

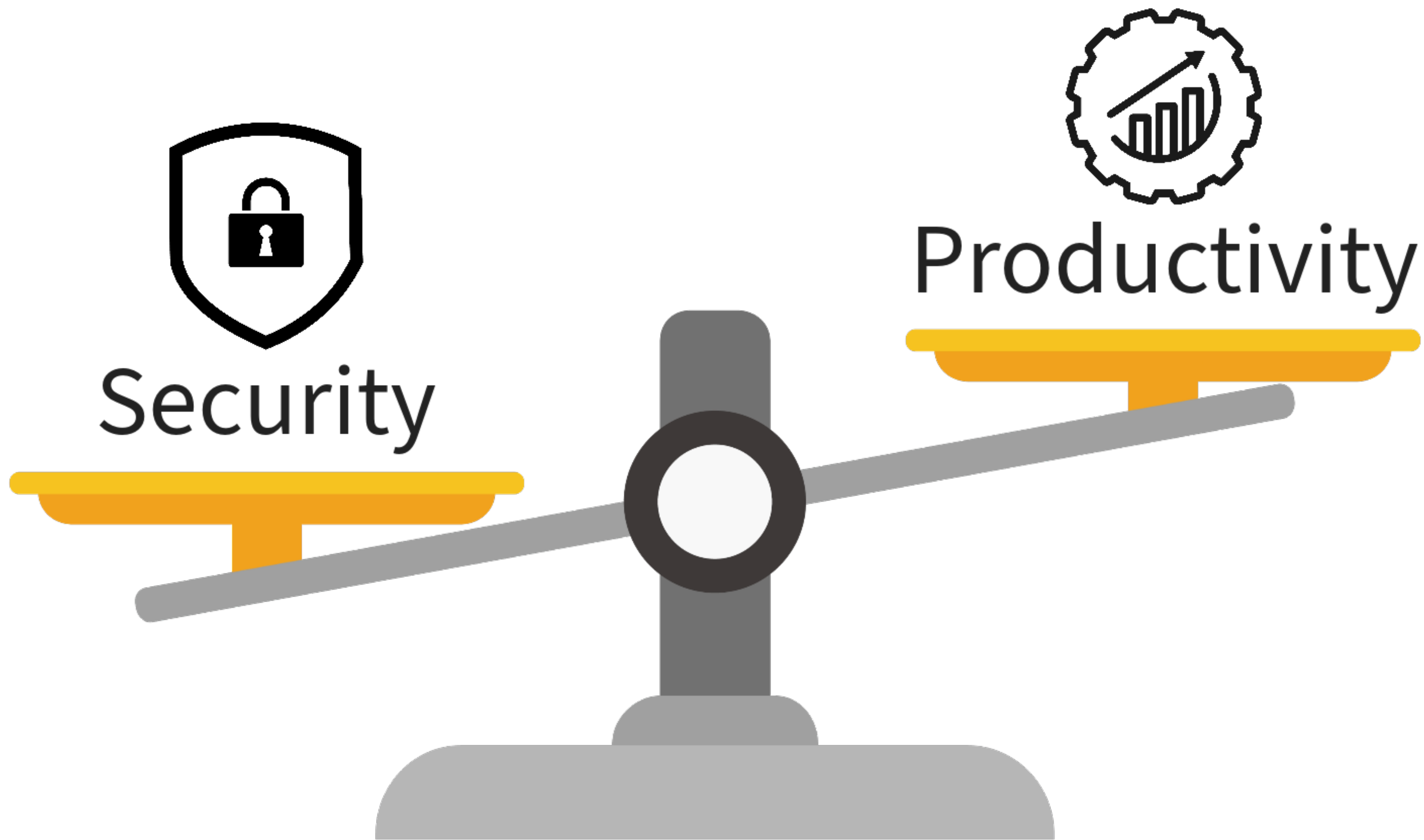


Security and Productivity Pick Two with Reproducible Builds

Brian Demers
Open Source Developer

 BrianDemers  bdemers





Who is this guy?



Java™
Champions



Maven™

Sonatype
Nexus





TABS

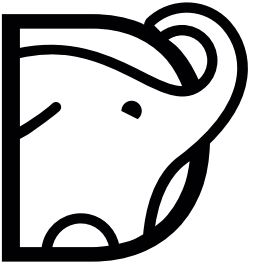
SPACES



vs



Gradle

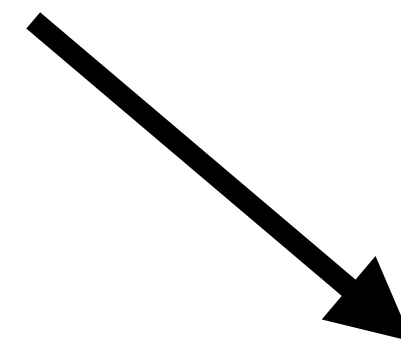
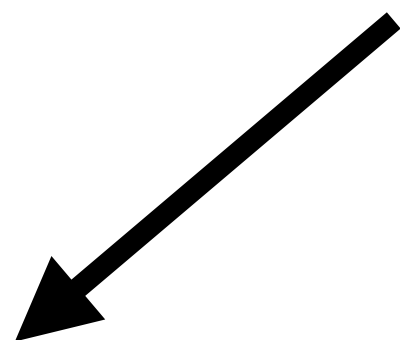
BUILD  TOOL

