GETTING BUZZED ON BUZZWORDS

MOLOCH
@littlejoetables

MANDATORY
@iammandatory

Hola!

*I am **Mandatory***

Hola!

*I am **Mandatory***

About

Security engineer, XSS Hunter, DNS, and more!

Hola!

I am Mandatory

About
Security engineer, XSS Hunter, DNS, and more!

Industry Certifications
High School Diploma

Hola!

I am Mandatory

About
Security engineer, XSS Hunter, DNS, and more!

Industry Certifications
High School Diploma

Blog
TheHackerBlog.com

Twitter
@iammandatory

EHLO

*I am **Moloch***

EHLO

I am Moloch

About
I like computers.

EHLO

I am Moloch

About
I like computers.

Industry Certifications
High School Diploma

EHLO

I am Moloch

About
I like computers.

Industry Certifications
High School Diploma

Occupation
Senior Associate, Bishop Fox

Twitter
@littlejoetables

The Cloud

The Deep Cloud?

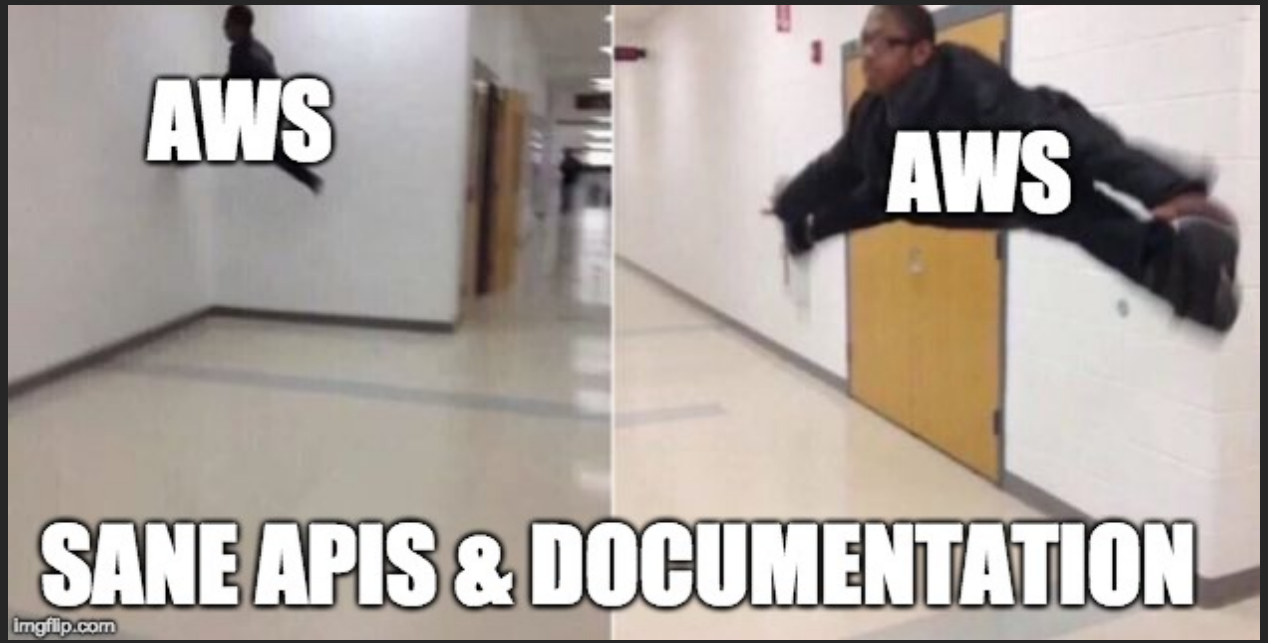
Distributed Cloud!

THE DARK CLOUD

Raise your hand if you're an AWS employee...

Raise your hand if you're a reverse engineer...

AWS Services



Let’s Get VC Funding

Let’s Get VC Funding

- Buy some eScooters off of Amazon …

Let’s Get VC Funding

Let’s Get VC Funding

- “Burp Intruder” at ∞ QPS

Let’s Get VC Funding

- “Burp Intruder” at ∞ QPS
- Cloud Rainbow Tables

Let’s Get VC Funding

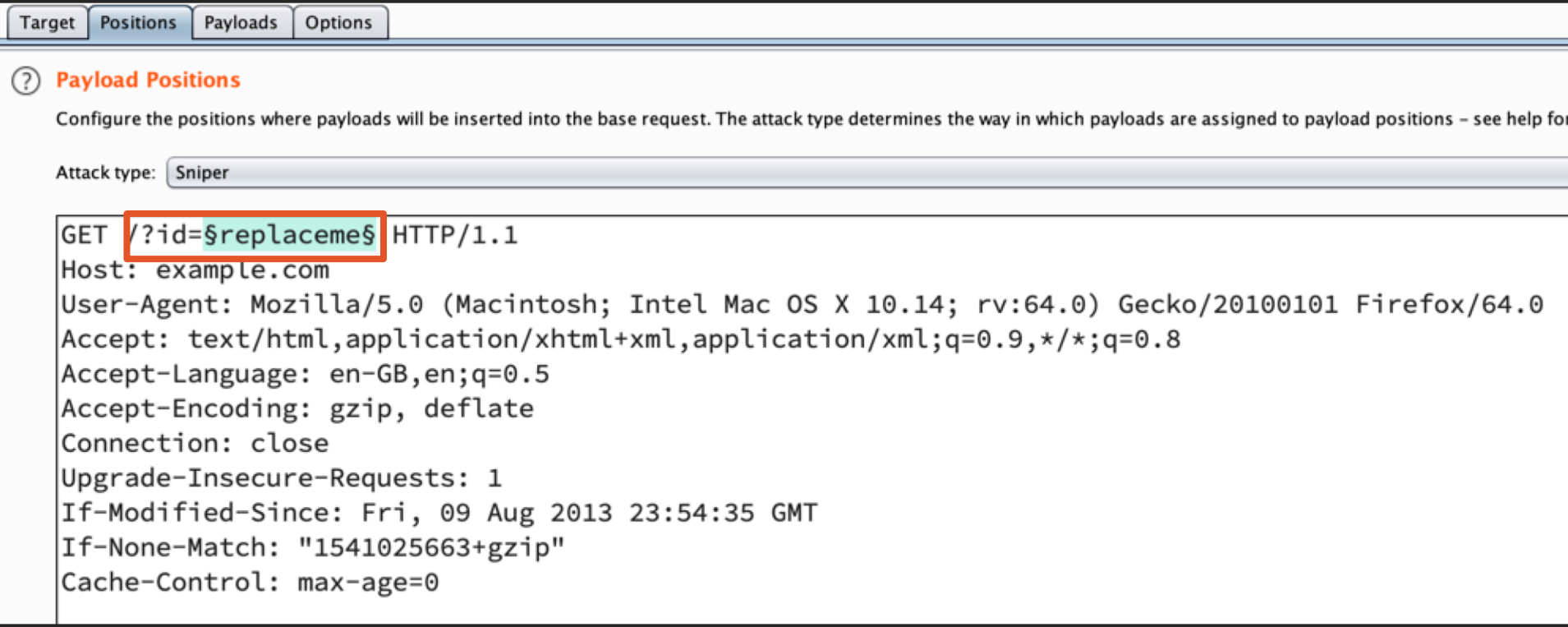
- “Burp Intruder” at ∞ QPS
- Cloud Rainbow Tables
- Cost effective GPU clusters

Let’s Get VC Funding

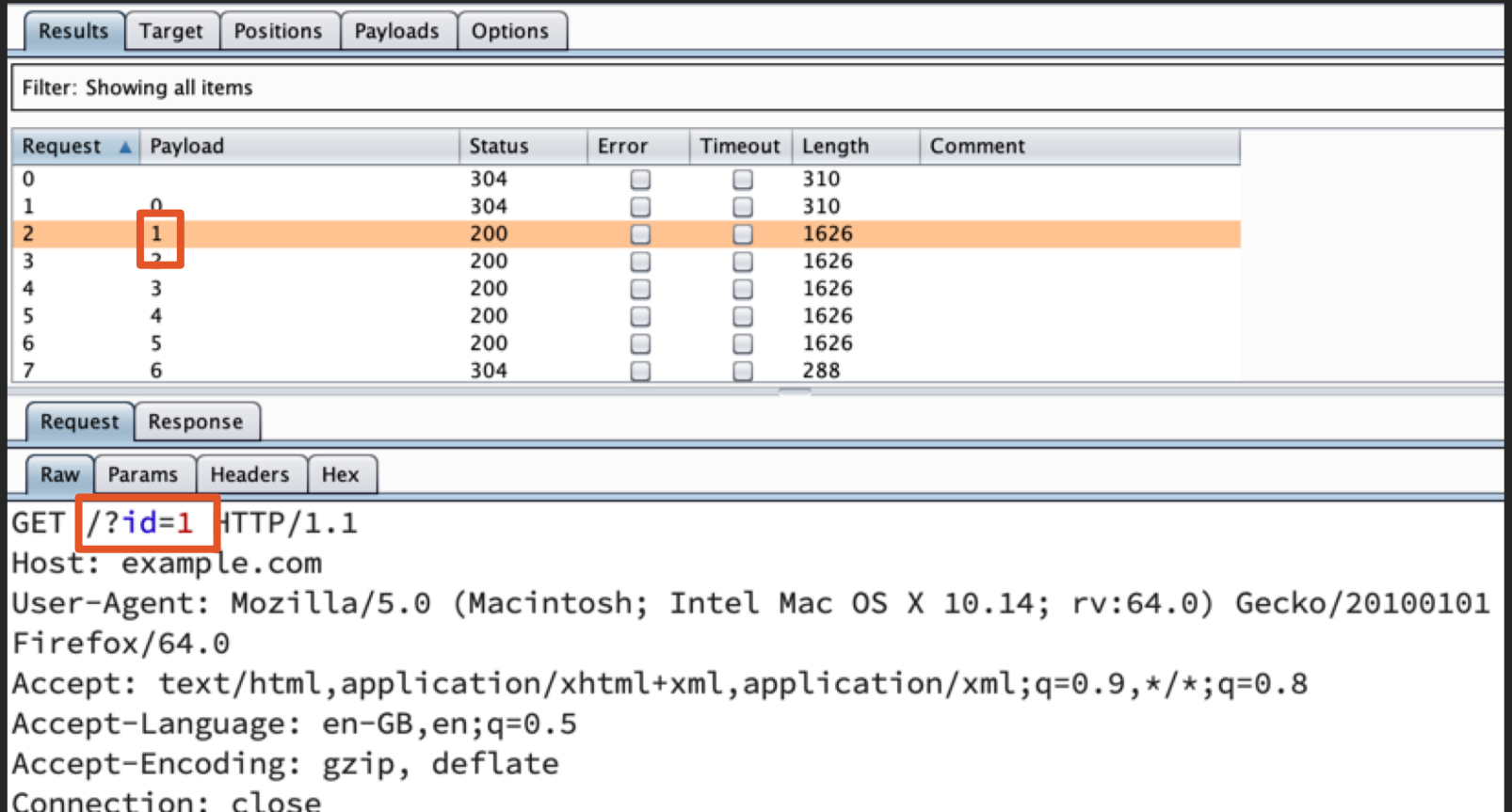
- “Burp Intruder” at ∞ QPS
- Cloud Rainbow Tables
- Cost effective GPU clusters
- *…maybe more time permitting*

”Burp Intruder” at ∞ QPS

Burp Intruder



Burp Intruder



Burp Limits

- Your laptop Internet speed
- Threaded model
- Single app, single computer

It’s not web scale!

Serverless “Burp Intruder”

- Do the same thing but with Lambdas
- Scale up to ∞ QPS
- Store all the results in S3

Lambda Functions

- Lambdas are self-contained code packages
- No “server” hence “serverless”
- Billed $0.20 per 1 million requests and ~$0.17 per 10K GB seconds
- “Event based” executions

Chicken & Egg

- Invoking a Lambda is 1 API call
- 10 API calls = 10 runs
- How we do quickly ramp up?

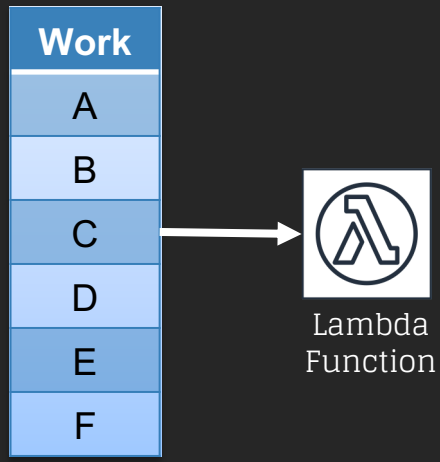
Serverless “Burp Intruder”

