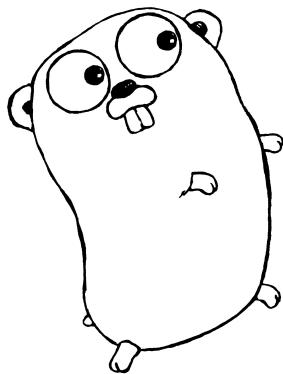


# Go Module Proxy

## Life of a Query



Katie Hockman, Google  
Go Open Source  
[github.com/katiehockman](https://github.com/katiehockman)  
[@katie\\_hockman](https://twitter.com/katie_hockman)



[github.com/katiehockman/puppies](https://github.com/katiehockman/puppies)







1. Non-reproducible builds
2. Disappearing source code
3. Dangerous downloads

# Some things we might consider

- Don't have any dependencies
- Vendors
- Do nothing

# Better solutions

- |                            |                      |
|----------------------------|----------------------|
| 1. Reproducible builds     | Modules              |
| 2. Persistent dependencies | Mirror               |
| 3. Trustworthy fetches     | Checksum<br>Database |

# 1. Modules



`github.com/katiehockman/puppies`

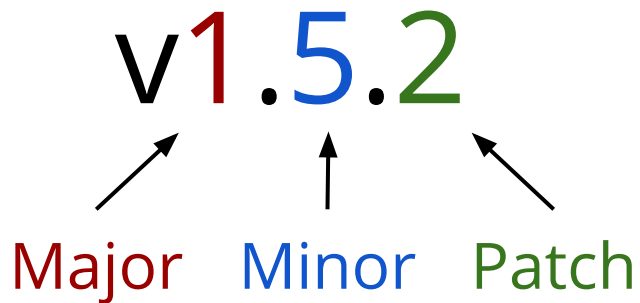
`package walk`

`package bark`

`package toys`

# Semantic versioning

v1.5.2



Major Minor Patch

The diagram illustrates the components of the semantic versioning string 'v1.5.2'. The 'v' is in black. The '1' is red, the '5' is blue, and the '2' is green. Below the string, the labels 'Major', 'Minor', and 'Patch' are written in red, blue, and green respectively. Arrows point from each label to its corresponding digit: from 'Major' to '1', from 'Minor' to '5', and from 'Patch' to '2'.

# go.mod

```
module github.com/katiehockman/puppies

require (
    github.com/go-sql-driver/mysql v1.4.1
    go.opencensus.io v0.19.2
    golang.org/x/crypto v0.0.0-20190308221718-c2843e01d9a2
)
```

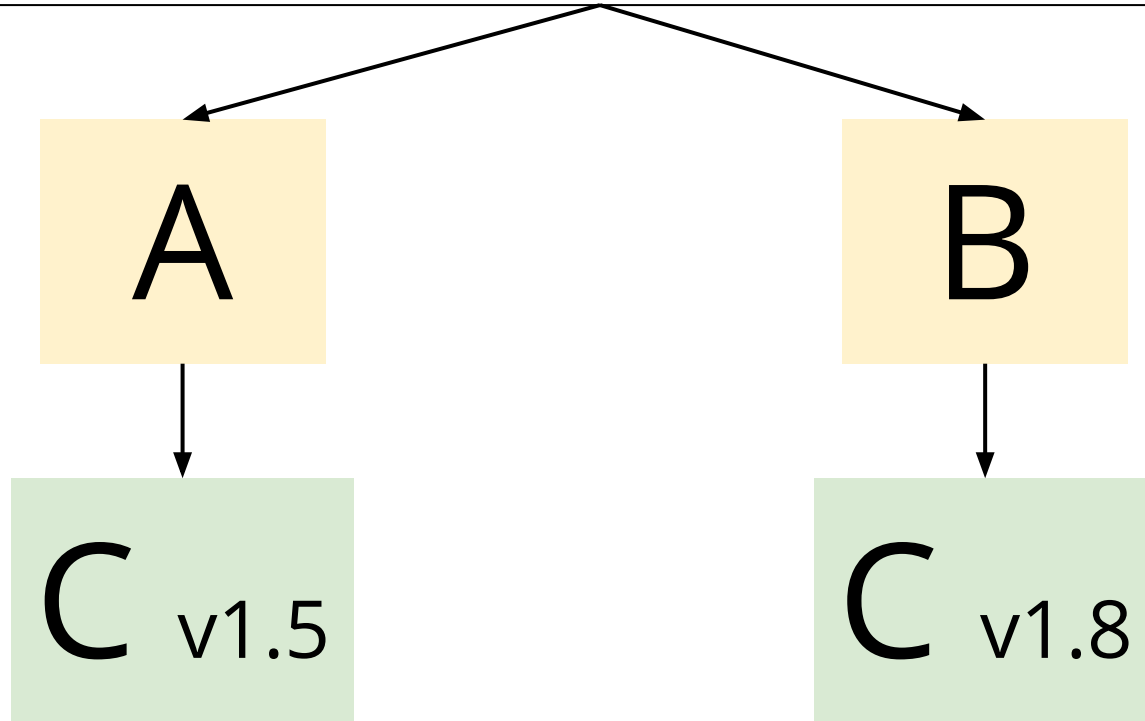
# go.mod

```
module github.com/katiehockman/puppies

require (
    github.com/go-sql-driver/mysql v1.4.1
    go.opencensus.io v0.19.2
    golang.org/x/crypto v0.0.0-20190308221718-c2843e01d9a2
)
```

