Agenda

- topic 1
- topic 2
- topic 3
- topic 4
- topic 5
- topic 6
- topic 7
- topic 8

OCI Refers

Brandon Mitchell
Twitter: @sudo_bmitch
GitHub: sudo-bmitch

```
$ whoami
- Brandon Mitchell
- Solutions Architect @ BoxBoat
- Docker Captain
- StackOverflow, OCI, CNCF
```

OCI Images

Image Config

```
$ regctl blob get localhost:5000/library/golang \
  sha256:505a511fa01d77d70aea3023014a0628c41111566ae907ec3a945294f691980b | jq .
{
  "created": "2022-08-23T20:07:38.575765178Z",
  "architecture": "amd64",
  "os": "linux",
  "config": {
    "Env": [
      "PATH=/go/bin:/usr/local/go/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin",
      "GOLANG_VERSION=1.19",
      "GOPATH=/go"
    ],
    "Cmd": [
      "bash"
    ],
    "WorkingDir": "/go"
  },
  "history": [
    {
      "created": "2022-08-23T00:20:40.144281895Z",
      "created_by": "/bin/sh -c #(nop) ADD file:6944d322f4c04bd2192061822af5cbec8ac0a6b4... in / "
    },
...
```

Layer

```
$ regctl blob get localhost:5000/library/golang \
  sha256:1671565cc8df8c365c9b661d3fbc164e73d01f1b0430c6179588428f99a9da2e | \
  tar -tvzf - | head -15
drwxr-xr-x 0/0               0 2022-08-21 20:00 bin/
-rwxr-xr-x 0/0         1234376 2022-03-27 14:40 bin/bash
-rwxr-xr-x 0/0           43936 2020-09-24 04:36 bin/cat
-rwxr-xr-x 0/0           72672 2020-09-24 04:36 bin/chgrp
-rwxr-xr-x 0/0           64448 2020-09-24 04:36 bin/chmod
-rwxr-xr-x 0/0           72672 2020-09-24 04:36 bin/chown
-rwxr-xr-x 0/0          151168 2020-09-24 04:36 bin/cp
-rwxr-xr-x 0/0          125560 2020-12-10 08:23 bin/dash
-rwxr-xr-x 0/0          113664 2020-09-24 04:36 bin/date
-rwxr-xr-x 0/0           80968 2020-09-24 04:36 bin/dd
-rwxr-xr-x 0/0           93936 2020-09-24 04:36 bin/df
-rwxr-xr-x 0/0          147176 2020-09-24 04:36 bin/dir
-rwxr-xr-x 0/0           84440 2022-01-20 15:10 bin/dmesg
lrwxrwxrwx 0/0               0 2019-11-07 06:31 bin/dnsdomainname -> hostname
lrwxrwxrwx 0/0               0 2019-11-07 06:31 bin/domainname -> hostname
```

Manifest

```
$ regctl manifest get localhost:5000/library/golang:1.19.0 \
  --platform linux/amd64 --format body | jq .
{
  "schemaVersion": 2,
  "mediaType": "application/vnd.docker.distribution.manifest.v2+json",
  "config": {
    "mediaType": "application/vnd.docker.container.image.v1+json",
    "size": 7085,
    "digest": "sha256:505a511fa01d77d70aea3023014a0628c41111566ae907ec3a945294f691980b"
  },
  "layers": [
    {
      "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip",
      "size": 55007555,
      "digest": "sha256:1671565cc8df8c365c9b661d3fbc164e73d01f1b0430c6179588428f99a9da2e"
    },
    {
      "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip",
      "size": 5163019,
      "digest": "sha256:3e94d13e55e7a4ef17ff21376f57fb95c7e1706931f8704aa99260968d81f6e4"
...
]}
```