VS

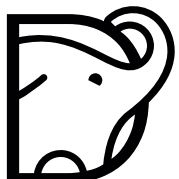
Maven  TM



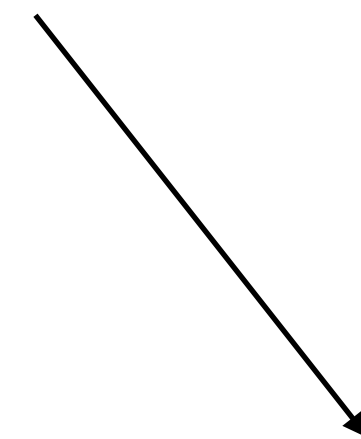
Gradle



Gradle

BUILD  TOOL

 DEVELOCITY



Developer
Productivity
Engineering

Gradle

BUILD  TOOL

*Maven*TM

 Bazel

sbt

Topics

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



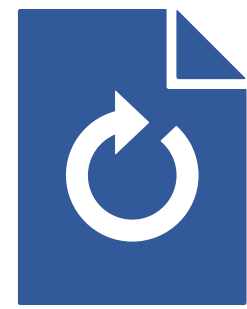
Reproducible Builds

reproducible-builds.org

Source



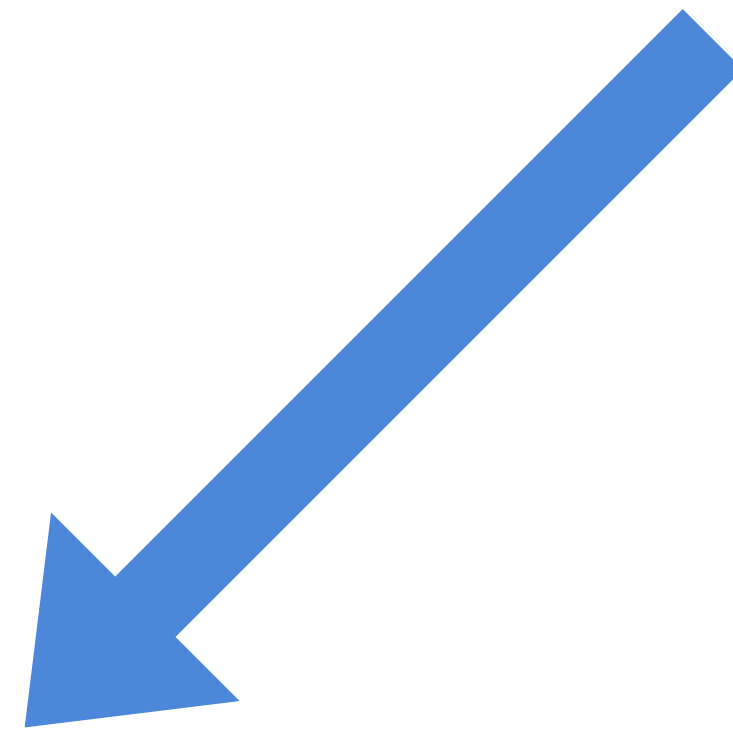
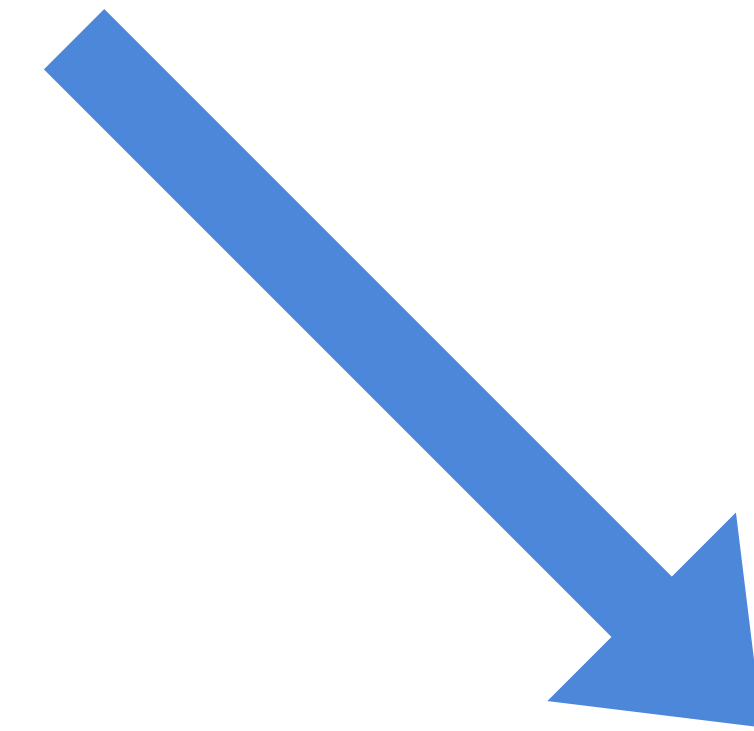
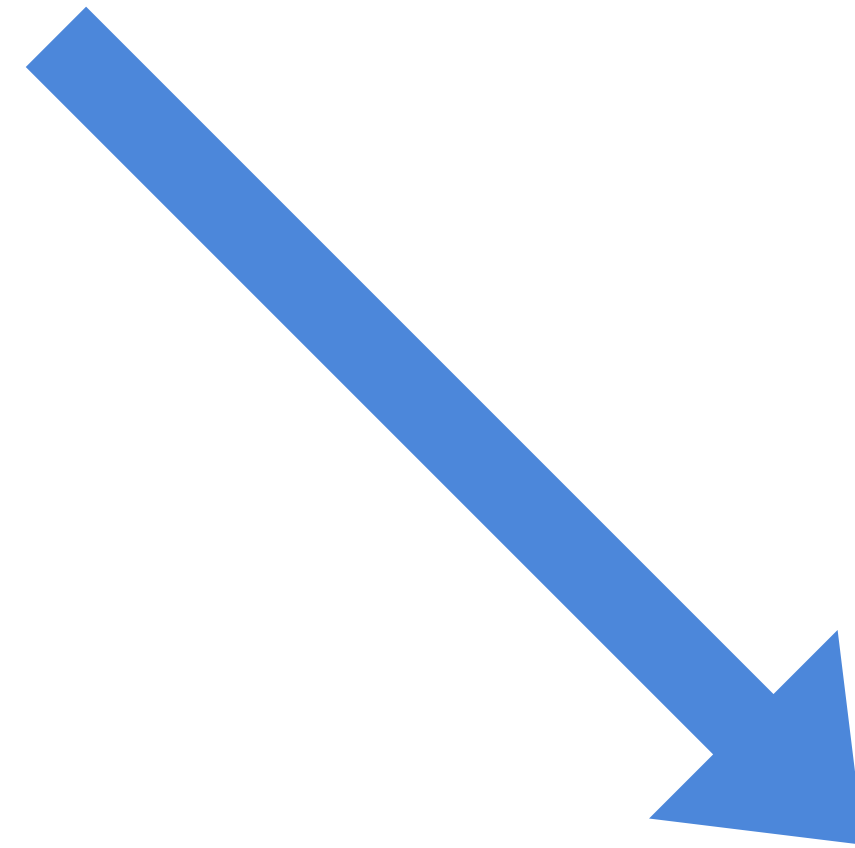
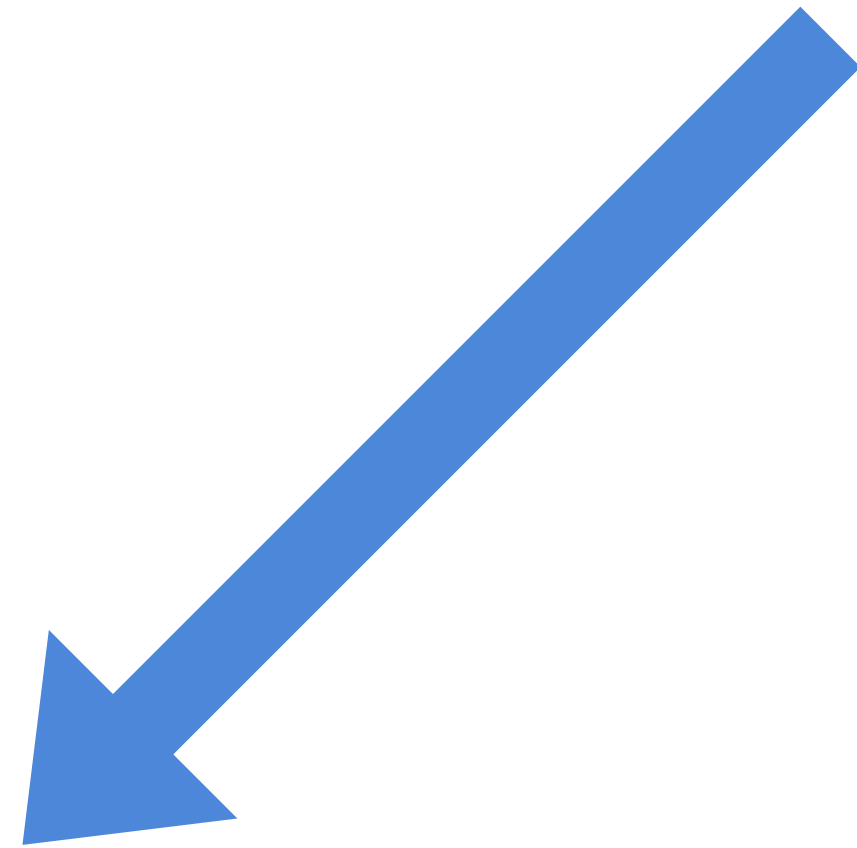
Build



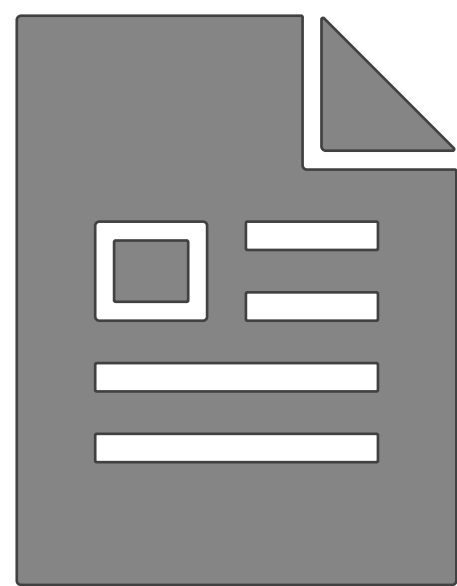
Build



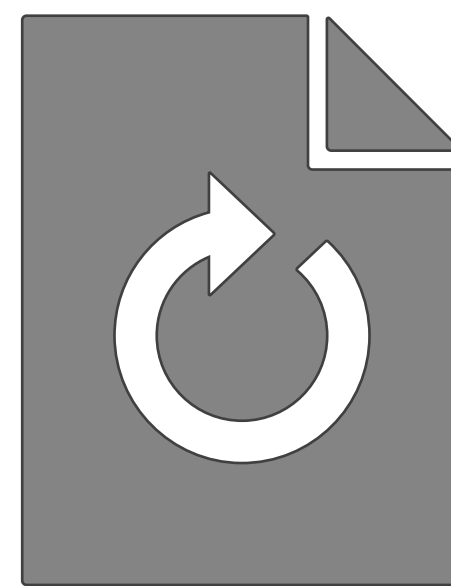
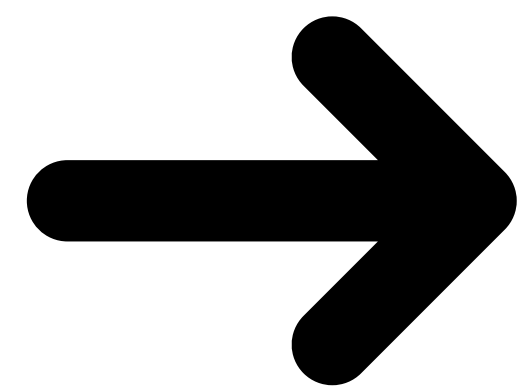
Verify