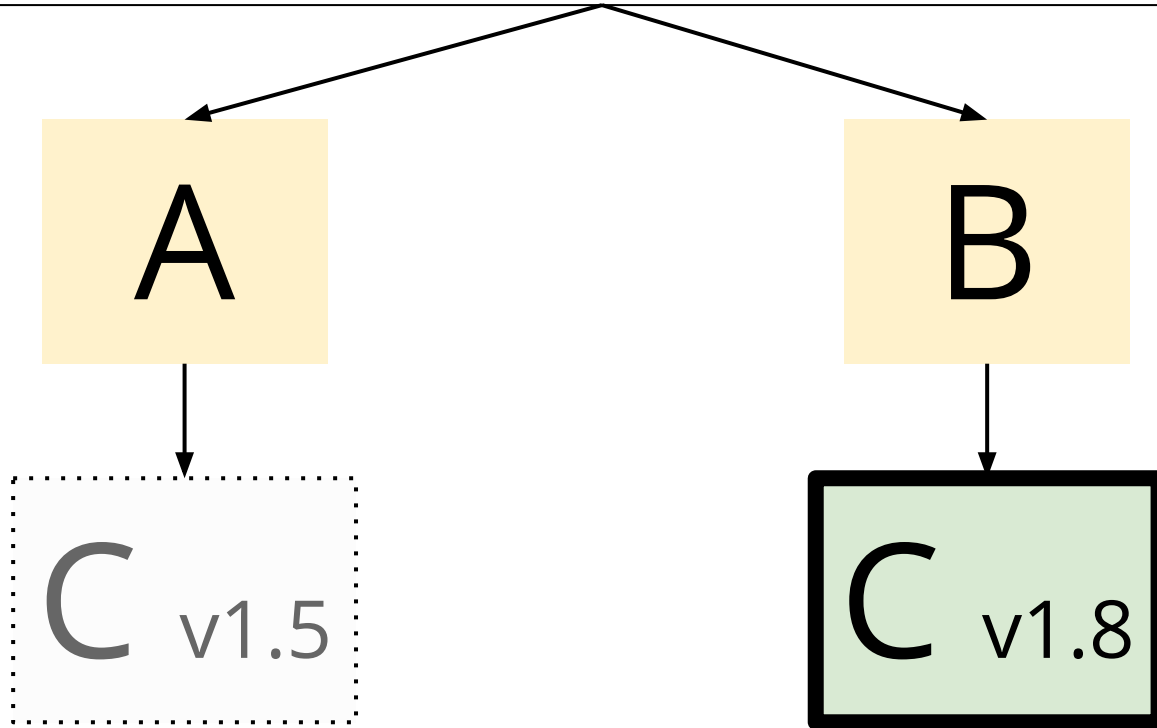
# Minimal version selection

`github.com/katiehockman/puppies`





`github.com/katiehockman/puppies`



Modules

# Better solutions

✓ Reproducible builds

Modules

2. Persistent dependencies

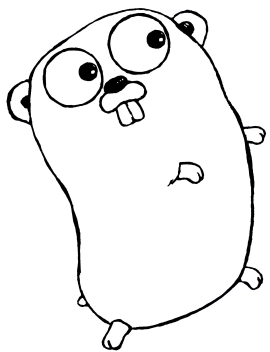
Mirror

3. Trustworthy fetches

Checksum  
Database

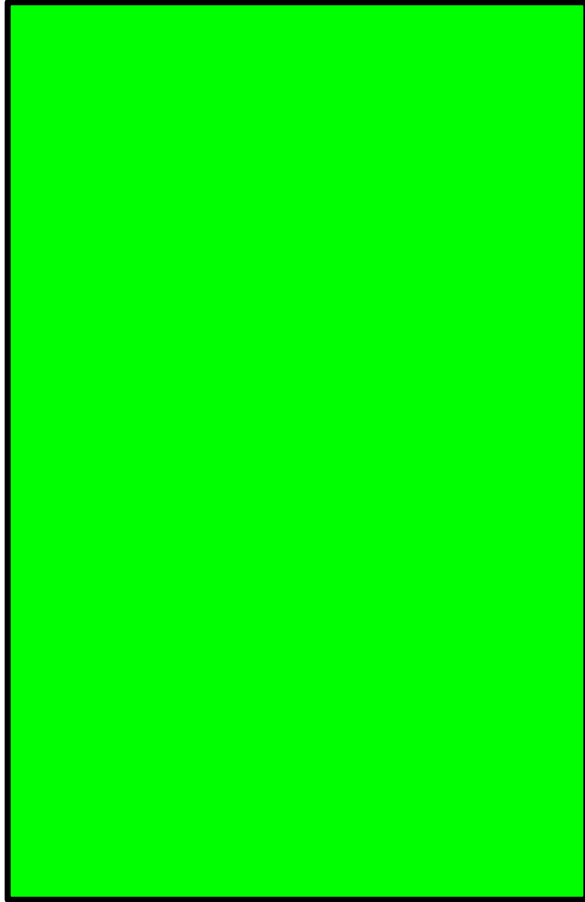
## 2. Mirror

Mirror = module proxy (+ caching)



Origin server  
(ie. GitHub)

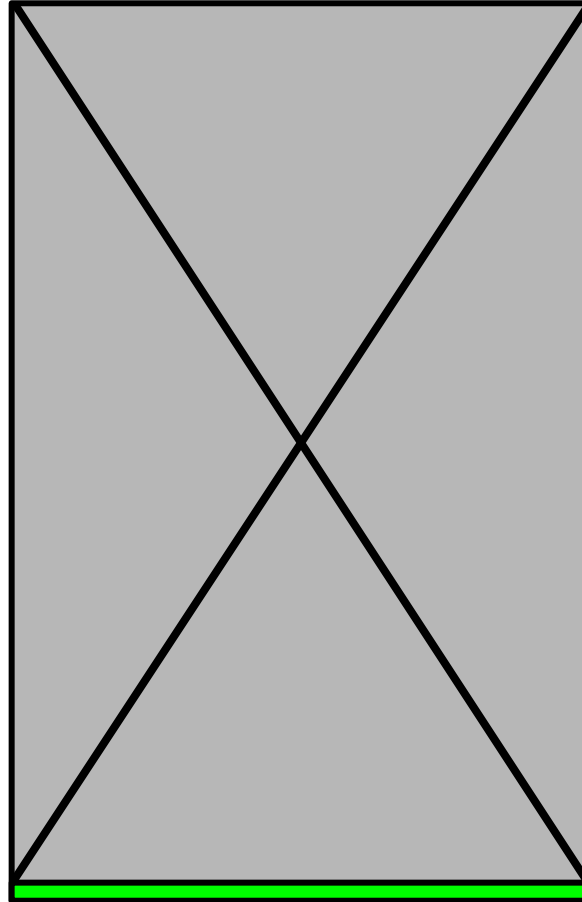
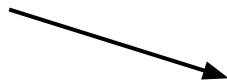
go command