- Self-invocating Lambda
- Take work
- Split work
- Call self with both halves

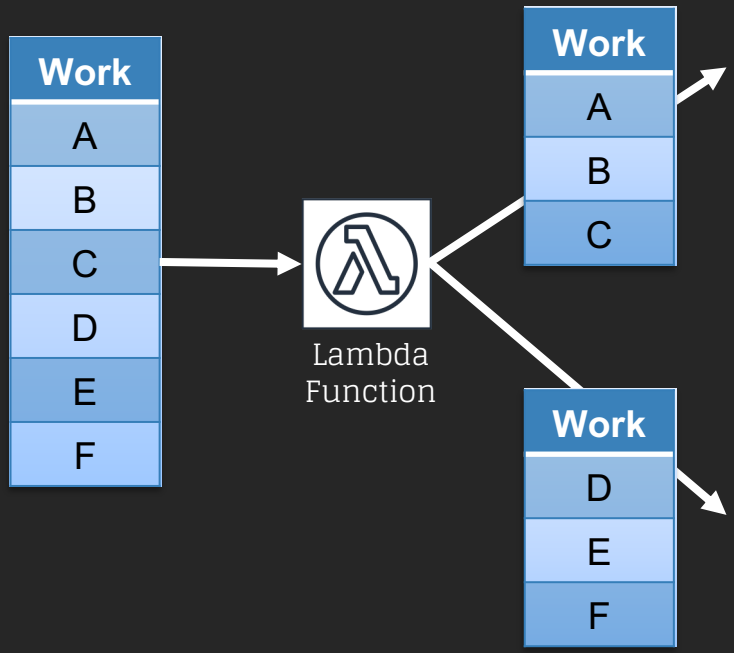
Rama Lambda Ding Dong

Lambda
Function

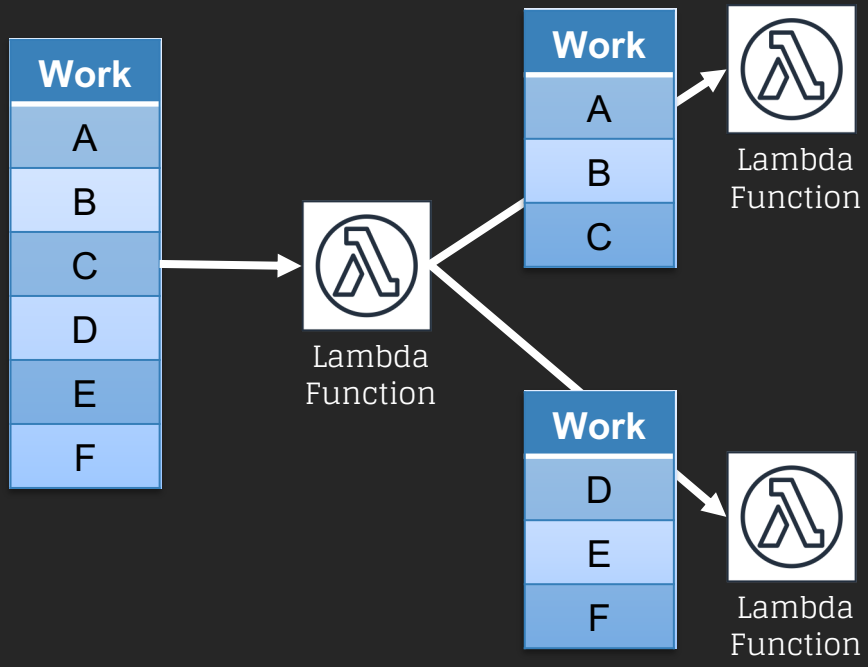
Rama Lambda Ding Dong



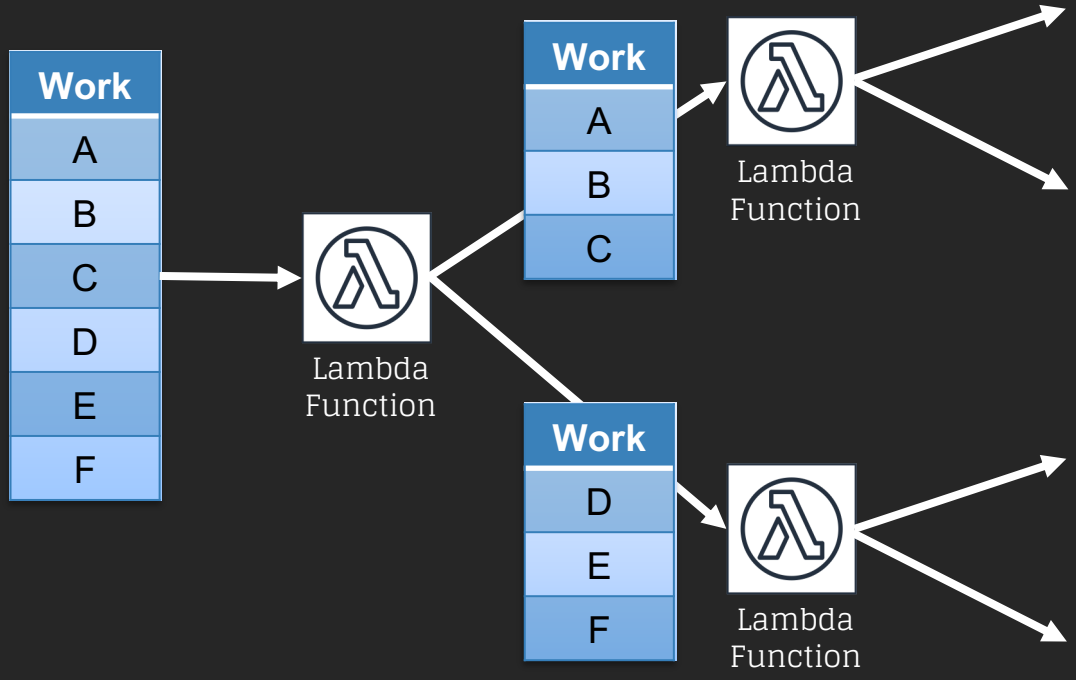
Rama Lambda Ding Dong



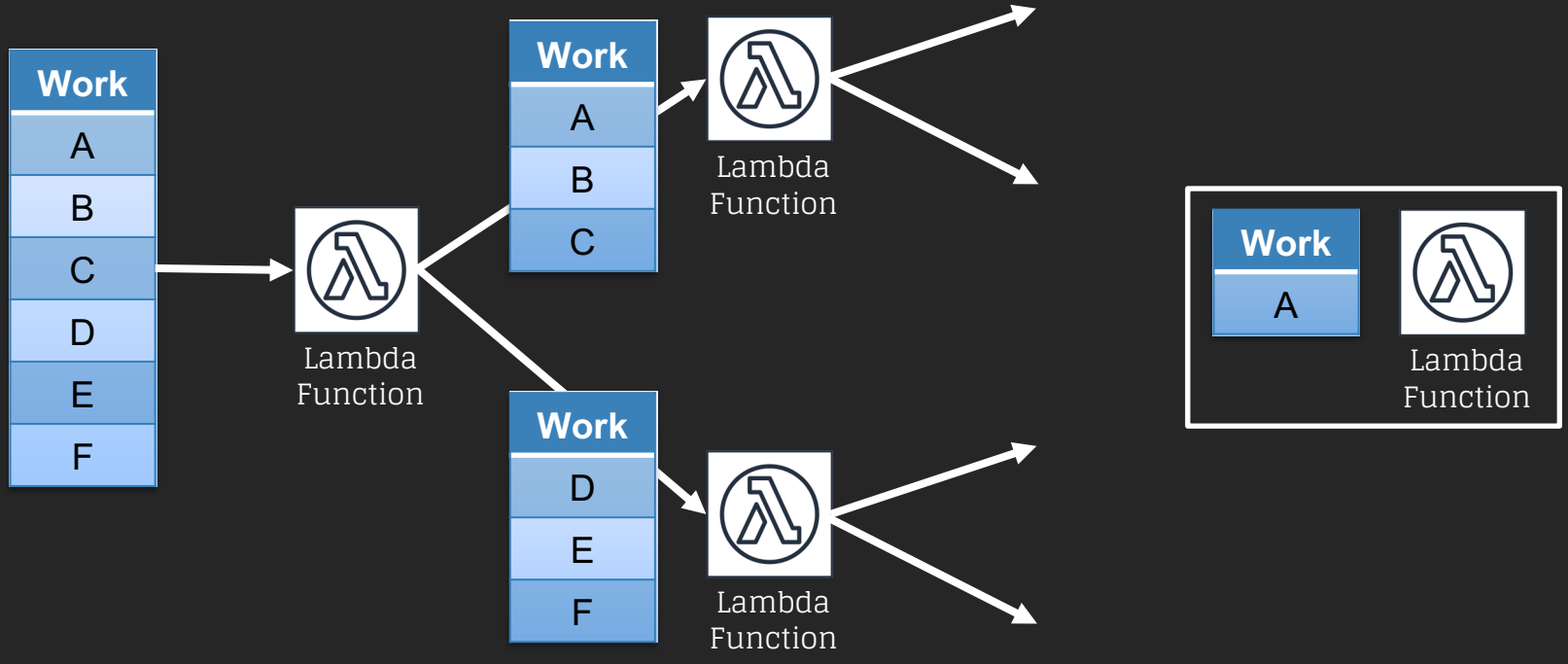
Rama Lambda Ding Dong



Rama Lambda Ding Dong



Rama Lambda Ding Dong




EVERYTHING JUST SCALES!
CONTACT SUPPORT FOR HIGHER QUOTA


AWS

Do NOT DoS the server!

The Design

- Payloads decoupled from requester
- Stateless
- Scales up infinitely (with $)

Available Now!

github.com/mandatoryprogrammer/lambda-intruder

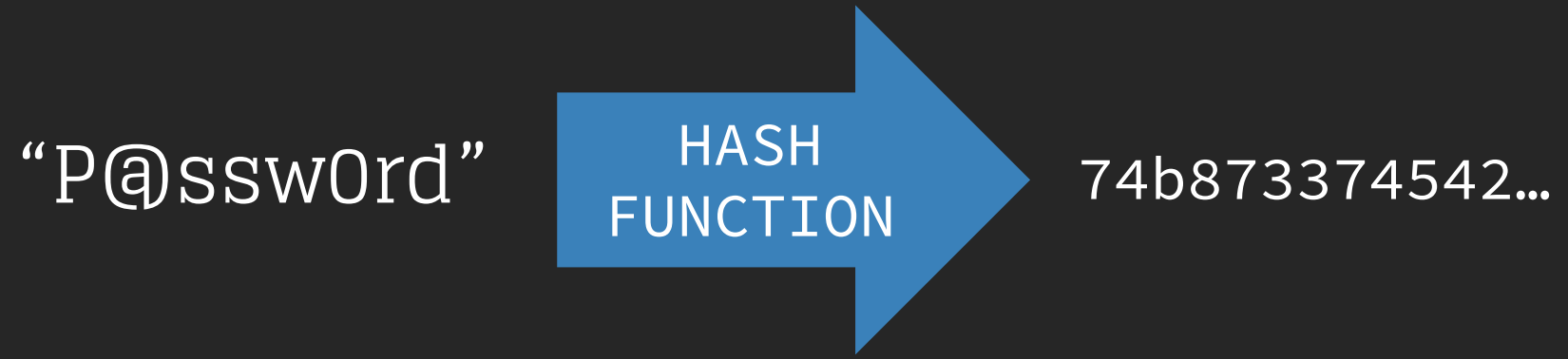
Rainbow Tables

What’s a Rainbow Table?

What's a Rainbow Table?

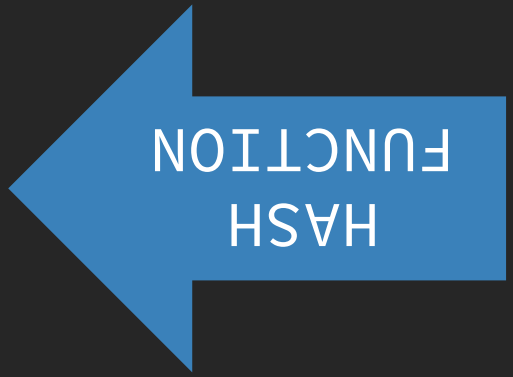
- Pre-computation attacks against password hashes

What's a Password Hash?



What's a Password Hash?

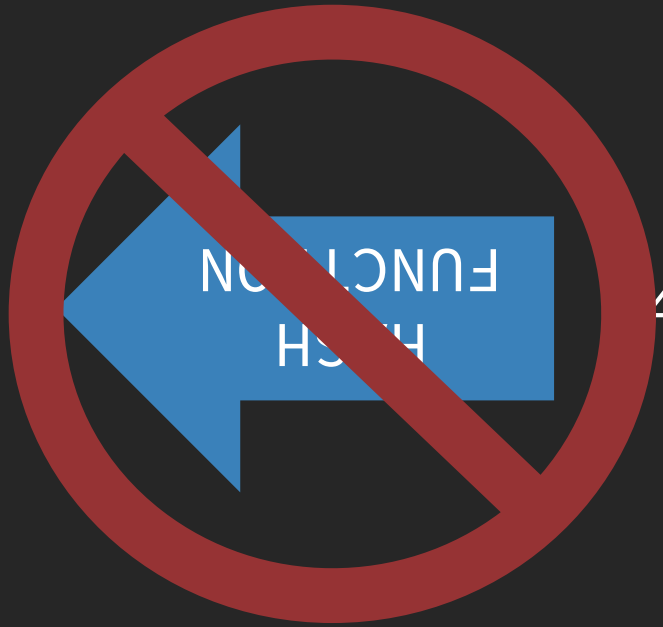
"Password"



74b873374542…

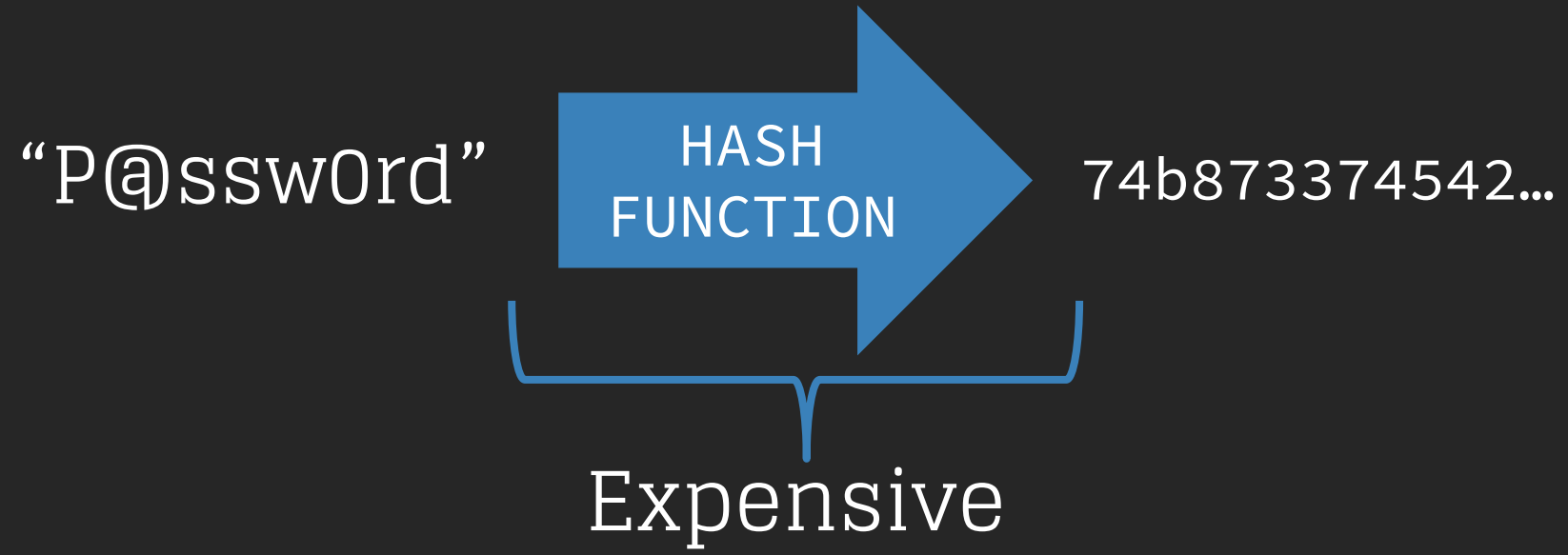
What's a Password Hash?