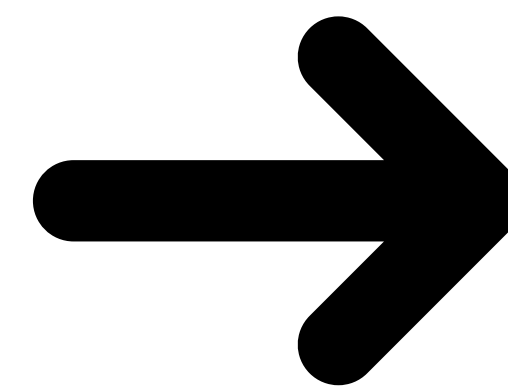
CHECKSUM



data



hash function



03ba204e50d126e4...

**HOW DID WE
GET HERE?**



Old way (META-INF/MANIFEST.MF)

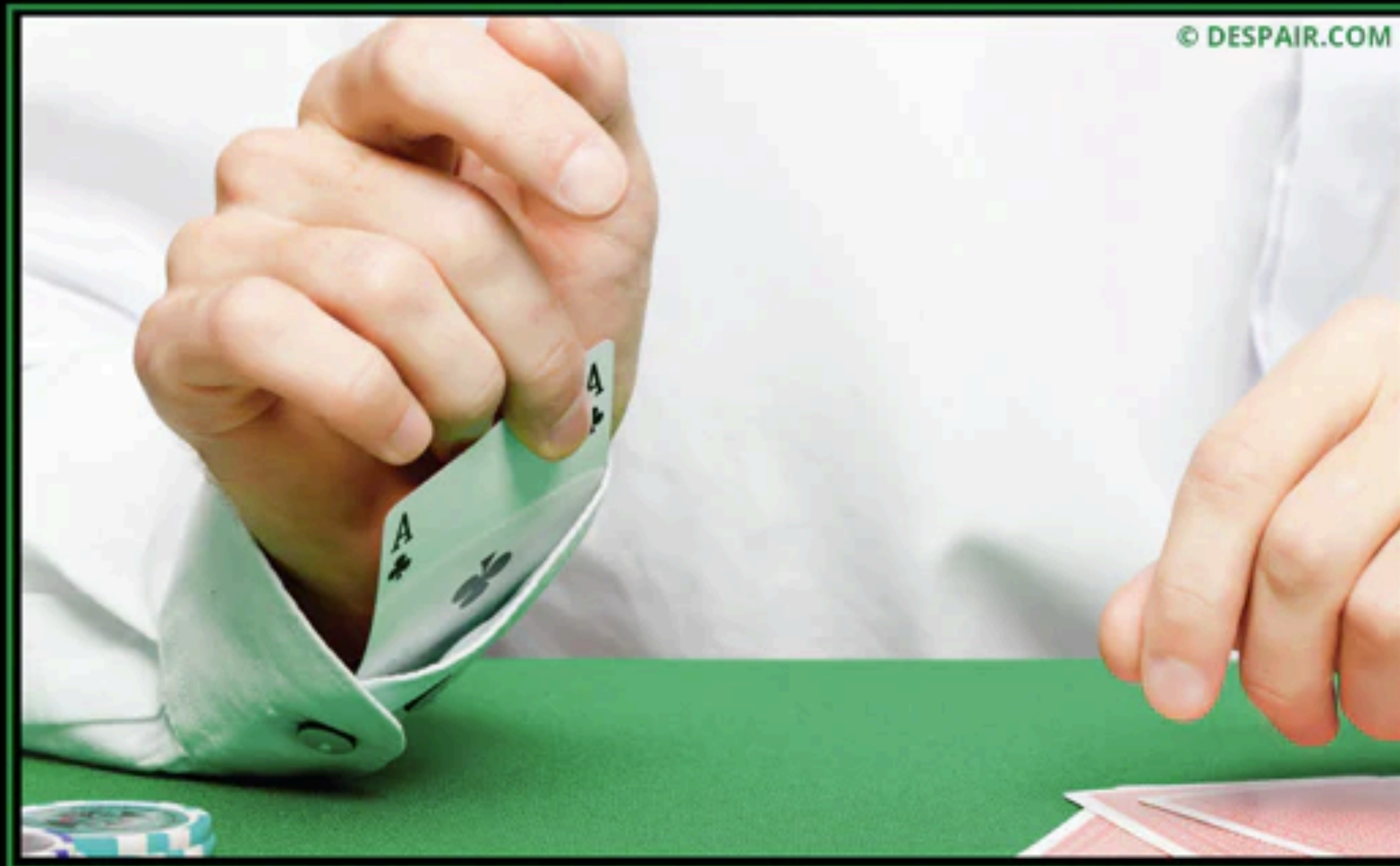
```
Manifest-Version: 1.0
Archiver-Version: Plexus Archiver
Created-By: Apache Maven
Built-By: jdcasey
Build-Jdk: 1.4.2_09
Extension-Name: maven-core
Specification-Title: Maven is a project development management and com
prehension tool. Based on the concept of a project object model: buil
ds, dependency 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 TAR 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
```



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 compromised
- 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



When Volvo invented the three-point seat belt in 1959, they made the patent free for all competitors to use in order to save lives because it had more value as a free life-saving tool than something to profit from.

Shouldn't All Builds be Reproducible?