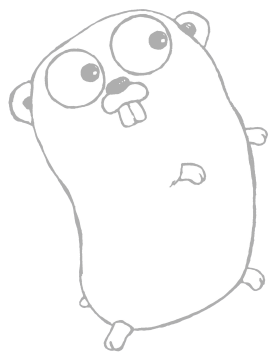
Mirror



what it actually  
needs



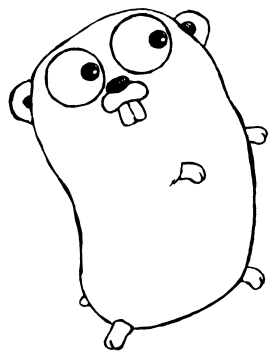
Mirror



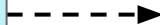
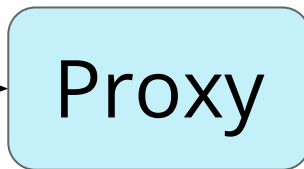
go command



Origin server  
(ie. GitHub)

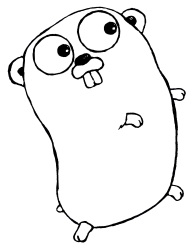


go command

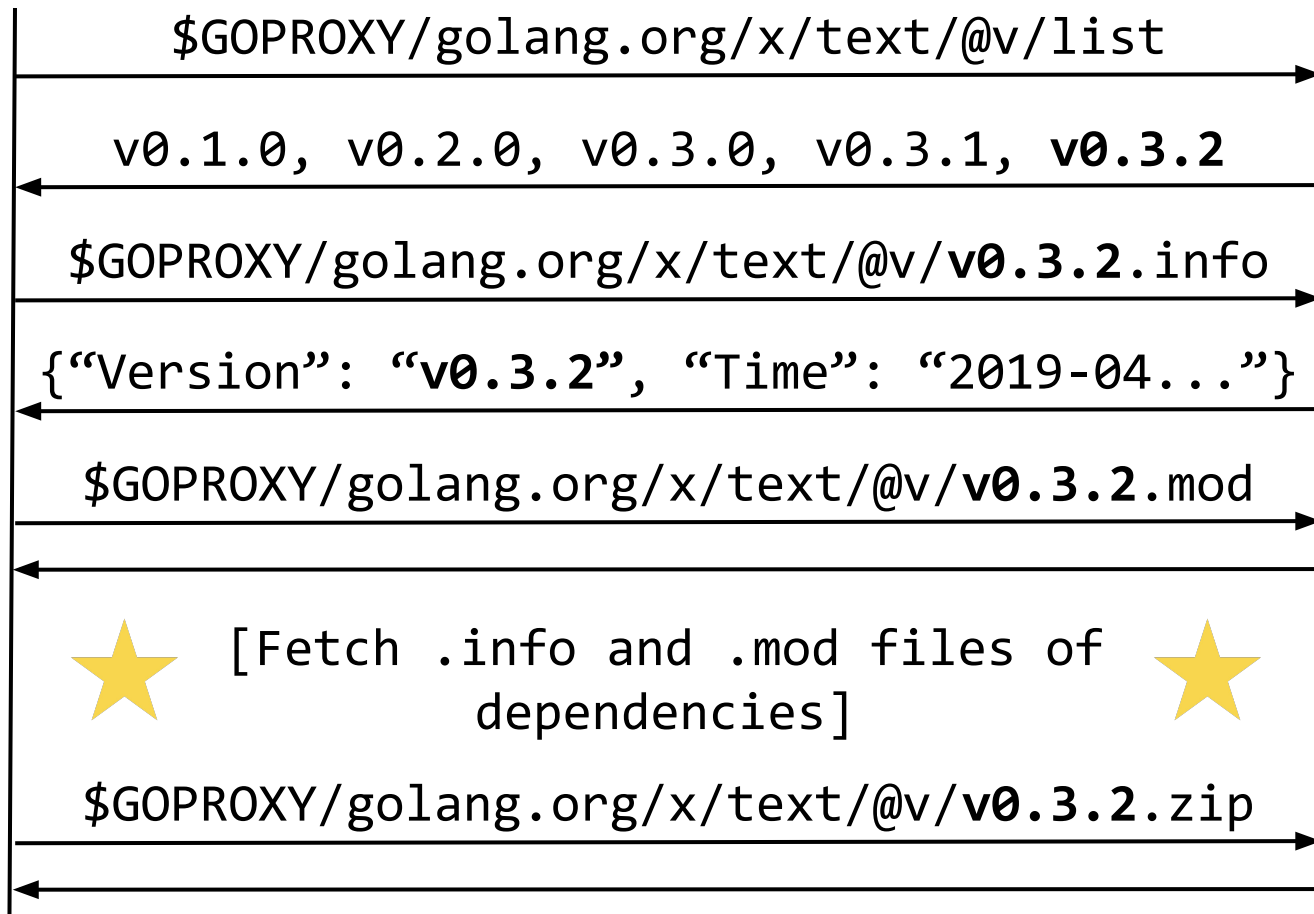


Origin server  
(ie. GitHub)

```
go get golang.org/x/text
```



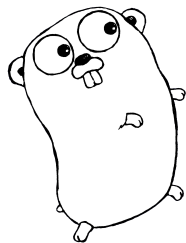
go  
command



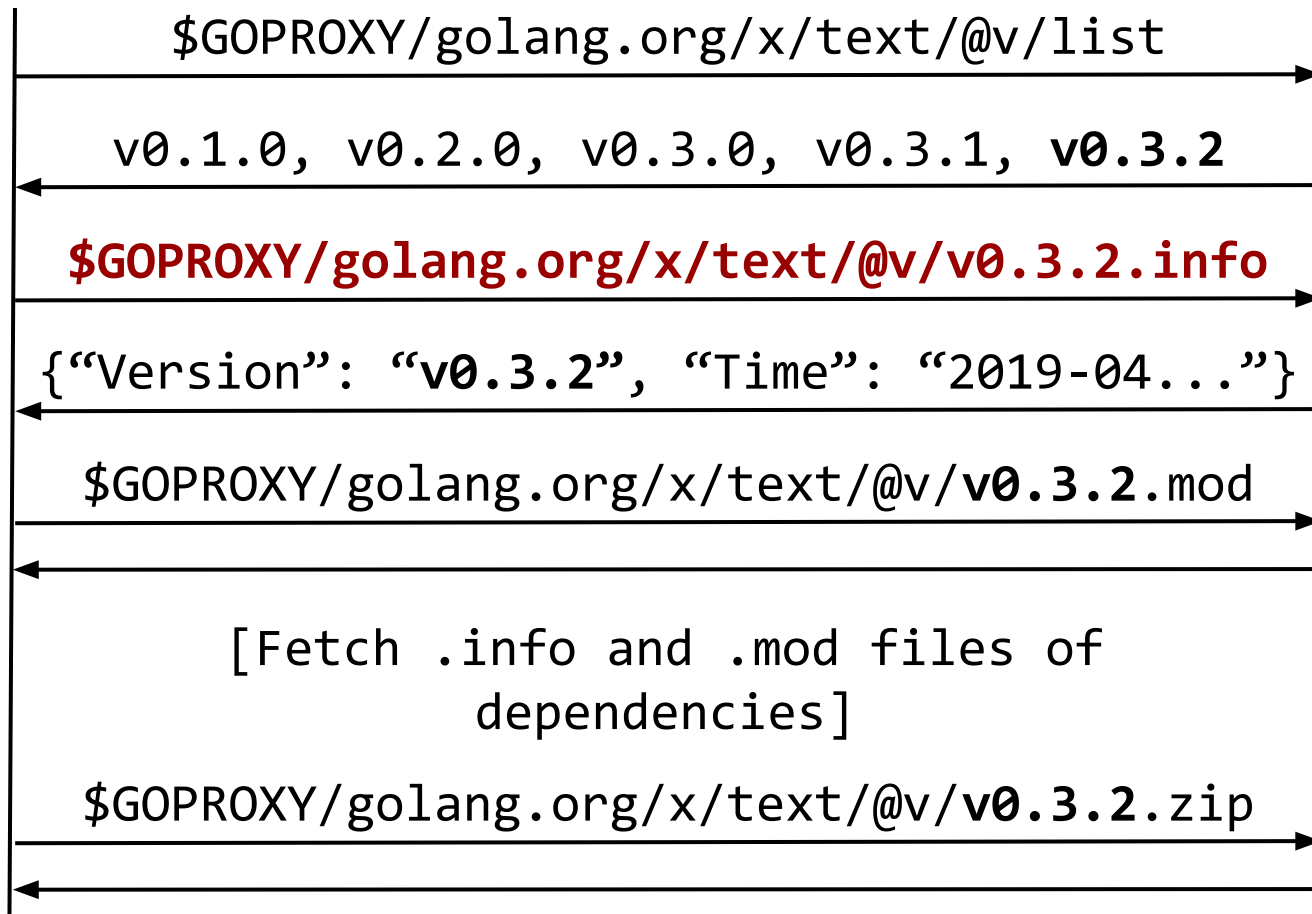
Proxy

Mirror

```
go get golang.org/x/text
```



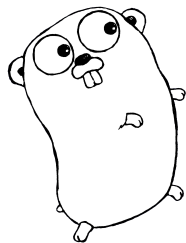
go  
command



Proxy

Mirror

```
go get golang.org/x/text@master
```



go  
command

`$GOPROXY/golang.org/x/text@master.info`

`{"Version": "v0.3.2-0.20190426035018", ...}`

`$GOPROXY/golang.org/x/text/@v/v0.3.2..mod`

...

Proxy

Mirror

# Proxy spec (go help goproxy)

GET `$GOPROXY/<module>/@v/list` returns a list of all known versions of the given module

GET `$GOPROXY/<module>/@v/<version>.info` returns JSON metadata about that version of the given module.

GET `$GOPROXY/<module>/@v/<version>.mod`

GET `$GOPROXY/<module>/@v/<version>.zip`



Why use a mirror?

- ✓ No more disappearing dependencies

