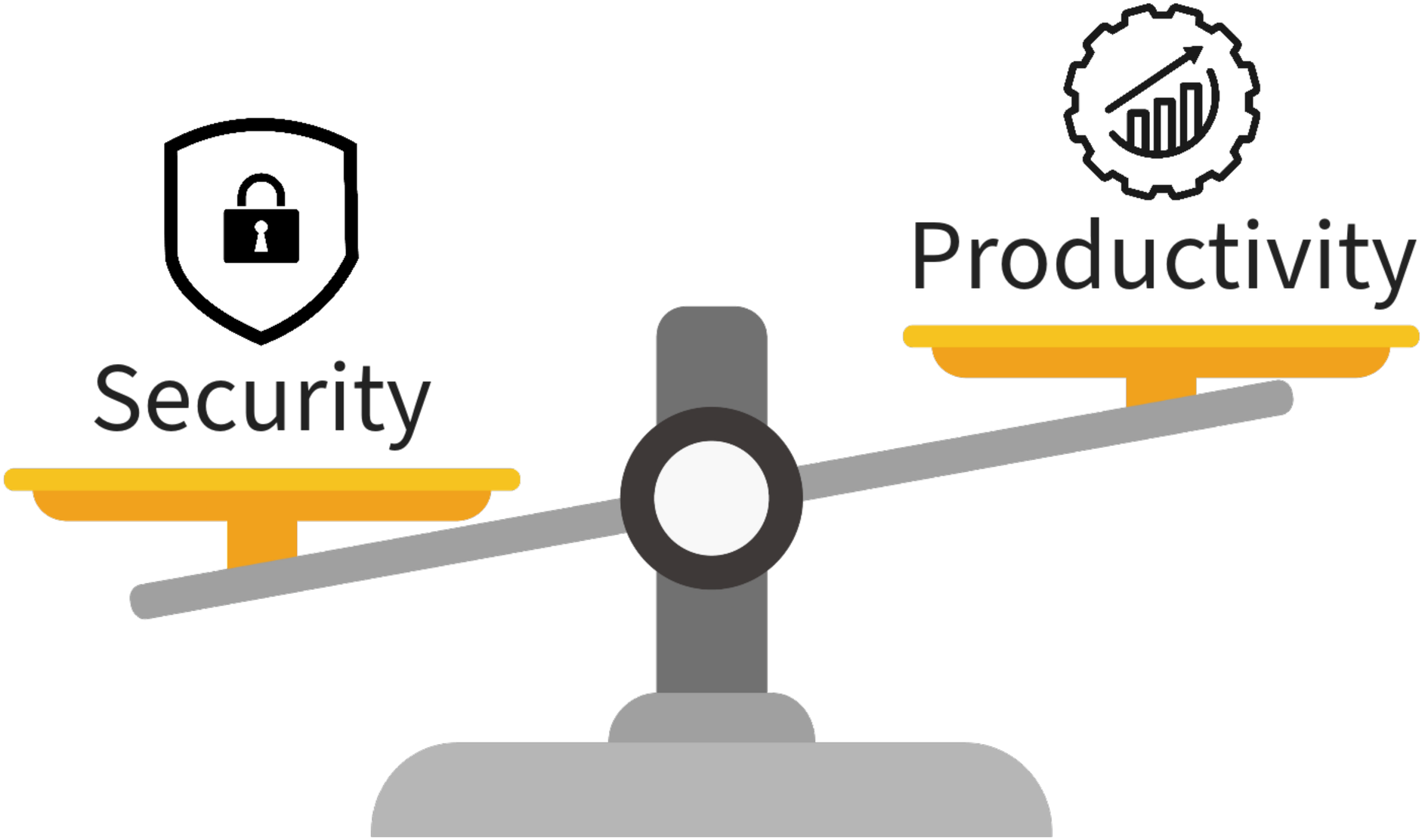
Security and Productivity

Pick Two with Reproducible Builds

Brian Demers
Open Source Developer

BrianDemers bdemers

Gradle


Security
Productivity

Who is this guy?

source: Silicon Valley

VS

Gradle Build Tool

VS

Maven™

Gradle

Gradle Build Tool

Gradle Enterprise

Developer
Productivity
Engineering

Gradle Build Tool

Maven™

Bazel

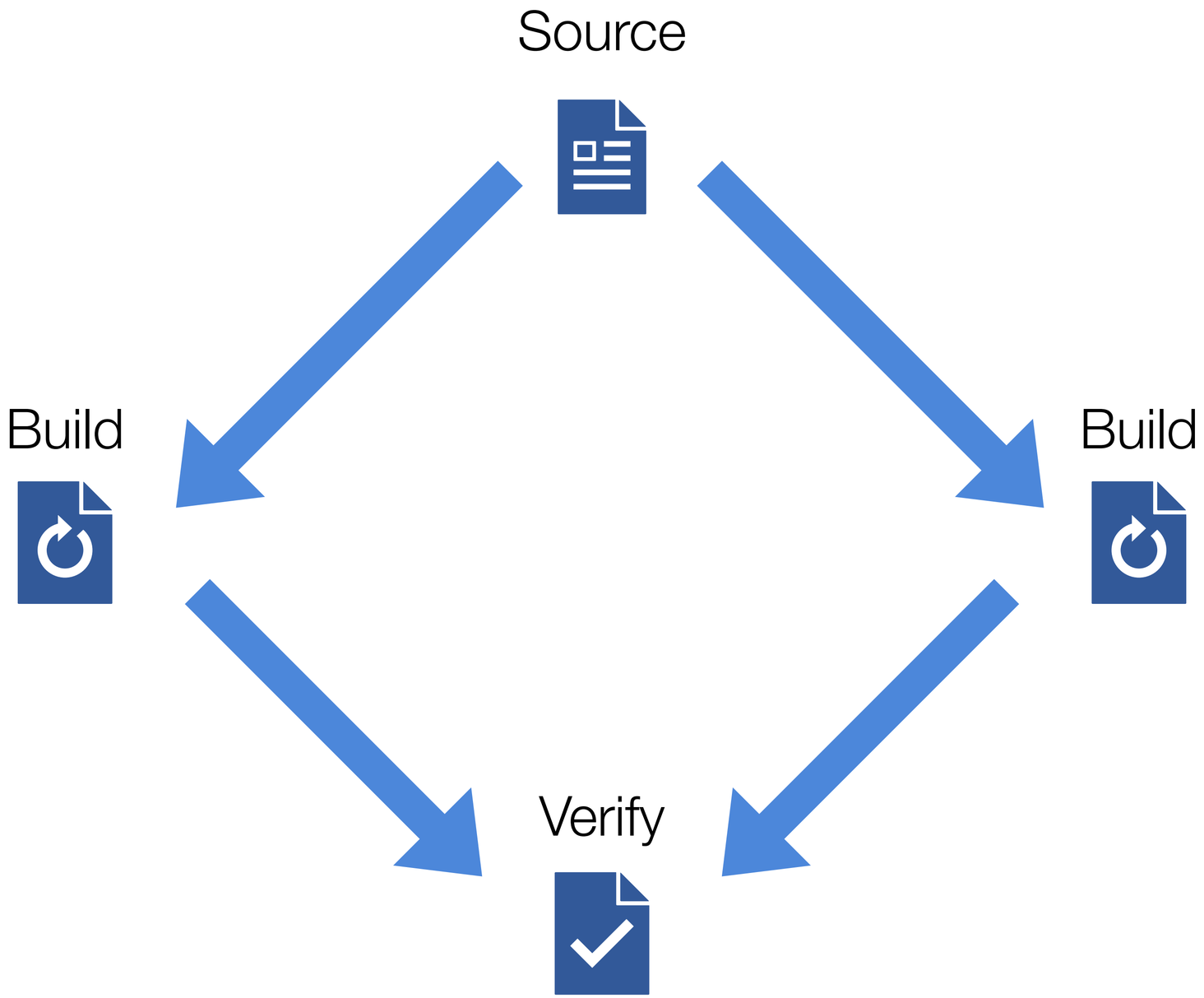
sbt

Topics

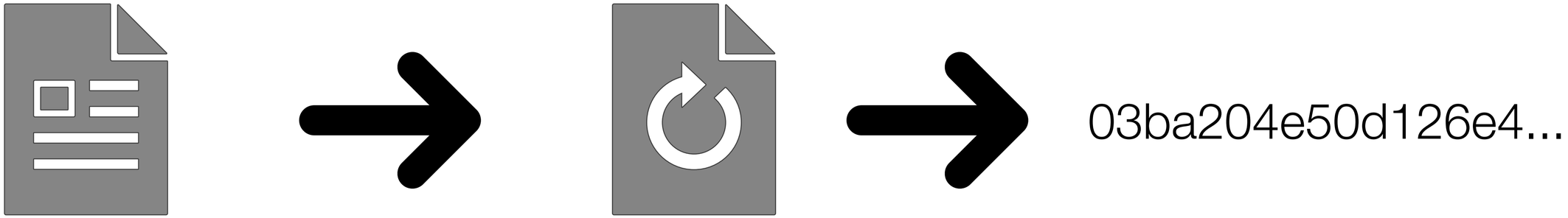
- Reproducible Builds
  - What is it?
  - Why should you care?
- Developer productivity
  - How are these related?
  - Build Cache
- Tips & Tricks

Reproducible Builds

reproducible-builds.org


Source
Build
Build
Verify

CHECKSUM



data

hash function

03ba204e50d126e4...