Index

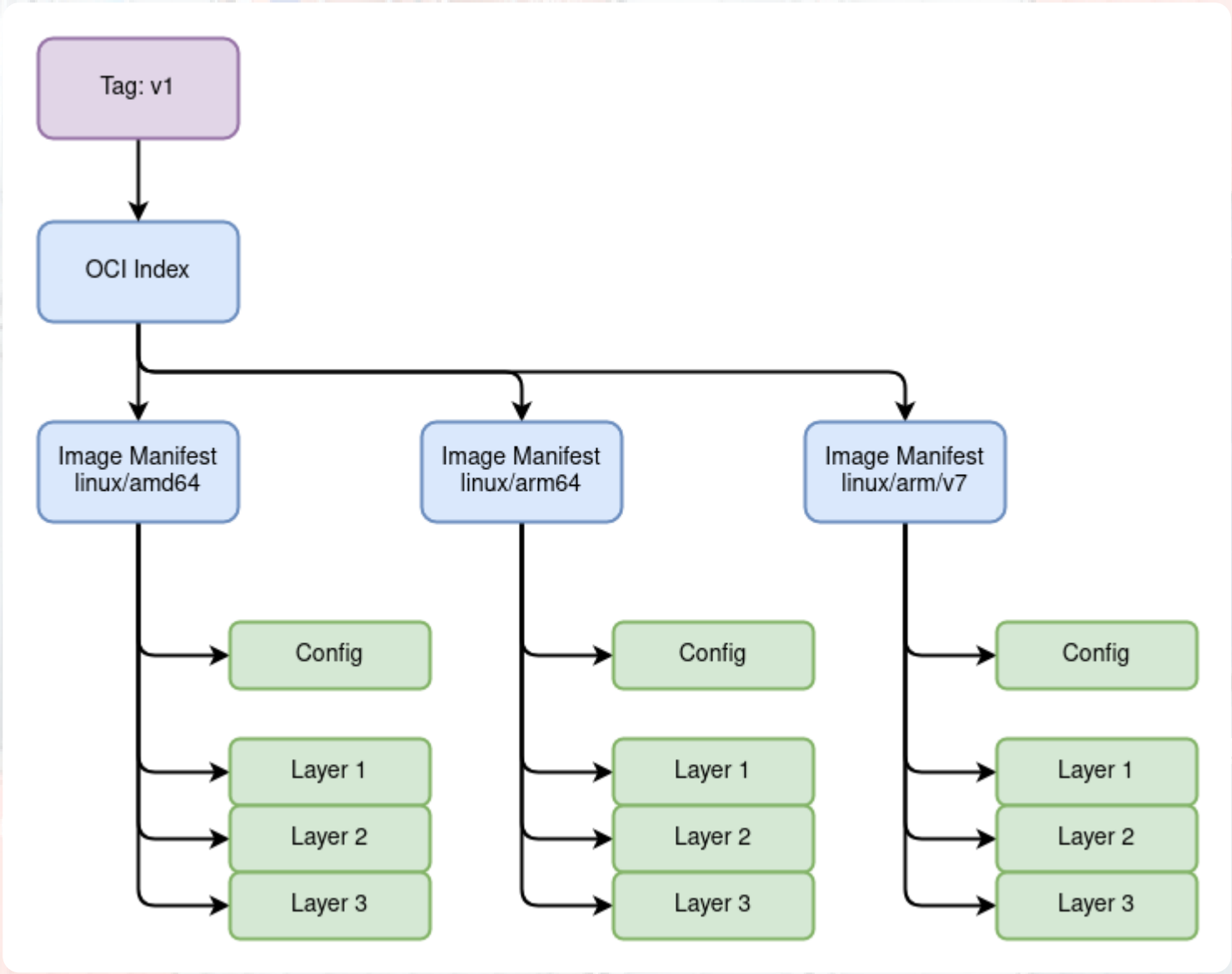
```
$ regctl manifest get localhost:5000/library/golang:1.19.0 --format body | jq .
{
  "manifests": [
    {
      "digest": "sha256:4c00329e17be6fedd8bd4412df454a205348da00f9e0e5d763380a29eb096b75",
      "mediaType": "application/vnd.docker.distribution.manifest.v2+json",
      "platform": {
        "architecture": "amd64",
        "os": "linux"
      },
      "size": 1796
    },
    {
      "digest": "sha256:5cd53f75e749fef8e85726357cbc7765cdb1a86dad3f2d4fccfaff9307f35a32",
      "mediaType": "application/vnd.docker.distribution.manifest.v2+json",
      "platform": {
        "architecture": "arm64",
        "os": "linux",
        "variant": "v8"
      },
      "size": 1796
    },
...
```

Content Addressable

```
$ regctl manifest get --format body \
  localhost:5000/library/golang@sha256:4c00329e17be6fedd8bd4412df454a205348da00f9e0e5d7633...6b75 |
  sha256sum
4c00329e17be6fedd8bd4412df454a205348da00f9e0e5d7633...6b75  -

$ regctl blob get localhost:5000/library/golang \
  sha256:505a511fa01d77d70aea3023014a0628c41111566ae907ec3a945294f691980b | \
  sha256sum
505a511fa01d77d70aea3023014a0628c41111566ae907ec3a945294f691980b  -

$ regctl blob get localhost:5000/library/golang \
  sha256:1671565cc8df8c365c9b661d3fbc164e73d01f1b0430c6179588428f99a9da2e | \
  sha256sum
1671565cc8df8c365c9b661d3fbc164e73d01f1b0430c6179588428f99a9da2e  -
```