# Why use a mirror?

# Why use a mirror?

- ✓ No more disappearing dependencies
- ✓ Faster downloads

## Why use a mirror?

- ✓ No more disappearing dependencies
- ✓ Faster downloads
- ✓ Less storage use

## Why use a mirror?

- ✓ No more disappearing dependencies
- ✓ Faster downloads
- ✓ Less storage use
- ✓ No more VCS tools required

# Better solutions

✓ Reproducible builds

Modules

✓ Persistent dependencies

Mirror

3. Trustworthy fetches

Checksum  
Database



### 3. Checksum Database

The (very) old way... direct HTTPS

The (less) old way... go.sum files

# go.sum for github.com/katiehockman/puppies

**github.com/go-sql-driver/mysql v1.4.1 h1:g24URVg00FbNUTx9qq...**

**github.com/go-sql-driver/mysql v1.4.1/go.mod h1:zAC/RDZ24gD...**

**go.opencensus.io v0.19.2 h1:ZZpq6xI6kv/LuE/5s5UQvBU5vMjvRnP...**

**go.opencensus.io v0.19.2/go.mod h1:NO/8qkisMZLZ1FCsKNqtJPwc...**

**golang.org/x/crypto v0.0.0-20190325154230-a5d413f7728c h1:V...**

**golang.org/x/crypto v0.0.0-20190325154230-a5d413f7728c/go.mod**

## My module's go.sum file

```
github.com/go-sql-driver/mysql v1.4.1 h1:g24URVg00FbNUTx9  
github.com/go-sql-driver/mysql v1.4.1/go.mod h1:zAC/RDZ24gD  
go.opencensus.io v0.19.2 h1:ZZpq6xI6kvLuE5s5U  
go.opencensus.io v0.19.2/go.mod h1:NO/8qkisMZ
```