HOW DID WE
GET HERE?
HISTORY

Old way (META-INF/MANIFEST.MF)

```
Manifest-Version: 1.0
Archiver-Version: Plexus Archiver
Created-By: Apache Maven
Built-By: jdcasey
Build-Jdk: 1.4.2_09
Extension-Name: maven-core
Specification-Title: Maven is a project development management and com
 prehension tool. Based on the concept of a project object model: buil
 ds, dependency management, documentation creation, site publication,
 and distribution publication are all controlled from the declarative
 file. Maven can be extended by plugins to utilise a number of other d
 evelopment tools for reporting or the build process.
Specification-Vendor: Apache Software Foundation
Implementation-Vendor: Apache Software Foundation
Implementation-Title: maven-core
Implementation-Version: 2.0.1
```

New Way (META-INF/MANIFEST.MF)

```
Manifest-Version: 1.0
Created-By: Maven JAR Plugin 3.3.0
Build-Jdk-Spec: 17
Specification-Title: Maven Core
Specification-Version: 3.9
Specification-Vendor: The Apache Software Foundation
Implementation-Title: Maven Core
Implementation-Version: 3.9.4
Implementation-Vendor: The Apache Software Foundation
```


WHY
SHOULD I CARE?
imgflip.com


© DESPAIR.COM
INTEGRITY
Play By The Rules,
Get Beat By Those Who Don't.

Reproducible builds for security

- Binaries are not tampered with
- Build system not comprimised
- Prevent backdoors
- Supply Chain attacks

Compromised Toolchain

```
$ cp evil-compiler /usr/bin/compiler
```

```
$ unzip evil.zip -d /src/project
  extracting   ../../etc/passwd
```

Who should care?

- Open Source Projects
- Distributions
- Companies
- Users

Shouldn't All Builds be Reproducible?

Dates

- Current date/time
- Time Zone
- Locale/Format
- Dates in versions

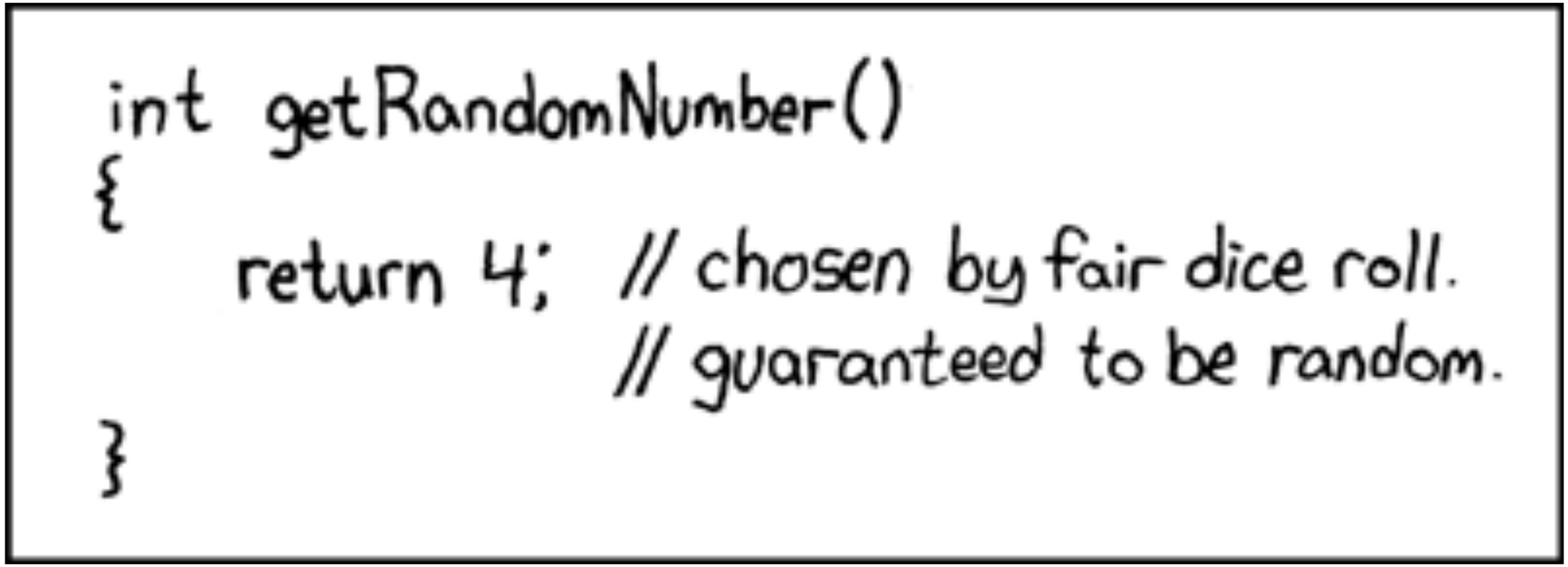
File Dates

```
$ ls -alh target/scim-core-1.0.0-SNAPSHOT.jar

-rw-r--r-- bdemers staff 56K Jul 27 12:32:43 2023
```

Dates in Archives (zip, tar, jar, etc)

```
Archive:  target/scim-core-1.0.0-SNAPSHOT.jar
   Date      Time    Name
---------- -----    ----
04-05-2023 08:23   META-INF/MANIFEST.MF
04-05-2023 08:23   META-INF/DEPENDENCIES
04-05-2023 08:23   META-INF/LICENSE
04-05-2023 08:23   META-INF/NOTICE
04-05-2023 08:23   META-INF/beans.xml
04-05-2023 08:23   META-INF/maven/org.apache.directory.scim/scim-core/pom.xml
04-05-2023 08:23   META-INF/maven/org.apache.directory.scim/scim-core/pom.properties
04-05-2023 08:23   org/apache/directory/scim/core/repository/PatchHandler.class
04-05-2023 08:23   org/apache/directory/scim/core/repository/Repository.class
04-05-2023 08:23   org/apache/directory/scim/core/repository/UpdateRequest.class
...
```