Tag: v1
OCI Index
Image Manifest
linux/amd64
Image Manifest
linux/arm64
Image Manifest
linux/arm/v7
Config
Layer 1
Layer 2
Layer 3
Config
Layer 1
Layer 2
Layer 3
Config
Layer 1
Layer 2
Layer 3

Not Just Container Images

A Blob is a Blob

- Arbitrary data can be pushed to a blob
- Manifests must have a known media type
- Helm Charts
- Cosign Signatures
- FluxCD State

Helm Chart

```
$ regctl manifest get localhost:5000/helm-charts/spire/spire:0.0.5 --format body | jq .
{
  "schemaVersion": 2,
  "config": {
    "mediaType": "application/vnd.cncf.helm.config.v1+json",
    "digest": "sha256:23b5b19b695d822e7c1e6e1bd17d49ec768ab4b4f71aeb7d20f0b378f6257298",
    "size": 139
  },
  "layers": [
    {
      "mediaType": "application/vnd.cncf.helm.chart.content.v1.tar+gzip",
      "digest": "sha256:ae2ef52c768449e51474033431f5c974a03d89278f89de0ed24f8b08d24f8447",
      "size": 6589
    }
  ]
}
```

Helm Chart

```
$ regctl blob get localhost:5000/helm-charts/spire/spire \
  sha256:23b5b19b695d822e7c1e6e1bd17d49ec768ab4b4f71aeb7d20f0b378f6257298 | \
  jq .
{
  "name": "spire",
  "version": "0.0.5",
  "description": "A Helm chart for Kubernetes",
  "apiVersion": "v2",
  "appVersion": "1.16.0",
  "type": "application"
}
```

Helm Chart

```
$ regctl blob get localhost:5000/helm-charts/spire/spire \
  sha256:ae2ef52c768449e51474033431f5c974a03d89278f89de0ed24f8b08d24f8447 | \
  tar -tvzf -
-rw-r--r-- 0/0             120 2022-03-17 17:51 spire/Chart.yaml
-rw-r--r-- 0/0            2657 2022-03-17 17:51 spire/values.yaml
-rw-r--r-- 0/0              24 2022-03-17 17:51 spire/templates/NOTES.txt
-rw-r--r-- 0/0            1786 2022-03-17 17:51 spire/templates/_helpers.tpl
-rw-r--r-- 0/0             325 2022-03-17 17:51 spire/templates/agent-account.yaml
-rw-r--r-- 0/0             866 2022-03-17 17:51 spire/templates/agent-cluster-role.yaml
-rw-r--r-- 0/0            1333 2022-03-17 17:51 spire/templates/agent-configmap.yaml
-rw-r--r-- 0/0            3609 2022-03-17 17:51 spire/templates/agent-daemonset.yaml
-rw-r--r-- 0/0             150 2022-03-17 17:51 spire/templates/bundle-configmap.yaml
-rw-r--r-- 0/0            1974 2022-03-17 17:51 spire/templates/client-deployment.yaml
-rw-r--r-- 0/0             728 2022-03-17 17:51 spire/templates/oidc-dp-configmap.yaml
-rw-r--r-- 0/0            2956 2022-03-17 17:51 spire/templates/oidc-ingress.yaml
-rw-r--r-- 0/0             890 2022-03-17 17:51 spire/templates/oidc-nginx-configmap.yaml
-rw-r--r-- 0/0             628 2022-03-17 17:51 spire/templates/oidc-service.yaml
-rw-r--r-- 0/0             326 2022-03-17 17:51 spire/templates/server-account.yaml
-rw-r--r-- 0/0            1008 2022-03-17 17:51 spire/templates/server-cluster-role.yaml
-rw-r--r-- 0/0            2006 2022-03-17 17:51 spire/templates/server-configmap.yaml
...
```

Working Group

The Problem

- Many artifacts reference an image
- Images a content addressable, we don't want to change the digest
- Signatures are on a digest, so that cannot be embedded in the thing being signed
- How do we associate additional data with an images?