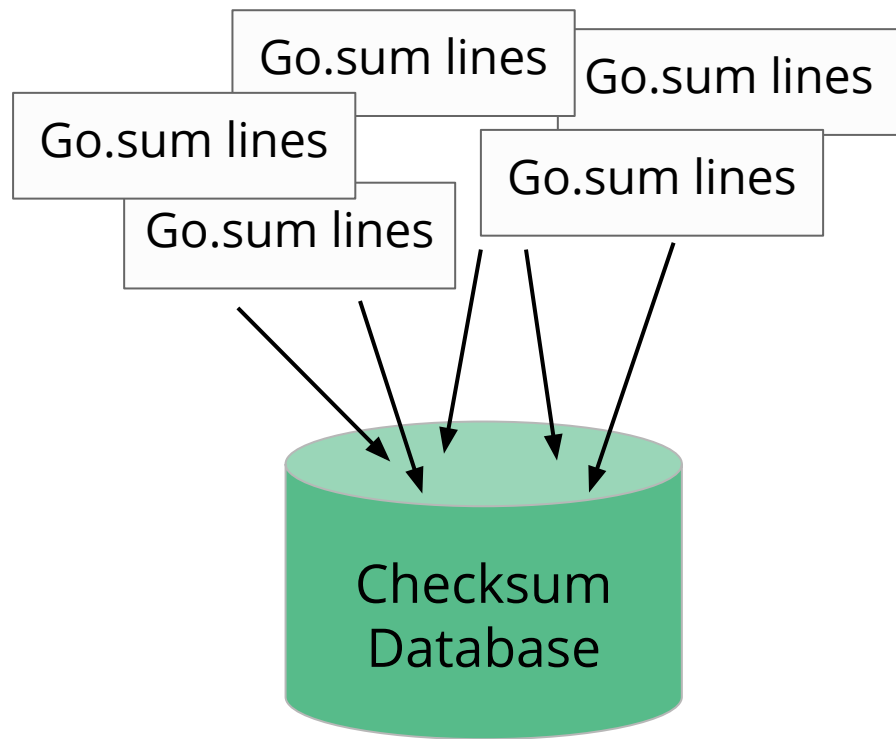
## Some other module's go.sum file

```
github.com/go-sql-driver/mysql v1.4.1 h1:g24URVg00FbNUTx9  
github.com/go-sql-driver/mysql v1.4.1/go.mod h1:zAC/RDZ24gD  
go.opencensus.io v0.19.2 h1:ABfk0xE3fdLeS8s3W  
go.opencensus.io v0.19.2/go.mod h1:HI/0dfjwDS
```

“Trust on *your* first use”

What about proxies?

The **new** way...



Checksum Database



# Who we trust

~~Origin server~~

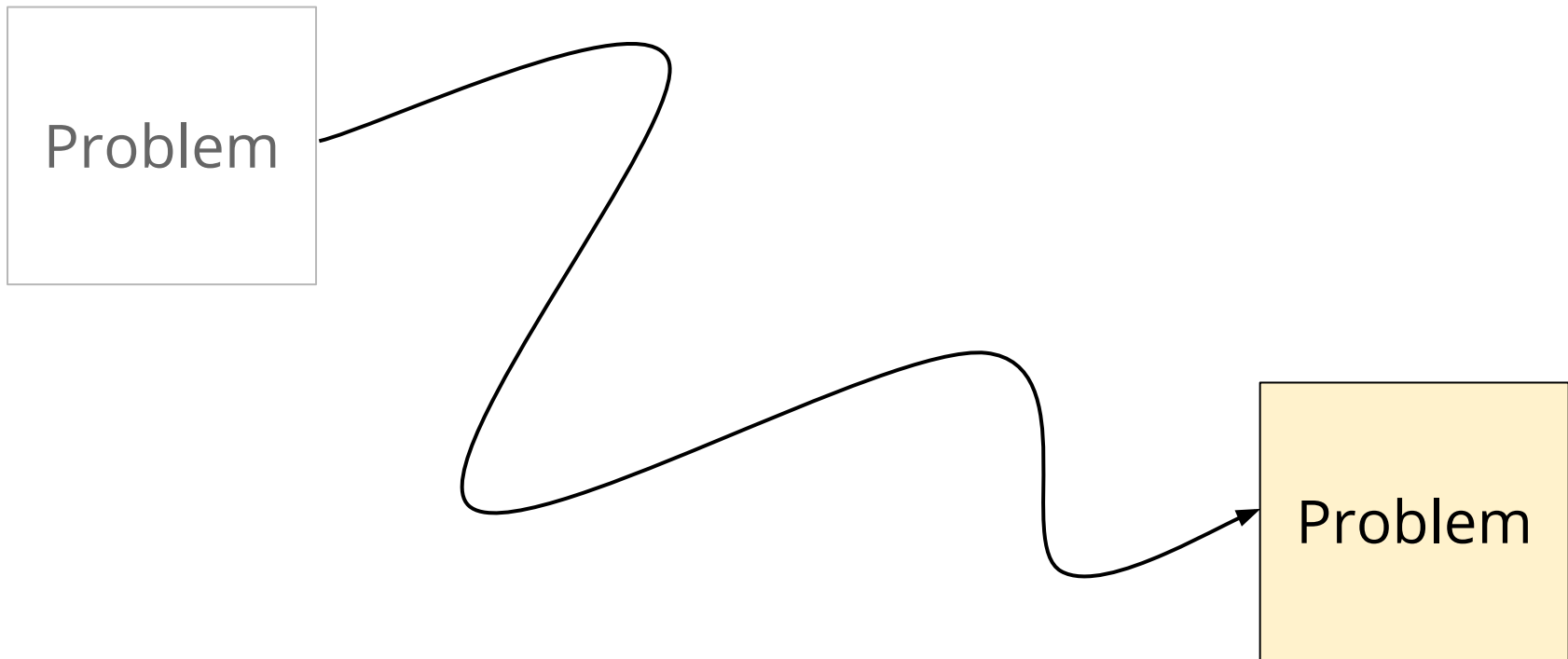
~~Proxy~~

~~A checked in go.sum file~~

No one!

