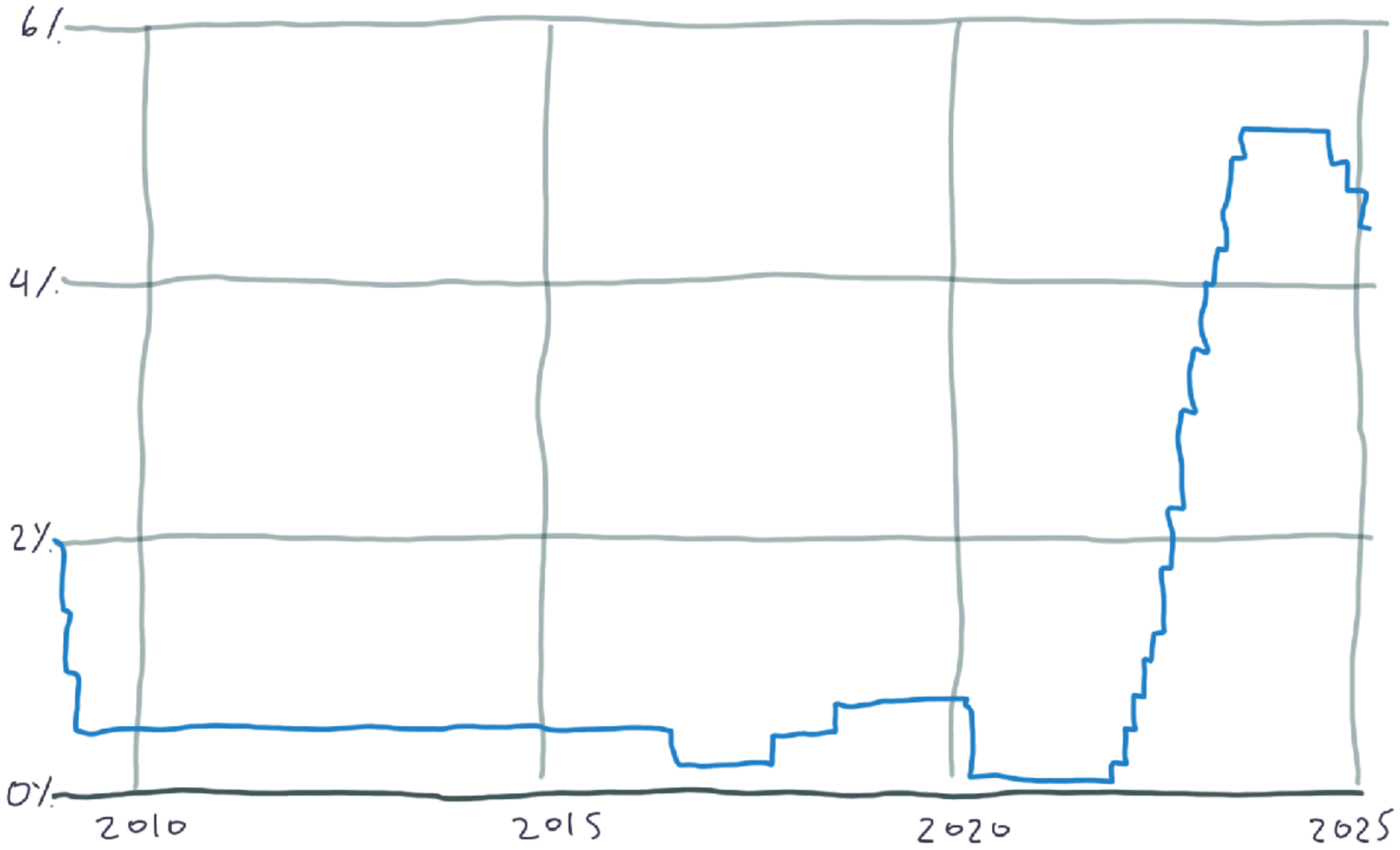
"zero interest-rate phenomenon"