Random bits



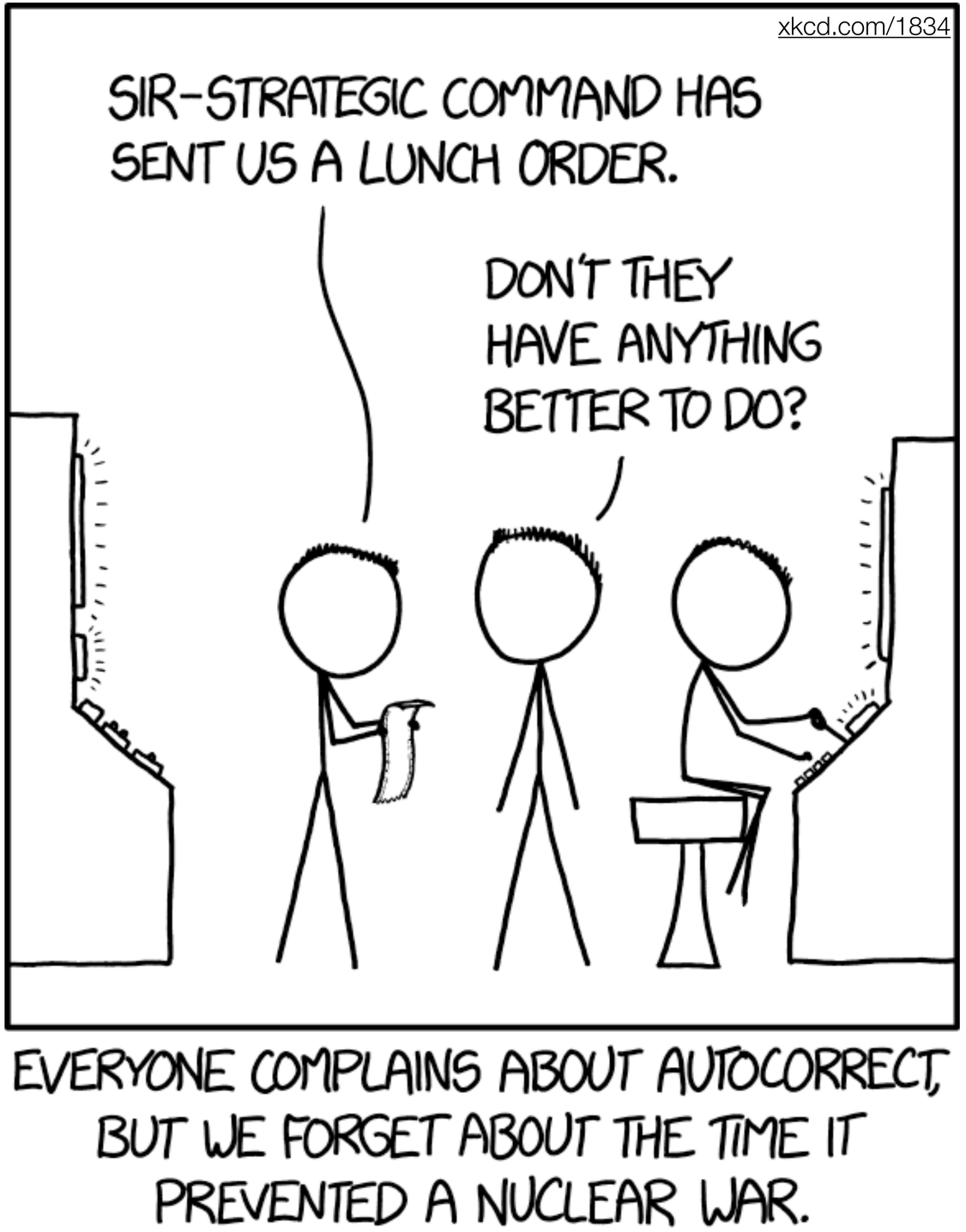
xkcd.com/221

OS & Environment

- File Encoding
- OS
- Tool Versions
- File Paths
- Locales
- .DS_Store

File Input / Output Order

- Hash Maps / Dictionaries
  - Serialized data
- File order in archives

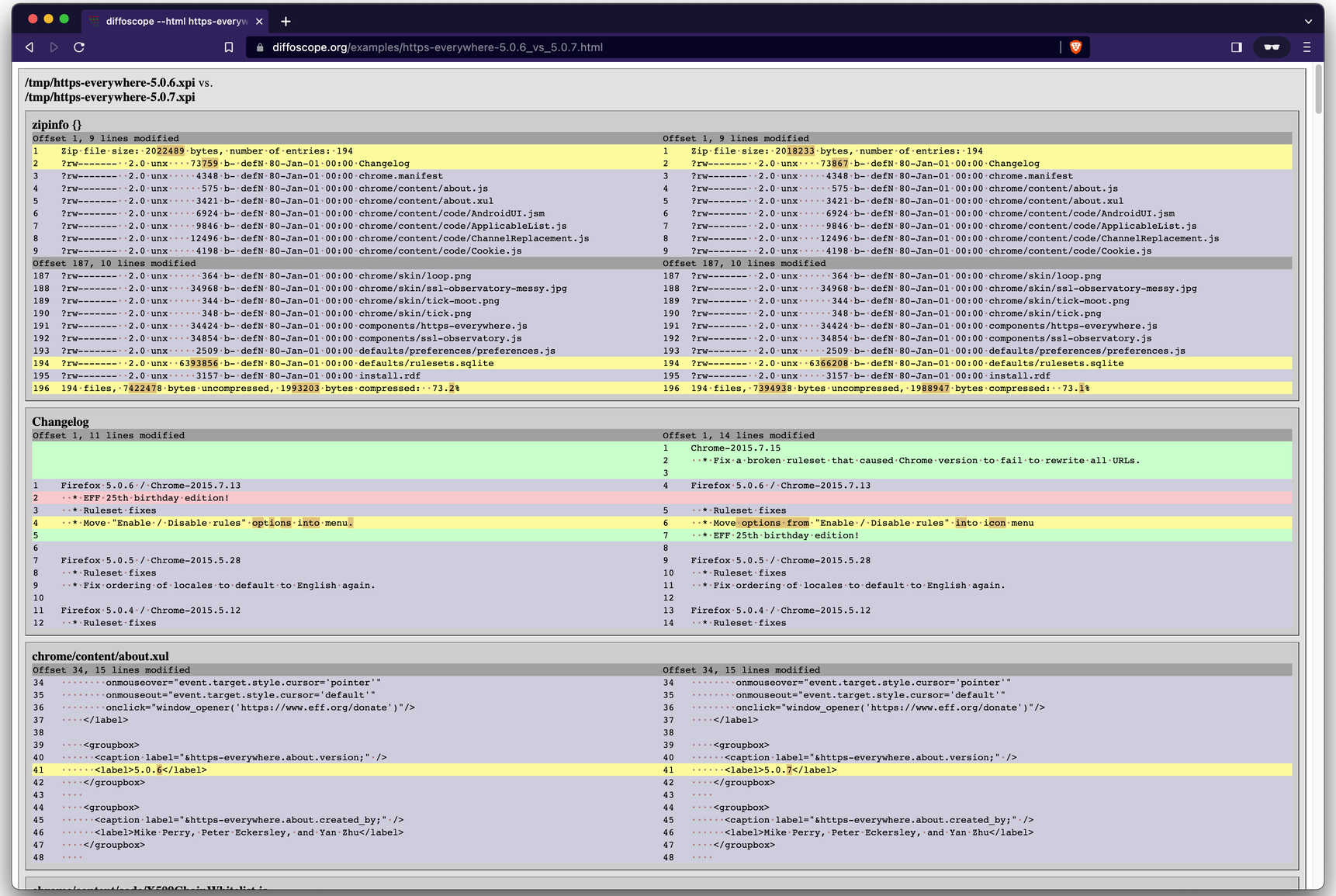



WORRY NOT
IT IS DETERMINISTIC
imgflip.com

How to Verify?

```
$ shasum -a 256 AAA-file.zip
80da7adf80a819db609ac6862931dc6c1cc04bf4c8ba292446021aa805aa3bfa

$ shasum -a 256 BBB-file.zip
80da7adf80a819db609ac6862931dc6c1cc04bf4c8ba292446021aa805aa3bfa
```

Diffoscope



/tmp/https-everywhere-5.0.6.xpi vs.
/tmp/https-everywhere-5.0.7.xpi

zipinfo {}

Offset 1, 9 lines modified	Offset 1, 9 lines modified
1 Zip file size: 2022489 bytes, number of entries: 194	1 Zip file size: 2018233 bytes, number of entries: 194
2 ?rw------- 2.0 unx 73759 b- defN 80-Jan-01 00:00 Changelog	2 ?rw------- 2.0 unx 73867 b- defN 80-Jan-01 00:00 Changelog
3 ?rw------- 2.0 unx 4348 b- defN 80-Jan-01 00:00 chrome.manifest	3 ?rw------- 2.0 unx 4348 b- defN 80-Jan-01 00:00 chrome.manifest
4 ?rw------- 2.0 unx 575 b- defN 80-Jan-01 00:00 chrome/content/about.js	4 ?rw------- 2.0 unx 575 b- defN 80-Jan-01 00:00 chrome/content/about.js
5 ?rw------- 2.0 unx 3421 b- defN 80-Jan-01 00:00 chrome/content/about.xul	5 ?rw------- 2.0 unx 3421 b- defN 80-Jan-01 00:00 chrome/content/about.xul
6 ?rw------- 2.0 unx 6924 b- defN 80-Jan-01 00:00 chrome/content/code/AndroidUI.jsm	6 ?rw------- 2.0 unx 6924 b- defN 80-Jan-01 00:00 chrome/content/code/AndroidUI.jsm
7 ?rw------- 2.0 unx 9846 b- defN 80-Jan-01 00:00 chrome/content/code/ApplicableList.js	7 ?rw------- 2.0 unx 9846 b- defN 80-Jan-01 00:00 chrome/content/code/ApplicableList.js
8 ?rw------- 2.0 unx 12496 b- defN 80-Jan-01 00:00 chrome/content/code/ChannelReplacement.js	8 ?rw------- 2.0 unx 12496 b- defN 80-Jan-01 00:00 chrome/content/code/ChannelReplacement.js
9 ?rw------- 2.0 unx 4198 b- defN 80-Jan-01 00:00 chrome/content/code/Cookie.js	9 ?rw------- 2.0 unx 4198 b- defN 80-Jan-01 00:00 chrome/content/code/Cookie.js
Offset 187, 10 lines modified	Offset 187, 10 lines modified
187 ?rw------- 2.0 unx 364 b- defN 80-Jan-01 00:00 chrome/skin/loop.png	187 ?rw------- 2.0 unx 364 b- defN 80-Jan-01 00:00 chrome/skin/loop.png
188 ?rw------- 2.0 unx 34968 b- defN 80-Jan-01 00:00 chrome/skin/ssl-observatory-messy.jpg	188 ?rw------- 2.0 unx 34968 b- defN 80-Jan-01 00:00 chrome/skin/ssl-observatory-messy.jpg
189 ?rw------- 2.0 unx 344 b- defN 80-Jan-01 00:00 chrome/skin/tick-moot.png	189 ?rw------- 2.0 unx 344 b- defN 80-Jan-01 00:00 chrome/skin/tick-moot.png
190 ?rw------- 2.0 unx 348 b- defN 80-Jan-01 00:00 chrome/skin/tick.png	190 ?rw------- 2.0 unx 348 b- defN 80-Jan-01 00:00 chrome/skin/tick.png
191 ?rw------- 2.0 unx 34424 b- defN 80-Jan-01 00:00 components/https-everywhere.js	191 ?rw------- 2.0 unx 34424 b- defN 80-Jan-01 00:00 components/https-everywhere.js
192 ?rw------- 2.0 unx 34854 b- defN 80-Jan-01 00:00 components/ssl-observatory.js	192 ?rw------- 2.0 unx 34854 b- defN 80-Jan-01 00:00 components/ssl-observatory.js
193 ?rw------- 2.0 unx 2509 b- defN 80-Jan-01 00:00 defaults/preferences/preferences.js	193 ?rw------- 2.0 unx 2509 b- defN 80-Jan-01 00:00 defaults/preferences/preferences.js
194 ?rw------- 2.0 unx 6393856 b- defN 80-Jan-01 00:00 defaults/rulesets.sqlite	194 ?rw------- 2.0 unx 6366208 b- defN 80-Jan-01 00:00 defaults/rulesets.sqlite
195 ?rw------- 2.0 unx 3157 b- defN 80-Jan-01 00:00 install.rdf	195 ?rw------- 2.0 unx 3157 b- defN 80-Jan-01 00:00 install.rdf
196 194 files, 7422478 bytes uncompressed, 1993203 bytes compressed: 73.2%	196 194 files, 7394938 bytes uncompressed, 1988947 bytes compressed: 73.1%