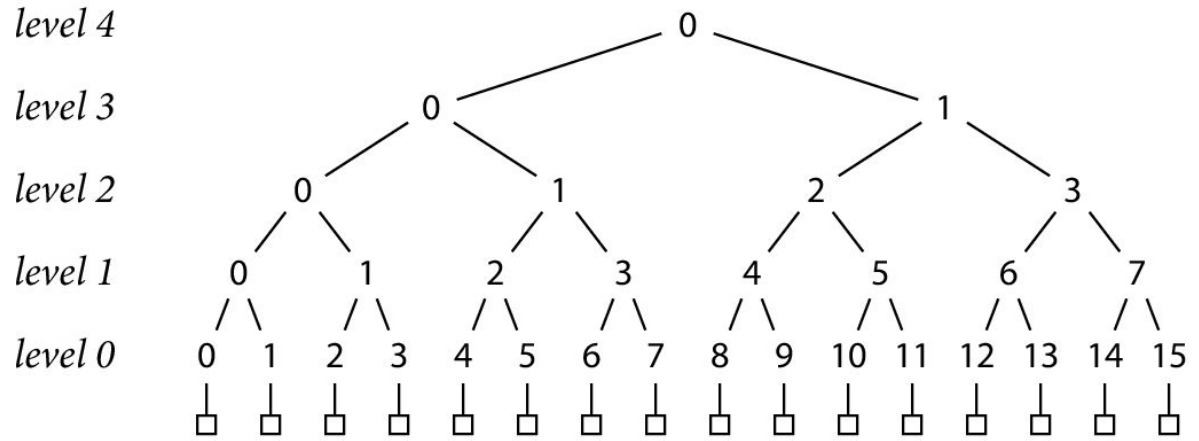
How about a database?