0%


<1%

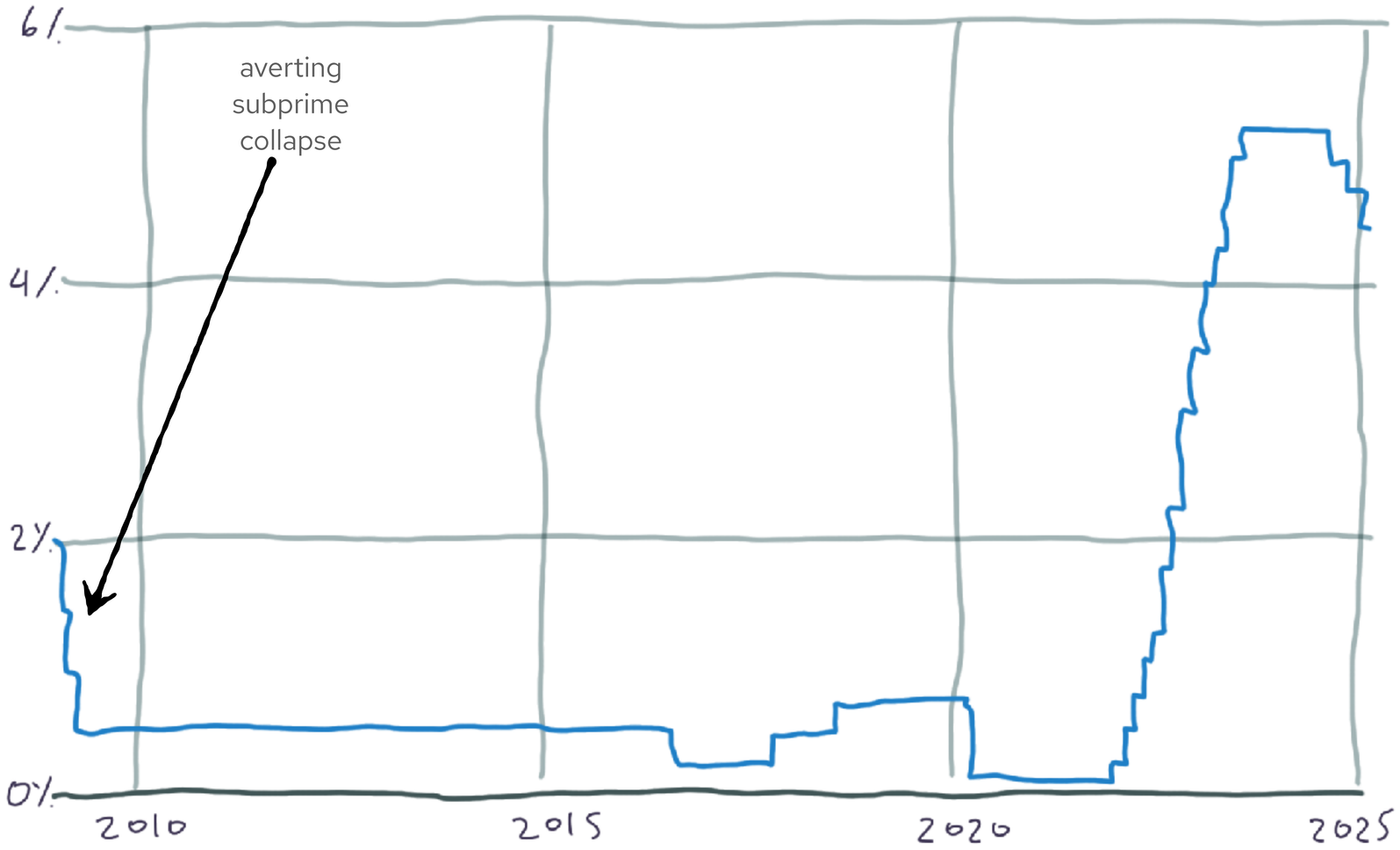
Source: Bank of England

UK interest rates



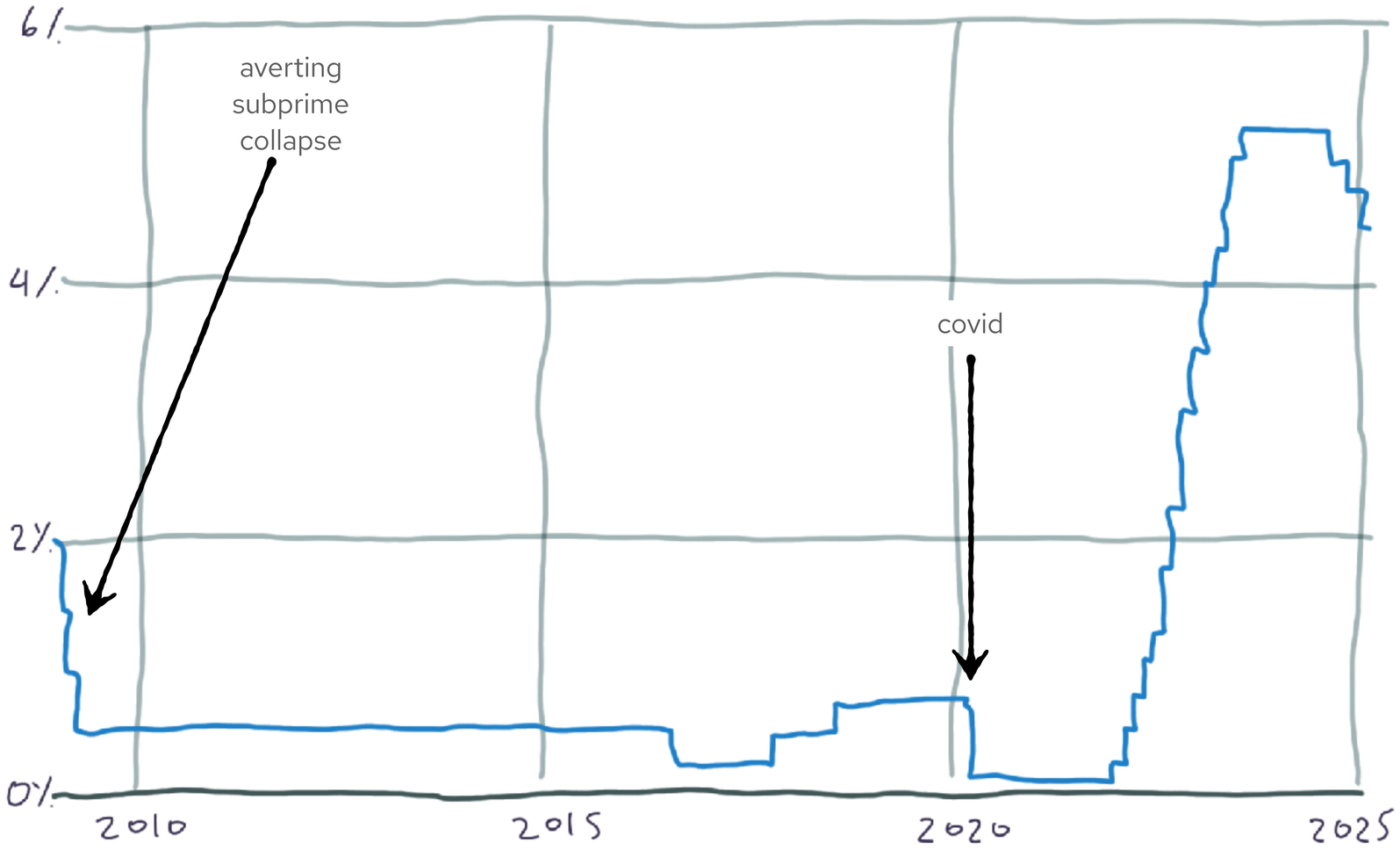
Source: Bank of England

UK interest rates



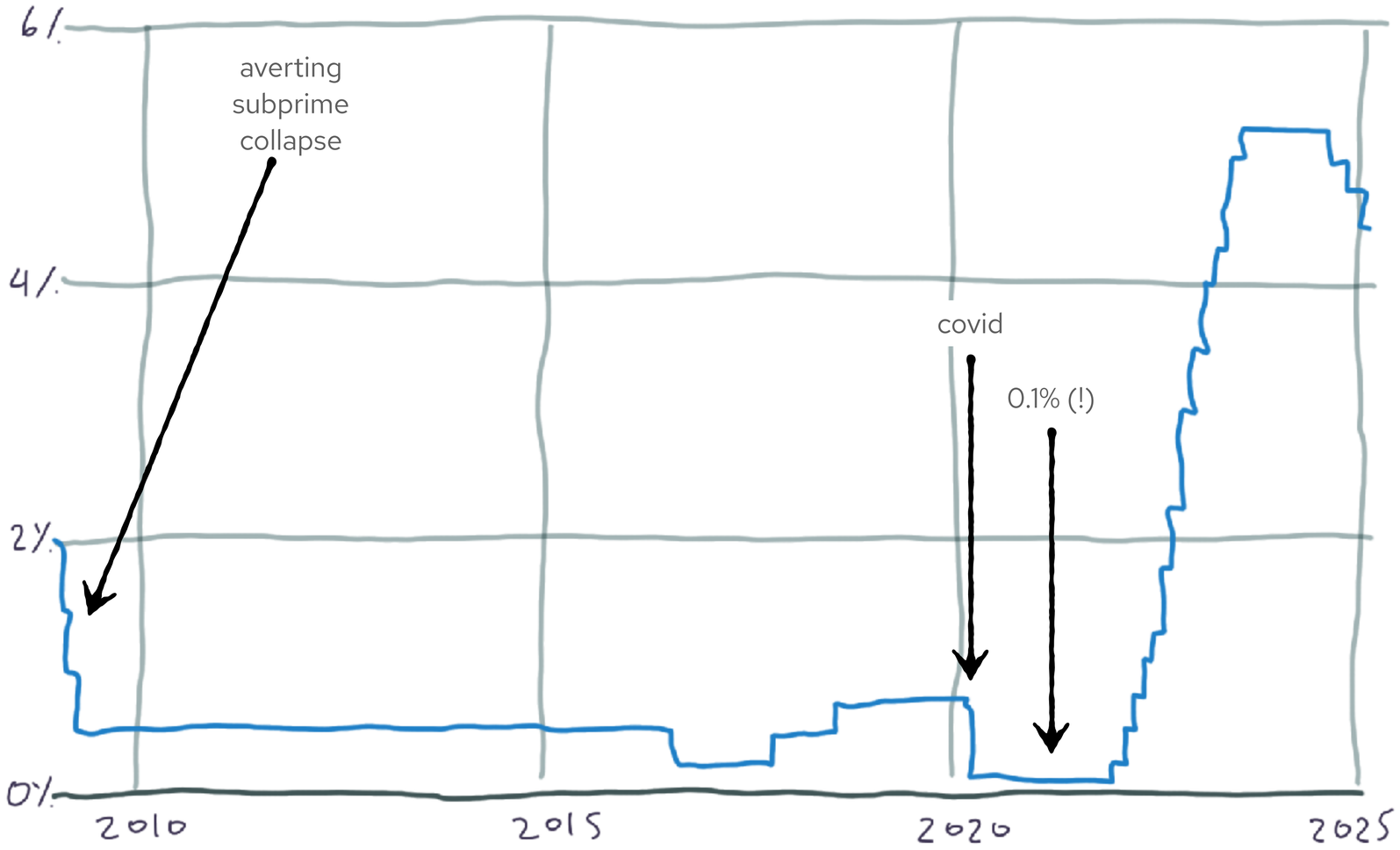
Source: Bank of England

UK interest rates



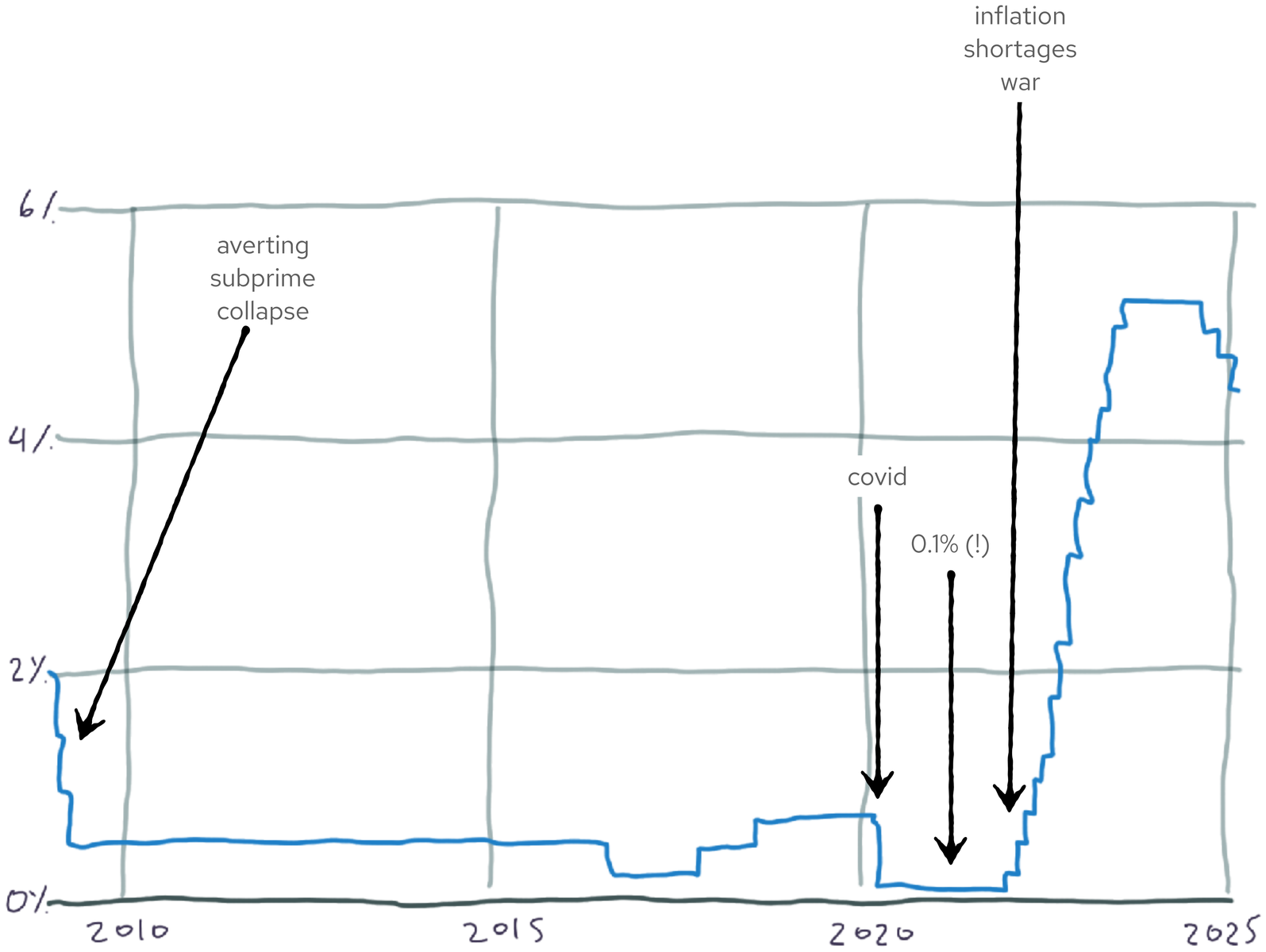
Source: Bank of England

UK interest rates



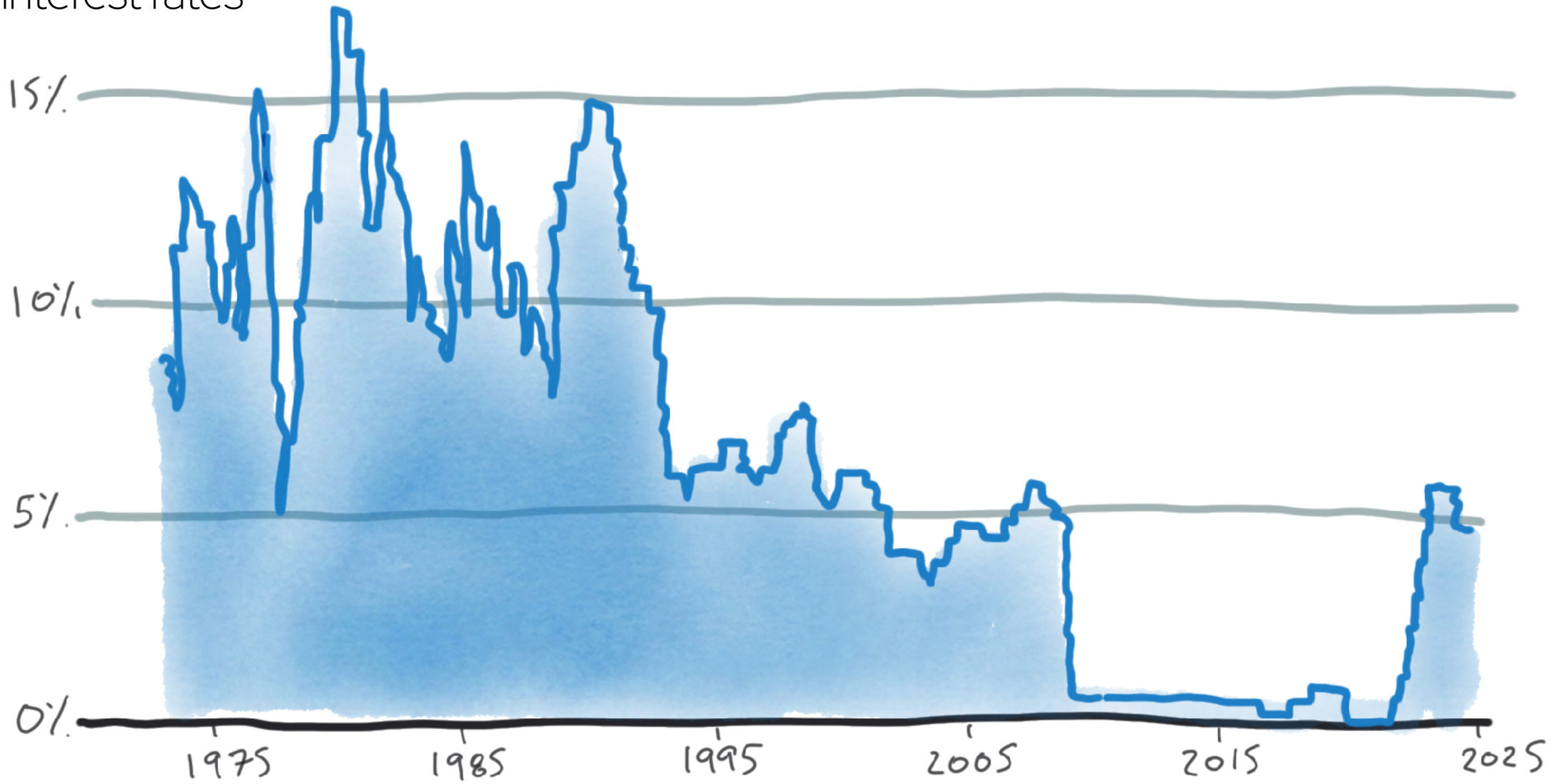
Source: Bank of England

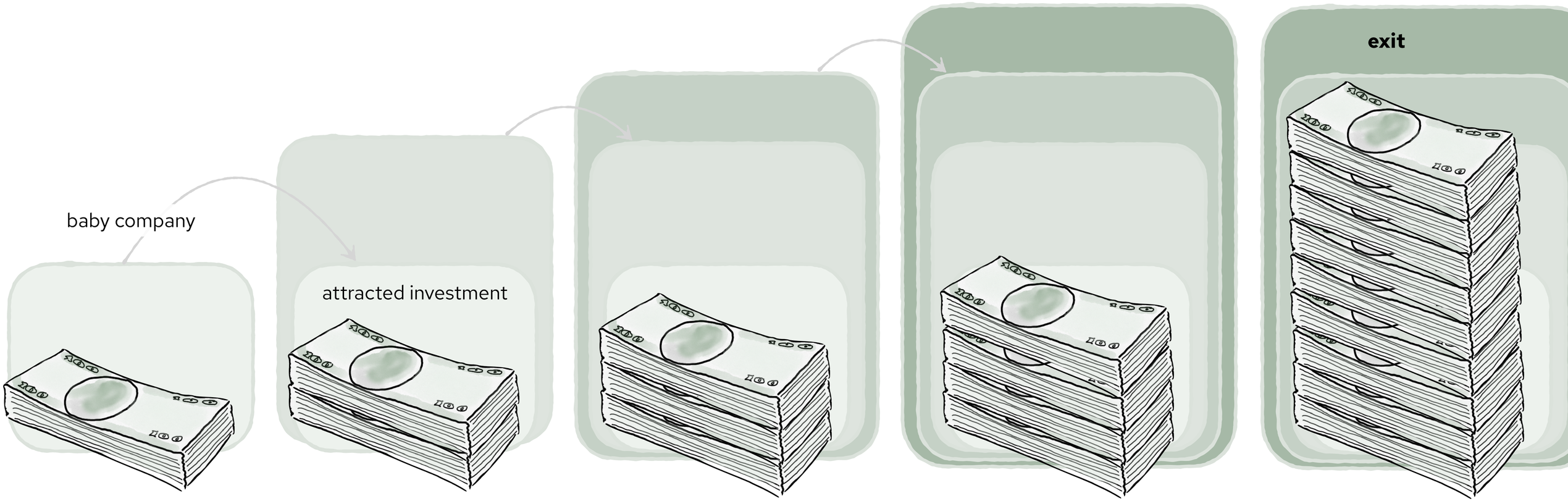
UK interest rates

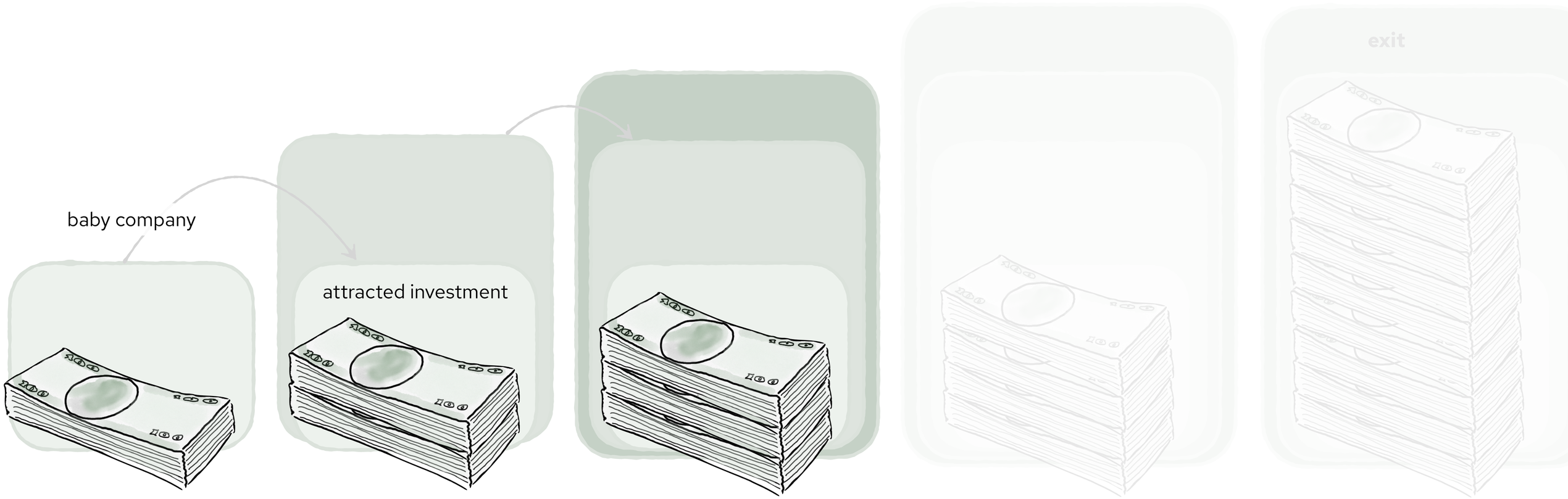


Source: Bank of England

UK interest rates