The Goals

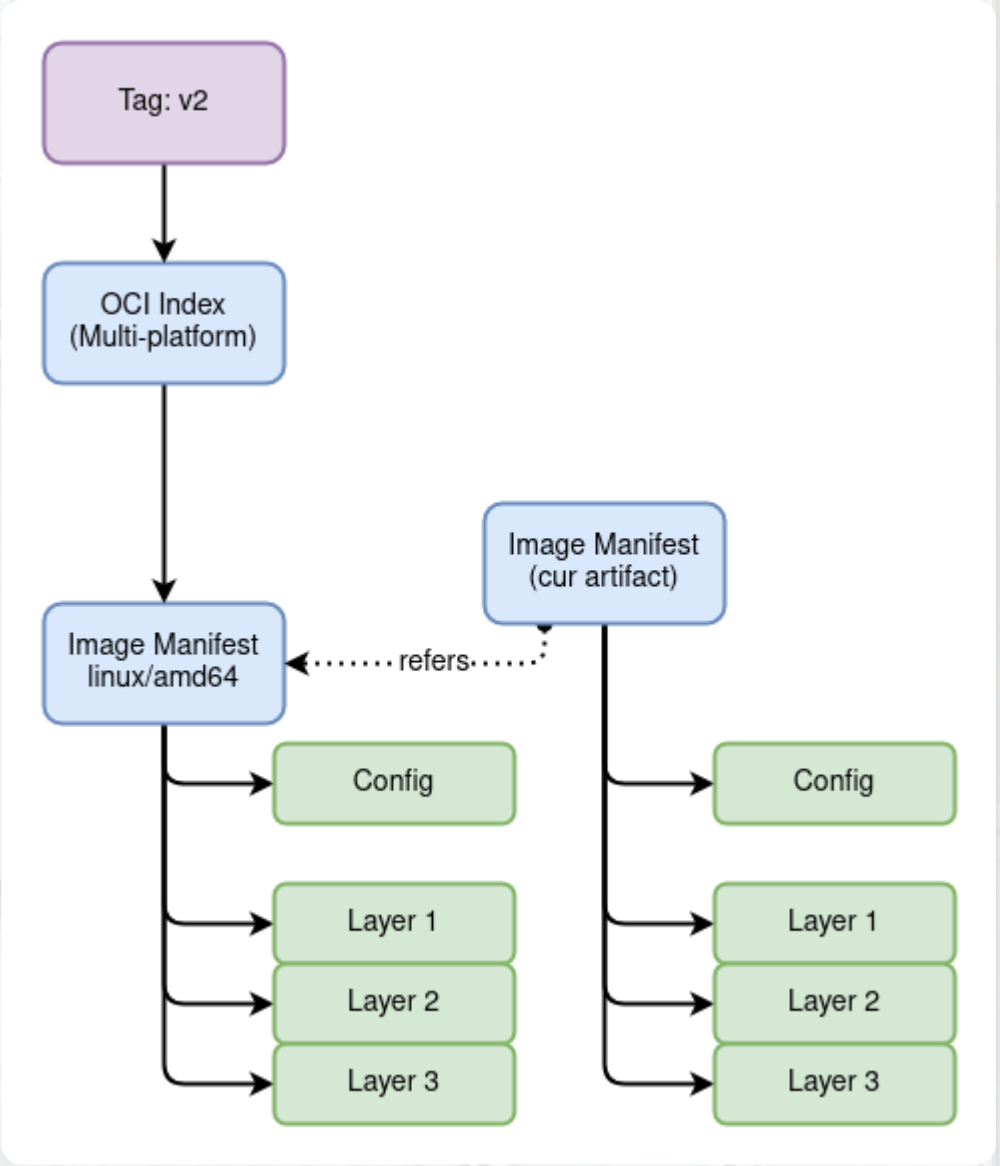
- Extend an existing image with new metadata
- Able to copy between registries
- Able to find a specific artifact from a list easily
- Minimize API calls
- Backwards compatibility

