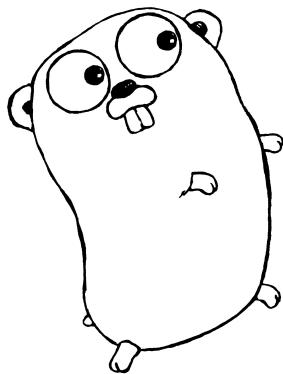


Go Module Proxy: Life of a Query



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



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
Database |

1. Modules

`github.com/katiehockman/puppies`

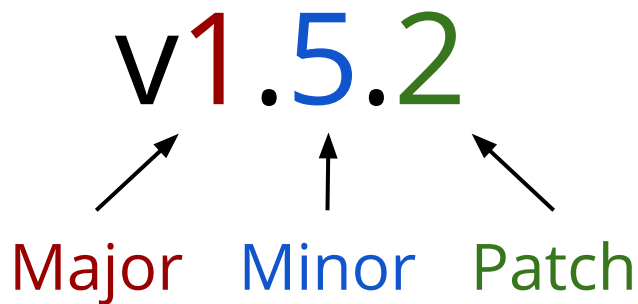
`package walk`

`package bark`

`package toys`

Semantic versioning

v1.5.2



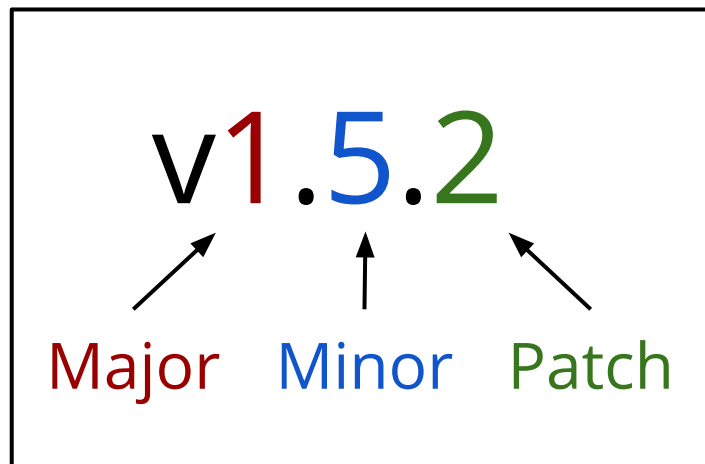
Major Minor Patch

The diagram illustrates the components of the semantic versioning string 'v1.5.2'. The 'v' prefix 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. Three arrows point from these labels to their corresponding parts of the version string: from 'Major' to '1', from 'Minor' to '5', and from 'Patch' to '2'.

Semantic versioning

Immutable!

Backwards
compatible!



go.mod

```
module github.com/katiehockman/puppies

require (
    github.com/maps/neighborhood v1.4.1
    github.com/audio/dogs v0.19.2
    golang.org/x/crypto v0.0.0-20190308221718-c2843e01d9a2
)
```