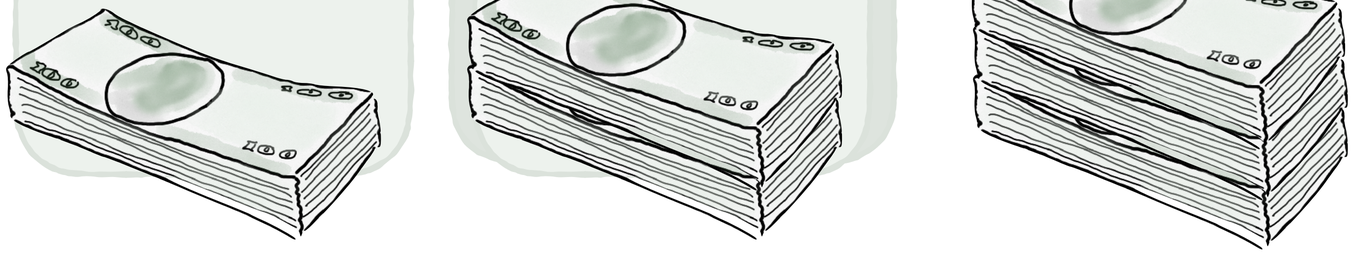



baby company
attracted investment
exit

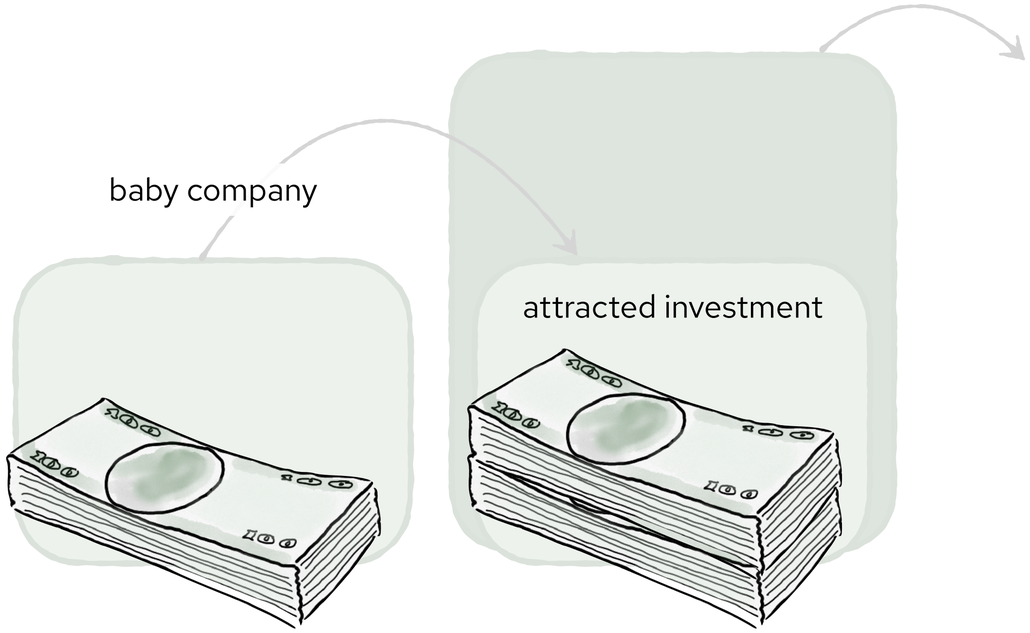

baby company
attracted investment
exit

baby company

attracted investment

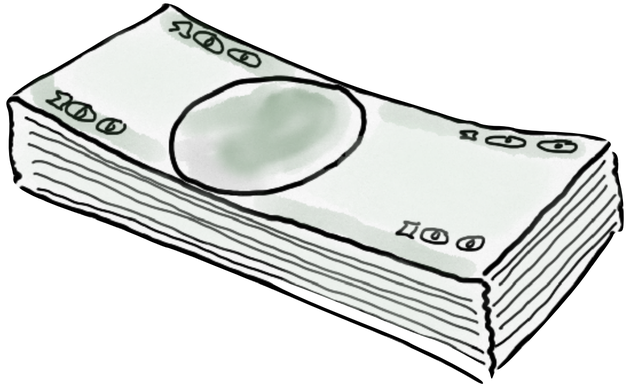


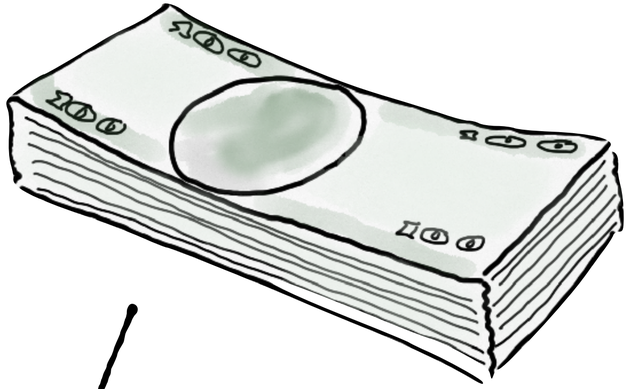
exit



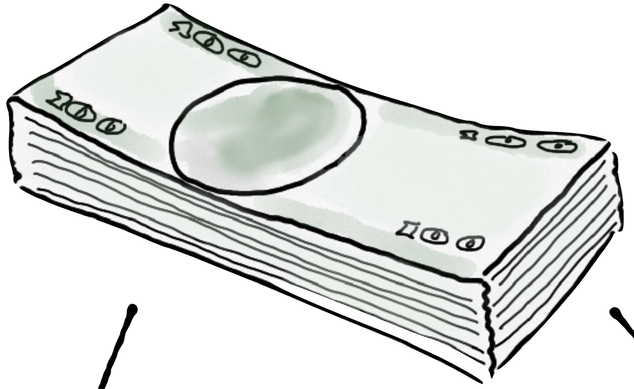
risk

ZIRP



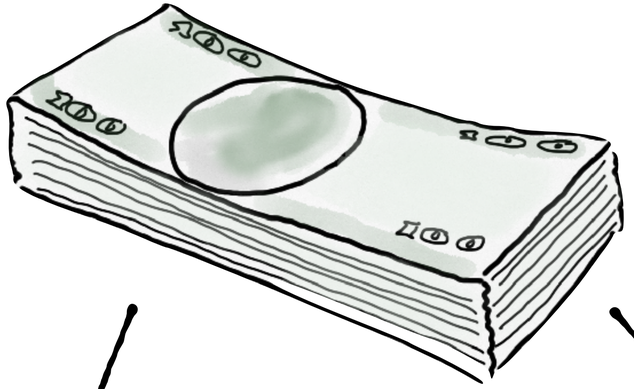


software company



software company

government bond

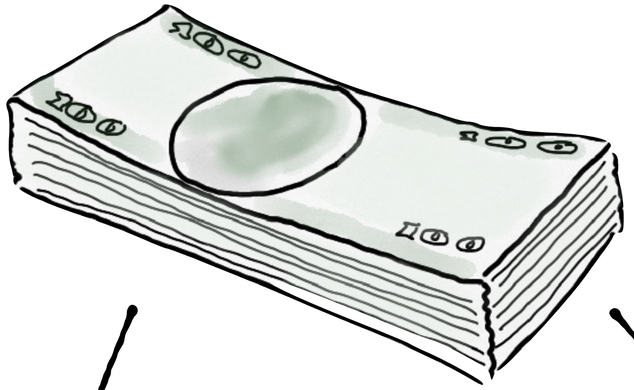


software company

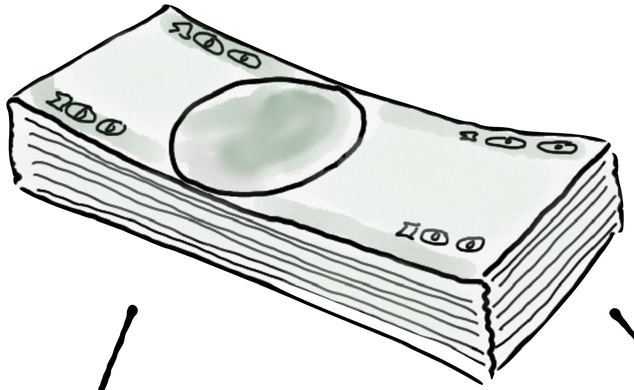
government bond

risk