Dates



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

Copyright 2005 by Randy Glasbergen.
www.glasbergen.com



**“Our biggest challenge is the time zone difference.
In New York, it’s 2:45 but at our headquarters it’s 1974.”**

File Dates

```
$ ls -al 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

```
int getRandomNumber()  
{  
    return 4; // chosen by fair dice roll.  
              // guaranteed to be random.  
}
```

xkcd.com/221

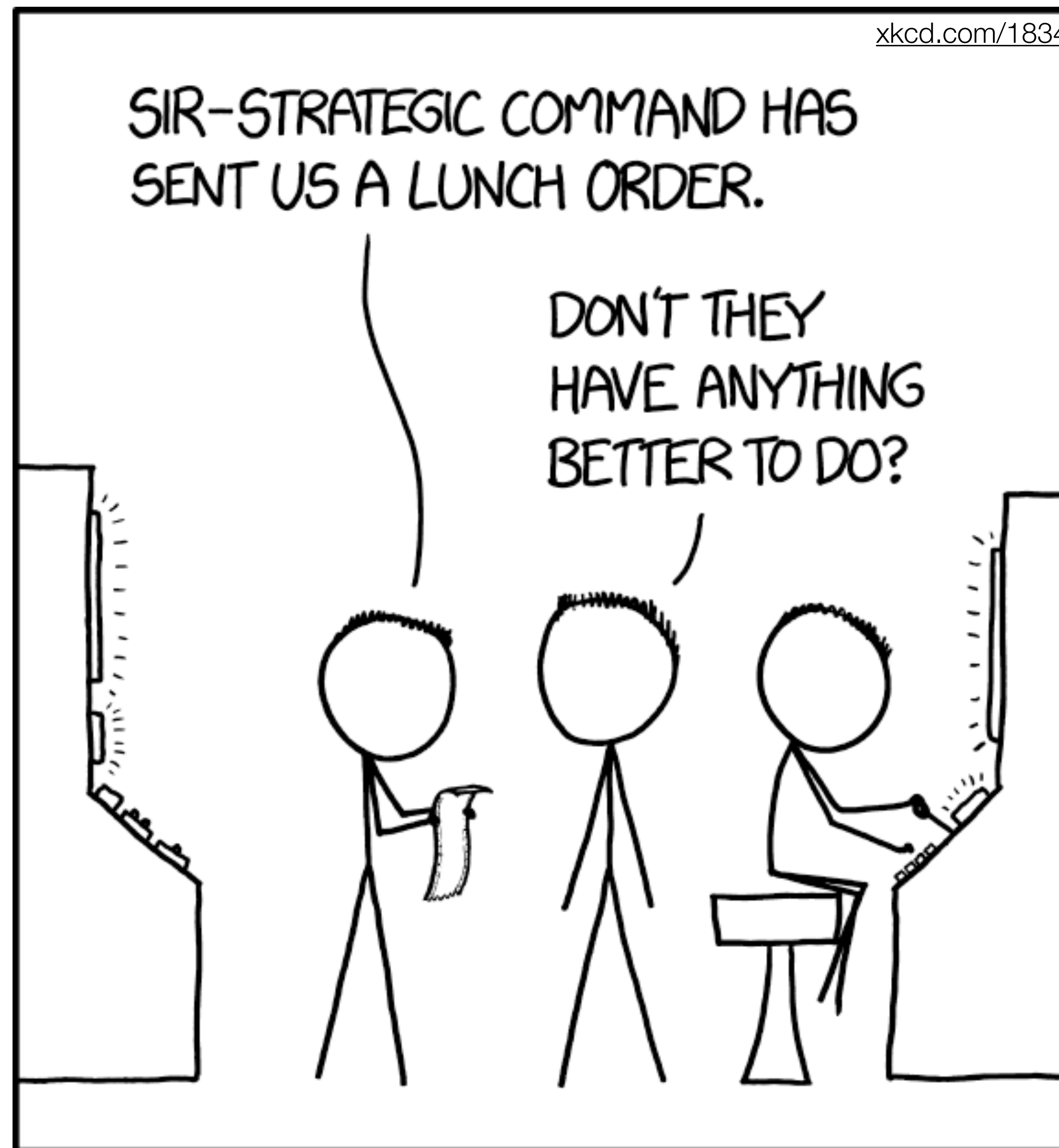
OS & Environment

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



File Input / Output Order

- Hash Maps
- Serialized data
- File order in archives



EVERYONE COMPLAINS ABOUT AUTOCORRECT,
BUT WE FORGET ABOUT THE TIME IT
PREVENTED A NUCLEAR WAR.



How to Verify?

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

```
80da7adf80a819db609ac6862931dc6c1cc04bf4c8ba292446021aa805aa3bfa
```

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

```
80da7adf80a819db609ac6862931dc6c1cc04bf4c8ba292446021aa805aa3bfa
```

Diffoscope

diffoscope --html https-everyw x +

diffoscope.org/examples/https-everywhere-5.0.6_vs_5.0.7.html

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

```
zipinfo {}
Offset 1, 9 lines modified
1 Zip file size: 2022489 bytes, number of entries: 194
2 ?rw-----2.0 unx .....73759 b-defN 80-Jan-01 00:00 Changelog
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
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
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
9 ?rw-----2.0 unx .....4198 b-defN 80-Jan-01 00:00 chrome/content/code/Cookie.js
Offset 187, 10 lines modified
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
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
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
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
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%
```

```
zipinfo {}
Offset 1, 9 lines modified
1 Zip file size: 2018233 bytes, number of entries: 194
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
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
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
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
Offset 187, 10 lines modified
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
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
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
193 ?rw-----2.0 unx .....2509 b-defN 80-Jan-01 00:00 defaults/preferences/preferences.js
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
196 194 files, 7394938 bytes uncompressed, 1988947 bytes compressed: 73.1%
```

```
Changelog
Offset 1, 11 lines modified
1 Firefox 5.0.6 / Chrome-2015.7.13
2 *** EFF 25th birthday edition!
3 *** Ruleset fixes
4 *** Move "Enable / Disable rules" options into menu.
5
6
7 Firefox 5.0.5 / Chrome-2015.5.28
8 *** Ruleset fixes
9 *** Fix ordering of locales to default to English again.
10
11 Firefox 5.0.4 / Chrome-2015.5.12
12 *** Ruleset fixes
```

```
Changelog
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
4 Firefox 5.0.6 / Chrome-2015.7.13
5 *** Ruleset fixes
6 *** Move options from "Enable / Disable rules" into icon menu
7 *** EFF 25th birthday edition!
8
9 Firefox 5.0.5 / Chrome-2015.5.28
10 *** Ruleset fixes
11 *** Fix ordering of locales to default to English again.
12
13 Firefox 5.0.4 / Chrome-2015.5.12
14 *** Ruleset fixes
```

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

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

☰ README.md

Reproducible Builds for Maven Central Repository

This project is the [Java part](#) of the [Reproducible Builds](#) effort:



Reproducible Builds

an independently-verifiable path from source to binary code



LET'S GET STARTED!

makeameme.org

Maven & Gradle

```
<!-- Maven -->
<properties>
  <project.build.outputTimestamp>
    2023-01-01T00:00:00Z
  </project.build.outputTimestamp>
</properties>