Changelog

Offset 1, 11 lines modified	Offset 1, 14 lines modified
	1 Chrome-2015.7.15
	2 * Fix a broken ruleset that caused Chrome version to fail to rewrite all URLs.
	3
1 Firefox 5.0.6 / Chrome-2015.7.13	4 Firefox 5.0.6 / Chrome-2015.7.13
2 * EFF 25th birthday edition!	
3 * Ruleset fixes	5 * Ruleset fixes
4 * Move "Enable / Disable rules" options into menu.	6 * Move options from "Enable / Disable rules" into icon menu
5	7 * EFF 25th birthday edition!
6	8
7 Firefox 5.0.5 / Chrome-2015.5.28	9 Firefox 5.0.5 / Chrome-2015.5.28
8 * Ruleset fixes	10 * Ruleset fixes
9 * Fix ordering of locales to default to English again.	11 * Fix ordering of locales to default to English again.
10	12
11 Firefox 5.0.4 / Chrome-2015.5.12	13 Firefox 5.0.4 / Chrome-2015.5.12
12 * Ruleset fixes	14 * Ruleset fixes

chrome/content/about.xul

Offset 34, 15 lines modified	Offset 34, 15 lines modified
34 onmouseover="event.target.style.cursor='pointer'"	34 onmouseover="event.target.style.cursor='pointer'"
35 onmouseout="event.target.style.cursor='default'"	35 onmouseout="event.target.style.cursor='default'"
36 onclick="window_opener('https://www.eff.org/donate')"/>	36 onclick="window_opener('https://www.eff.org/donate')"/>
37 </label>	37 </label>
38	38
39 <groupbox>	39 <groupbox>
40 <caption label="&https-everywhere.about.version;" />	40 <caption label="&https-everywhere.about.version;" />
41 <label>5.0.6</label>	41 <label>5.0.7</label>
42 </groupbox>	42 </groupbox>
43	43
44 <groupbox>	44 <groupbox>
45 <caption label="&https-everywhere.about.created_by;" />	45 <caption label="&https-everywhere.about.created_by;" />
46 <label>Mike Perry, Peter Eckersley, and Yan Zhu</label>	46 <label>Mike Perry, Peter Eckersley, and Yan Zhu</label>
47 </groupbox>	47 </groupbox>
48	48


LET'S GET STARTED!
makeameme.org

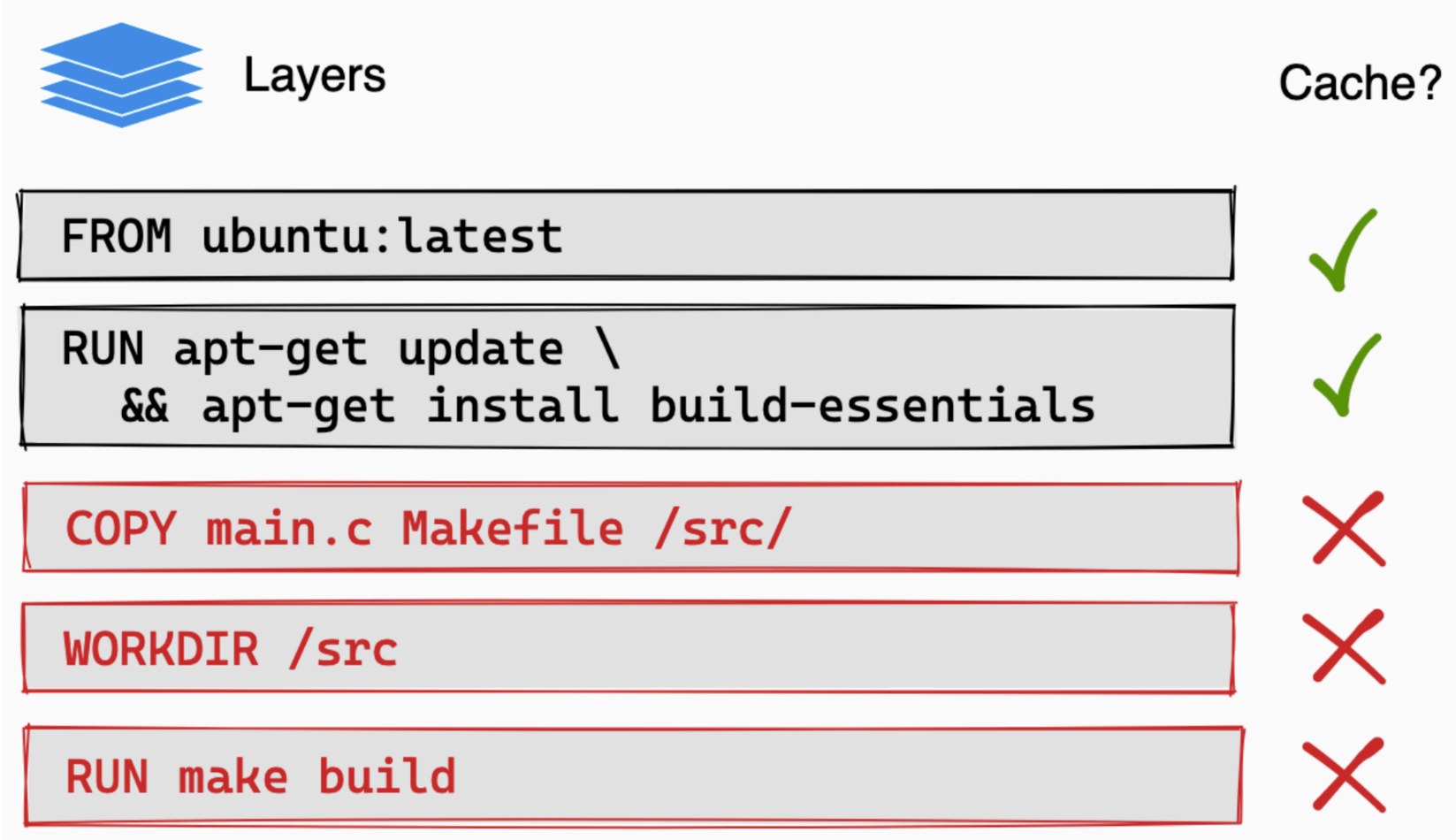
Record how to rebuild

```
groupId=org.apache.commo
artifactId=commons-numbe
display=${groupId}:${art
version=1.1

gitRepo=https://github.c
gitTag=rel/commons-numbe

tool=mvn
jdk=8
newline=lf

command="mvn -Prelease c                                    doc.skip \
             -Dgpg.skip                                     elease.isDistModule=false"
buildinfo=target/${artif
```

Other Benifits

- Quality
- Debugging
- Smaller deltas in releases
- Cacheable

Think about a Docker builds

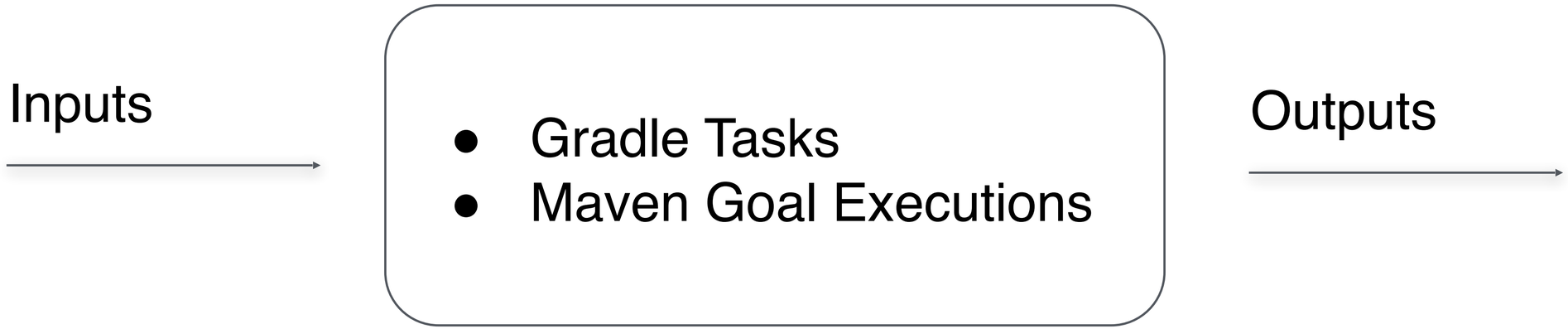


Build Caching

- Ccache < 2002
- Introduced to the Java world by Gradle in 2017
- Maven has an open source build cache too
- **Used by leading technology companies** like Google and Facebook
- Can support both **user local and remote caching** for distributed teams

- Build caches are **complementary to dependency caches**, not mutually exclusive:
  - A dependency cache caches **fully compiled dependencies**
  - A build cache accelerates **building a single source repository**
  - A build cache caches build actions (e.g. Gradle tasks or Maven goals)

What is a Build Cache?



When the inputs have not changed, the **output can be reused** from a previous run.

Cache Key/Value Calculation

The ***cacheKey*** for Gradle Tasks/Maven Goals is based on the Inputs:

```
cacheKey(javaCompile) = hash(sourceFiles,
                             jdk version,
                             classpath,
                             compiler args)
```