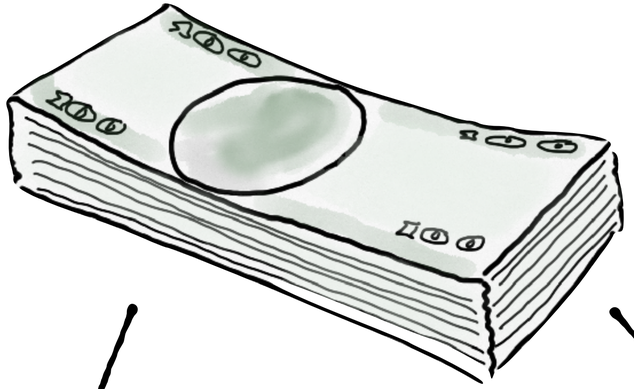
return



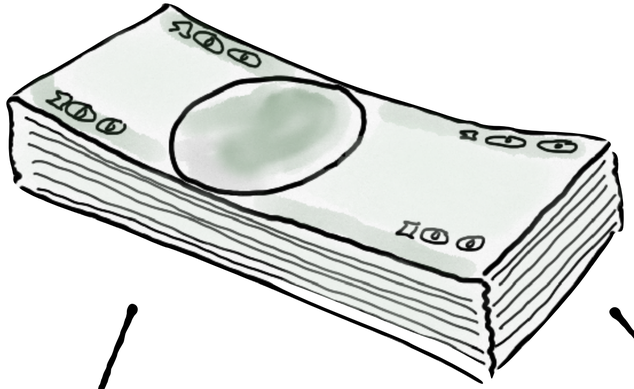
	software company	government bond
risk	high	
return		



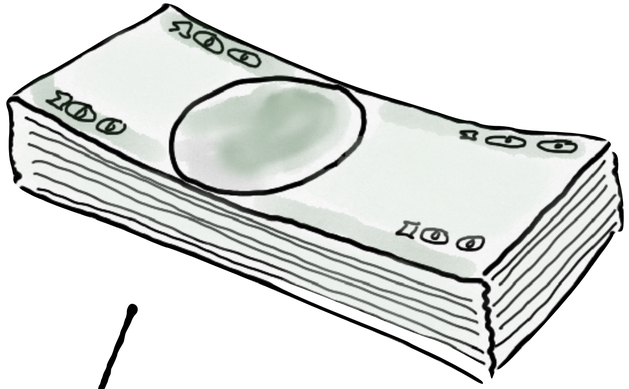
	software company	government bond
risk	high	
return	20% - 500%	



	software company	government bond
risk	high	low
return	20% - 500%	

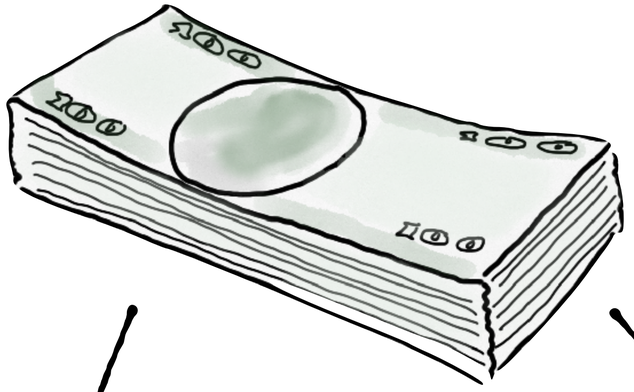


	software company	government bond
risk	high	low
return	20% - 500%	0%

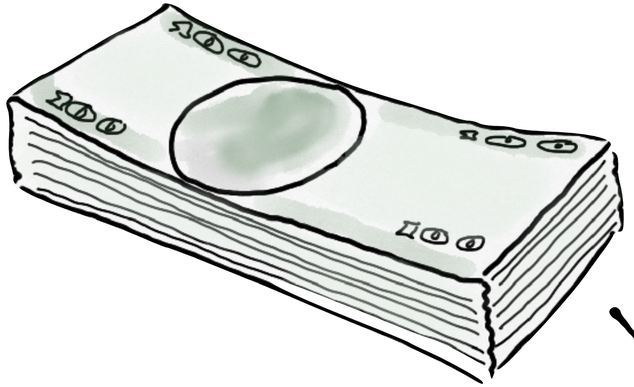




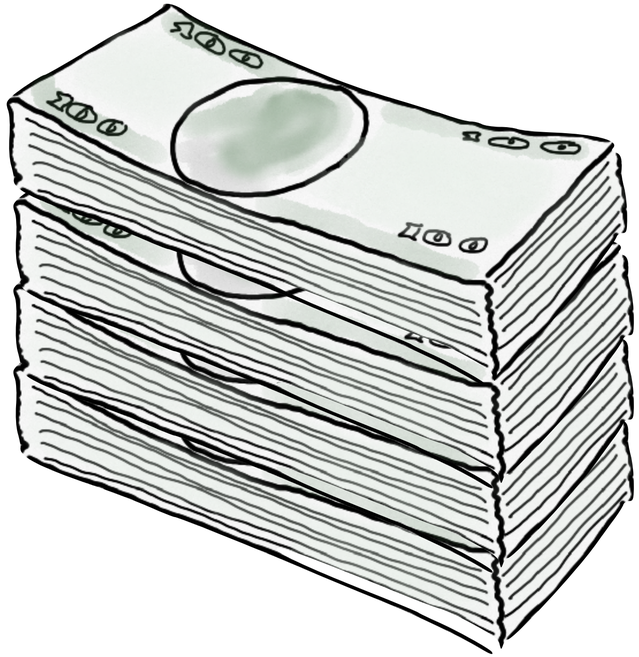
	software company	government bond
risk	high	low
return	20% - 500%	0%