Problem



Checksum Database

# Transparent Log



Inclusion proof ✓

Consistency proof ✓

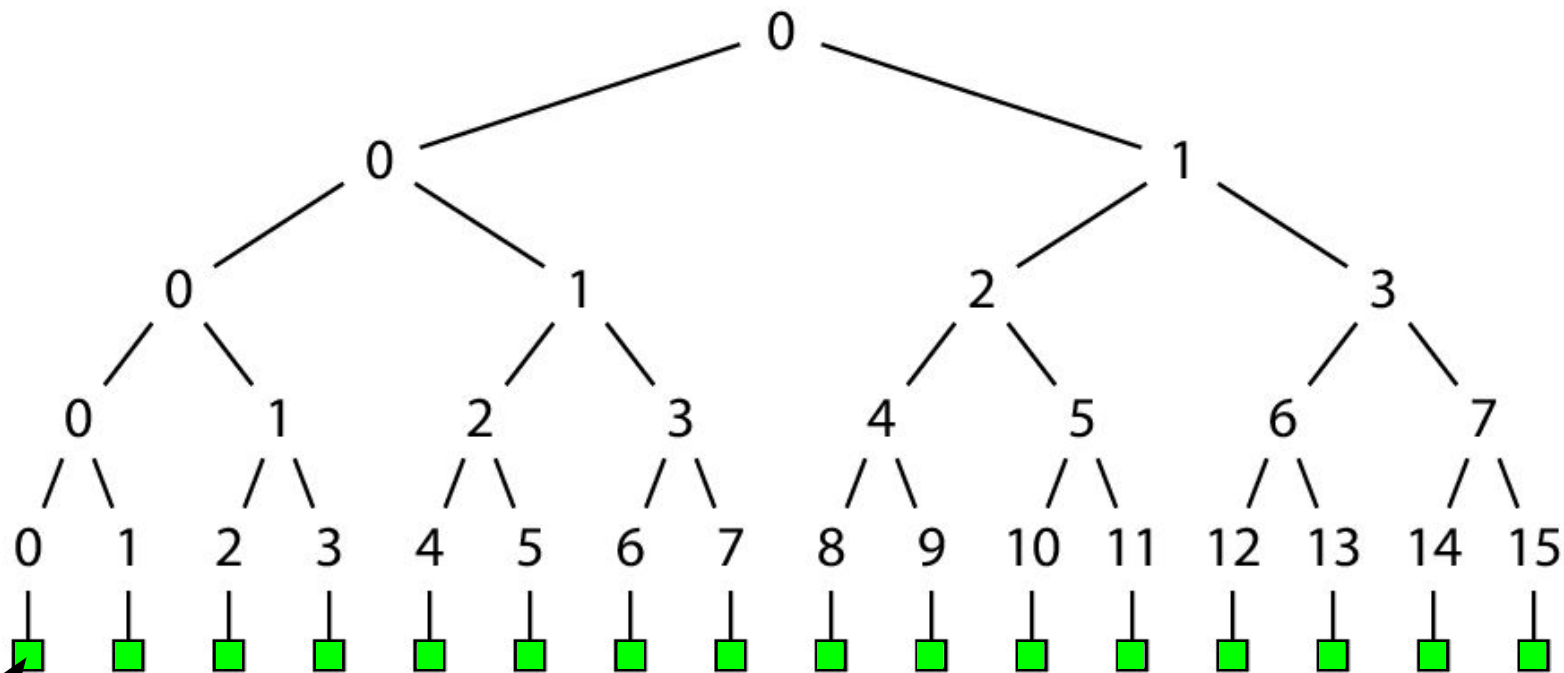
level 4

level 3

level 2

level 1

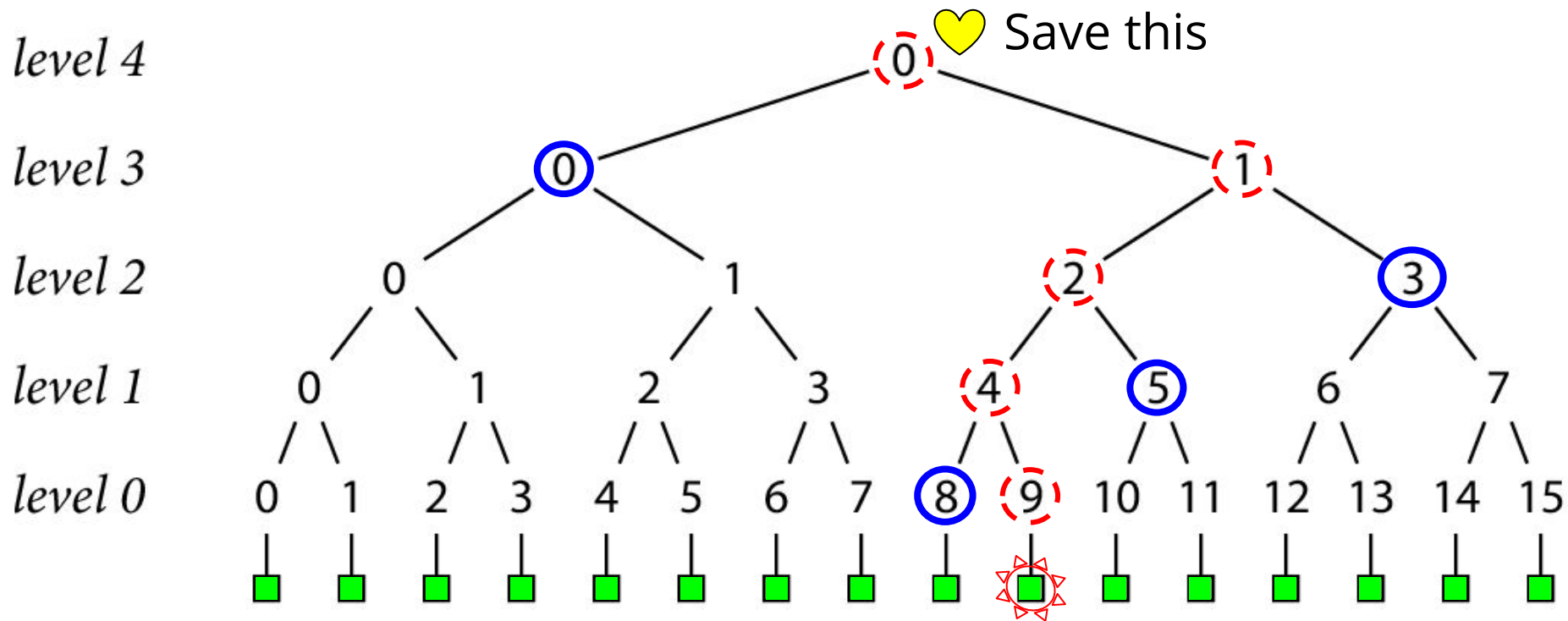
level 0



go.opencensus.io v0.19.2 h1:ZZpq6xI6kv/LuE/5s5UQvB...

go.opencensus.io v0.19.2/go.mod h1:N0/8qkisMZLZ1FC...