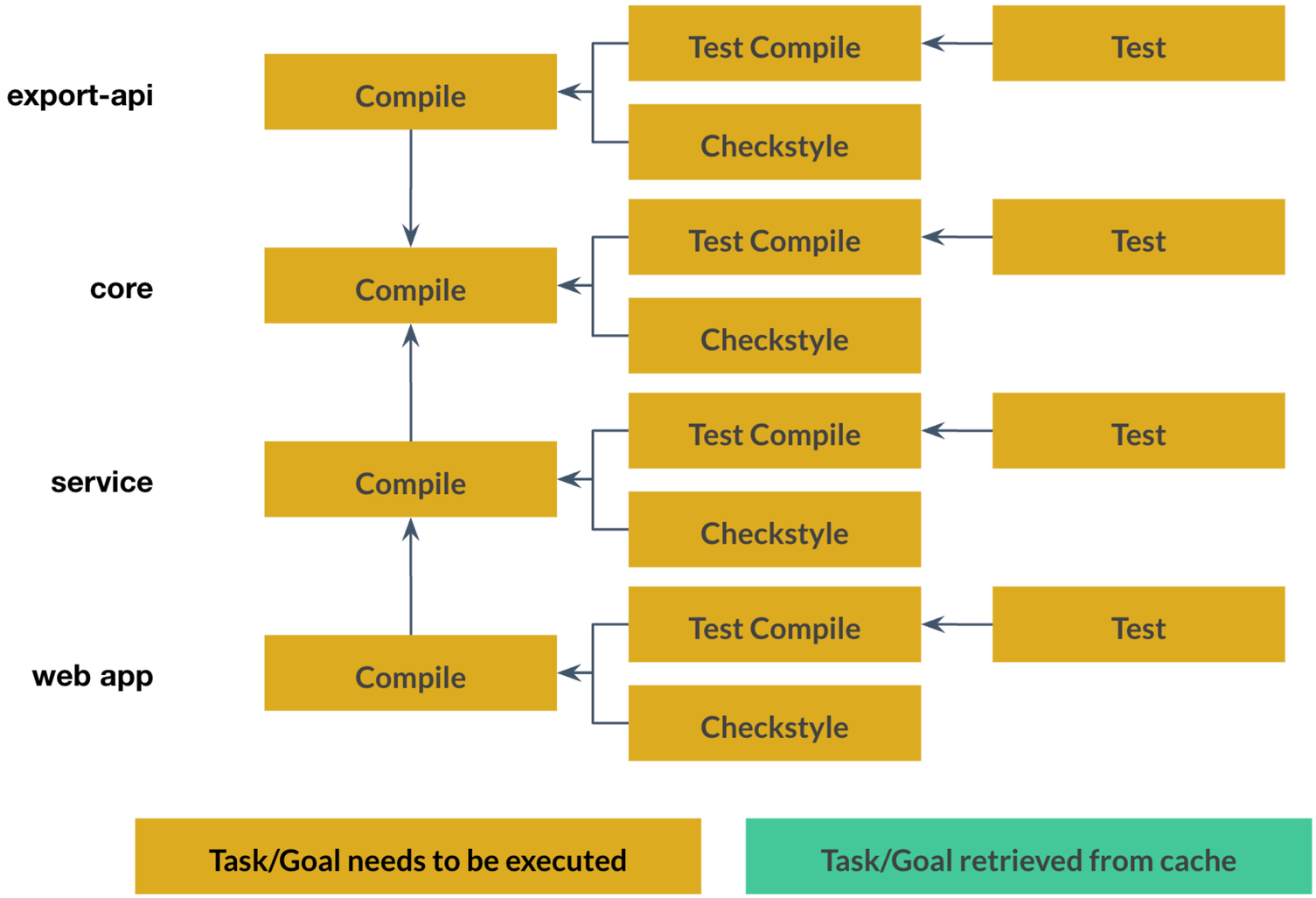
The ***cacheEntry*** contains the output:

```
cacheEntry[cacheKey(javaCompile)] = fileTree(classFiles)
```

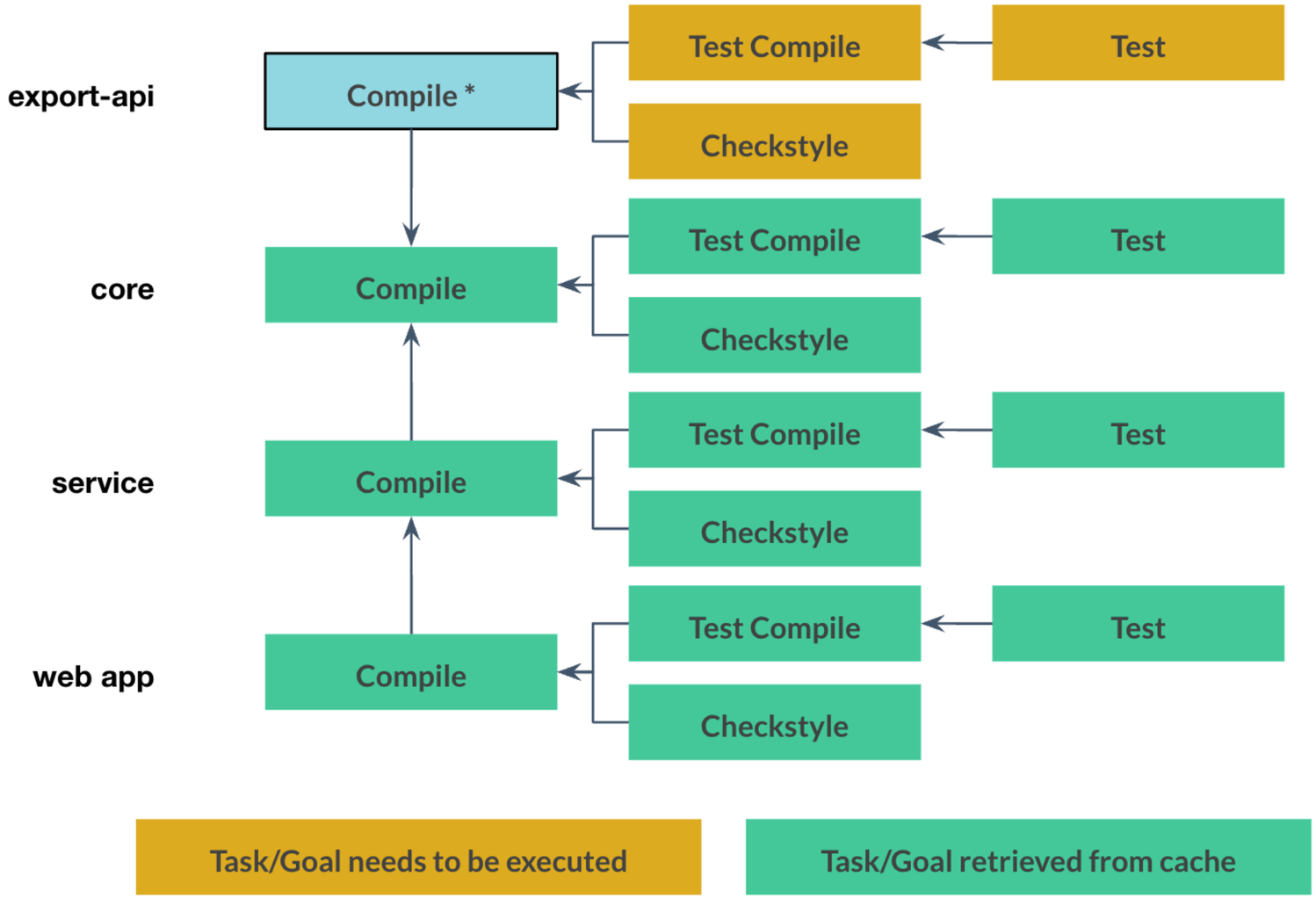
For more information, see:

https://docs.gradle.org/current/userguide/build_cache.html

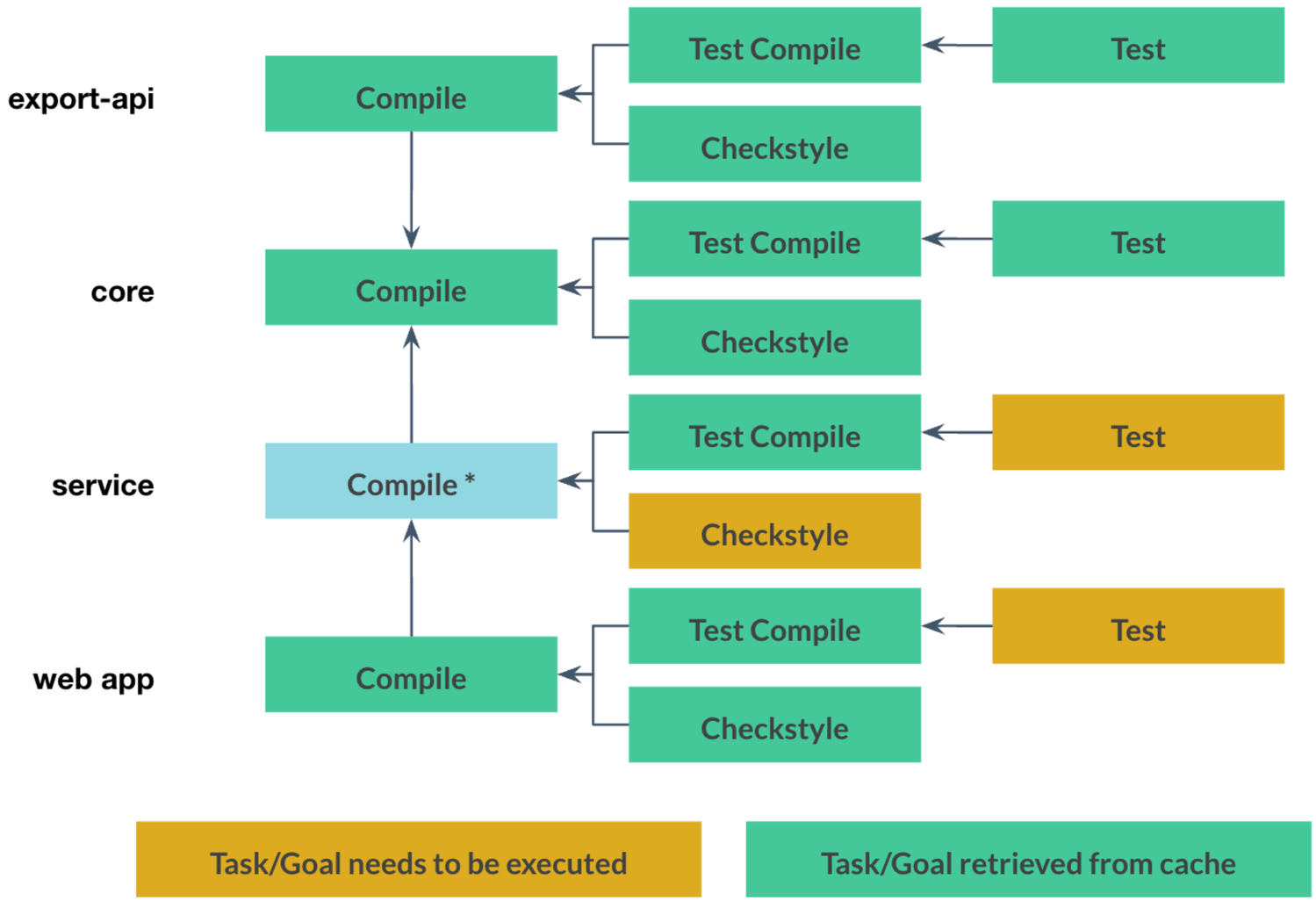
When not using the build cache, with Maven any change will require a **full build**. For Gradle this is the case when doing clean builds and switching between branches.