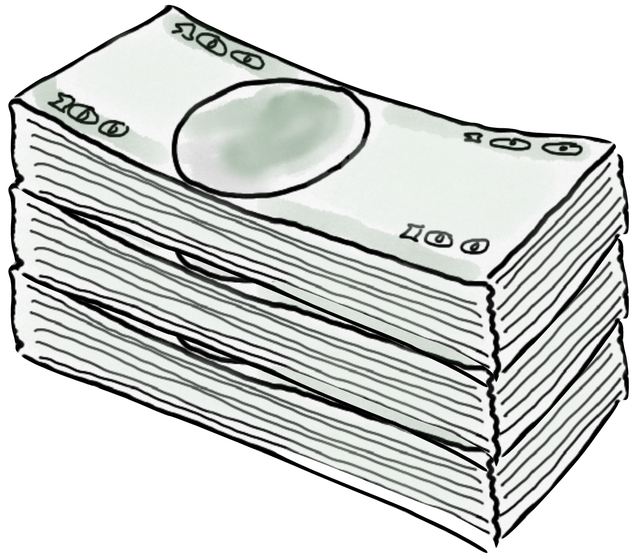
	software company	government bond
risk	high	low
return	20% - 500%	4%



	software company	government bond
risk	high	low
return	20% - 500%	4%

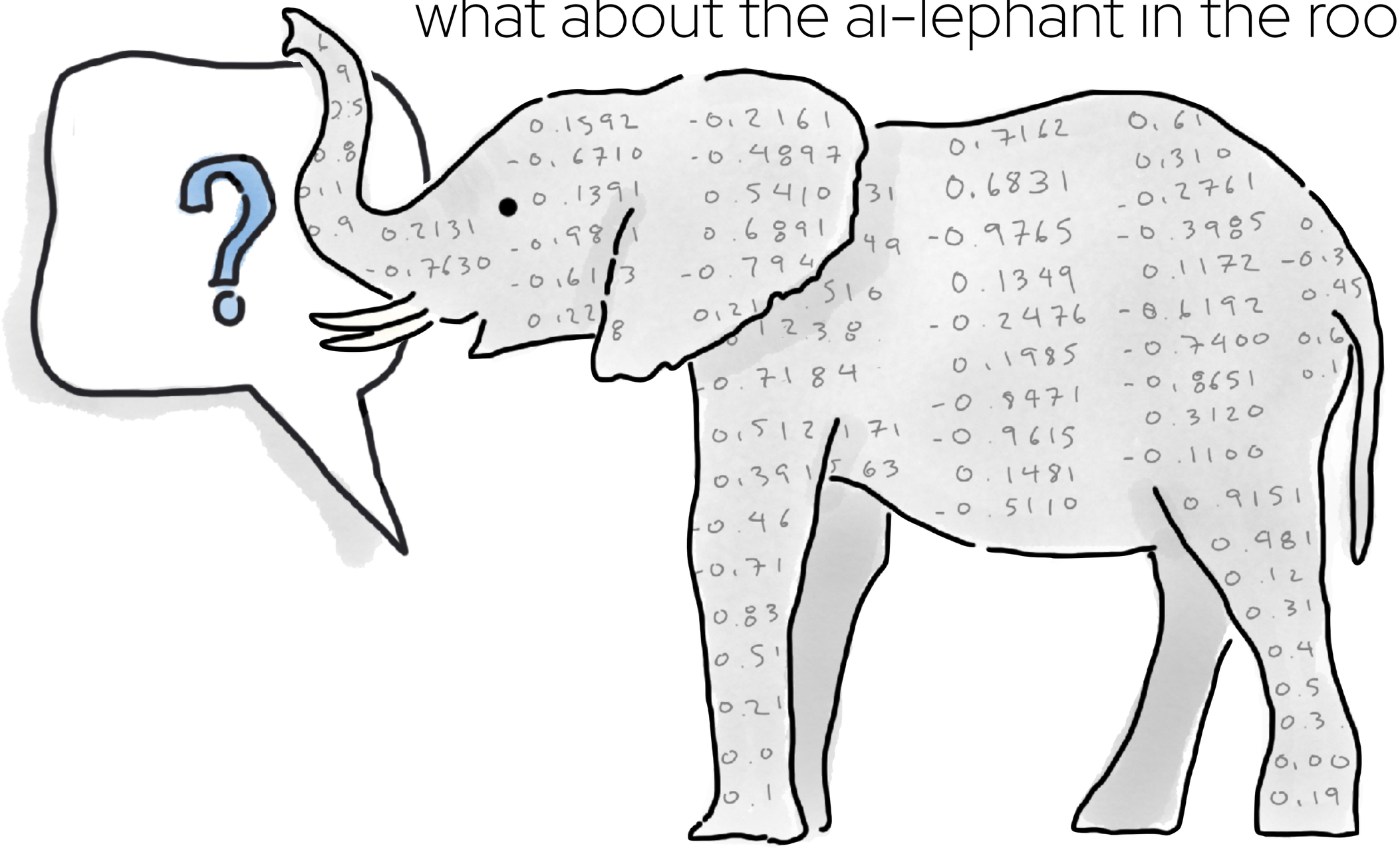


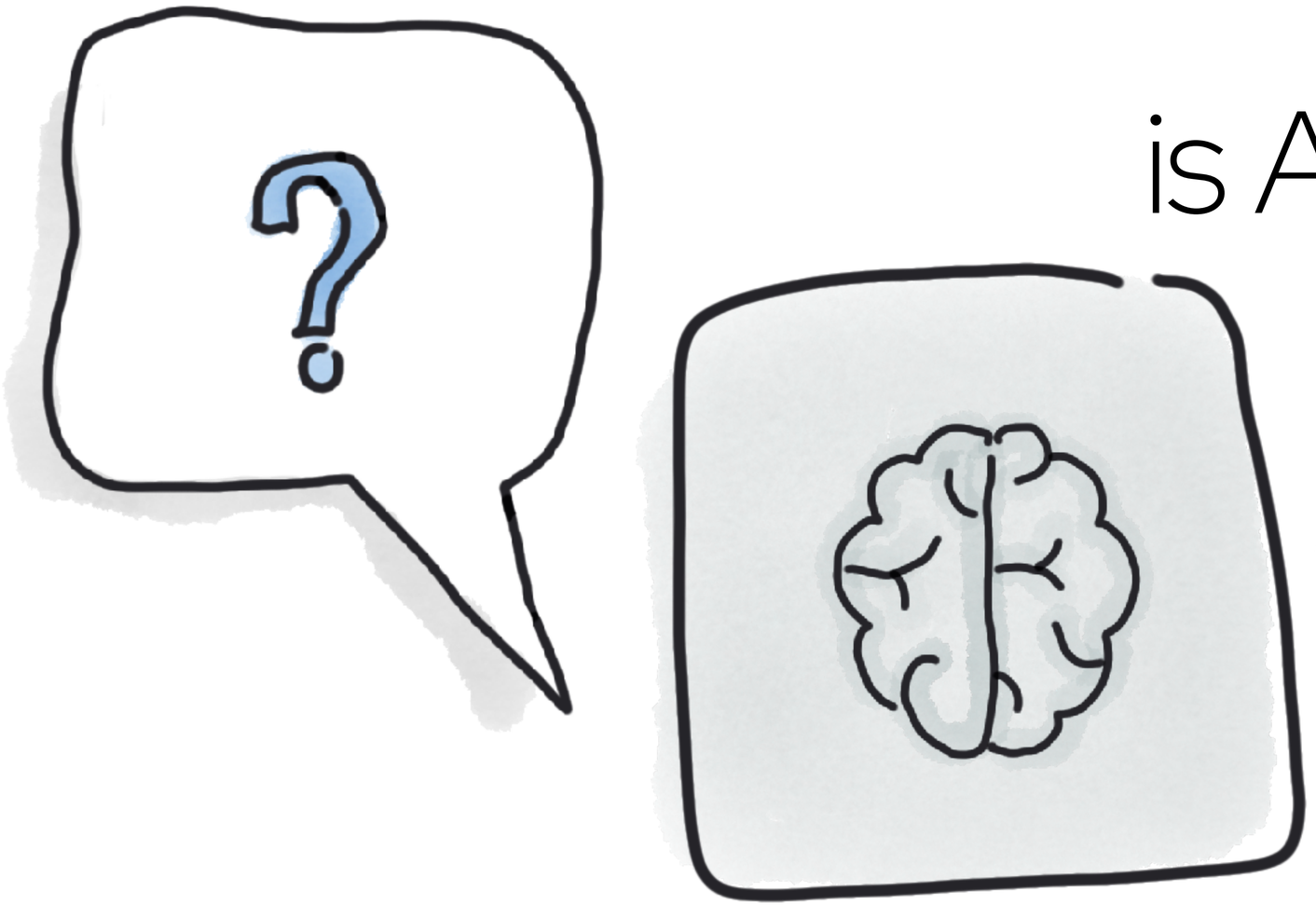
less investment means less hiring



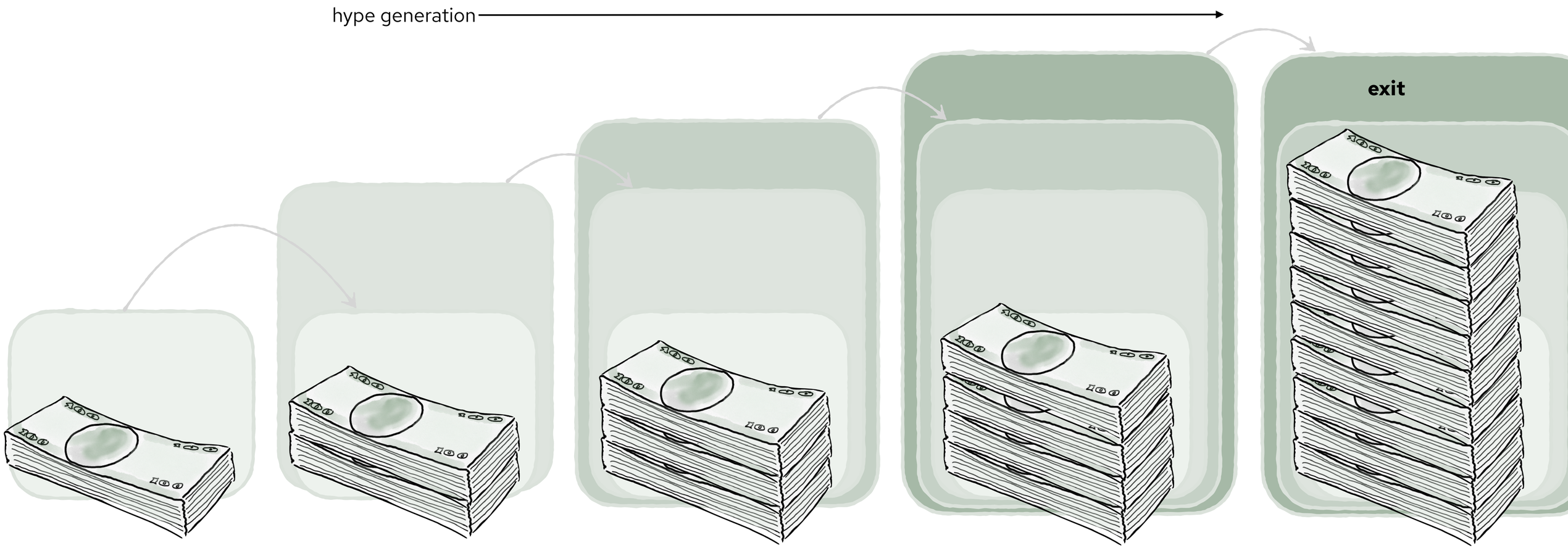
less investment means less hiring

what about the ai-lephant in the room?