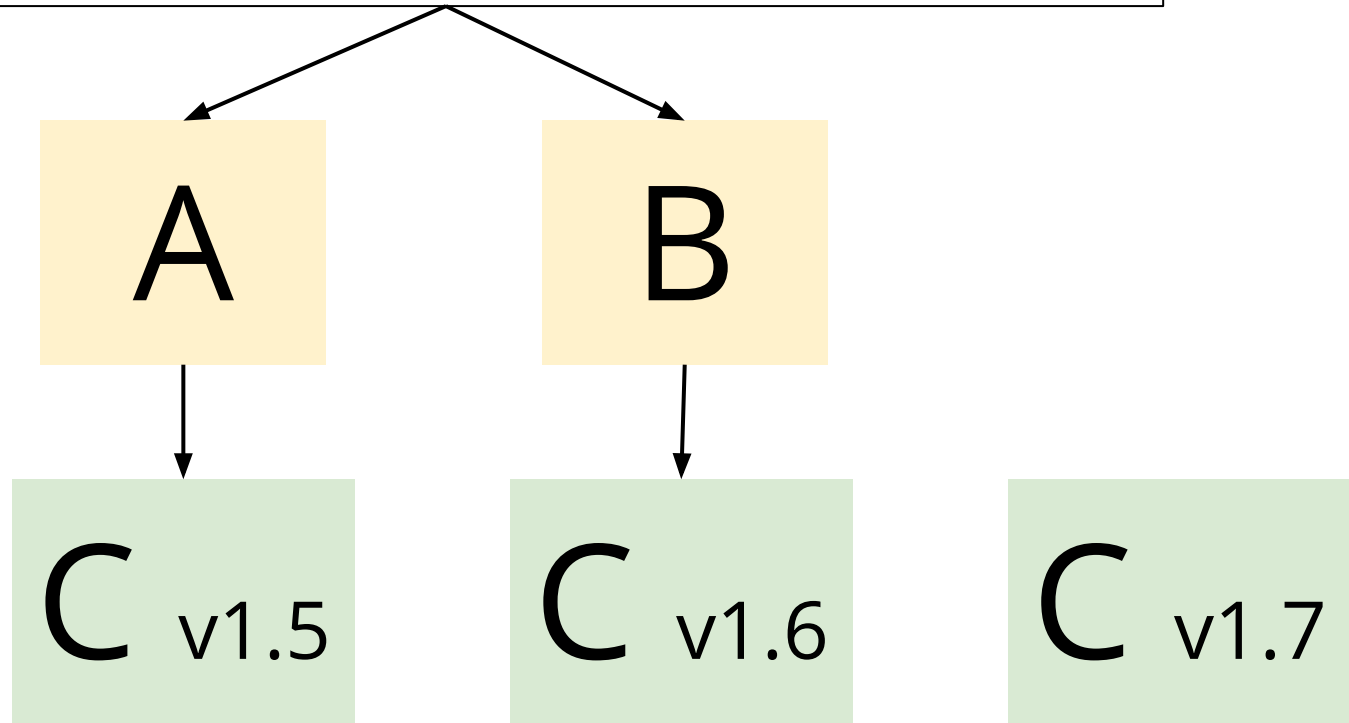
go.mod

```
module github.com/katiehockman/puppies

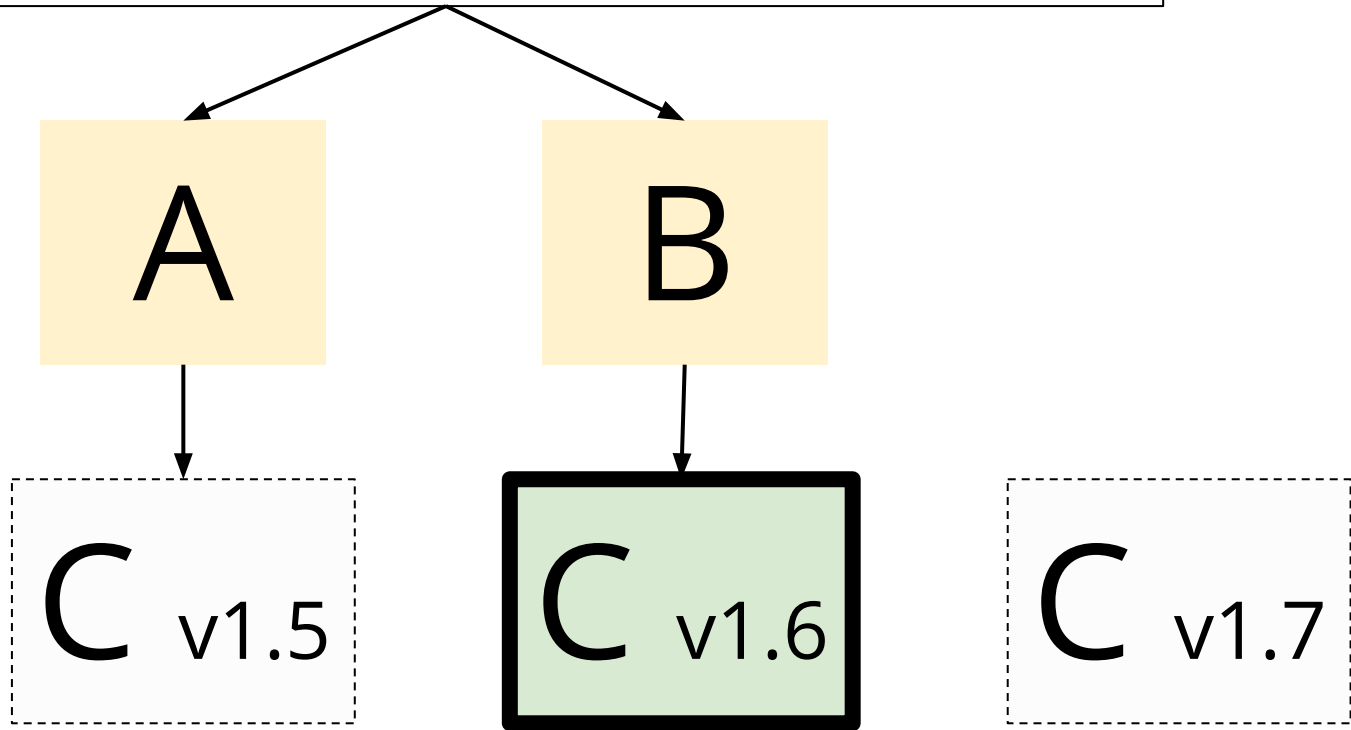
require (
    github.com/maps/neighborhood v1.4.1
    github.com/audio/dogs v0.19.2
    golang.org/x/crypto v0.0.0-20190308221718-c2843e01d9a2
)
```