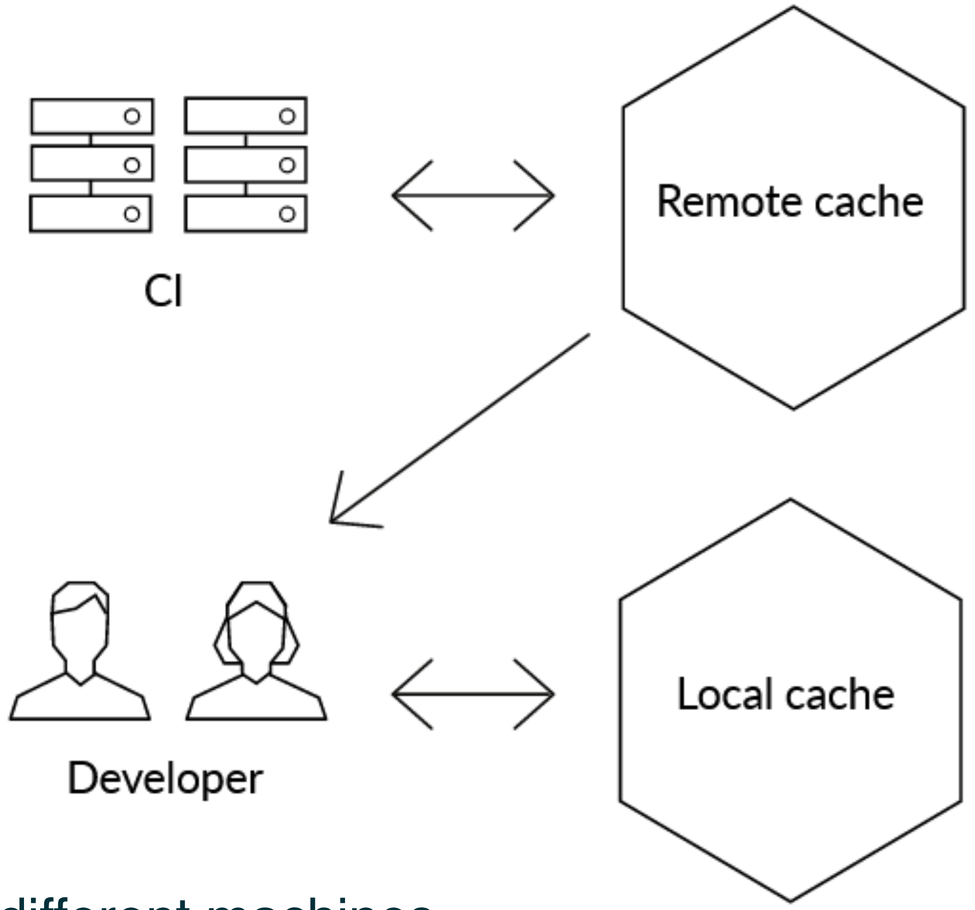
Changing an **public method** in the **export-api** module



