`ghasum`: Integrity for GitHub Actions

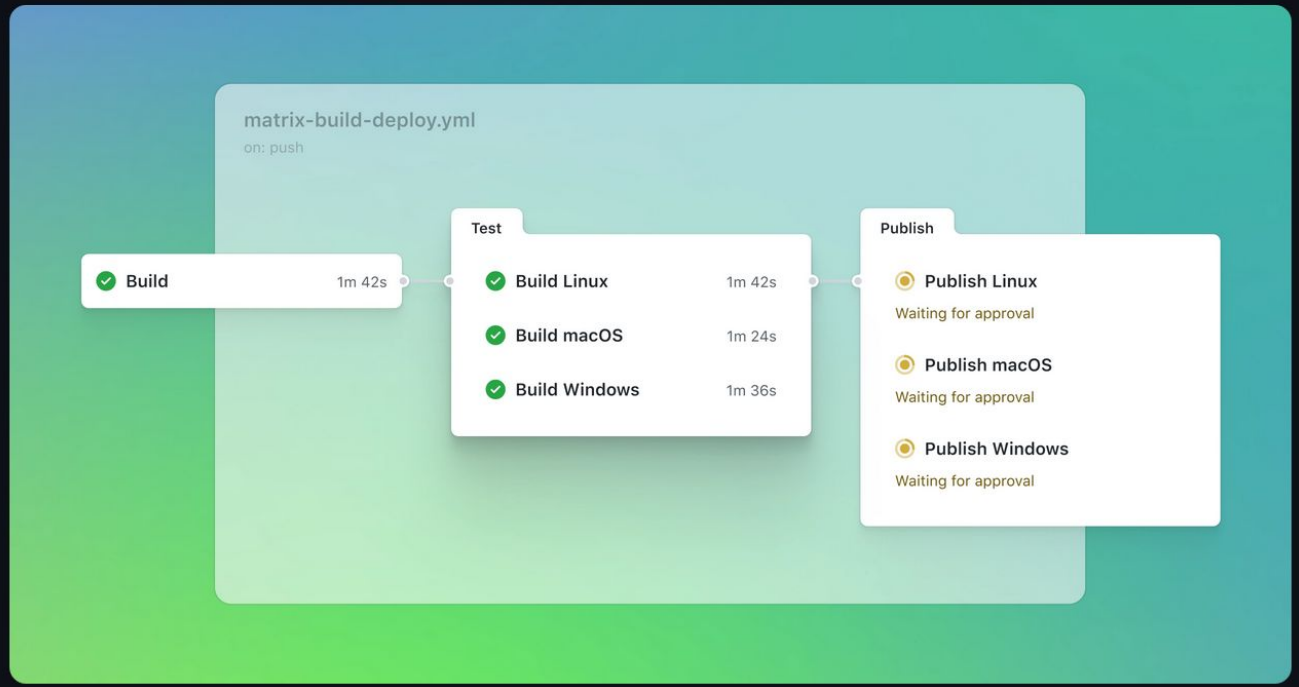
Eric Cornelissen (ericco@kth.se)

Overview

- Background
- Tool
- Demo
- Roadmap
- Takeaways

Background

- GitHub Actions
  - Continuous Integration & Deployment system



source: https://github.com/features/actions

Background

- GitHub Actions
  - Continuous Integration & Deployment system
  - Reusable components called "Actions"

```
14        steps:
15        - name: Checkout repository
16          uses: actions/checkout@v4.2.0
```

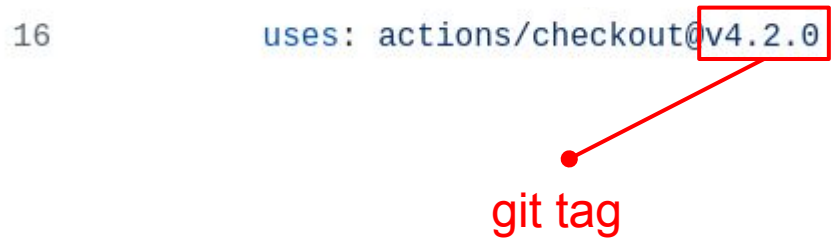
Background

- GitHub Actions
  - Continuous Integration & Deployment system
  - Reusable components called "Actions"

```
14        steps:
15        - name: Checkout repository
16          uses: actions/checkout@v4.2.0
```

Background

- GitHub Actions
  - Continuous Integration & Deployment system
  - Reusable components called "Actions"
  - Versioned using git refs



Background

- GitHub Actions
  - Continuous Integration & Deployment system
  - Reusable components called "Actions"
  - Versioned using git refs

Background

- GitHub Actions
  - Continuous Integration & Deployment system
  - Reusable components called "Actions"
  - Versioned using git refs

Background

- GitHub Actions
  - Continuous Integration system
  - Reusable components called "Actions"
  - Versioned using git refs *(branch name, git tag, commit sha)*
  - Fetched at runtime

```
16          uses: actions/checkout@v4.2.0
```