"Password"



4b873374542...

What's a Password Hash?



What's a Rainbow Table?

- Pre-computation attacks against password hashes

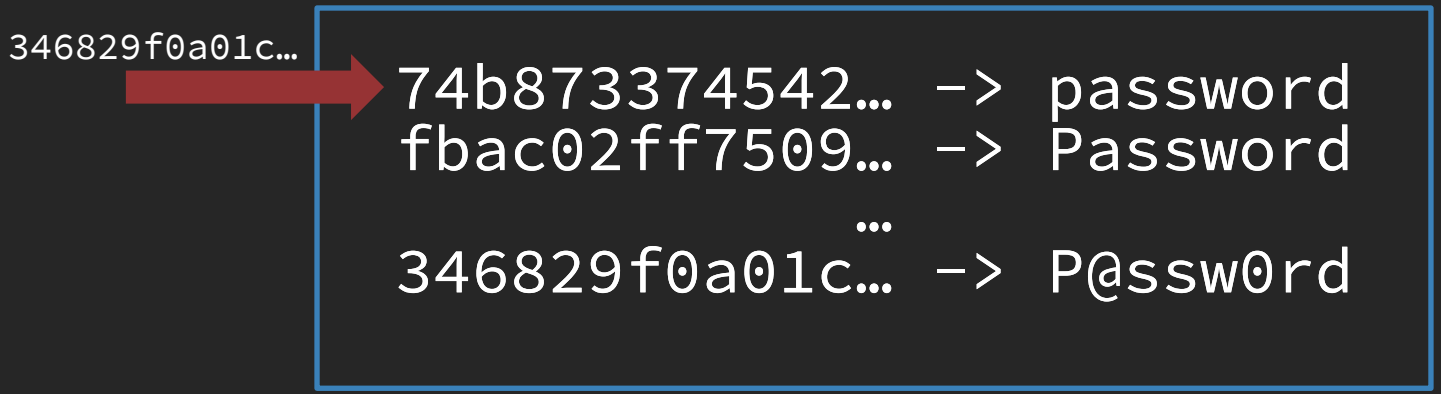
What's a Rainbow Table?

- Pre-computation attacks against password hashes

```
74b873374542… -> password
fbac02ff7509… -> Password
            …
346829f0a01c… -> P@ssw0rd
```

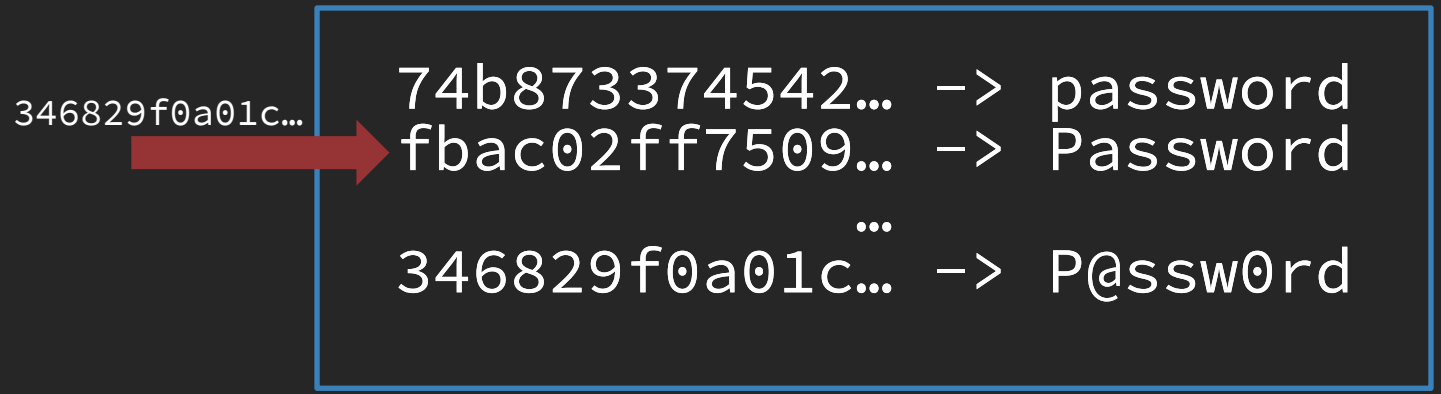
What's a Rainbow Table?

- Pre-computation attacks against password hashes



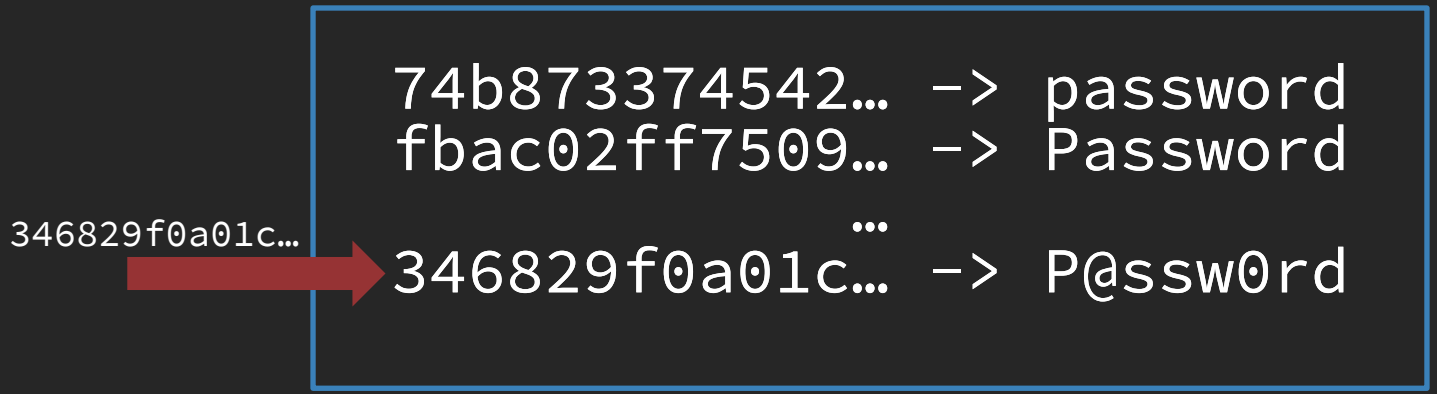
What's a Rainbow Table?

- Pre-computation attacks against password hashes



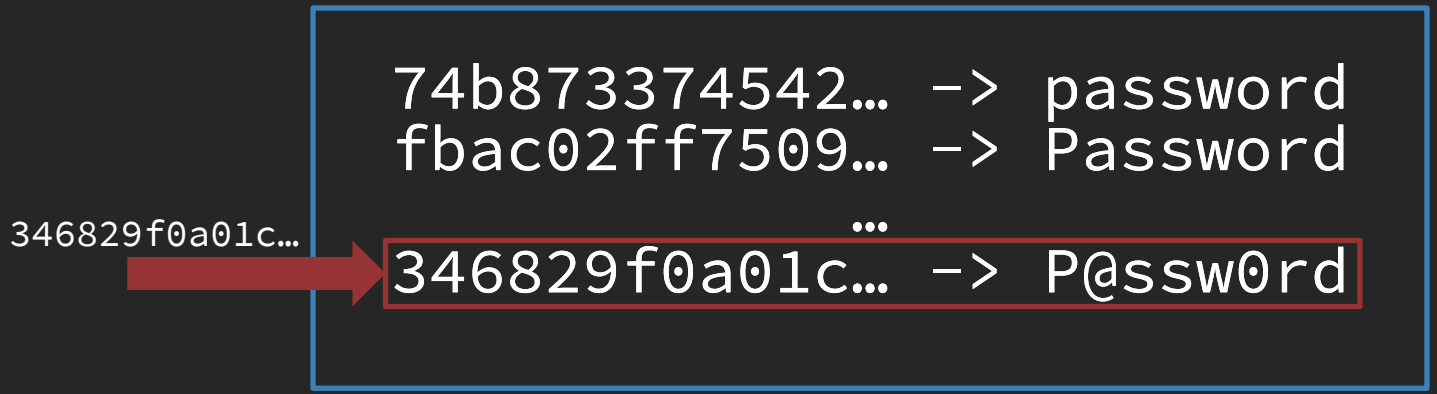
What's a Rainbow Table?

- Pre-computation attacks against password hashes



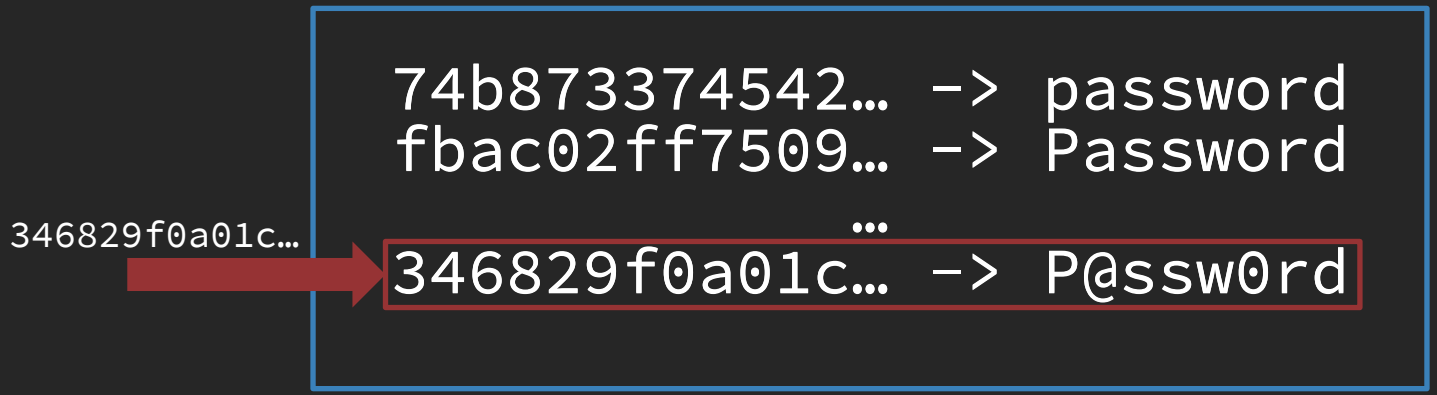
What's a Rainbow Table?

- Pre-computation attacks against password hashes

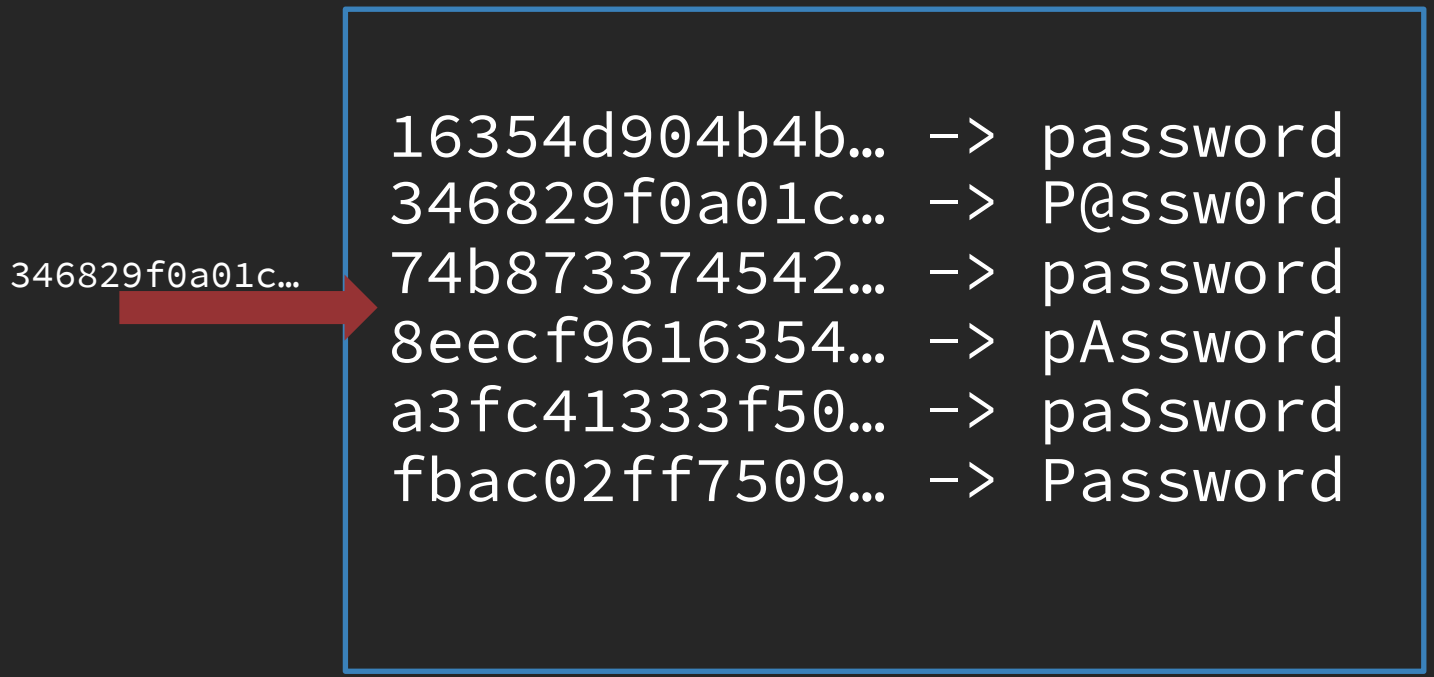


What's a Rainbow Table?