// Gradle
tasks.withType(AbstractArchiveTask).configureEach {
  preserveFileTimestamps = false
  reproducibleFileOrder  = true
}
```


Other Benefits

- Quality
- Debugging
- Smaller deltas in releases
- Cacheable



Think about a Docker builds

 Layers	Cache?
<code>FROM ubuntu:latest</code>	✓
<code>RUN apt-get update \ && apt-get install build-essentials</code>	✓
<code>COPY main.c Makefile /src/</code>	✗
<code>WORKDIR /src</code>	✗
<code>RUN make build</code>	✗

Build Caching

- ◆ 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?

Inputs



- Gradle Tasks
- Maven Goal Executions

Outputs



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:

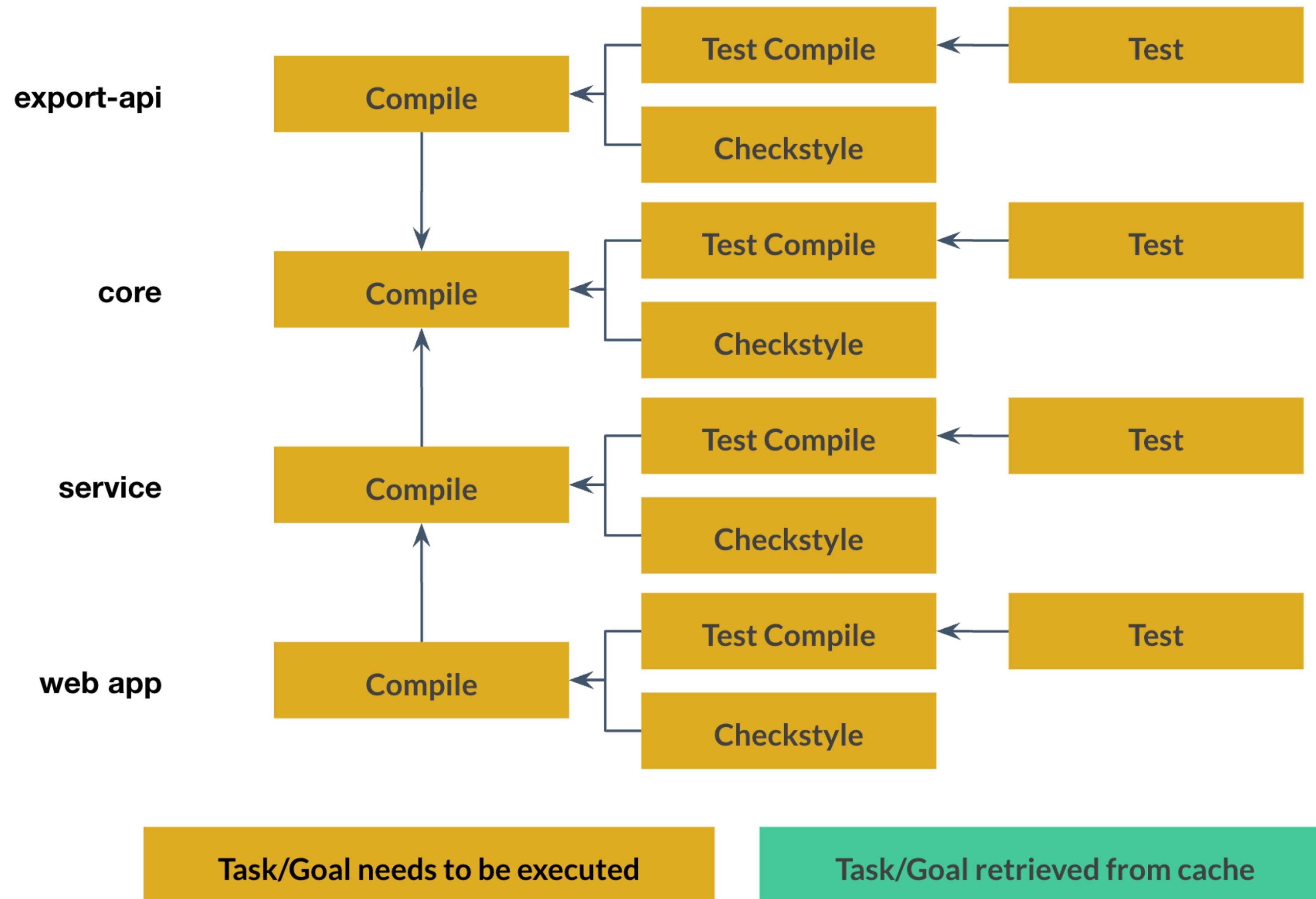
```
cacheEntry[cacheKey(javaCompile)] = fileTree(classFiles)
```

For more information, see:

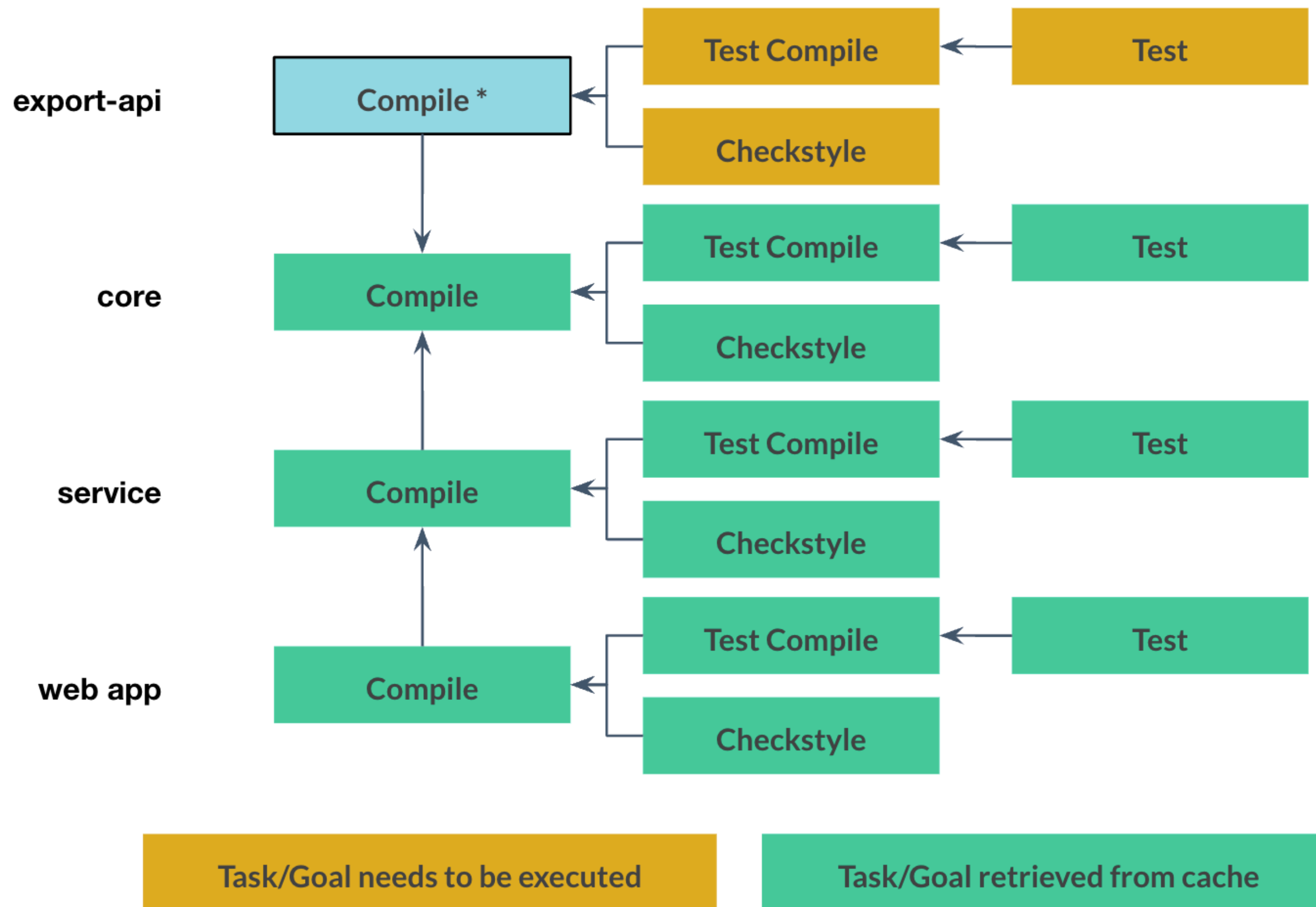
https://docs.gradle.org/current/userguide/build_cache.html



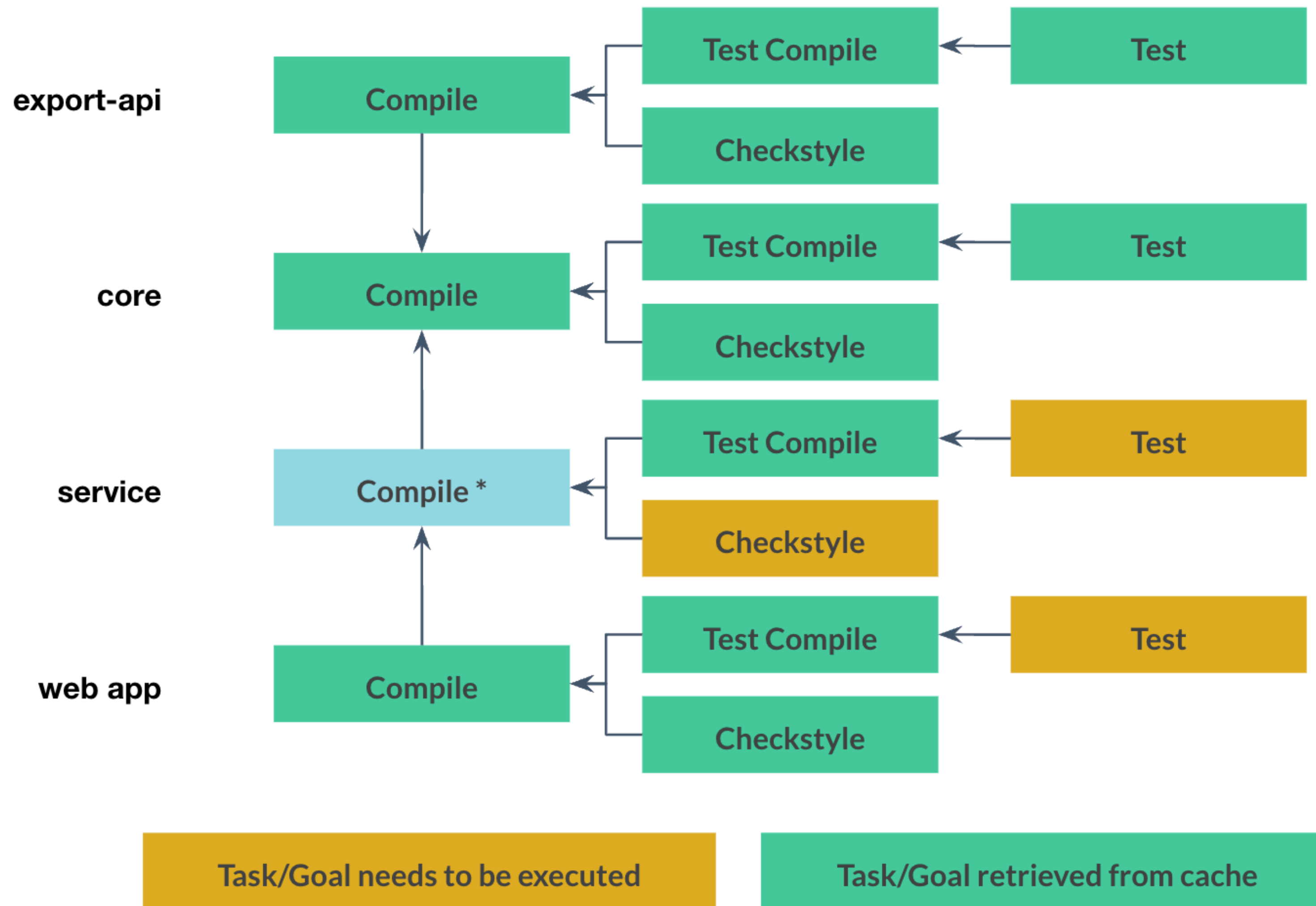