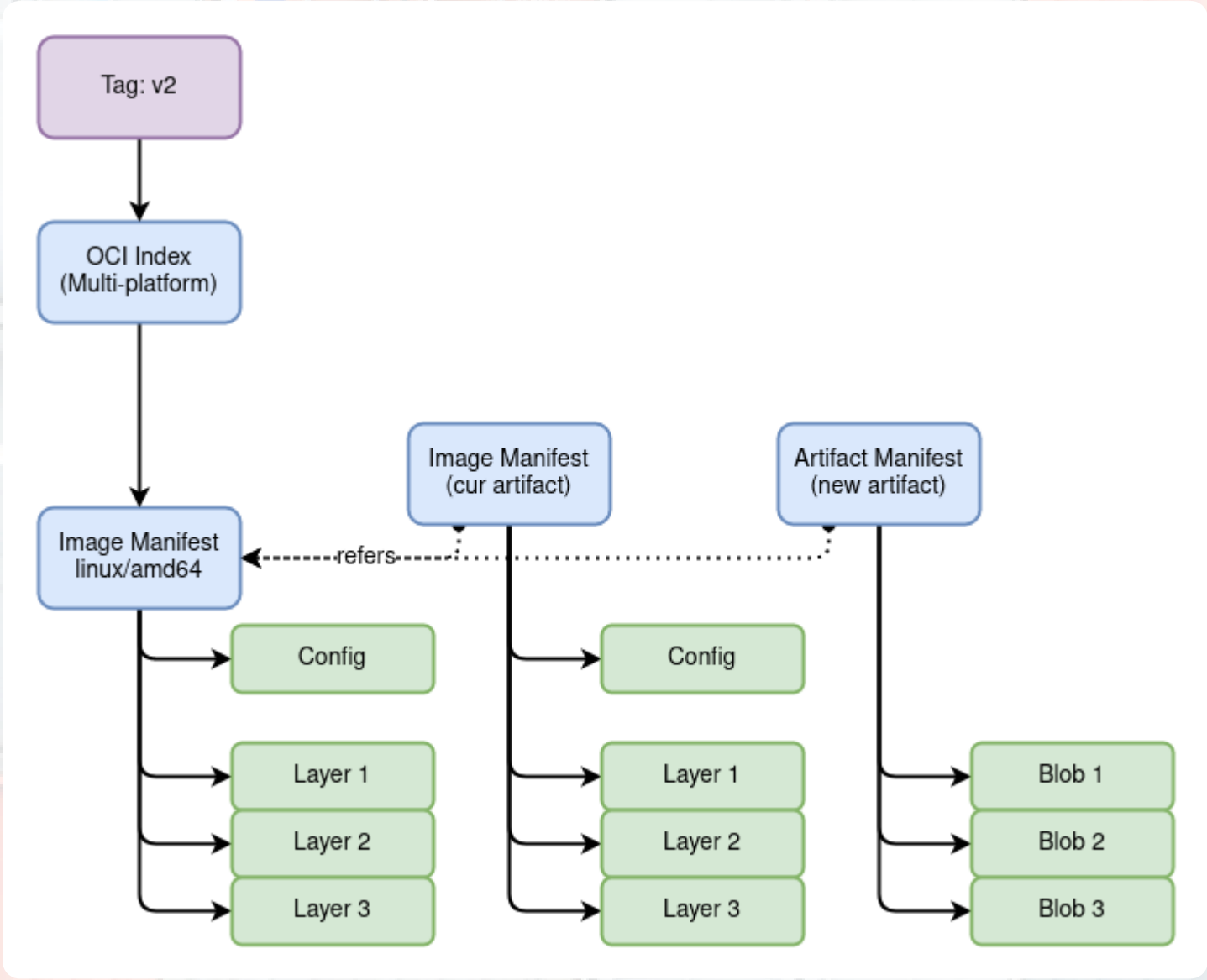
The Solution

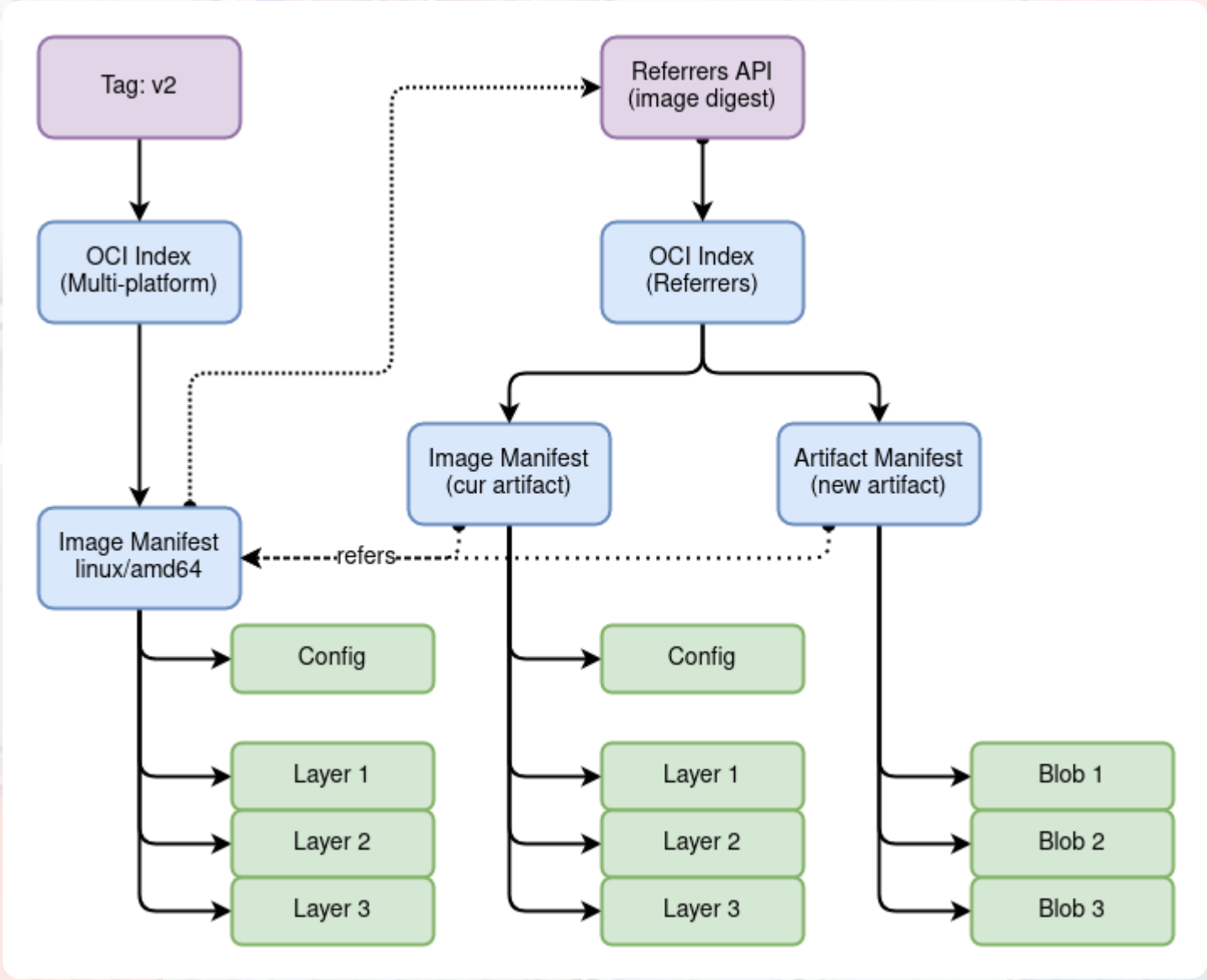
- Add a new `refers` field
  - An artifact manifest will have a `refers` that points to an image
- Add a new API to list the referrers
  - When pulling an image, you can list all artifact manifests with a `refers` pointing to it
  - Response is an OCI Index (list of manifests)
- Each entry in the referrers list includes data from the artifact manifest
  - Artifact Type and Annotations
  - Clients can filter for specific entries to minimize artifact pulls

New Artifact Manifest

- Artifacts today are pushed with the Image manifest
- Removed the config descriptor
- Config mediaType => artifactType
- Ordered Layers => Optional Blob List


Tag: v2
OCI Index
(Multi-platform)
Image Manifest
(cur artifact)
Image Manifest
linux/amd64
refers
Config
Config
Layer 1
Layer 2
Layer 3
Layer 1
Layer 2
Layer 3


Tag: v2
OCI Index
(Multi-platform)
Image Manifest
linux/amd64
refers
Image Manifest
(cur artifact)
Artifact Manifest
(new artifact)
Config
Layer 1
Layer 2
Layer 3
Config
Layer 1
Layer 2
Layer 3
Blob 1
Blob 2
Blob 3


Tag: v2
Referrers API
(image digest)
OCI Index
(Multi-platform)
OCI Index
(Referrers)
Image Manifest
(cur artifact)
Artifact Manifest
(new artifact)
Image Manifest
linux/amd64
refers
Config
Config
Layer 1
Layer 2
Layer 3
Layer 1
Layer 2
Layer 3
Blob 1
Blob 2
Blob 3

Backwards Compatibility

- Registries reject unknown manifests and won't have the new API
- Continue using image manifests for some time
- If the API isn't available, clients maintain the same Index using a well known tag
- API is useful to avoid race conditions, bad clients, and GC