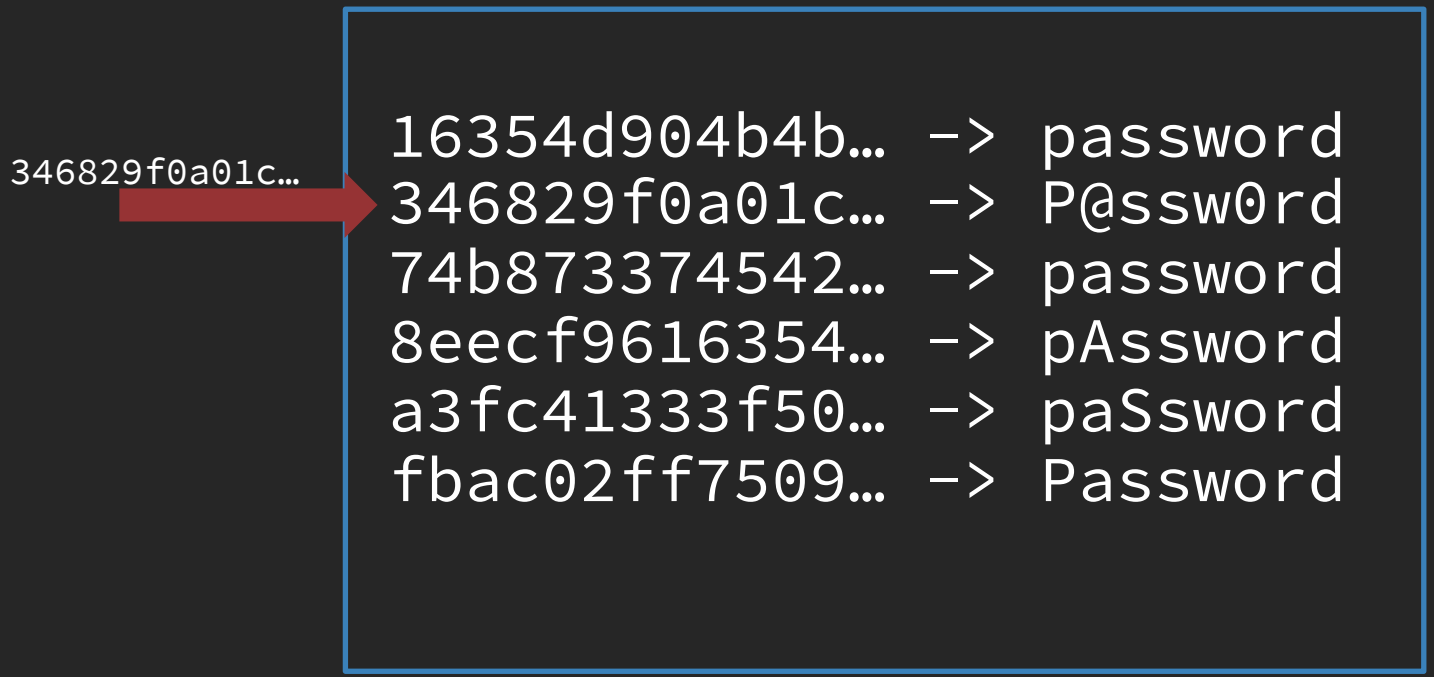
- Pre-computation attacks against password hashes



What's a Rainbow Table?



What's a Rainbow Table?



What's a Rainbow Table?

Team Logistics

- Large file sizes (hundreds of GBs)
- Remote access (servers)
- Server maintenance, hard drive failures, redundancy

Why not use a database?

Rainbow Tables

?

Database Tables

Why not use a database?

Why not use a database?

Google Big Query

What is Big Query?

What is Big Query?

BigQuery is Google's serverless, highly scalable, enterprise data warehouse designed to make all your data analysts productive at an unmatched price-performance.

What is Big Query?

It’s a big database you can crap terabytes of JSON into and query it.

Big Query


```
{

    "preimage": "0000",
    "md4": "+f1Xv3XKVdu0kX2fFp/Luw==",
    "md5": "Sn0e1BRHTkAzrCnMuGU9mw==",
    "sha1": "Od+lUoMxjTGv5aP/Sg4yU+IEXkM=",

…}\n
```

Big Query


```
{

    "preimage": "0000",
    "md4": "+f1Xv3XKVdu0kX2fFp/Luw==",
    "md5": "Sn0e1BRHTkAzrCnMuGU9mw==",
    "sha1": "Od+lUoMxjTGv5aP/Sg4yU+IEXkM=",

…}\n
```

Big Query

```
{

    "preimage": "0000",
    "md4": "+f1Xv3XKVdu0kX2fFp/Luw==",
    "md5": "Sn0e1BRHTkAzrCnMuGU9mw==",
    "sha1": "Od+lUoMxjTGv5aP/Sg4yU+IEXkM=",

…}\n
```

Big Query


```
{

    "preimage": "0000",
    "md4": "+f1Xv3XKVdu0kX2fFp/Luw==",
    "md5": "Sn0e1BRHTkAzrCnMuGU9mw==",
    "sha1": "Od+lUoMxjTGv5aP/Sg4yU+IEXkM=",

…}\n
```

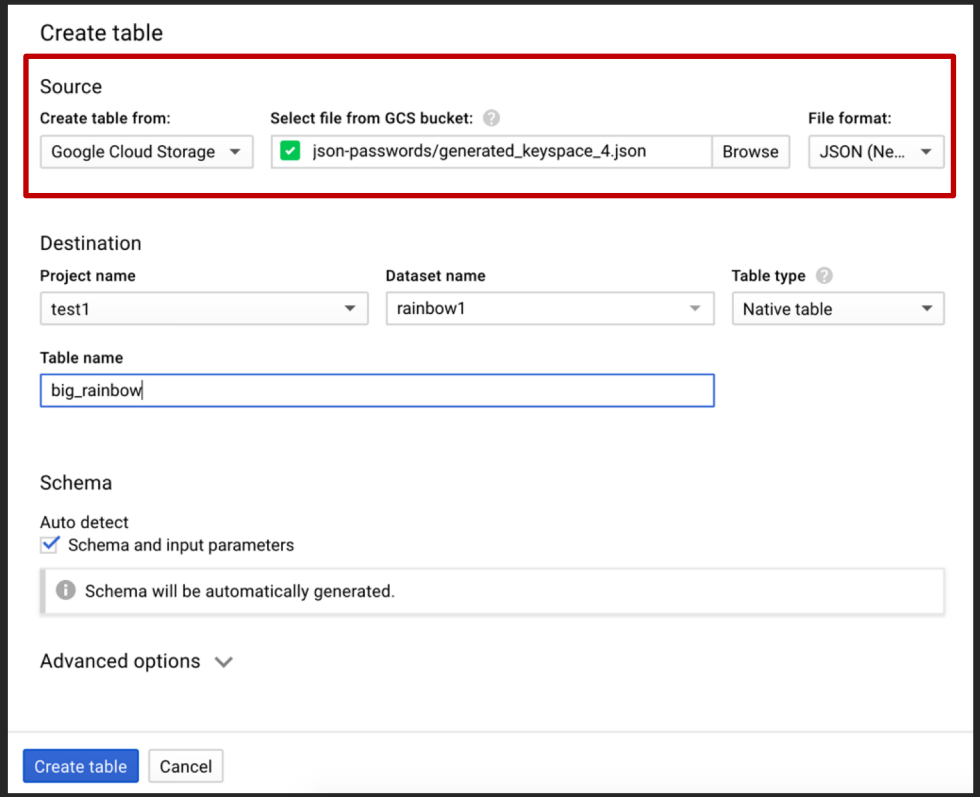
Big Query

```
{

    "preimage": "0000",
    "md4": "+f1Xv3XKVdu0kX2fFp/Luw==",
    "md5": "Sn0e1BRHTkAzrCnMuGU9mw==",
    "sha1": "Od+lUoMxjTGv5aP/Sg4yU+IEXkM=",

…}\n
```

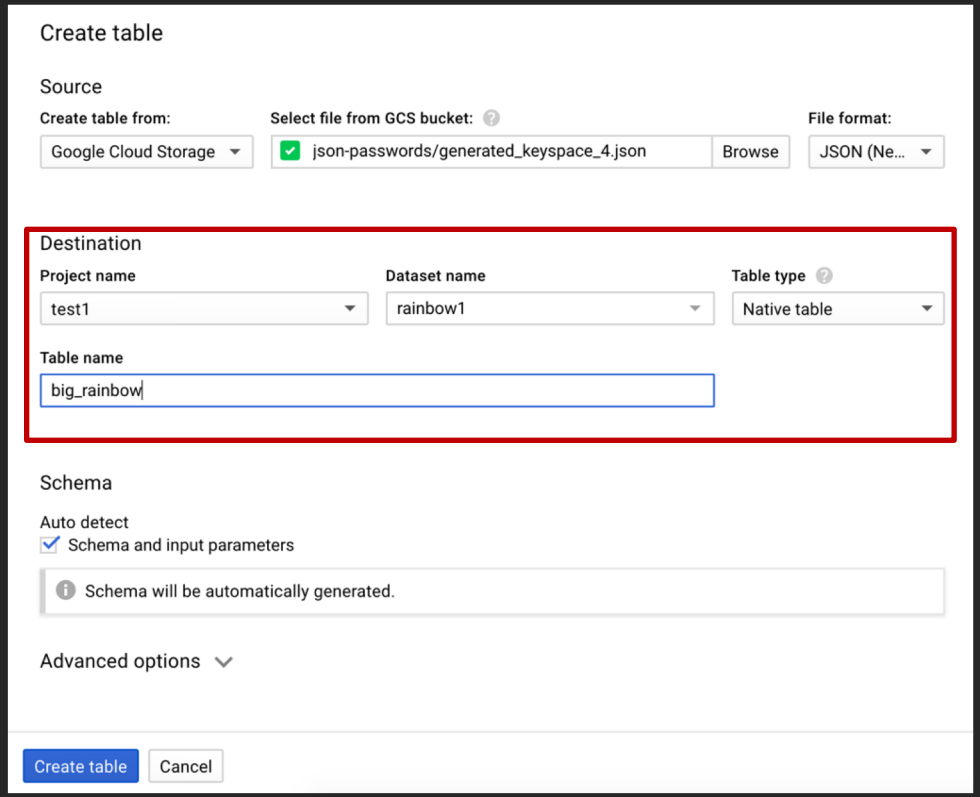
Big Query

(Repeat a few hundred million times)

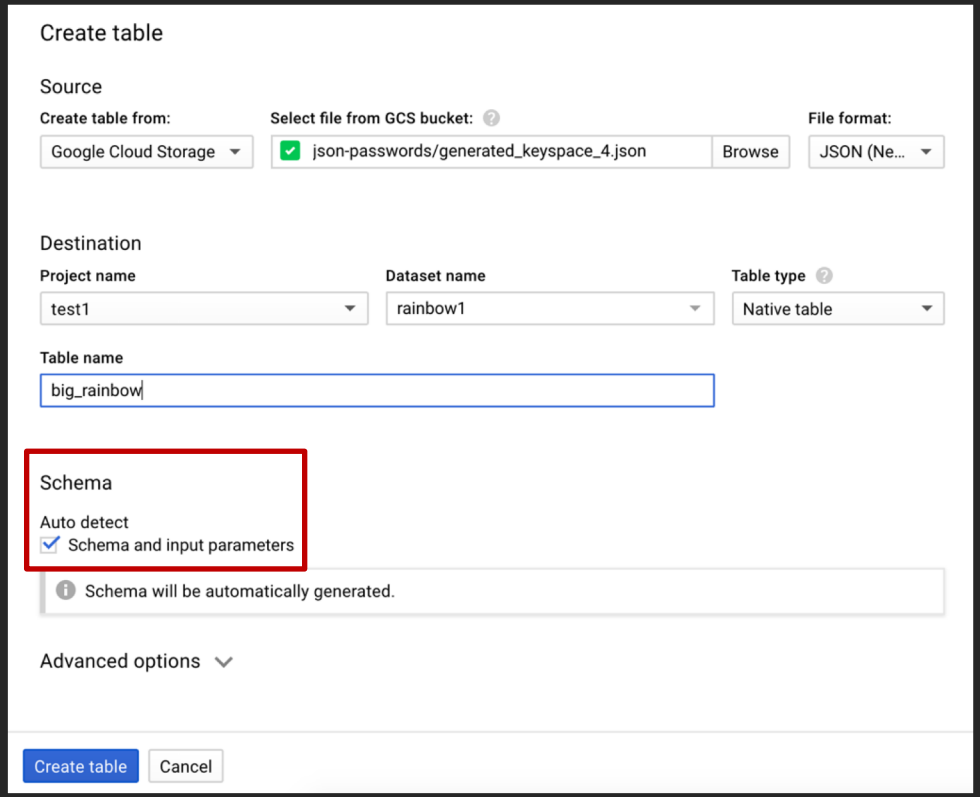
Big Query


Create table
Source
Create table from:
Google Cloud Storage
Select file from GCS bucket:
json-passwords/generated_keyspace_4.json
Browse
File format:
JSON (Ne...
Destination
Project name
test1
Dataset name
rainbow1
Table type
Native table
Table name
big_rainbow
Schema
Auto detect
Schema and input parameters
Schema will be automatically generated.
Advanced options
Create table
Cancel

Big Query

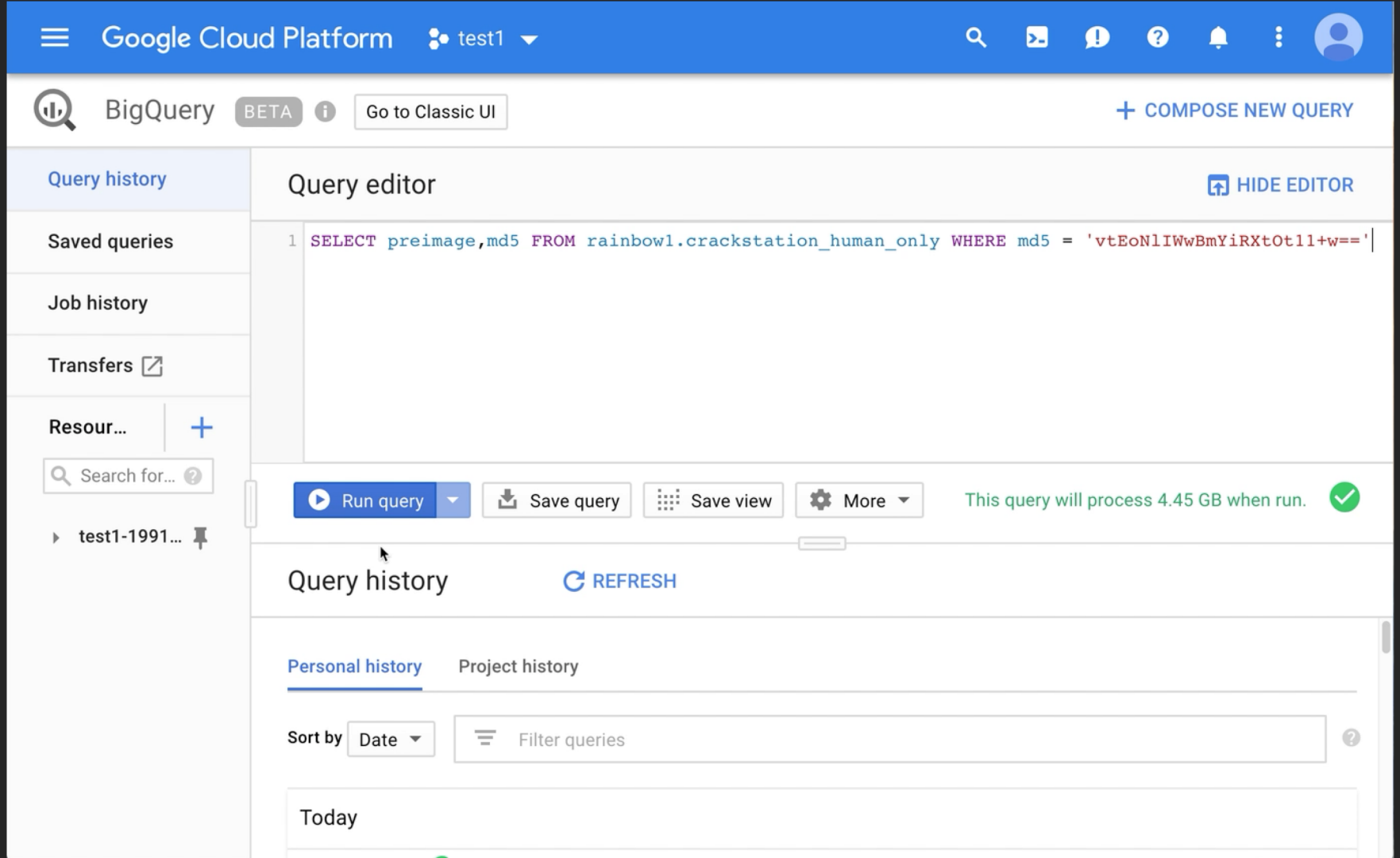

Create table
Source
Create table from:
Google Cloud Storage
Select file from GCS bucket:
json-passwords/generated_keyspace_4.json
Browse
File format:
JSON (Ne...
Destination
Project name
test1
Dataset name
rainbow1
Table type
Native table
Table name
big_rainbow
Schema
Auto detect
Schema and input parameters
Schema will be automatically generated.
Advanced options
Create table
Cancel