When not using the build cache, with Maven any change will require a **full build**. For Gradle this is the case when doing clean builds and switching between branches.



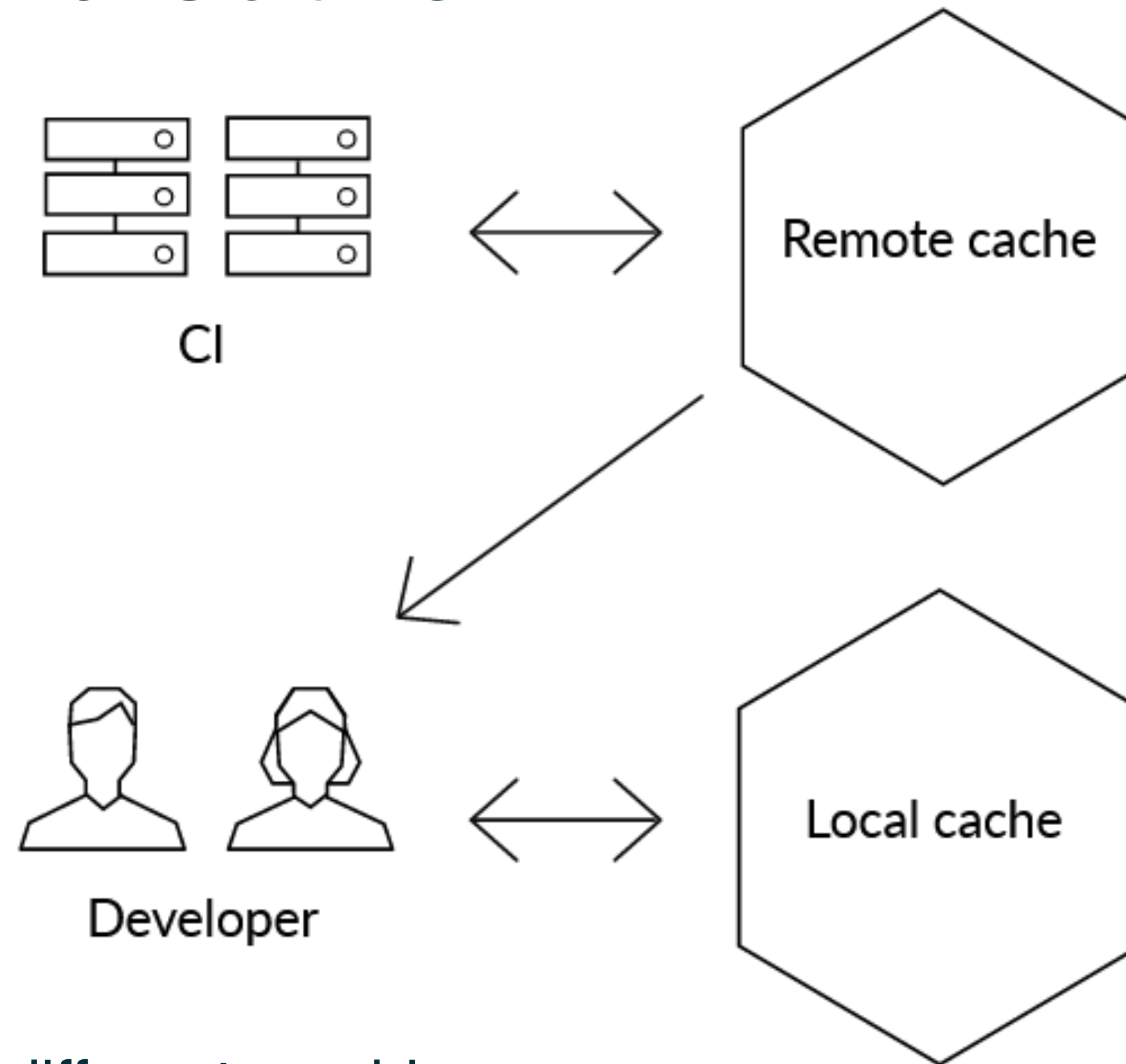
Changing an public method in the `export-api` module



Changing an implementation detail of a method in the service module

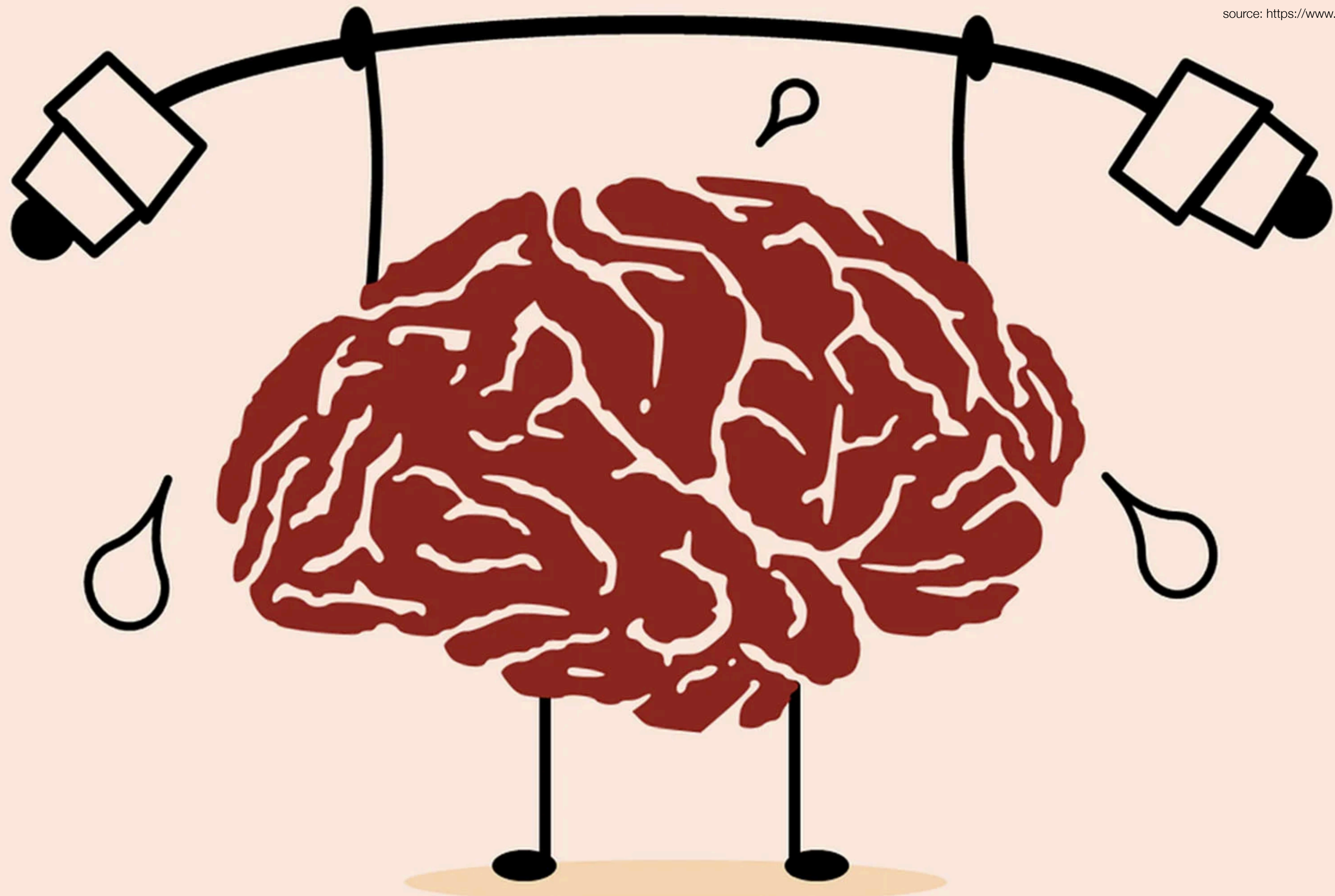


Remote Build Cache

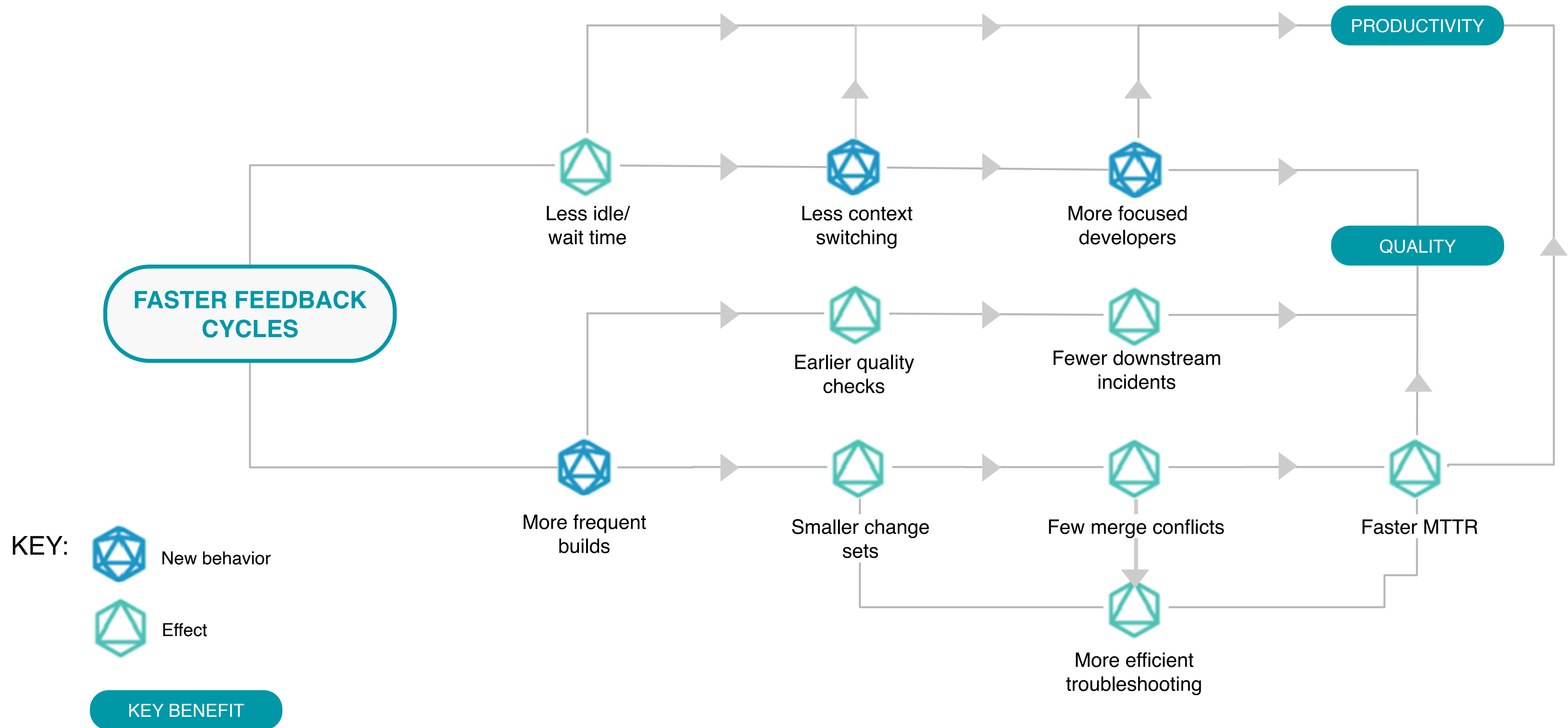


- ◆ Shared among different machines
- ◆ Speeds up development for the whole team