Changing an **implementation detail** of a method in the **service** module

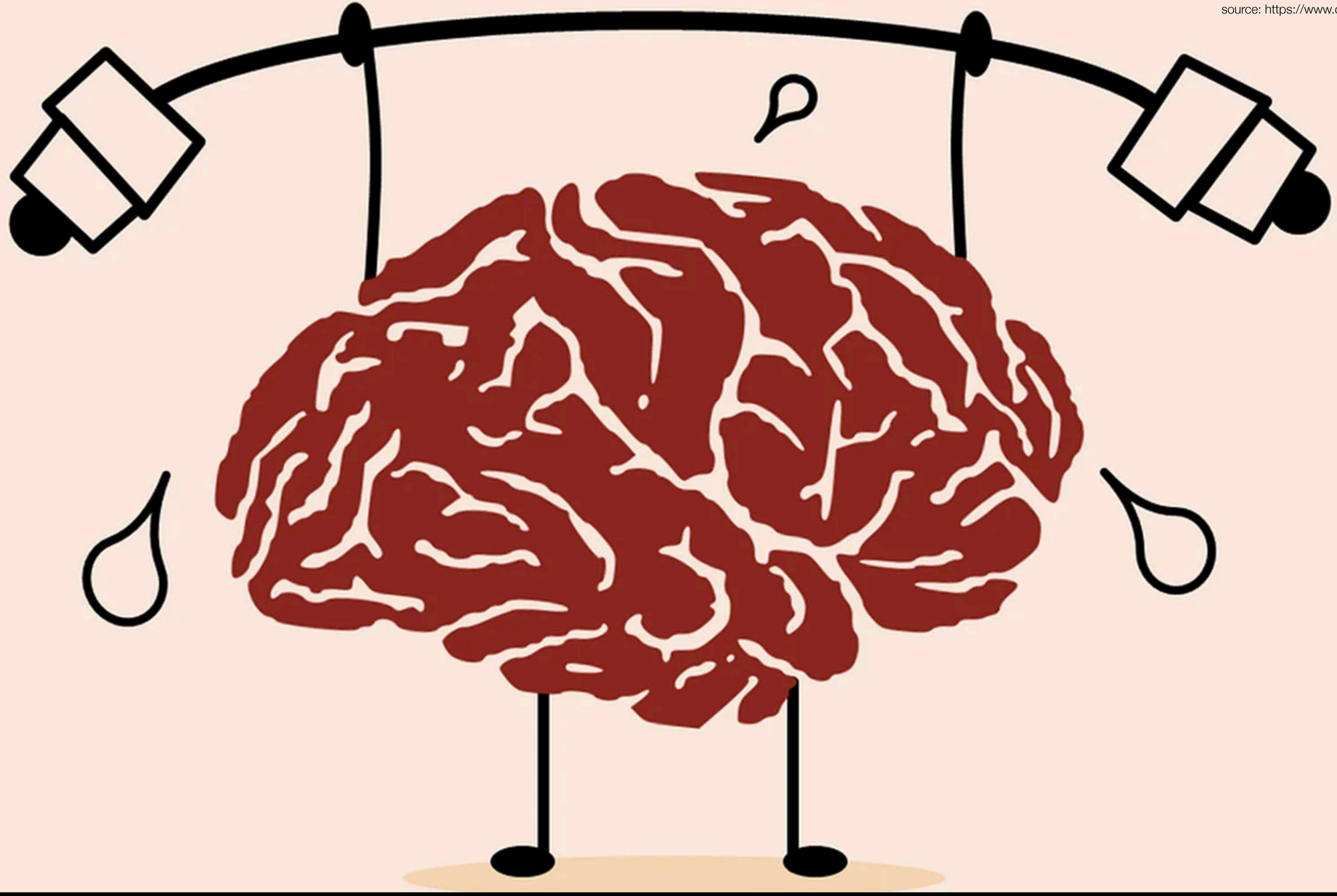


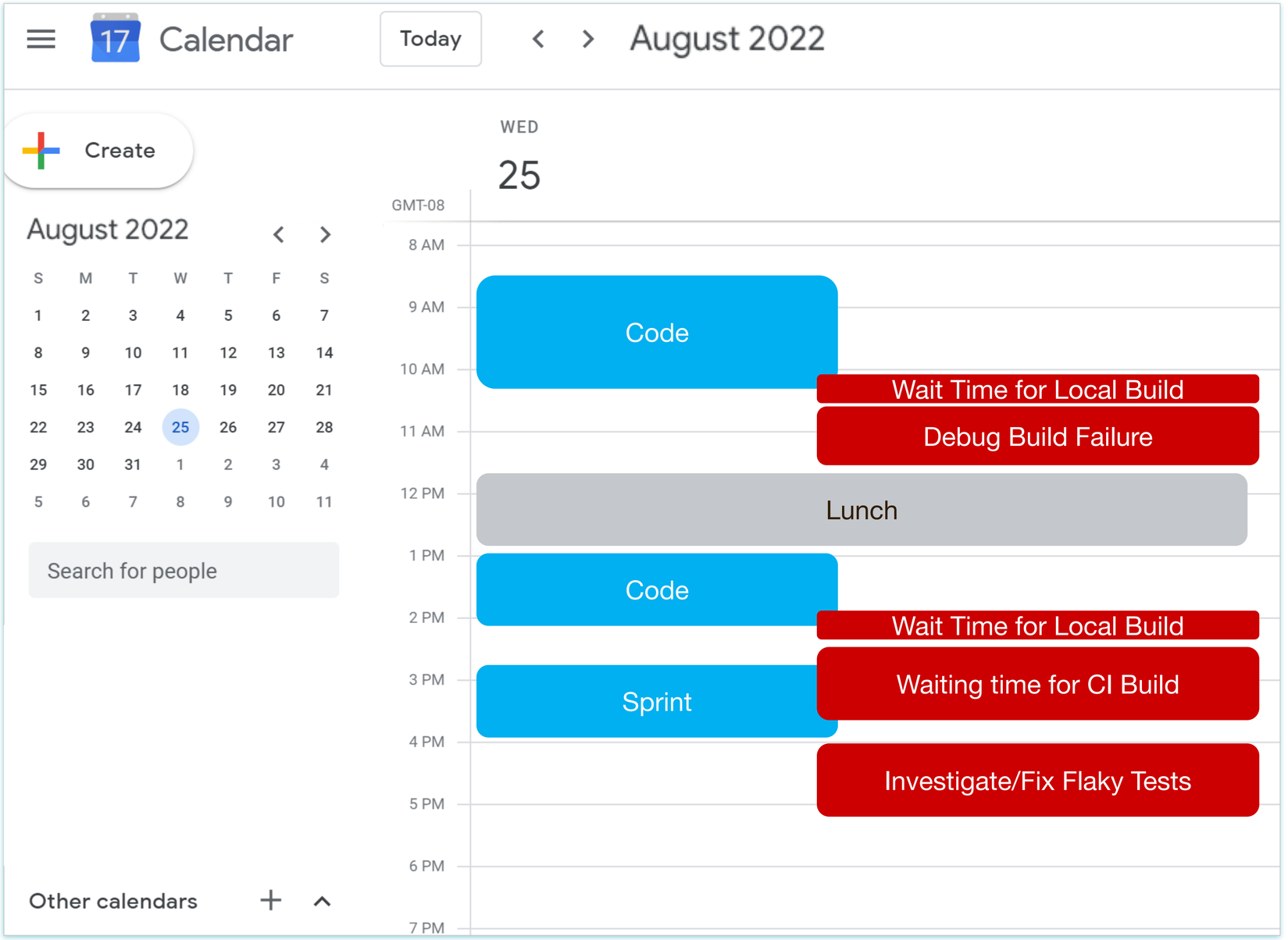
Remote Build Cache



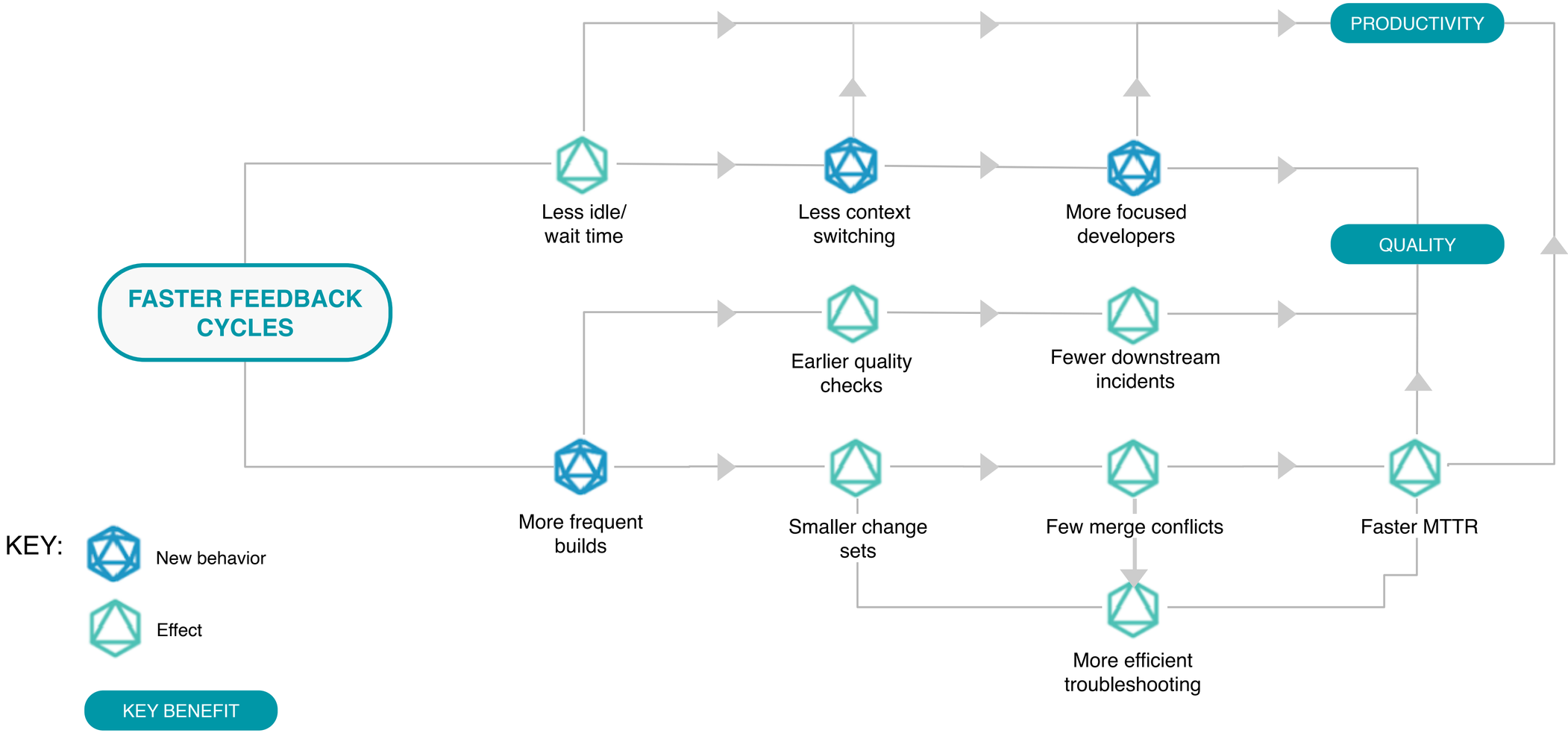
- Shared among different machines
- Speeds up development for the whole team
- Reuses build results among CI agents/jobs and individual developers

source: https://www.cshl.edu/quiz/brain-interrupted/



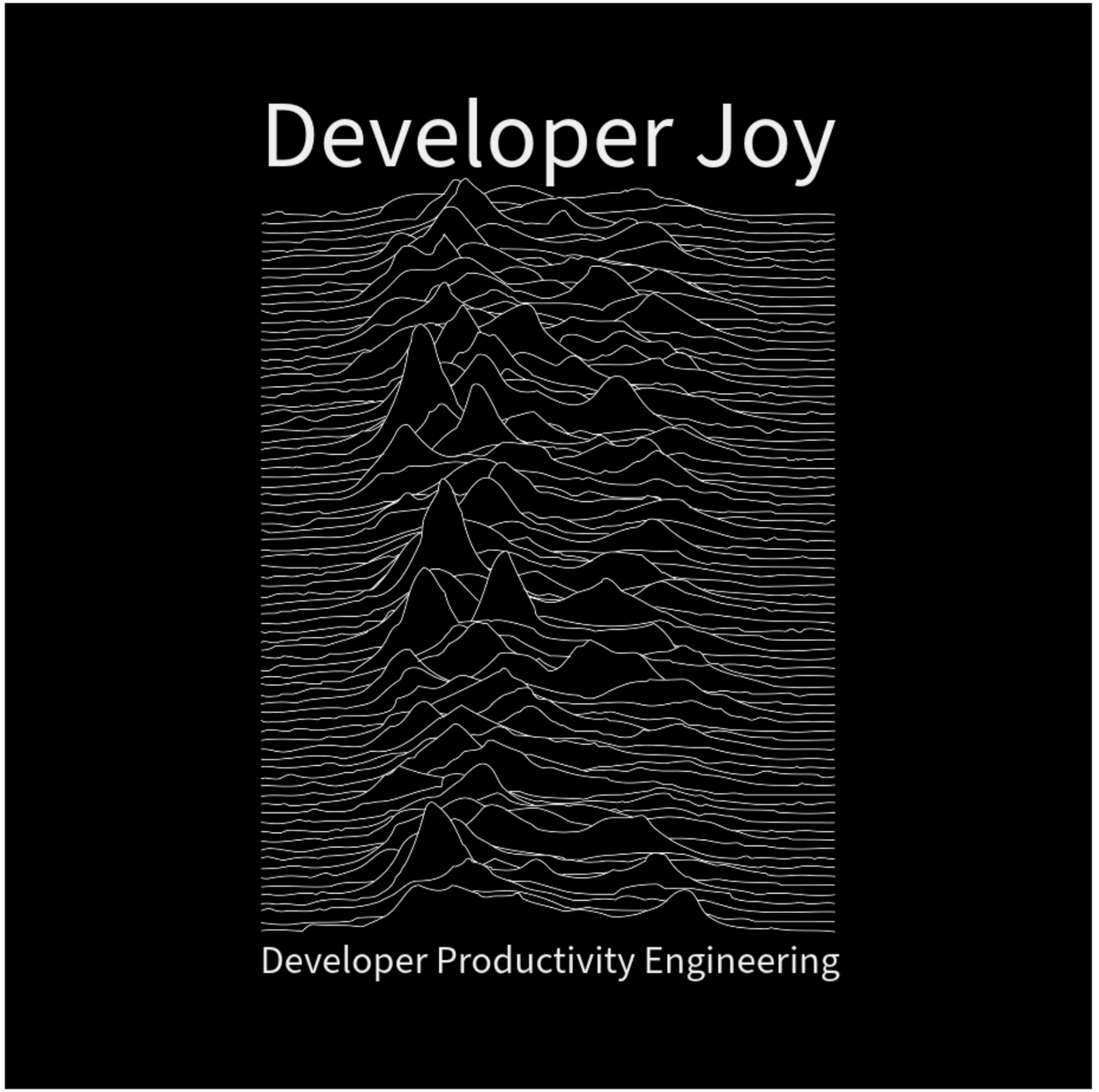

Calendar
Today
August 2022
Create
August 2022
S M T W T F S
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30 31 1 2 3 4
5 6 7 8 9 10 11
Search for people
Other calendars
WED
25
GMT-08
8 AM
9 AM
10 AM
11 AM
12 PM
1 PM
2 PM
3 PM
4 PM
5 PM
6 PM
7 PM
Code
Wait Time for Local Build
Debug Build Failure
Lunch
Code
Wait Time for Local Build
Sprint
Waiting time for CI Build
Investigate/Fix Flaky Tests