Container Security

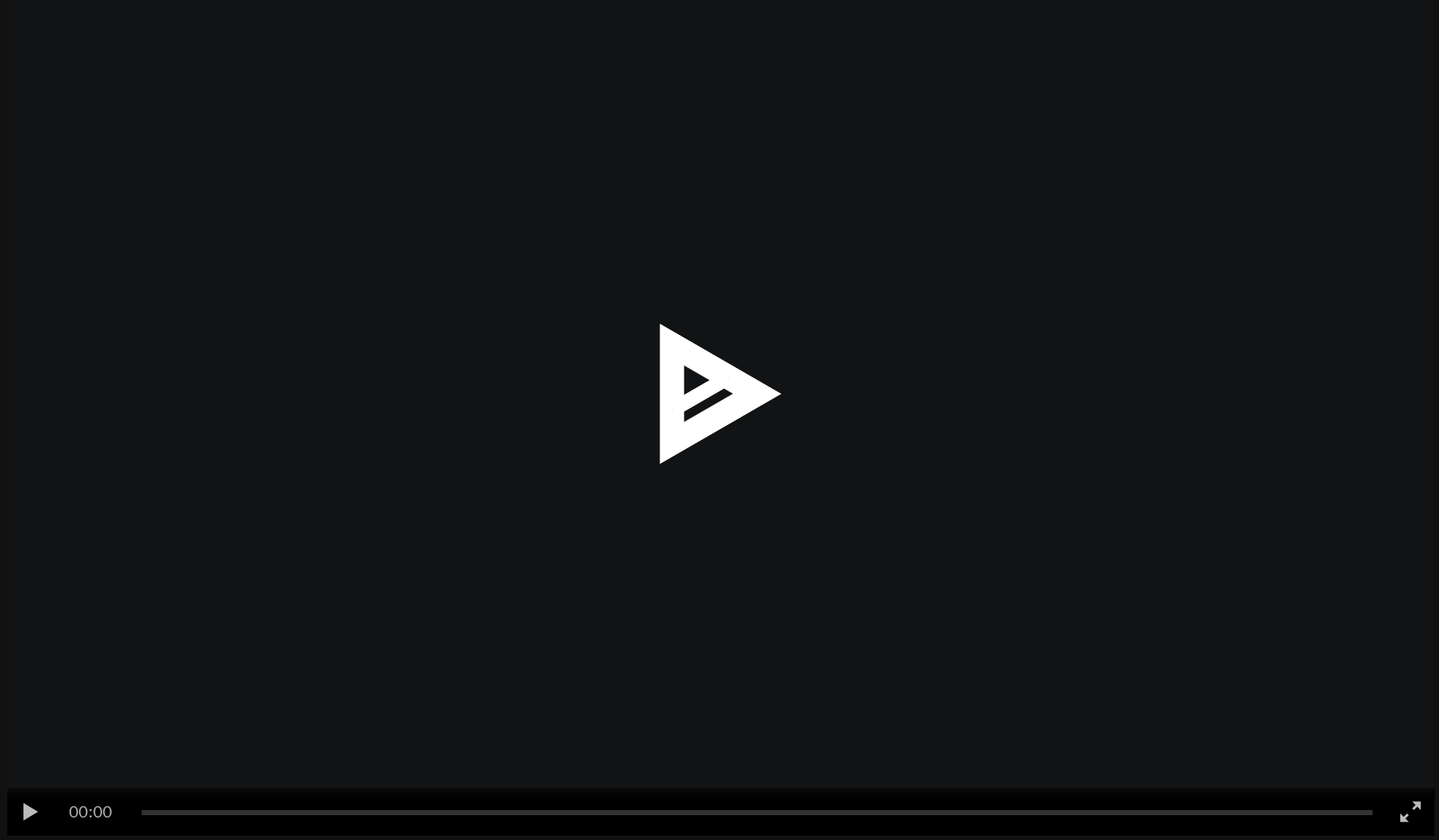
- Package signatures and SBOMs with the image
- Copy those artifacts with the image between registries
- Add your own artifacts to an image on your registry without changing the digest
- Package additional metadata like build attestations and reproducibility information