- ◆ Reuses build results among CI agents/jobs and individual developers





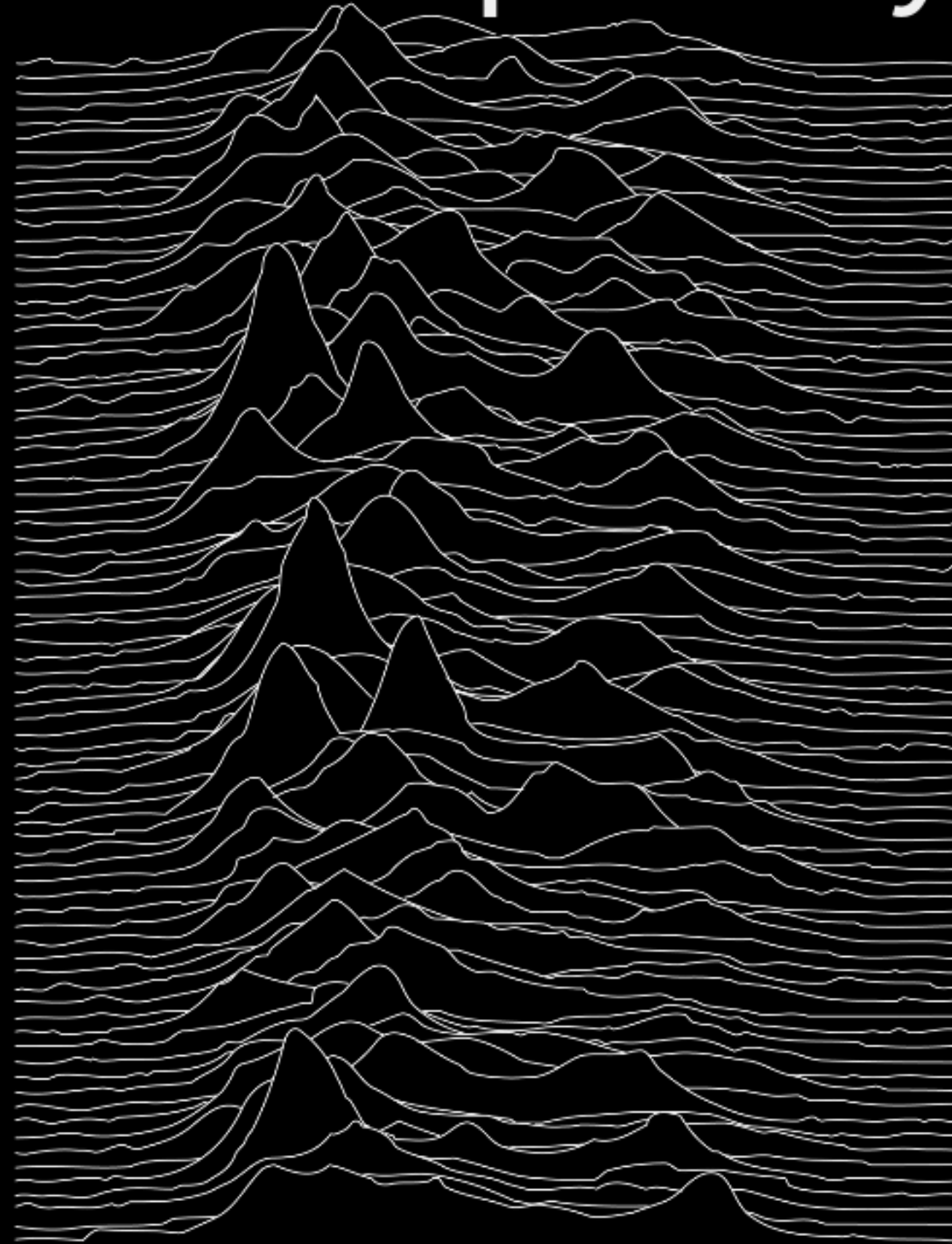
The anatomy of fast feedback cycles



Developer Productivity Engineering (DPE)



Developer Joy



Developer Productivity Engineering

Progression of Productivity



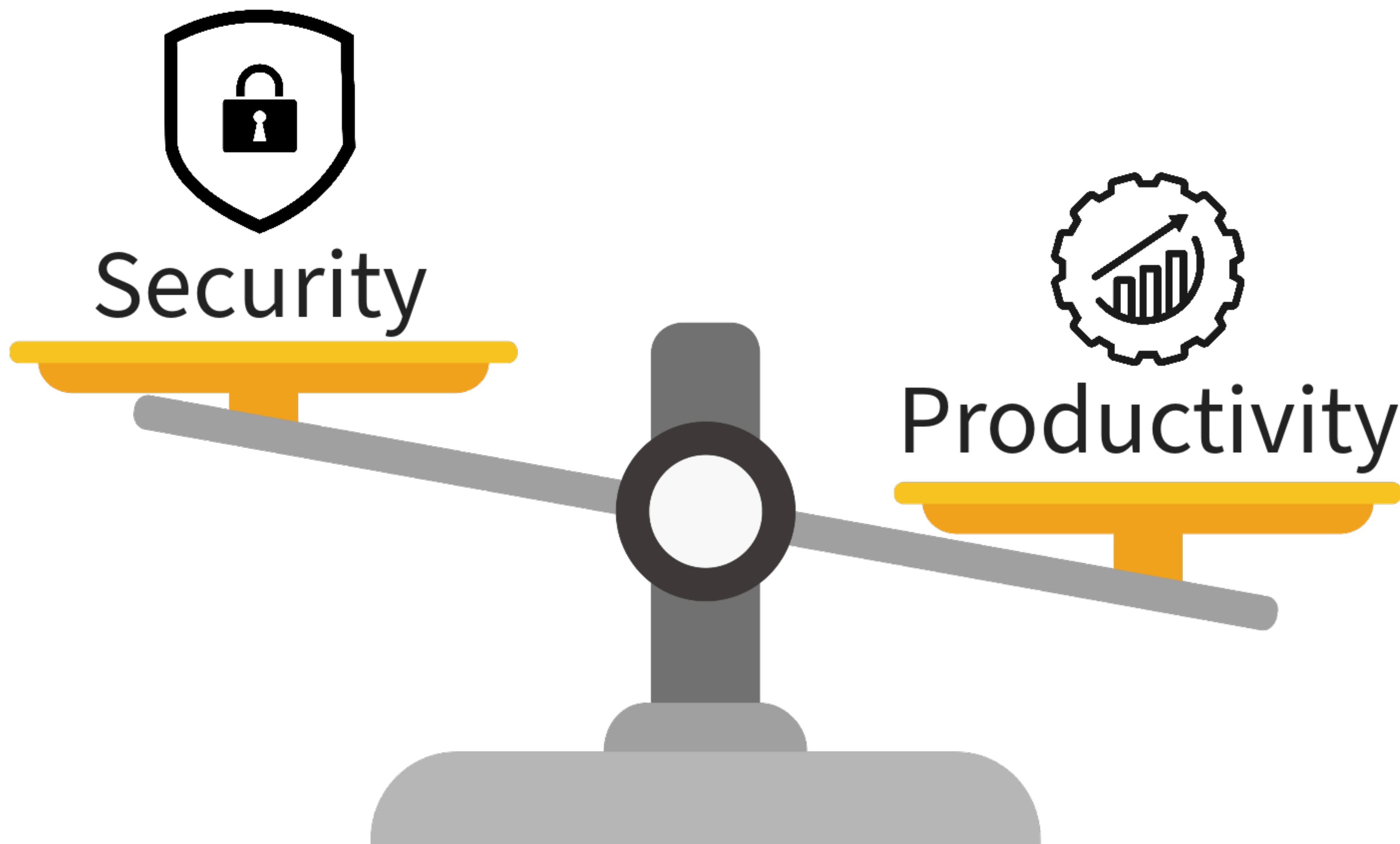
The Future

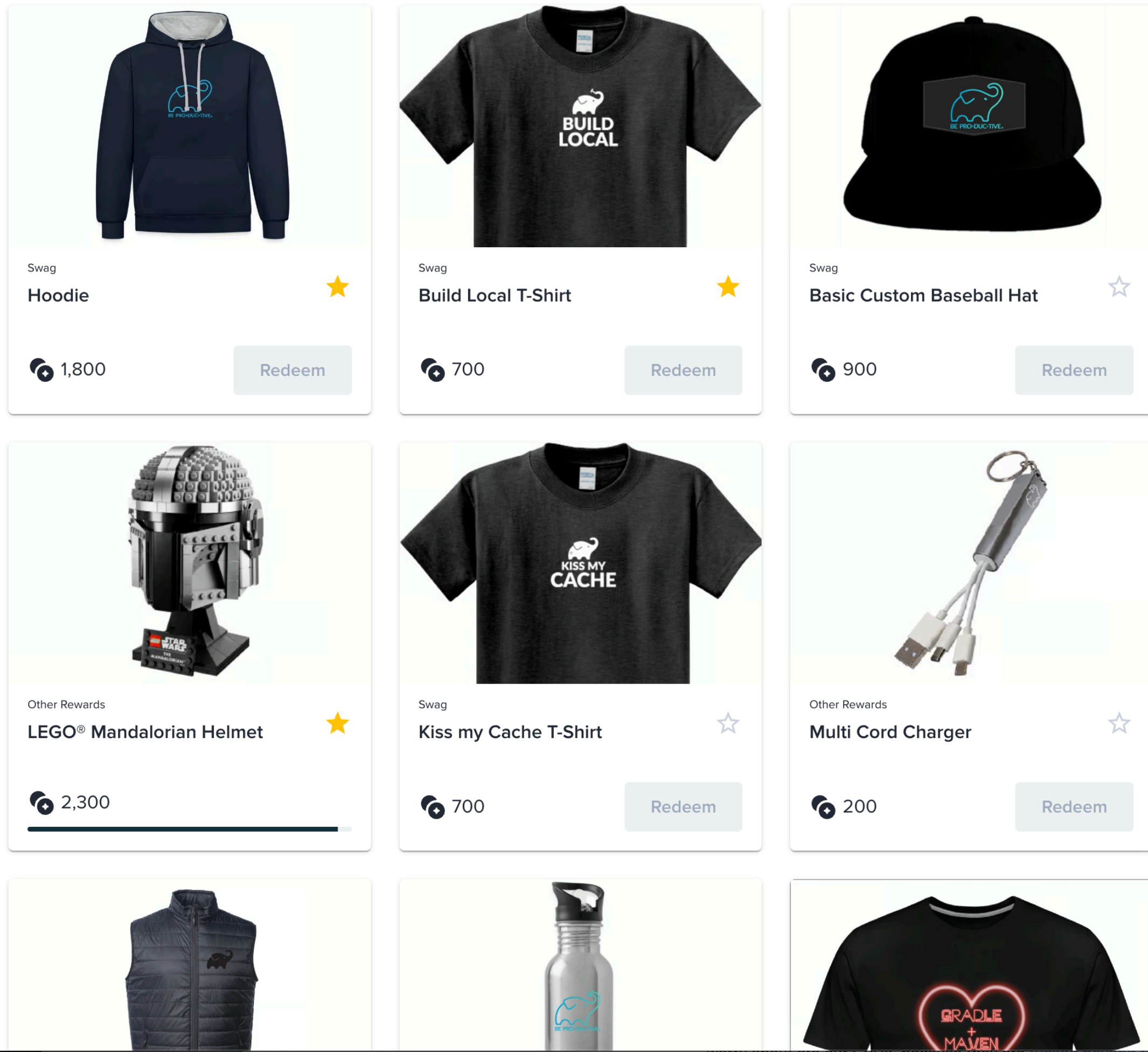


Other Ways to Speed up Builds

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







 **BrianDemers**

 **bdemers**

Learn more & get free swag