Big Query

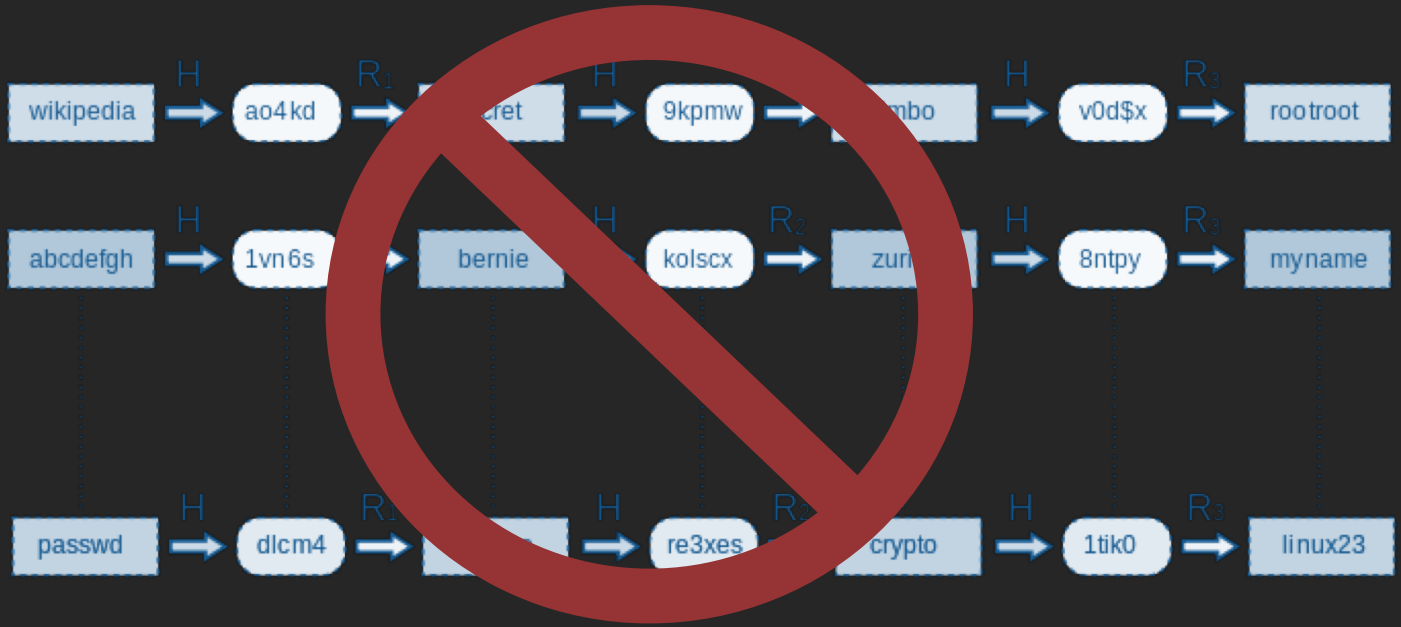

Create table
Source
Create table from:
Google Cloud Storage
Select file from GCS bucket:
json-passwords/generated_keyspace_4.json
Browse
File format:
JSON (Ne...
Destination
Project name
test1
Dataset name
rainbow1
Table type
Native table
Table name
big_rainbow
Schema
Auto detect
Schema and input parameters
Schema will be automatically generated.
Advanced options
Create table
Cancel

Big Query

You're done!


Google Cloud Platform
test1
BigQuery
BETA
Go to Classic UI
+ COMPOSE NEW QUERY
Query history
Saved queries
Job history
Transfers
Resour...
Search for...
test1-1991...
Query editor
HIDE EDITOR
1 SELECT preimage,md5 FROM rainbow1.crackstation_human_only WHERE md5 = 'vtEoNlIWwBmYiRXtOt11+w=='
Run query
Save query
Save view
More
This query will process 4.45 GB when run.
Query history
REFRESH
Personal history
Project history
Sort by
Date
Filter queries
Today

No Specialized Software



Big Query Optimization Tips

- Pay for storage $0.02/GB
- Pay per query $5/TB

- Base64 encoding or better
- Truncate hashes at 48-bits

Big Query De-Duplication

Big Query De-Duplication

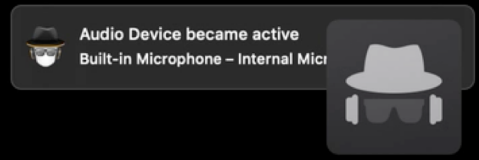
The Capitalist Algorithm

(Who cares?)

Big Rainbow

Big Rainbow

```
➜  cli git:(master) ./bigrainbow -e hex -a md5  bed128365216c019988915ed3add75fb
```



Big Rainbow

- lm
- md4
- md5
- msdcc
- msdcc2
- mssql41
- mysql323
- ntlm
- oracle10g-sys
- oracle10g-system
- whirlpool

Big Rainbow

- lm
- md4
- md5
- msdcc
- msdcc2
- mssql41
- mysql323
- ntlm
- oracle10g-sys
- oracle10g-system
- whirlpool
- ripemd160
- sha1
- sha2-224
- sha2-256
- sha2-384
- sha2-512
- sha3-224
- sha3-256
- sha3-384
- sha3-512

Available Now!

github.com/moloch--/big-rainbow

Auto-Scaling GPU Clusters

Traditional GPU Clusters

- High upfront costs ($2-3k+)
- Server maintenance
- User & resource management
- Hardware failures are expensive
- Power consumption

Let's Design a Serverless-ish Password Cracking Cluster

AWS Services

- Spot Instances
- Elastic Beanstalk
- Lambda Functions
- API Gateway
- Simple Queue Service (SQS)
- Simple Storage Service (S3)

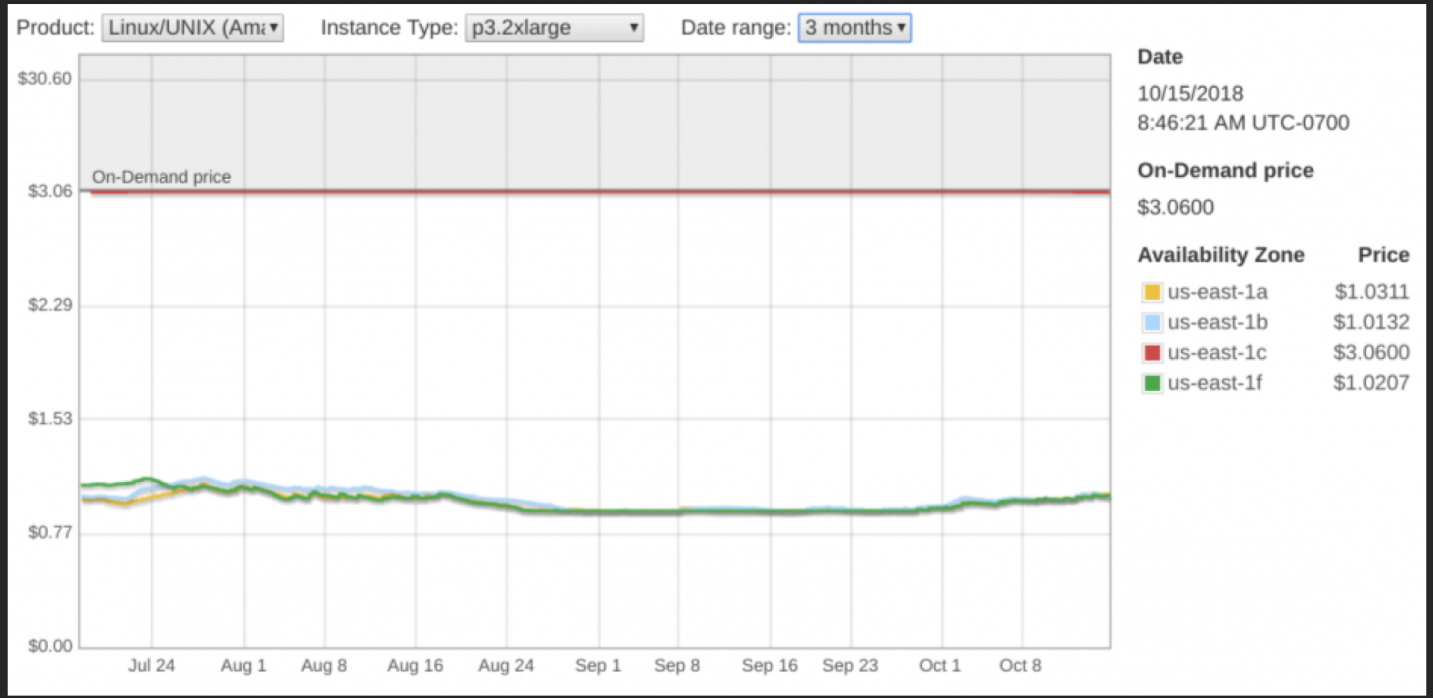
AWS Services

- Spot Instances
- Elastic Beanstalk
- Lambda Functions
- API Gateway
- Simple Queue Service (SQS)
- Simple Storage Service (S3)

AWS Spot Instances

- It’s EC2 but at up to 90% off the regular pricing
- You set a bid price, if the current price is below yours then instances are started, if they’re above then they are killed (2 minute warning)

AWS Spot Instances



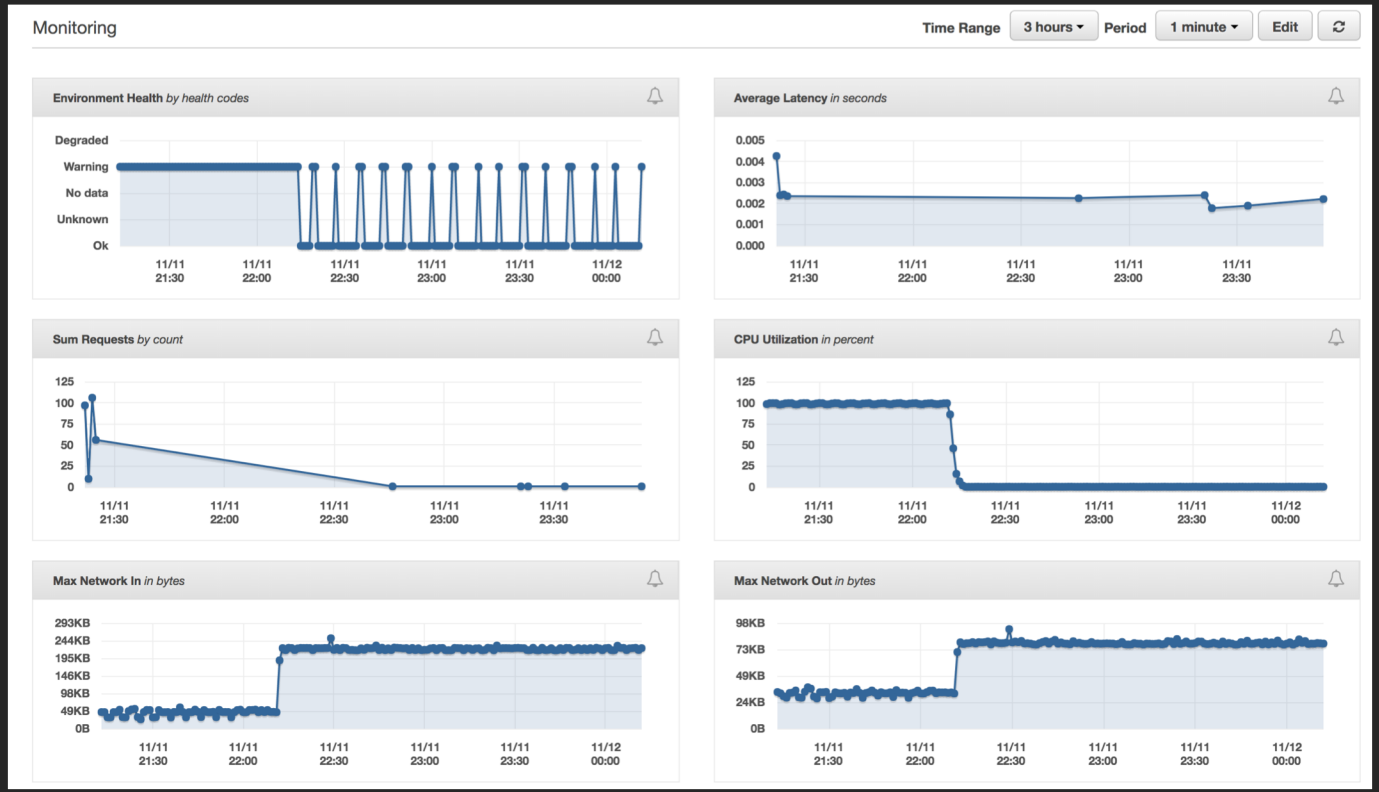
AWS Services

- Spot Instances
- Elastic Beanstalk
- Lambda Functions
- API Gateway
- Simple Queue Service (SQS)
- Simple Storage Service (S3)