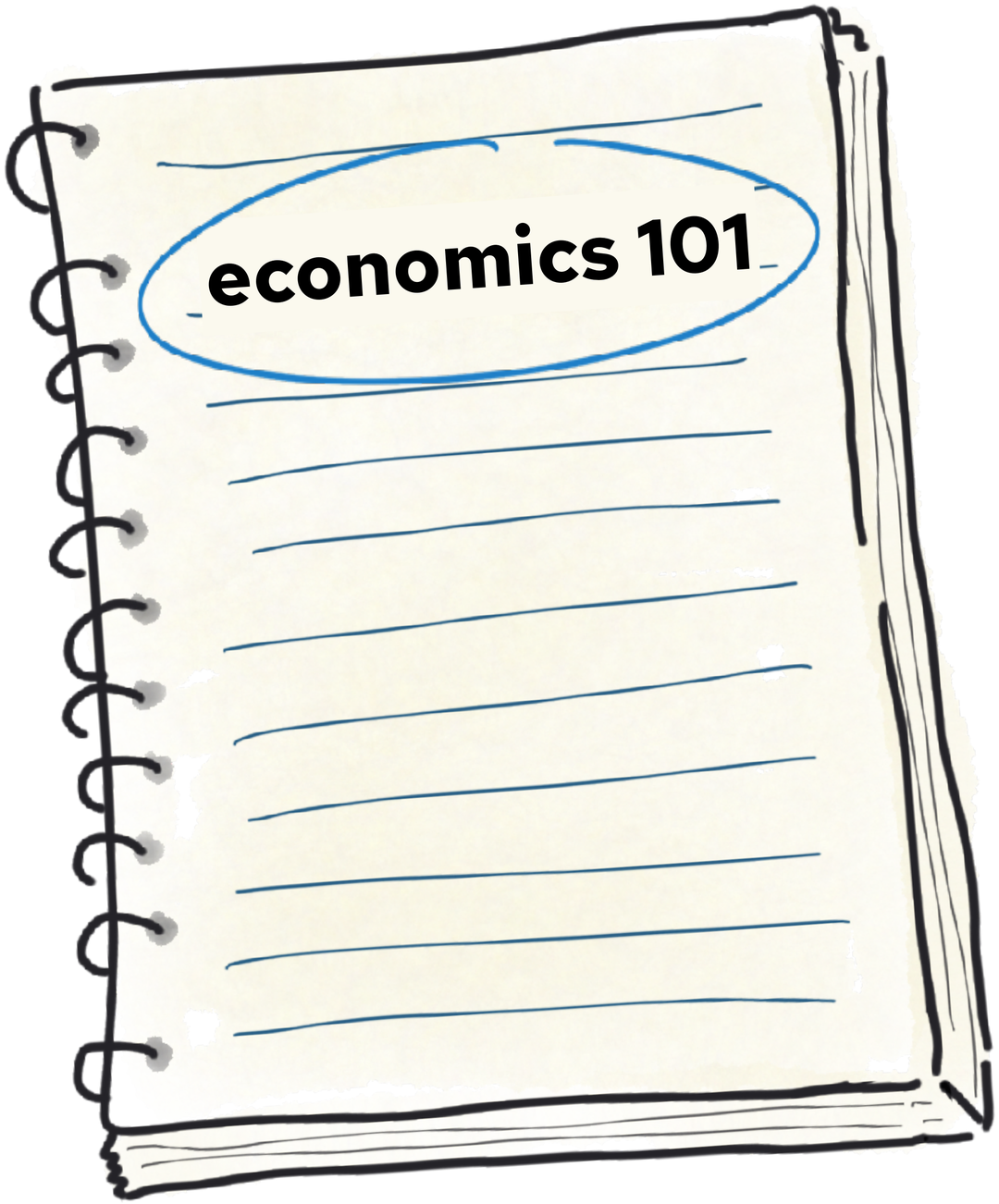
is AI killing jobs?



AI is attracting heavy investment

“our AI strategy is working”

just because AI makes developers more productive,
doesn't mean it will reduce the number of developers