The anatomy of fast feedback cycles

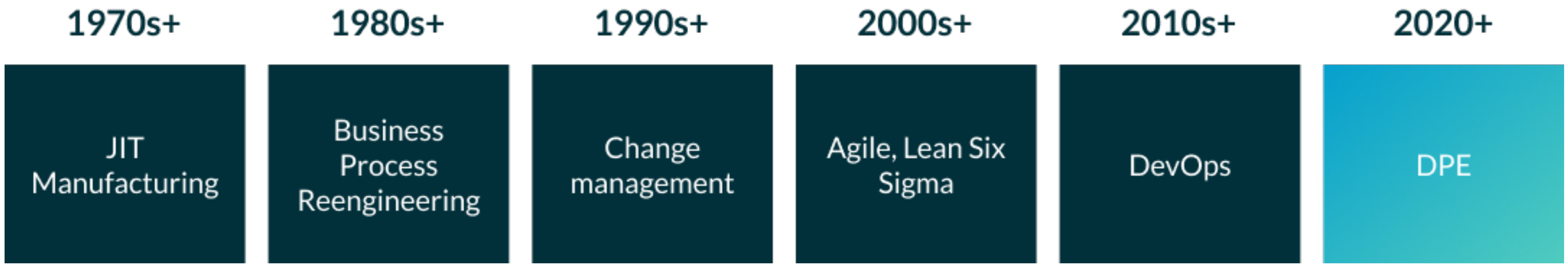


Gradle

Developer Productivity Engineering (DPE)


Developer Joy
Developer Productivity Engineering

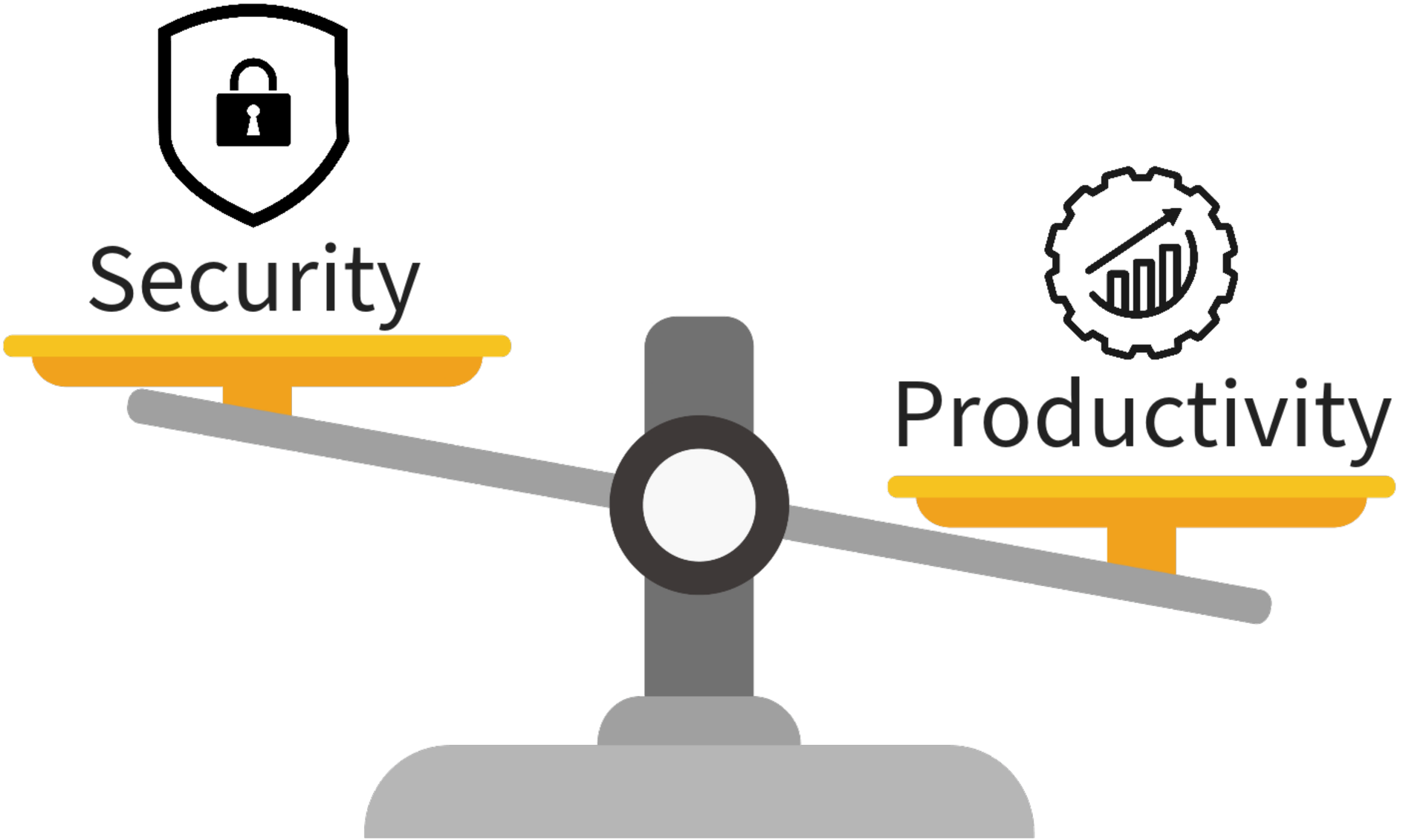
Progression of Productivity

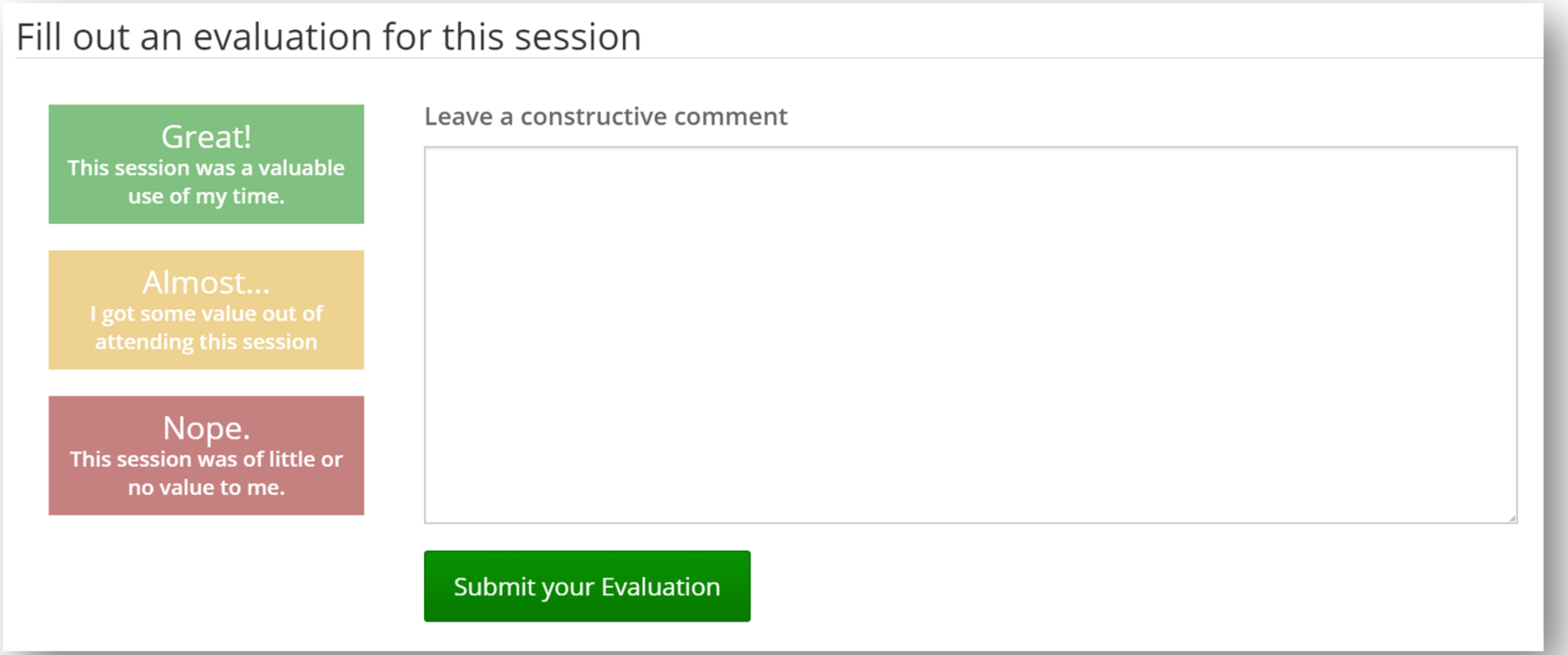


The Future

Other Ways to Speed up Builds

- Update your build tool
- Break project into modules
- Predictive Test Selection
- Test Distribution


Security
Productivity



https://indycode.amegala.com/schedule

Swag

Hoodie

1,800 Redeem

Swag

Build Local T-Shirt

700 Redeem

Swag

Basic Custom Baseball Hat

900 Redeem

Other Rewards

LEGO® Mandalorian Helmet

2,300

Swag

Kiss my Cache T-Shirt

700 Redeem

Other Rewards

Multi Cord Charger

200 Redeem

worry about are our CPUs, because they are tucked beyond rat

Slides, Links & Free Swag