Elastic Beanstalk

- Manages AWS EC2 instances
- Load balances inbound requests or SQS messages
- No additional charge
- Pretty graphs & stuffs

Elastic Beanstalk



Auto-Scale Spot

```
Resources:
  AWSEBAutoScalingLaunchConfiguration:
  Type: "AWS::AutoScaling::LaunchConfiguration"
  Properties:
   SpotPrice:
     "Fn::GetOptionSetting":
        Namespace: "aws:elasticbeanstalk:application:environment"
        OptionName: "EC2_SPOT_PRICE"
        DefaultValue: {"Ref":"AWS::NoValue"}
```

.ebextensions/01_setup.config

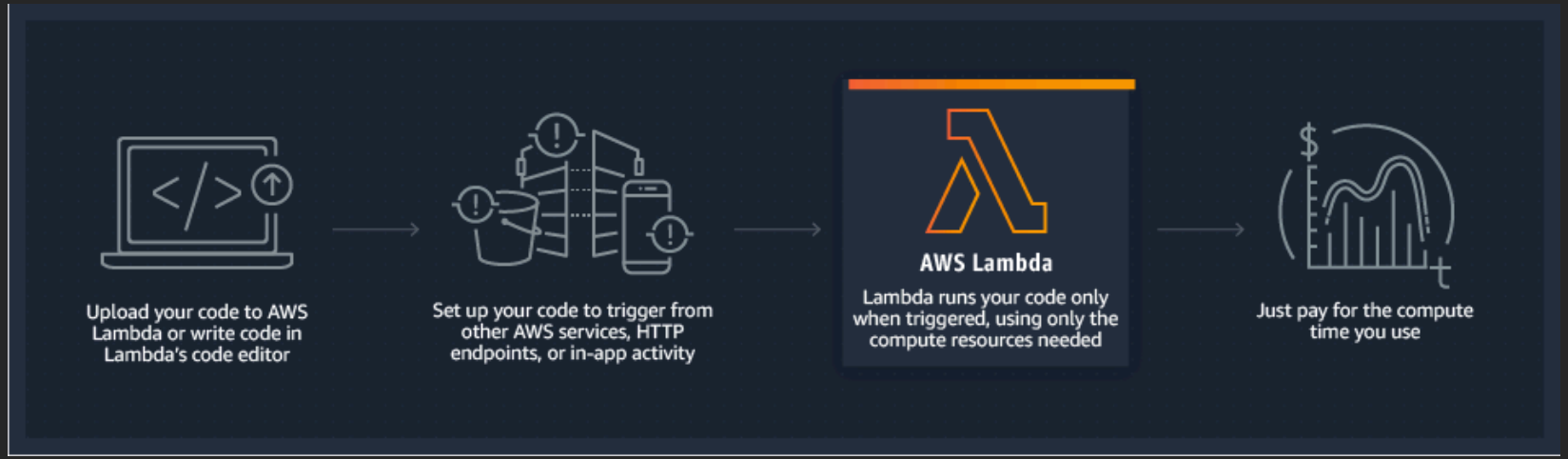
UNLIMITED POWER

AWS Services

- Spot Instances
- Elastic Beanstalk
- Lambda Functions
- API Gateway
- Simple Queue Service (SQS)
- Simple Storage Service (S3)

Lambda Functions

- Trigger-based architecture
- Required to be stateless *(web scale)*



API Gateway

- Fully managed API endpoints
- Magical load balancing, etc.
- *Timeouts after 29 seconds

AWS Services

- Spot Instances
- Elastic Beanstalk
- Lambda Functions
- API Gateway
- Simple Queue Service (SQS)
- Simple Storage Service (S3)

Simple Queue Service

- Standard Queues
- *FIFO Queues

AWS Services

- Spot Instances
- Elastic Beanstalk
- Lambda Functions
- API Gateway
- Simple Queue Service (SQS)
- Simple Storage Service (S3)

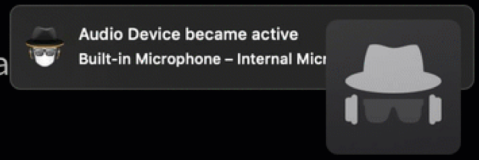
Hash Cat Pro-tips

- `--keyspace != key space`
- Values are specific to Hash Cat (`--skip` / `--limit`)

Disturbing Key Spaces

How do we jump to the n’th value?

```
➜  ~ ipython2
Python 2.7.15 (default, Jun 17 2018, 12:46:58)
Type "copyright", "credits" or "license" for more informa

IPython 5.4.1 -- An enhanced Interactive Python.
?         -> Introduction and overview of IPython's features.
%quickref -> Quick reference.
help      -> Python's own help system.
object?   -> Details about 'object', use 'object??' for extra details.

In [1]:
```

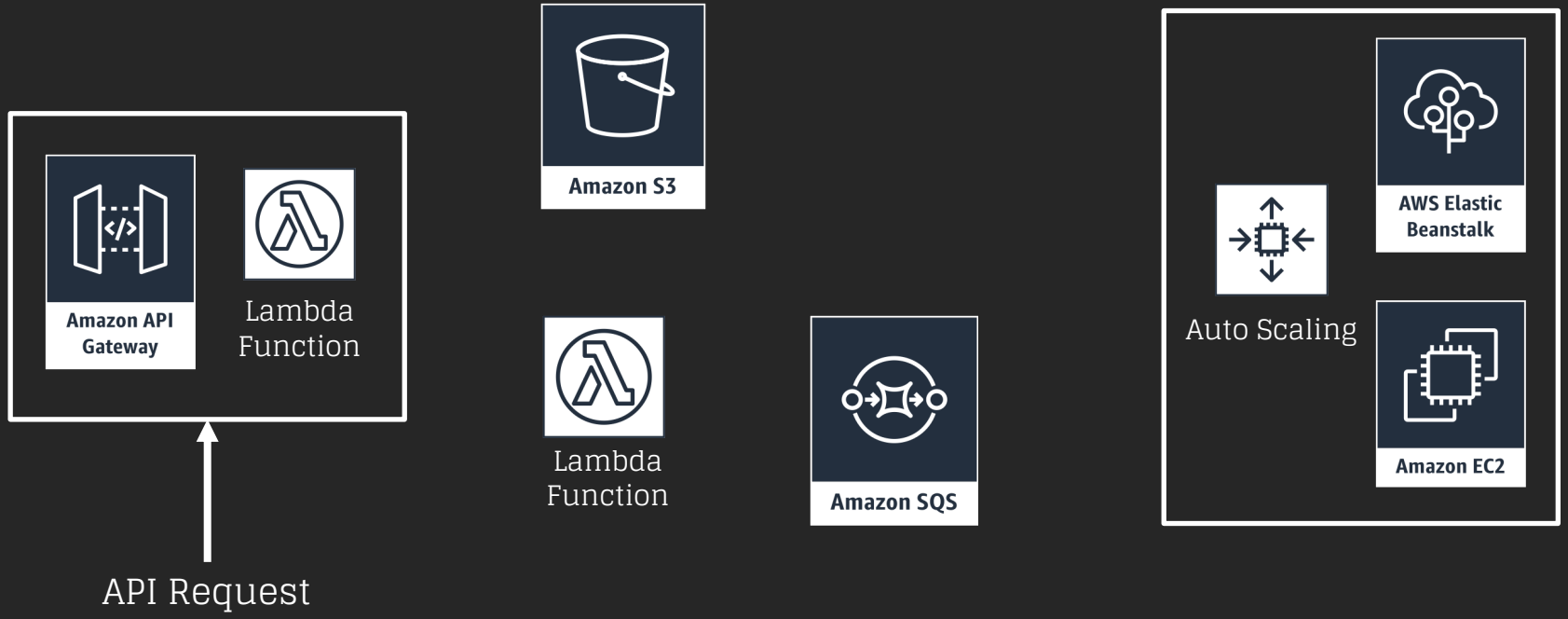


Disturbing Key Spaces

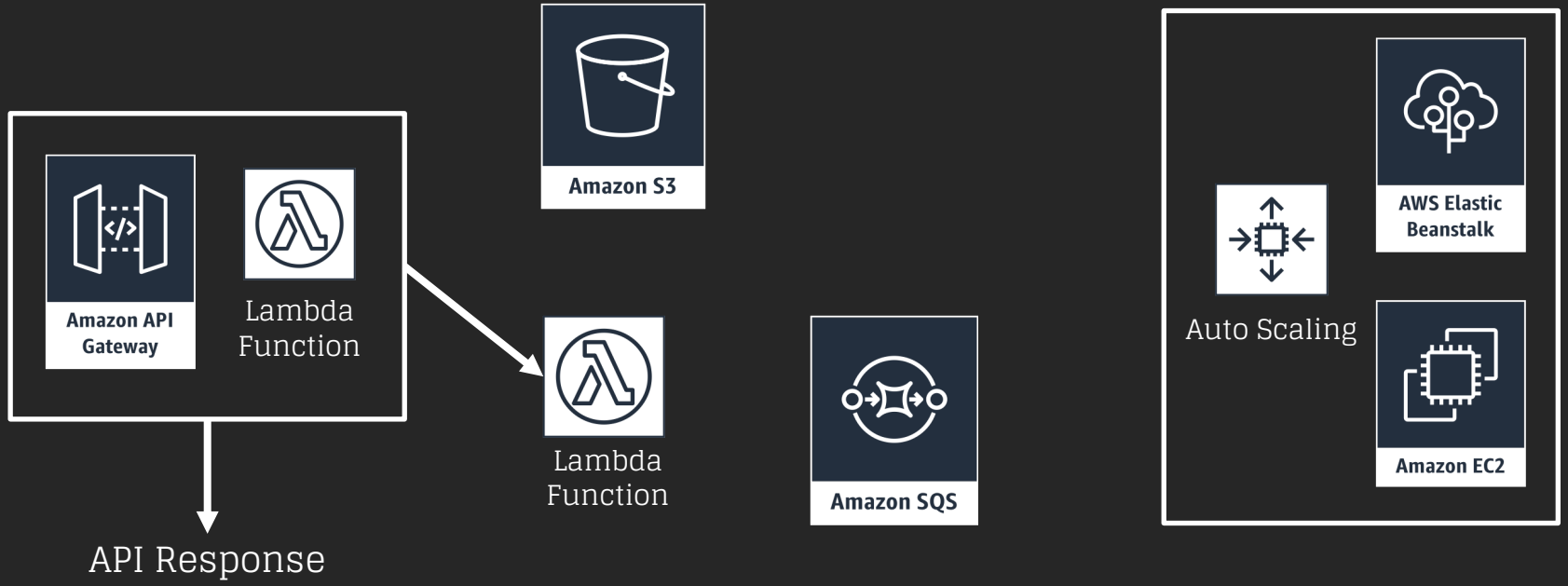
- It’s actually a counting problem
- Count in base ‘n’ *(n = length)*