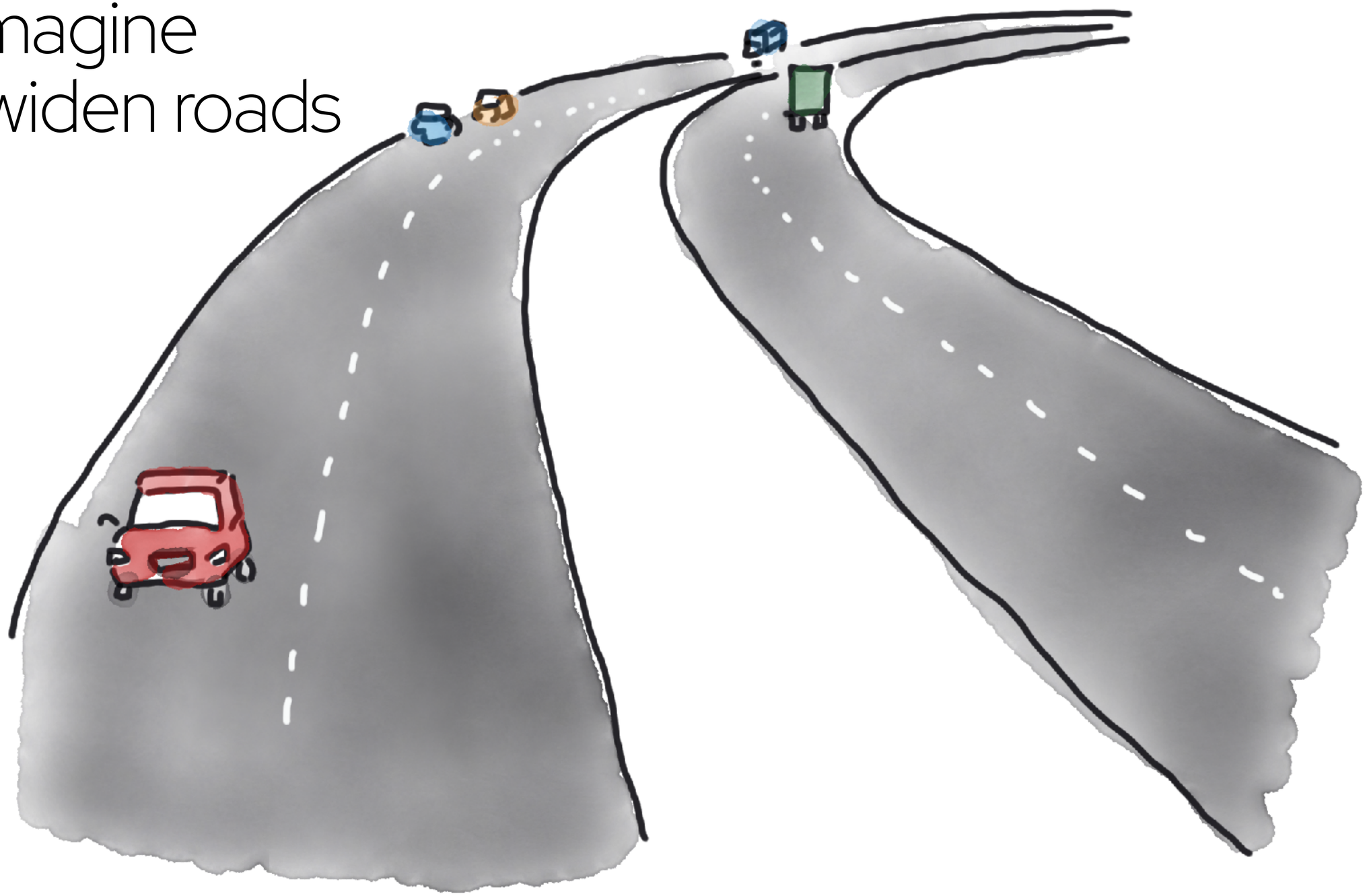
jevon's paradox

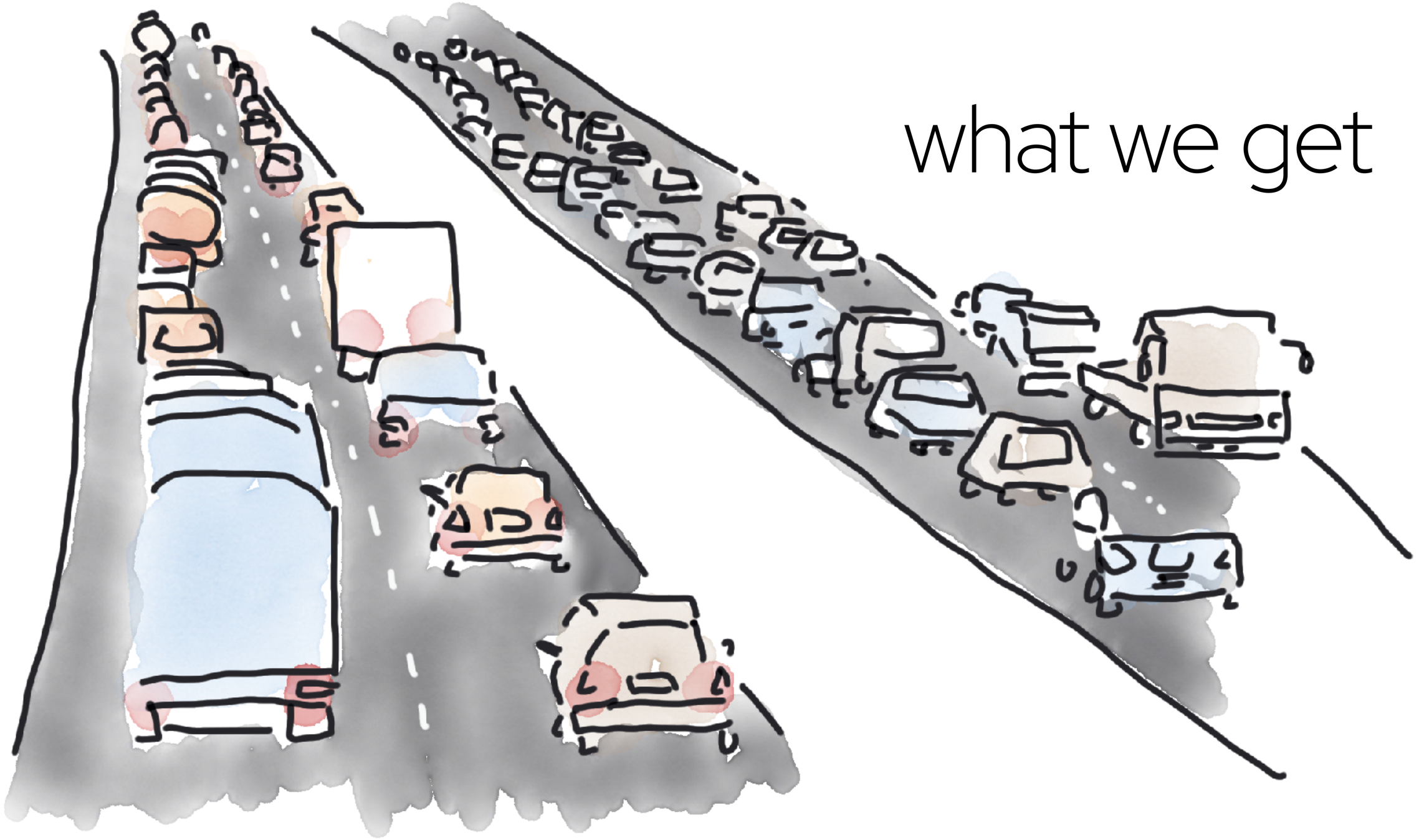
jevon's paradox

jevon's paradox

"efficiency improvements can lead to increased consumption"

what we imagine
when we widen roads





what we get

software is not going away

1800s



1800s

"knocker-up"



1800s

"knocker-up"

human alarm clock



1800s - 1940s

"knocker-up"

human alarm clock



1800s - 1940s

"knocker-up"

human alarm clock

finite demand



1800s - 1940s

"knocker-up"

human alarm clock

finite demand

only employees need waking up



1800s - 1940s



“knocker-up”

human alarm clock

finite demand

only employees need waking up

no one needs waking up more than once

the more software we have,
the more we want

software to do stuff

software to do stuff
software to do more stuff

software to do stuff
software to do more stuff
software to tell people about software

software to do stuff
software to do more stuff
software to tell people about software
software to bypass advertisements in the software

software to do stuff
software to do more stuff
software to tell people about software
software to bypass advertisements in the software
software to bypass the bypass software so ads still show

software to do stuff
software to do more stuff
software to tell people about software
software to bypass advertisements in the software
software to bypass the bypass software so ads still show
software to gamify software

software to do stuff
software to do more stuff
software to tell people about software
software to bypass advertisements in the software
software to bypass the bypass software so ads still show
software to gamify software
software to monitor the software

software to do stuff
software to do more stuff
software to tell people about software
software to bypass advertisements in the software
software to bypass the bypass software so ads still show
software to gamify software
software to monitor the software
software to debug the vibe-coded software

software to do stuff
software to do more stuff
software to tell people about software
software to bypass advertisements in the software
software to bypass the bypass software so ads still show
software to gamify software
software to monitor the software
software to debug the vibe-coded software
software to manage the software

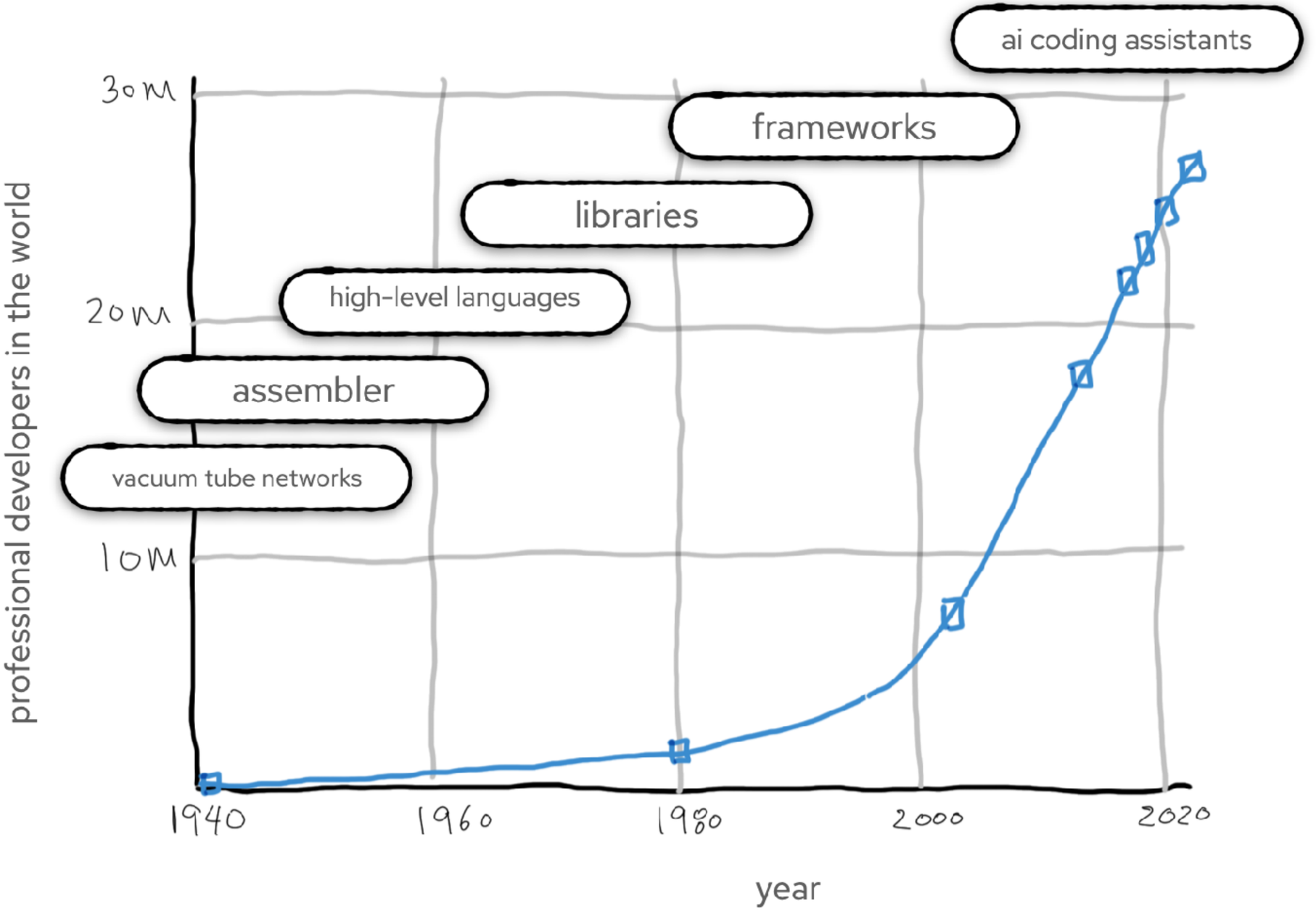
software to do stuff
software to do more stuff
software to tell people about software
software to bypass advertisements in the software
software to bypass the bypass software so ads still show
software to gamify software
software to monitor the software
software to debug the vibe-coded software
software to manage the software
software to write the software

software to do stuff
software to do more stuff
software to tell people about software
software to bypass advertisements in the software
software to bypass the bypass software so ads still show
software to gamify software
software to monitor the software
software to debug the vibe-coded software
software to manage the software
software to write the software
software to manage the software that writes the software

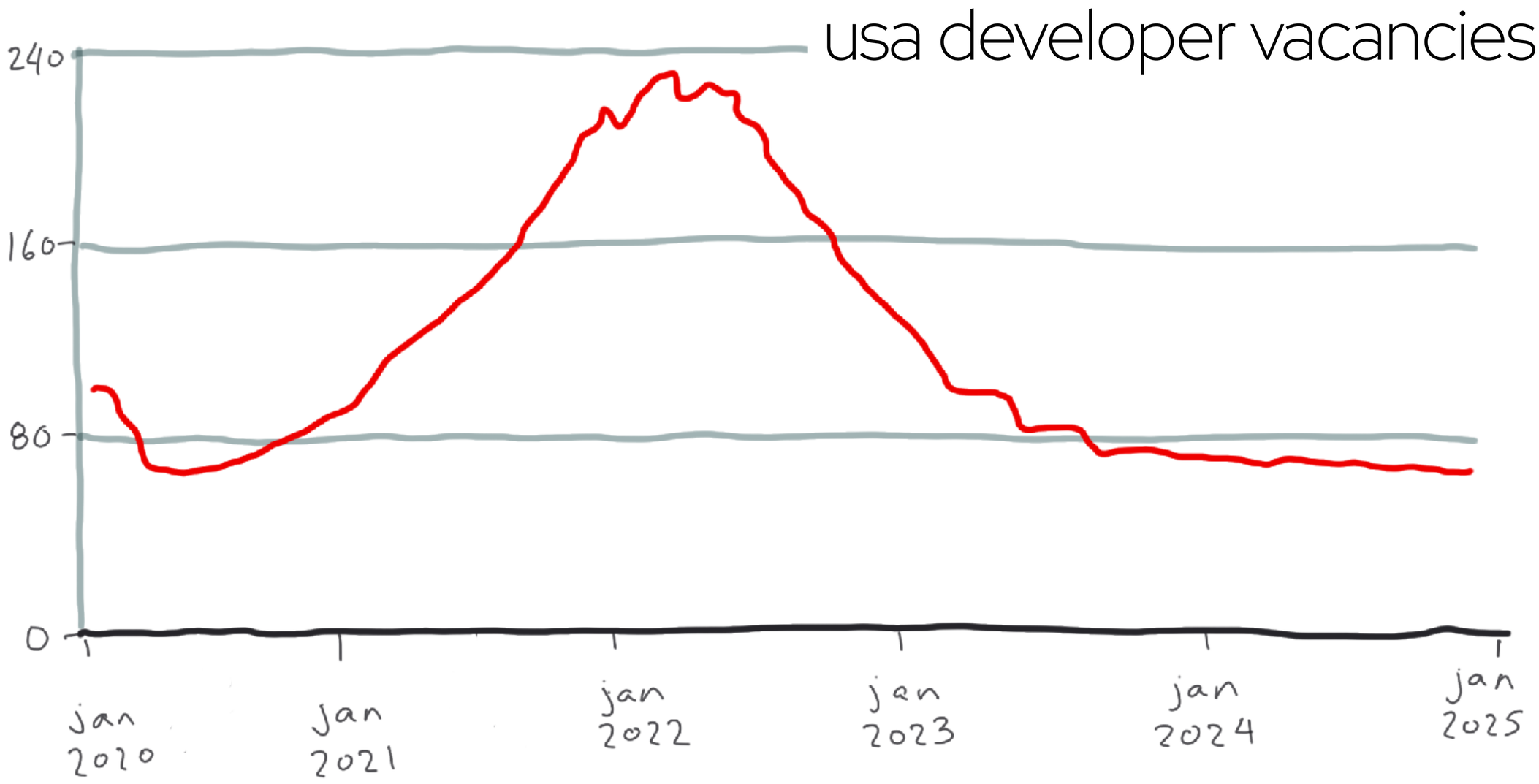
software to do stuff
software to do more stuff
software to tell people about software
software to bypass advertisements in the software
software to bypass the bypass software so ads still show
software to gamify software
software to monitor the software
software to debug the vibe-coded software
software to manage the software
software to write the software
software to manage the software that writes the software
software to try and avoid skynet