Background

- GitHub Actions
  - Continuous Integration system
  - Reusable components called "Actions"
  - Versioned using git refs *(branch name, git tag, commit sha)*
  - Fetched at runtime
- Risks
  - Branch names and git tags are mutable (*ref confusion*)

chains-project/ghasum#143

Background

- GitHub Actions
  - Continuous Integration system
  - Reusable components called "Actions"
  - Versioned using git refs *(branch name, git tag, commit sha)*
  - Fetched at runtime
- Risks
  - Branch names and git tags are mutable (*ref confusion*)
  - Network commits can be used (*imposter commit*)

chains-project/ghasum#143

Background

- GitHub Actions
  - Continuous Integration system
  - Reusable components called "Actions"
  - Versioned using git refs *(branch name, git tag, commit sha)*
  - Fetched at runtime
- Risks
  - Branch names and git tags are mutable (*ref confusion*)
  - Network commits can be used (*imposter commit*)
  - SHA1 hash collisions (SHAttered, SHAmbles)

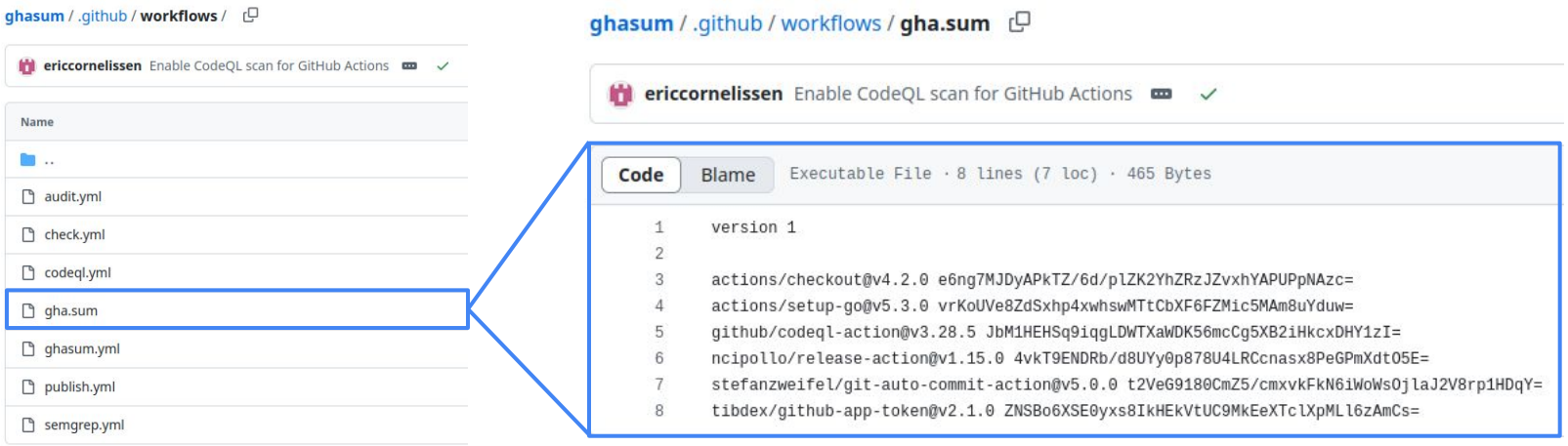
Background

- GitHub Actions
  - Continuous Integration system
  - Reusable components called "Actions"
  - Versioned using git refs *(branch name, git tag, commit sha)*
  - Fetched at runtime
- Risks
  - Branch names and git tags are mutable (*ref confusion*)
  - Network commits can be used (*imposter commit*)
  - SHA1 hash collisions (SHAttered, SHAmbles)
  - Transitive and unpinnable actions

chains-project/ghasum#49

Tool Description

- Proper (SHA256) checksums for your GitHub Actions
- Better guarantees about what your CI is running
- Build using the libraries behind `go.sum`



Tool Benefits

- Checksums for branch and tag refs
- Network commits are disallowed
- Stronger checksum algorithm

Demo

Roadmap

- Support checking integrity during CI runs (#4)
- Configurable hash algorithm (#5)
- Transitive pinning for composite Actions (#49 → #209)
- Update checksums when updating Actions (#9)

Roadmap

- Support checking integrity during CI runs (#4)
- Configurable hash algorithm (#5)
- Transitive pinning for composite Actions (#49 → #209)
- Update checksums when updating Actions (#9)
- Suggestions…? Open an issue! *(after checking for duplicates)*

Takeaways

- `ghasum` > commit hash > tag ref > branch ref
  - Immutable actions?
- Checksums require configurable hashes
  - See also npm/rfcs#757
- Trust?
  - Checksum: today is the same as yesterday
  - Reproducible: I have the same as you
    - github.com/ericcornelissen/reproducing-actions

`ghasum` can be adopted today (but it's a bit rough)

ghasum

github.com/chains-project/ghasum

Eric Cornelissen (ericco@kth.se)