Serverless-ish GPU Clusters

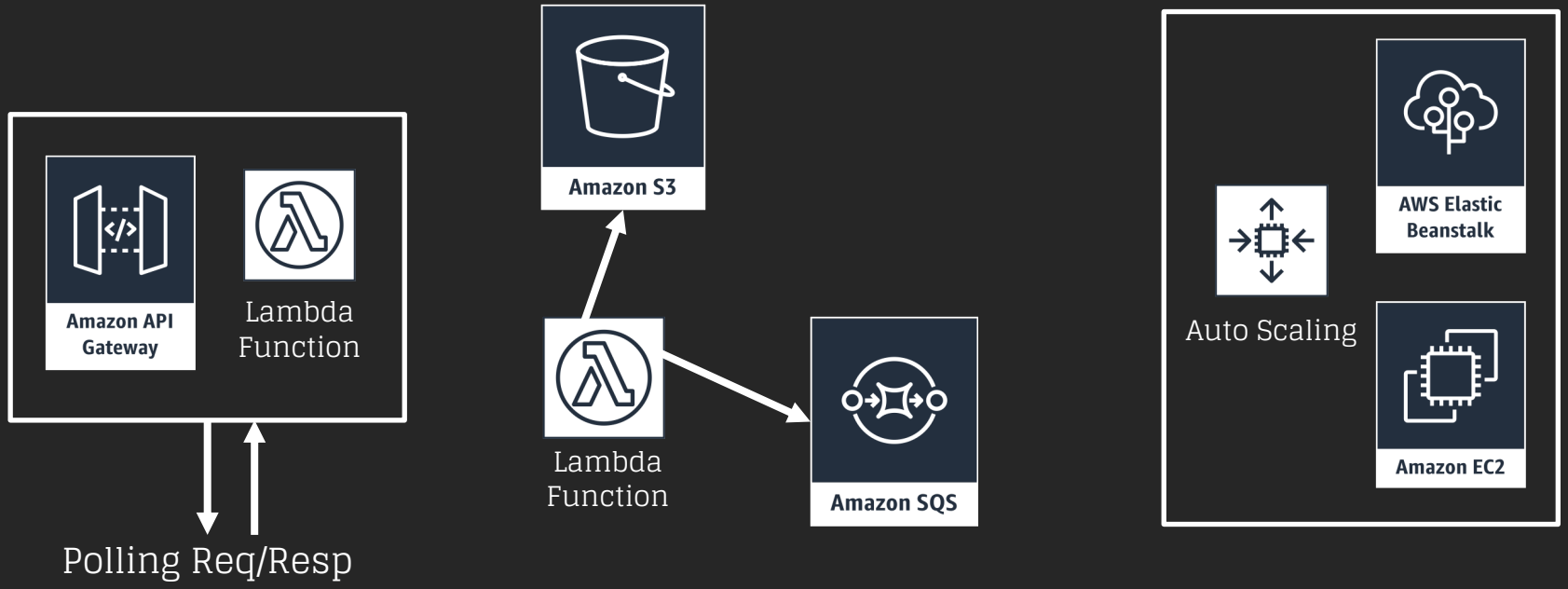
Serverless-ish GPU Clusters



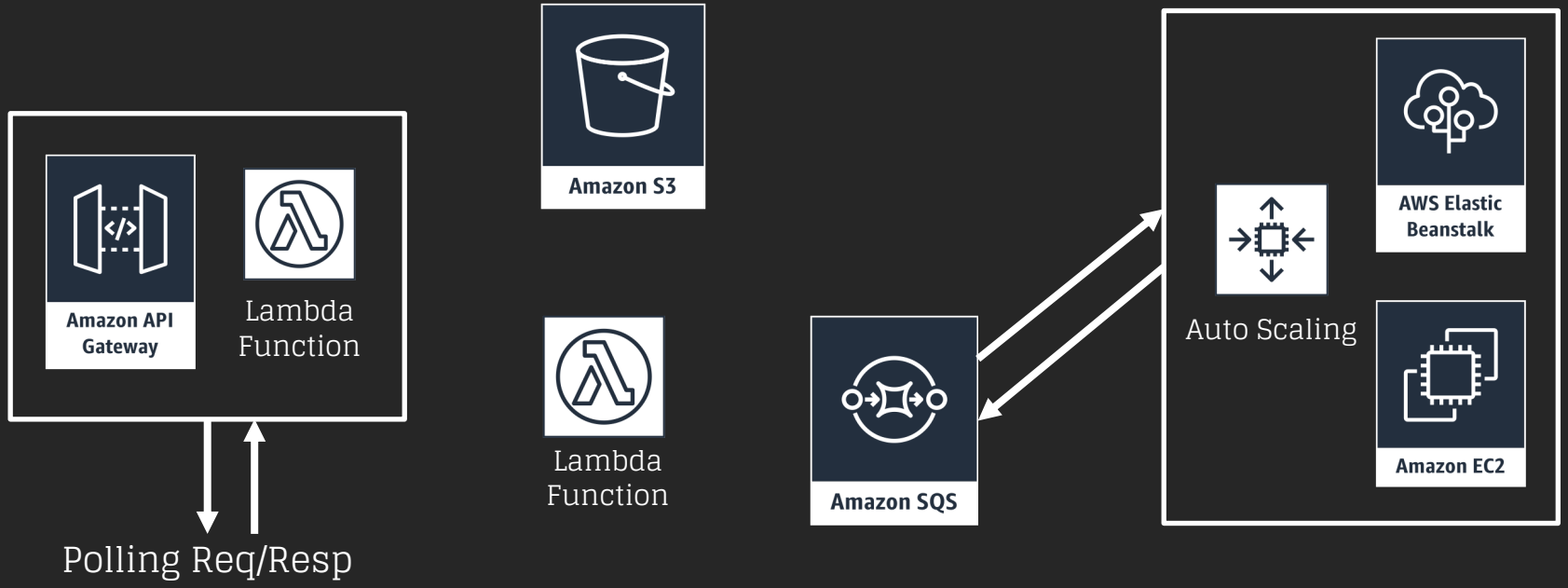
Serverless-ish GPU Clusters



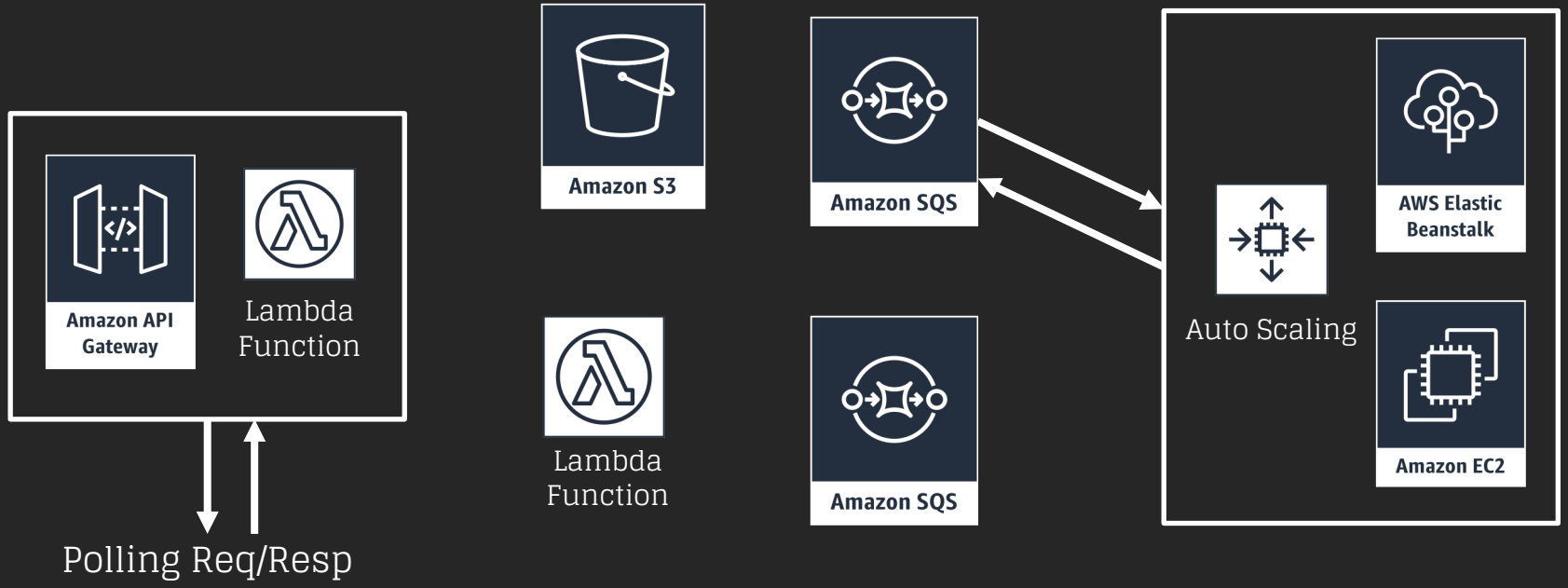
Serverless-ish GPU Clusters



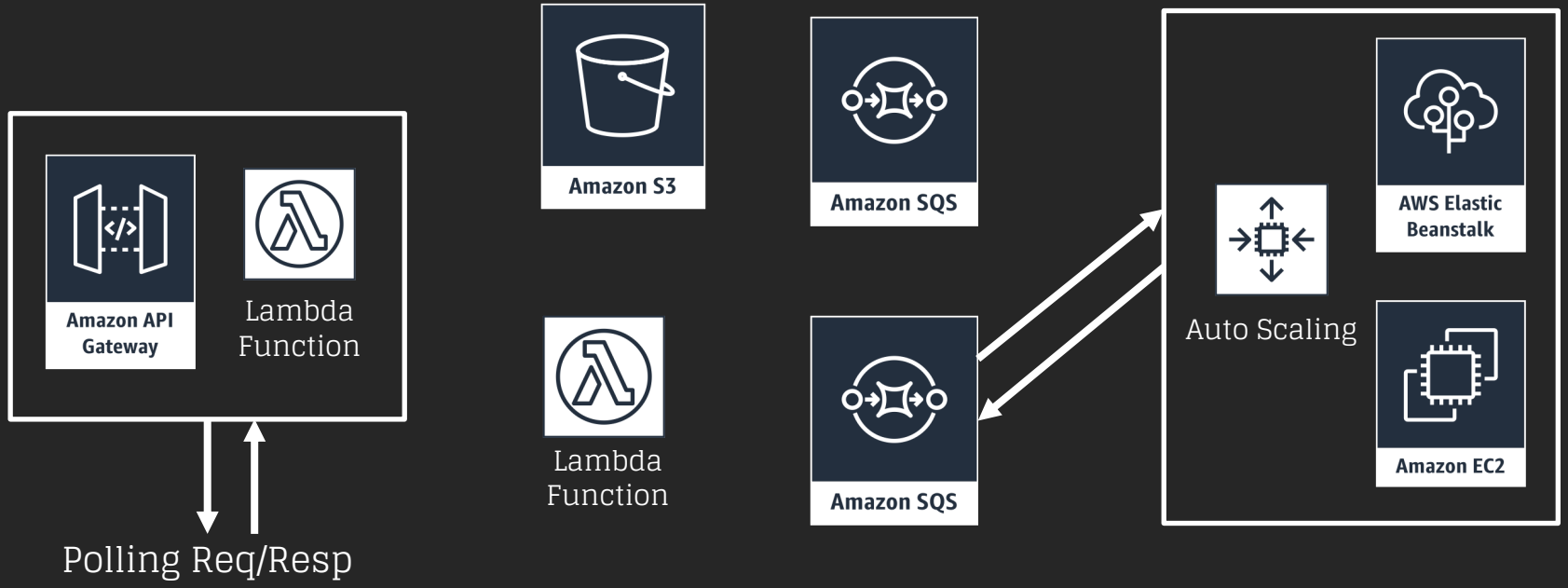
Serverless-ish GPU Clusters



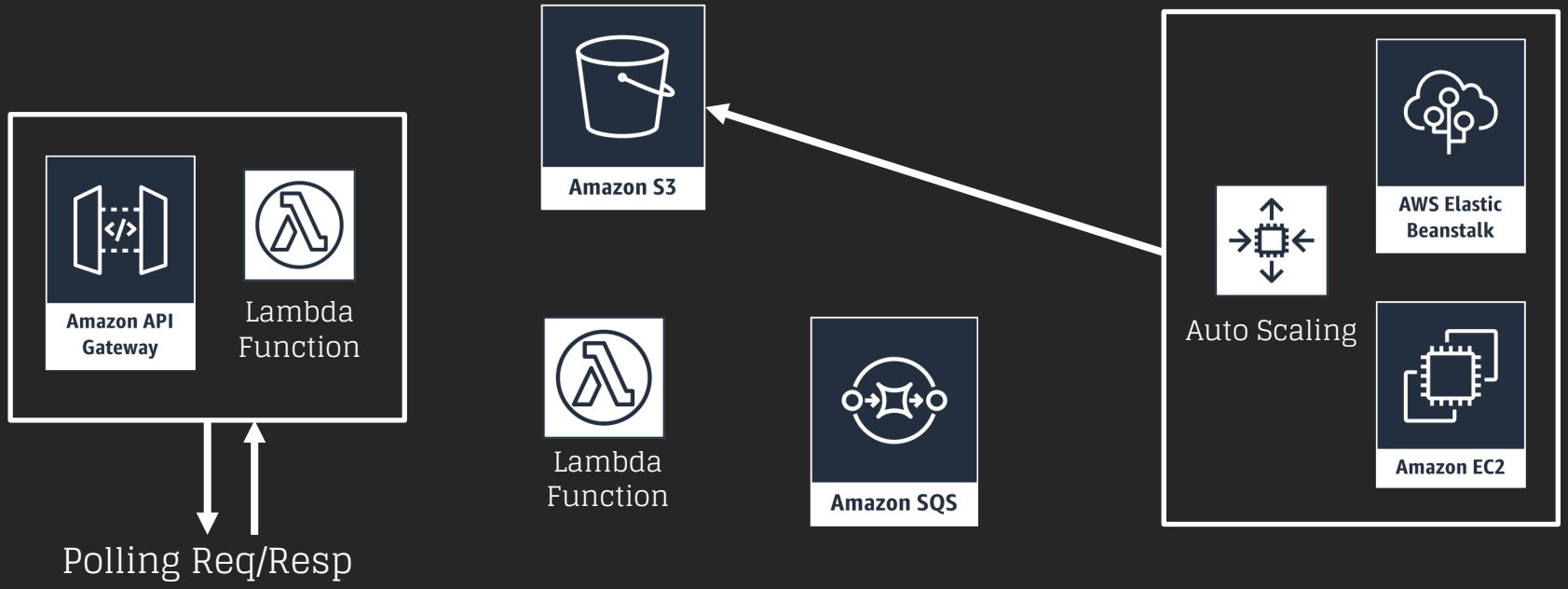
Serverless-ish GPU Clusters



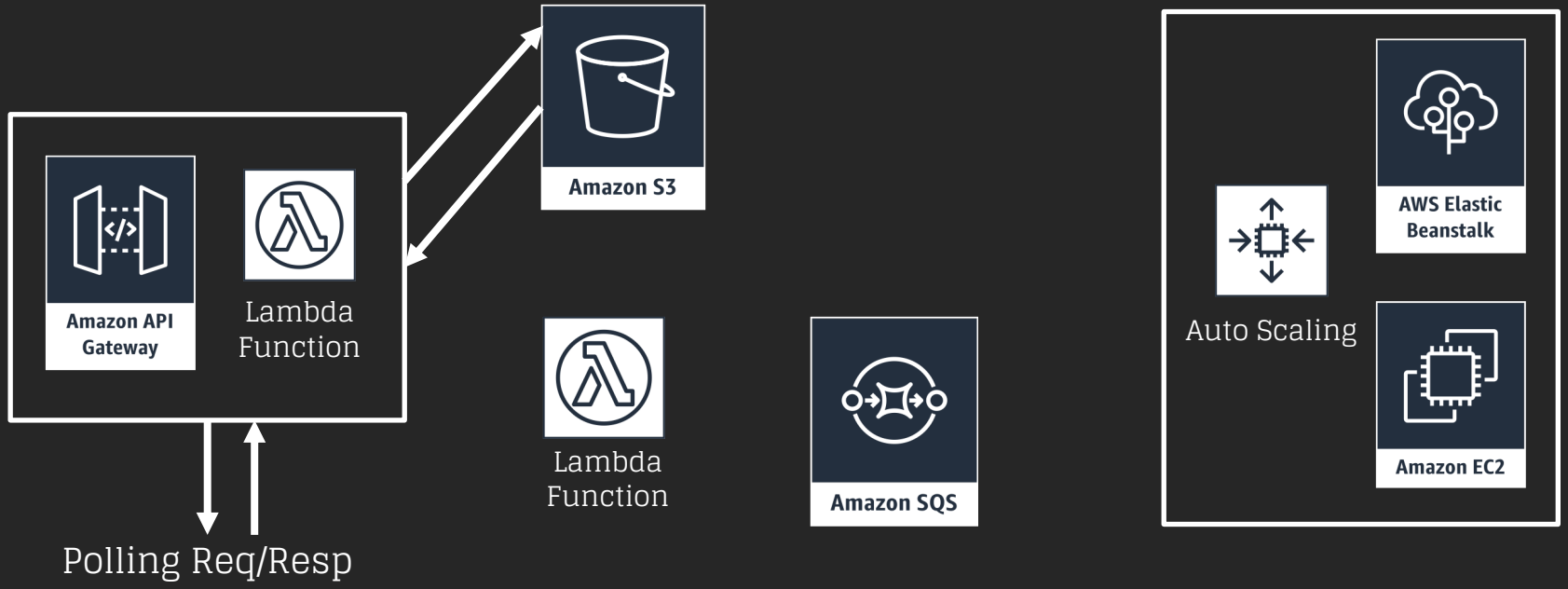
Serverless-ish GPU Clusters



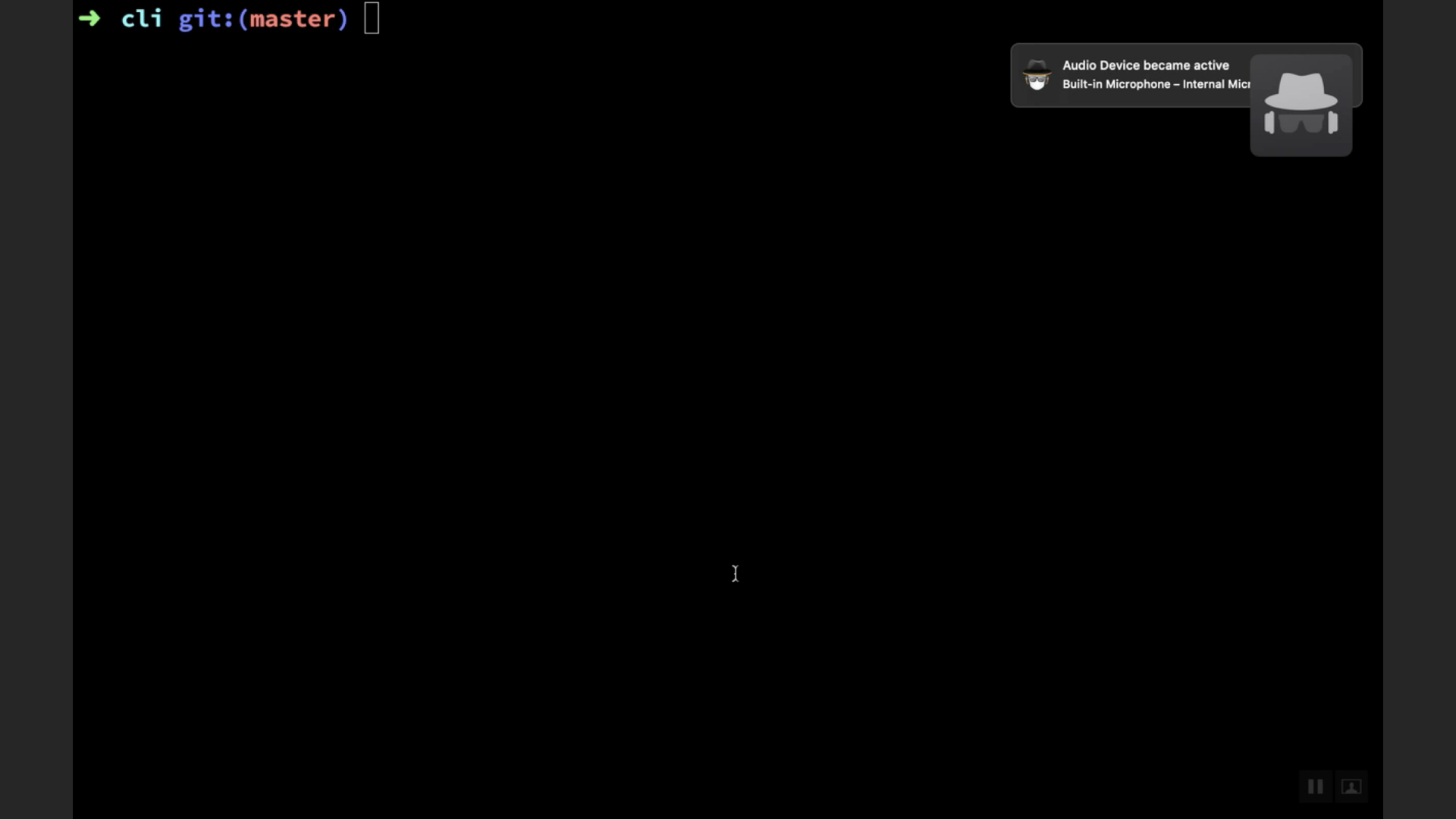
Serverless-ish GPU Clusters



Serverless-ish GPU Clusters



Serverless-ish GPU Clusters


➜ cli git:(master)
Audio Device became active
Built-in Microphone – Internal Micr

Coming Soon!

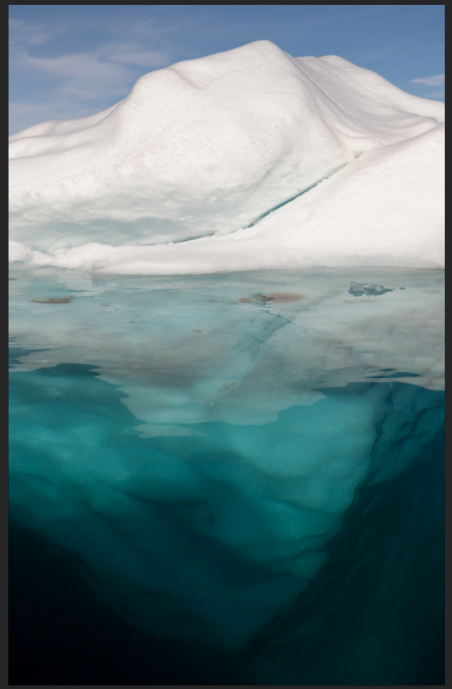
github.com/mandatoryprogrammer/masscat

Untwister
F5 Edition

Untwister

- Multi-threaded ”seed recovery” tool
- Brute-forces PRNG seeds
- Seed space varies per PRNG

The Depth Problem



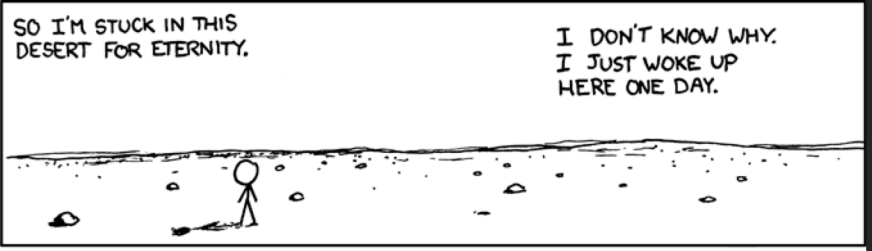
- PRNGs instantiated once
- DoS bug (XXE, etc.)
- Halting problem

Serverless-ish CPU Clusters

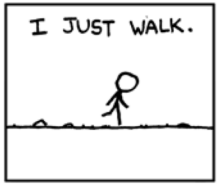
Coming Soon!

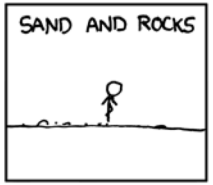
github.com/moloch--/untwister

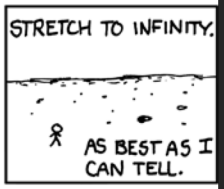
How to Actually Think About AWS

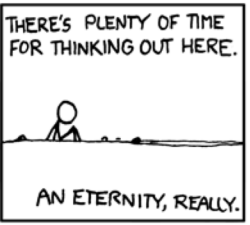

SO I'M STUCK IN THIS DESERT FOR ETERNITY.
I DON'T KNOW WHY. I JUST WOKE UP HERE ONE DAY.

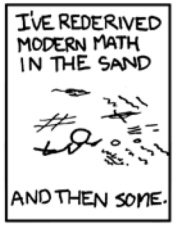

I NEVER FEEL HUNGRY OR THIRSTY.

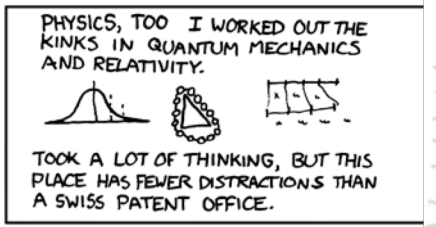

I JUST WALK.

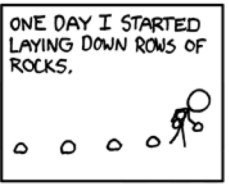

SAND AND ROCKS

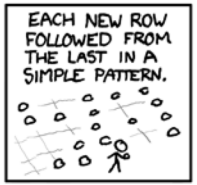

STRETCH TO INFINITY.
AS BEST AS I CAN TELL.

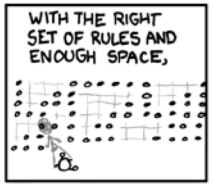

THERE'S PLENTY OF TIME FOR THINKING OUT HERE.
AN ETERNITY, REALLY.

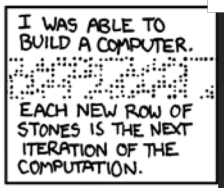

I'VE REDERIVED MODERN MATH IN THE SAND
AND THEN SOME.