software to do stuff
software to do more stuff
software to tell people about software
software to bypass advertisements in the software
software to bypass the bypass software so ads still show
software to gamify software
software to monitor the software
software to debug the vibe-coded software
software to manage the software
software to write the software
software to manage the software that writes the software
software to try and avoid skynet
software to work out the meaning of life

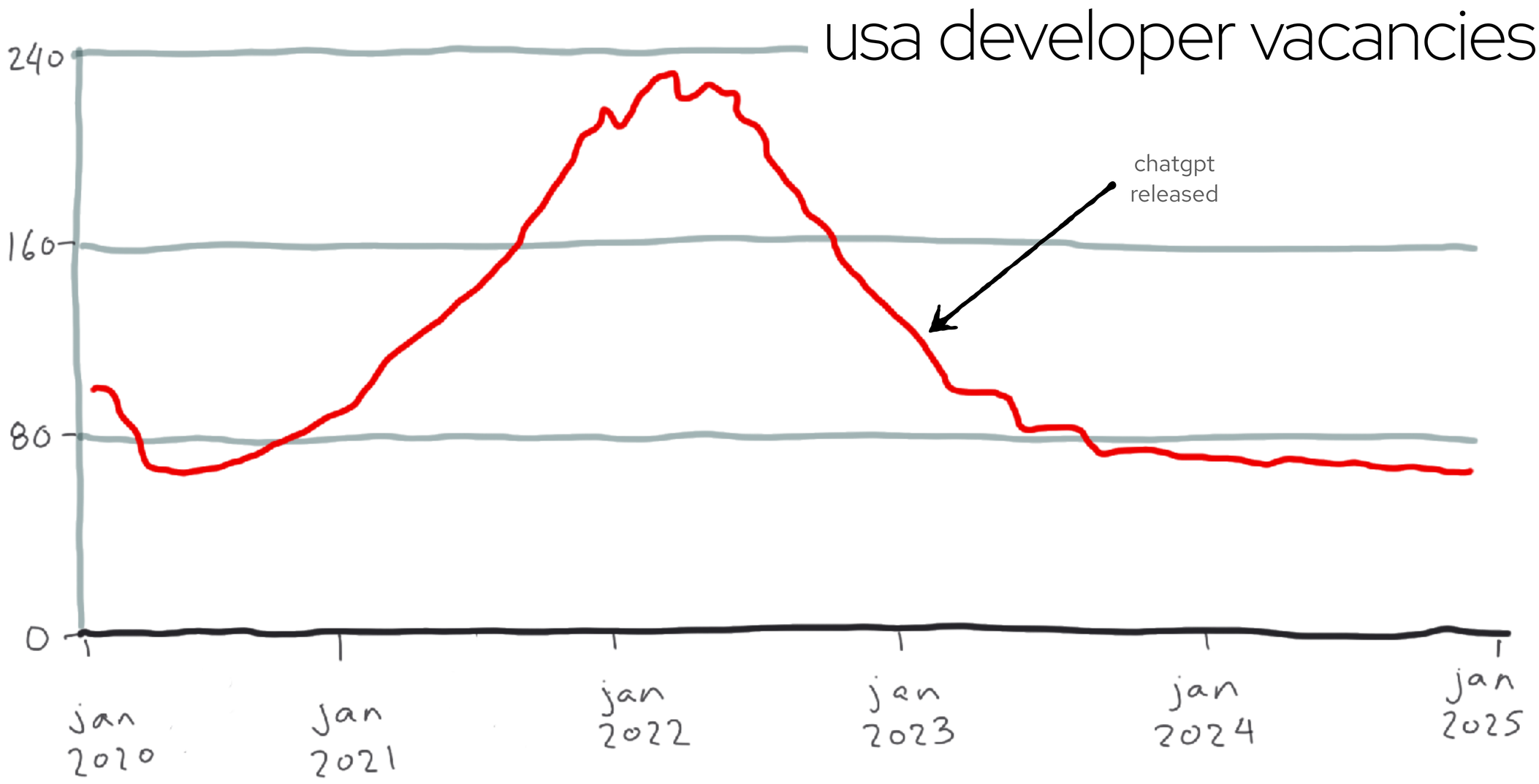
software to do stuff
software to do more stuff
software to tell people about software
software to bypass advertisements in the software
software to bypass the bypass software so ads still show
software to gamify software
software to monitor the software
software to debug the vibe-coded software
software to manage the software
software to write the software
software to manage the software that writes the software
software to try and avoid skynet
software to work out the meaning of life
...


ai coding assistants
frameworks
libraries
high-level languages
assembler
vacuum tube networks
30M
20M
10M
professional developers in the world
1940
1960
1980
2000
2020
year

Source: indeed.com via https://newsletter.pragmaticengineer.com/p/software-engineering-job-openings?publication_id=458709



Source: indeed.com via https://newsletter.pragmaticengineer.com/p/software-engineering-job-openings?publication_id=458709



tl;dpa

(too long; didn't pay attention)



tl;dpa

(too long; didn't pay attention)



- statistics is (annoyingly) important, especially bayes

tl;dpa

(too long; didn't pay attention)



- statistics is (annoyingly) important, especially bayes
- to achieve more power, computers have to add more cores

tl;dpa

(too long; didn't pay attention)



- statistics is (annoyingly) important, especially bayes
- to achieve more power, computers have to add more cores
- software is not very good at taking advantage of these cores

tl;dpa

(too long; didn't pay attention)



- statistics is (annoyingly) important, especially bayes
- to achieve more power, computers have to add more cores
- software is not very good at taking advantage of these cores
- for data you want to be secret in 10 years, use quantum-safe crypto

tl;dpa

(too long; didn't pay attention)



- statistics is (annoyingly) important, especially bayes
- to achieve more power, computers have to add more cores
- software is not very good at taking advantage of these cores
- for data you want to be secret in 10 years, use quantum-safe crypto
- the rise of interest rates means a tougher job market

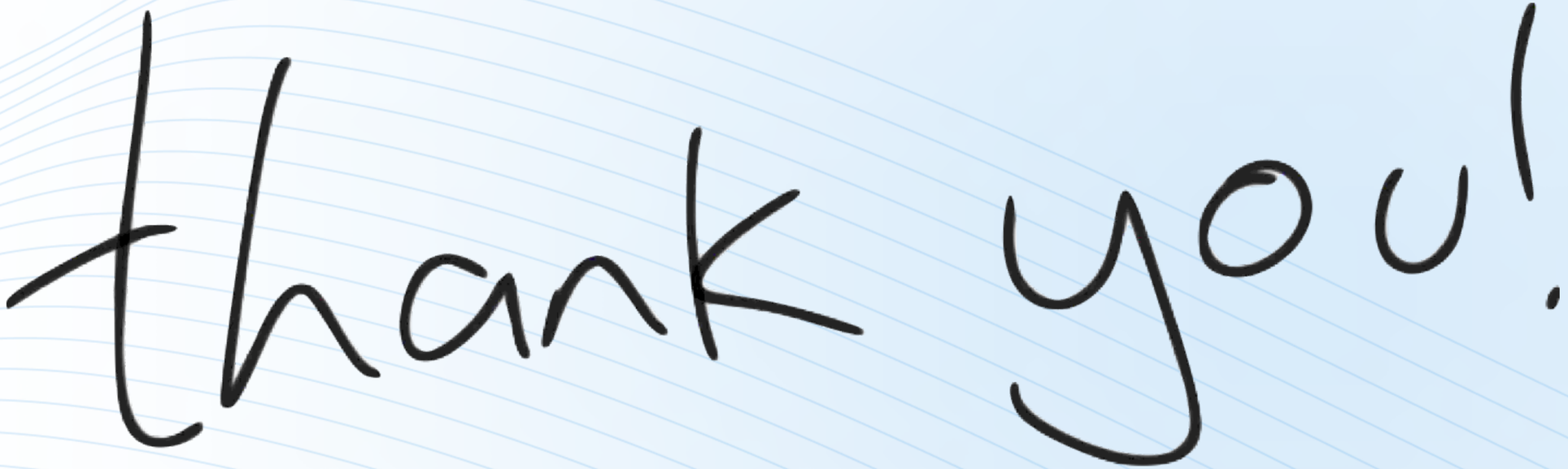
tl;dpa

(too long; didn't pay attention)



- statistics is (annoyingly) important, especially bayes
- to achieve more power, computers have to add more cores
- software is not very good at taking advantage of these cores
- for data you want to be secret in 10 years, use quantum-safe crypto
- the rise of interest rates means a tougher job market
- jevon's paradox means demand for software will go up even if ai makes producing software cheaper

goto;



QUESTIONS?

ASK ME IN THE APP

goto;

RATE THIS SESSION

YES, YOU'LL GET A REWARD

goto;



http://hollycummins.com/things-to-care-about-goto/