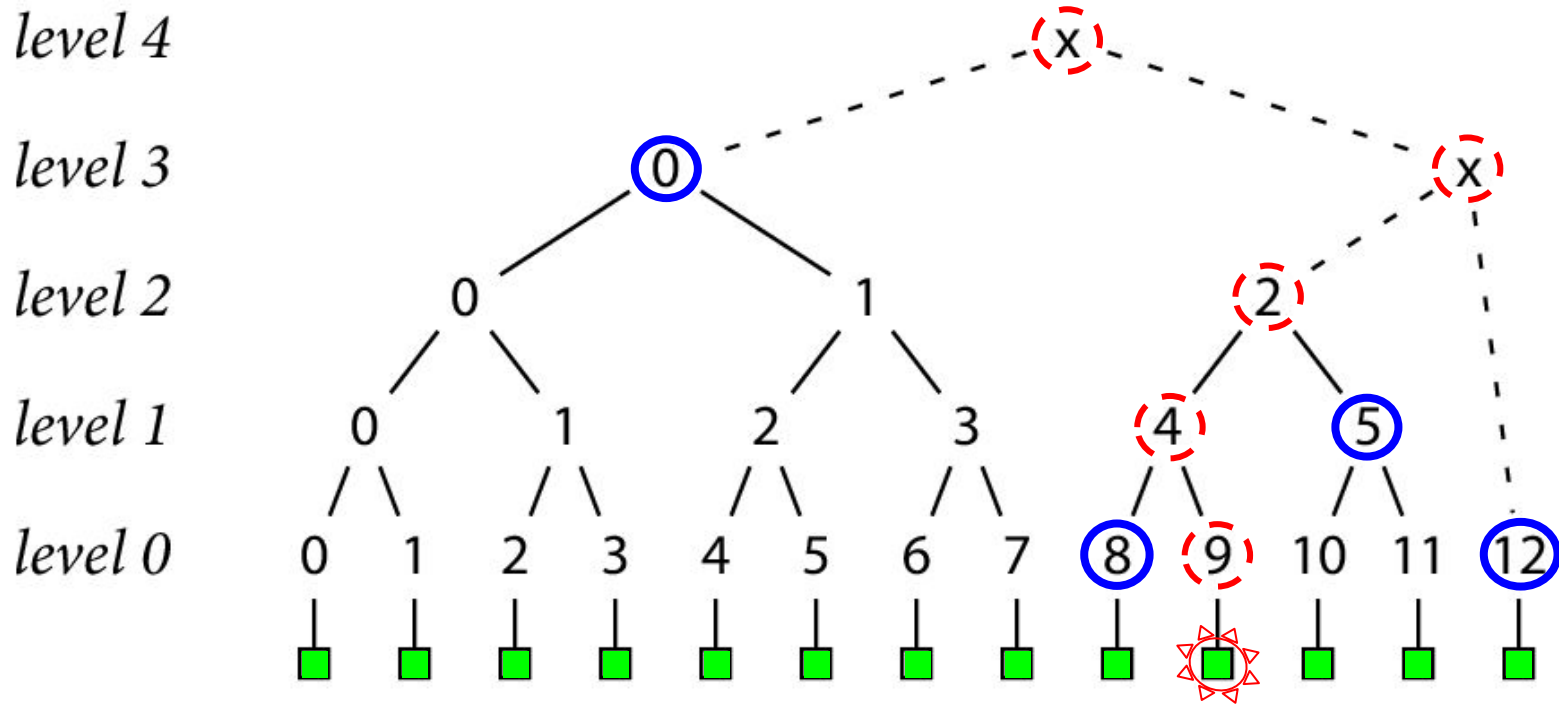
Checksum Database



**`/lookup/golang.org/x/text@v0.3.2`**

1. record number (9)
2. go.sum lines
3. tree head

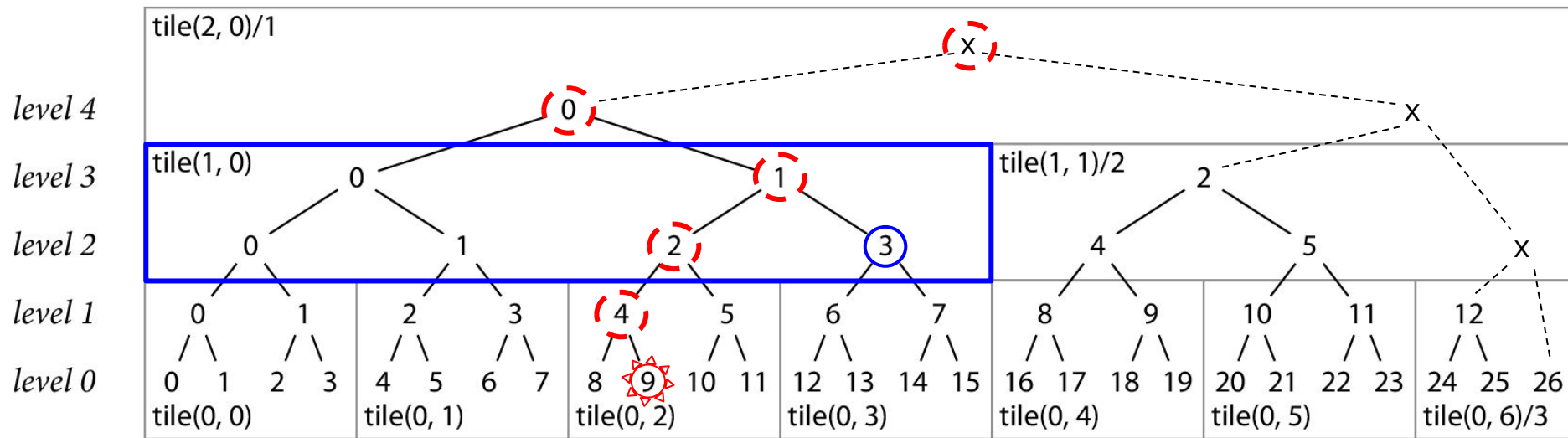
Checksum Database





# Tiles!





✓ Cache friendly

✓ Less storage

Won't the storage become too expensive?

# Checksum Database spec

GET \$GOSUMDB/lookup/M@V returns the 1) record # of the module version, 2) its go.sum lines, and 3) a tree head.

GET \$GOSUMDB/tile/H/L/K[.p/W]

GET \$GOSUMDB/tile/H/data/K[.p/W] returns record data

For auditors: GET \$GOSUMDB/latest returns the latest signed tree head for a log.

# /latest

go.sum database tree

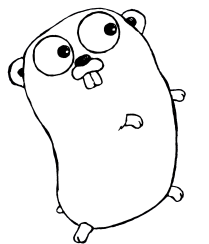
11131

uJ+UzAf0s0Gi22MuICyemMge4fp8gI3+5+wZF5t1aXU=

– sum.golang.org

Az3grjQmIfBoZv0eH1eRf4gu7VNSS8Lv sdfECddEnVIA1drPr  
g29LDmVliD3dshfo9ZYr1Gq0HWyVWXJ96ZjDpiSvgY=

go get golang.org/x/text



go  
command

\$GOSUMDB/lookup/golang.org/x/text@v0.3.2

Checksum  
database

5427

golang.org/x/text v0.3.2 <hash>  
golang.org/x/text v0.3.2/go.mod <hash>  
<STH>

\$GOSUMDB/tile/8/0/005

\$GOSUMDB/tile/8/1/000.p/59

[... more tiles]

Checksum Database

# What guarantees does this provide?

1. Everyone gets the same code every time
2. A proxy can't lie to you without being caught



“Trust on *anyone’s* first use”

# Better solutions

✓ Reproducible builds

Modules

✓ Persistent dependencies

Mirror

✓ Trustworthy fetches

Checksum  
Database



# Setting up your environment



# Environment variables

- GO111MODULE
- GOPROXY
- GOSUMDB (only 1.13)

**GOPROXY=**<https://proxy.golang.org>  
(will use sum.golang.org for GOSUMDB by default in 1.13)

# For private modules

GONOPROXY, GONOSUMDB

`GONOPROXY=*.corp.google.com,rsc.io/private`

Your environment

# Trillian

<https://github.com/google/trillian>

Append-only, Certificate Transparency style log



One more cool thing





# index.golang.org/index

- Feed of new modules discovered by proxy.golang.org

<https://index.golang.org/index?since=2019-03-04T18:00:15.161182-07:00>

# The future of Go