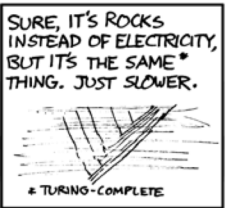

PHYSICS, TOO I WORKED OUT THE KINKS IN QUANTUM MECHANICS AND RELATIVITY.
TOOK A LOT OF THINKING, BUT THIS PLACE HAS FEWER DISTRACTIONS THAN A SWISS PATENT OFFICE.

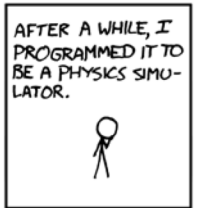

ONE DAY I STARTED LAYING DOWN ROWS OF ROCKS.

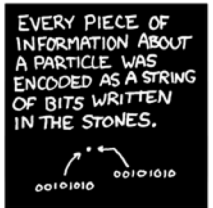

EACH NEW ROW FOLLOWED FROM THE LAST IN A SIMPLE PATTERN.

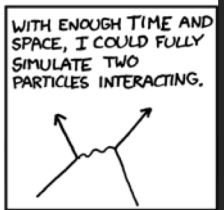

WITH THE RIGHT SET OF RULES AND ENOUGH SPACE,

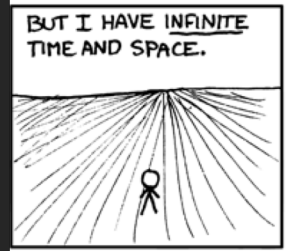

I WAS ABLE TO BUILD A COMPUTER.
EACH NEW ROW OF STONES IS THE NEXT ITERATION OF THE COMPUTATION.

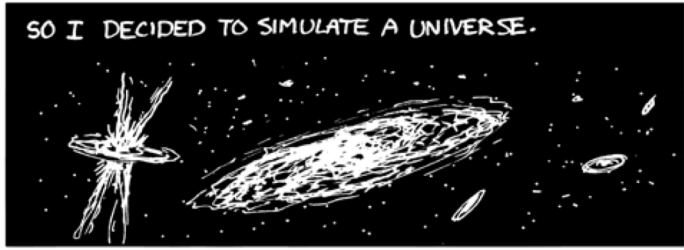

SURE, IT'S ROCKS INSTEAD OF ELECTRICITY, BUT IT'S THE SAME* THING. JUST SLOWER.
* TURING-COMPLETE

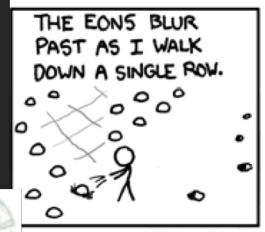

AFTER A WHILE, I PROGRAMMED IT TO BE A PHYSICS SIMULATOR.

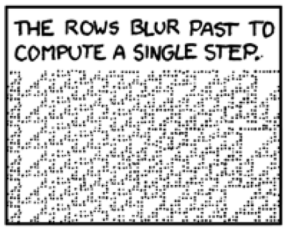

EVERY PIECE OF INFORMATION ABOUT A PARTICLE WAS ENCODED AS A STRING OF BITS WRITTEN IN THE STONES.
00101010
00101010


WITH ENOUGH TIME AND SPACE, I COULD FULLY SIMULATE TWO PARTICLES INTERACTING.


BUT I HAVE INFINITE TIME AND SPACE.

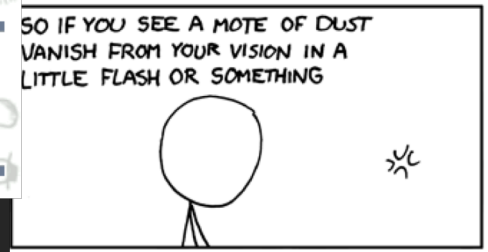

SO I DECIDED TO SIMULATE A UNIVERSE.

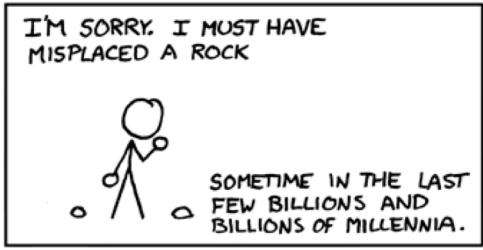

THE EONS BLUR PAST AS I WALK DOWN A SINGLE ROW.

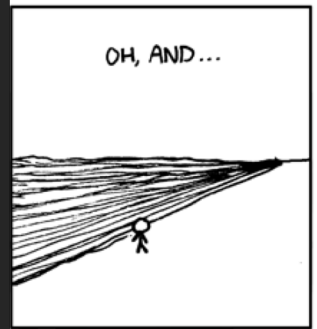

THE ROWS BLUR PAST TO COMPUTE A SINGLE STEP.

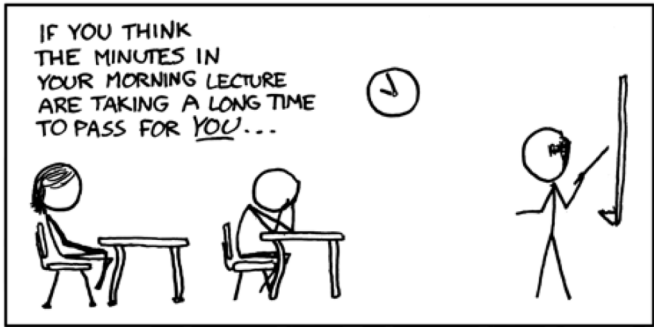

AND IN THE SIMULATION


ANOTHER INSTANT TICKS BY.


SO IF YOU SEE A MOTE OF DUST VANISH FROM YOUR VISION IN A LITTLE FLASH OR SOMETHING


I'M SORRY. I MUST HAVE MISPLACED A ROCK
SOMETIME IN THE LAST FEW BILLIONS AND BILLIONS OF MILLENNIA.


OH, AND...


IF YOU THINK THE MINUTES IN YOUR MORNING LECTURE ARE TAKING A LONG TIME TO PASS FOR YOU...

Thanks!

*Any **questions** ?*

Thanks to `@0xkitty` for the slide design!