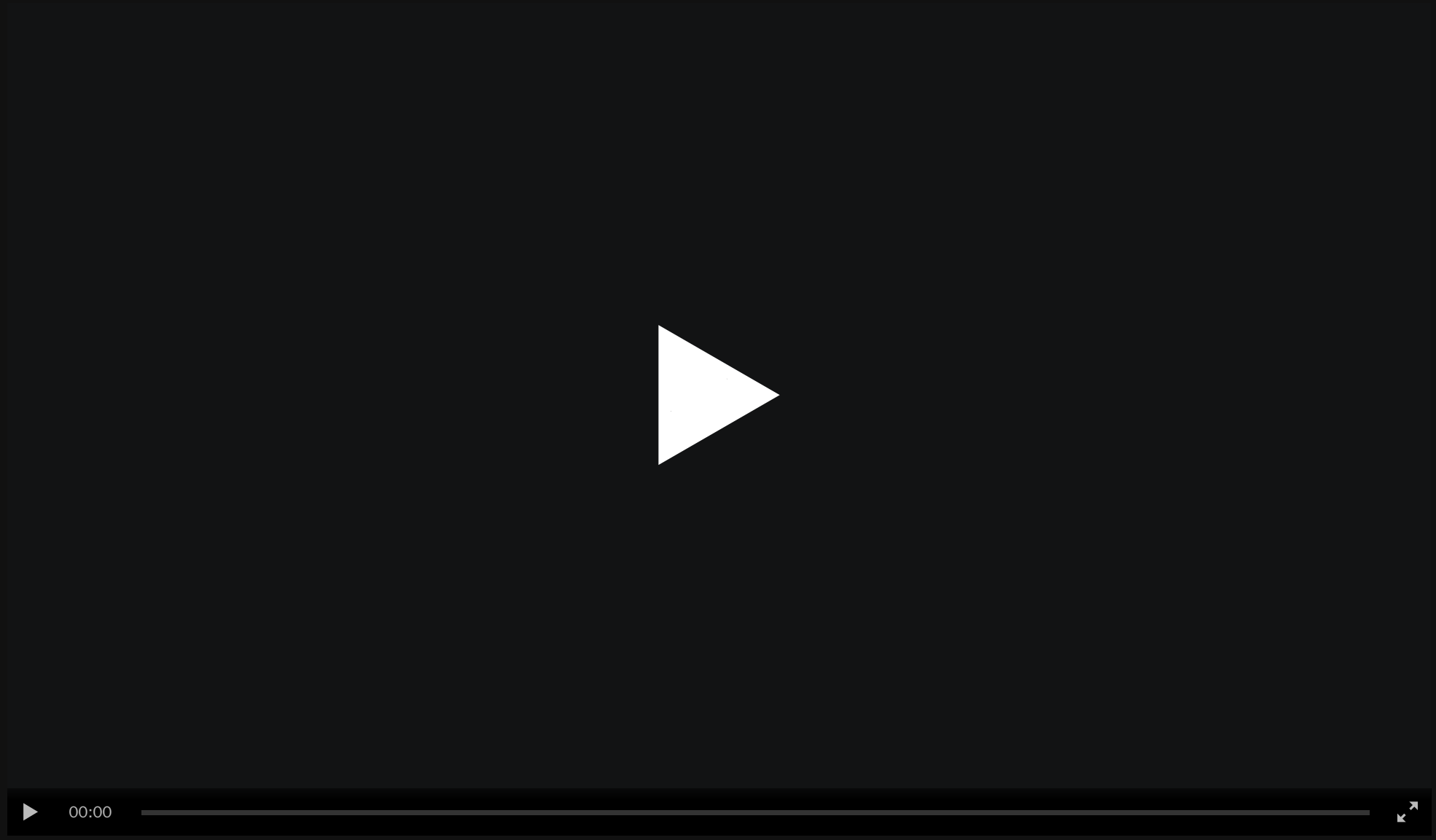
regclient

regclient

- `regclient` : Go library for registry clients
- `regsync` : copy images between registries for mirrors
- `regbot` : create automations with Lua scripts (retention policies)
- `regctl` : CLI interface to `regclient`
  - Shipped as a binary, container, and GHA
  - querying a registry (fetch a digest, list tags)
  - copy/retag an image
  - export/import images using OCI Layout
  - delete tags or manifests
  - modify images
  - push/list/pull artifacts

Demo


00:00


00:00

Wrapping Up

Summary

- Registries can store anything in a blob
- We can associate artifacts with our image
- We can copy them together and extend existing images
- The refers listing includes enough details to select an artifact

Gotchas

- The standard isn't tagged yet
- Tooling hasn't been updated to support this
- Registries need to be updated

Thank You

github.com/sudo-bmitch/presentations

Brandon Mitchell
Twitter: @sudo_bmitch
GitHub: sudo-bmitch