Minimal version selection

`github.com/katiehockman/puppies`



`github.com/katiehockman/puppies`



Better solutions

✓ Reproducible builds

Modules

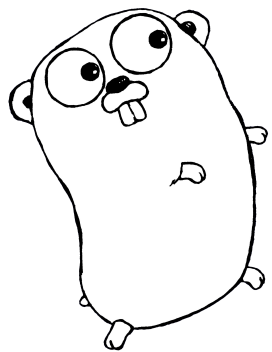
2. Persistent dependencies

Mirror

3. Trustworthy fetches

Checksum
Database

2. Mirror/Proxy



go command



Origin server
(ie. GitHub)

go get

1. Fetch the source code
2. Resolve dependencies

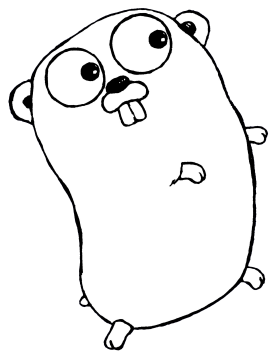




A large light gray rectangle with a black border represents a file system. The text "All other files" is centered in the upper half. A thin green horizontal line is at the bottom, with an arrow pointing to it from the text "go.mod file (what it actually needs)".

All other files

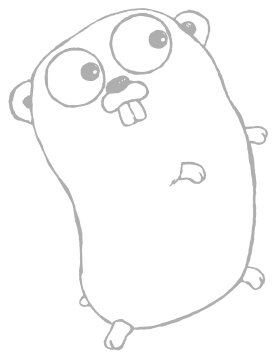
go.mod file
(what it actually needs)



go command



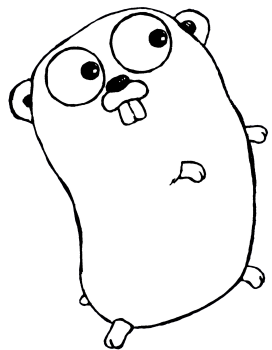
Origin server
(ie. GitHub)



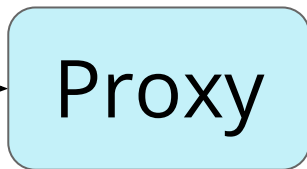
go command



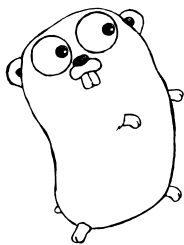
Origin server
(ie. GitHub)



go command



Origin server
(ie. GitHub)

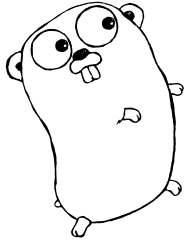


go
command

Proxy

Mirror

go get go.dog/breeds

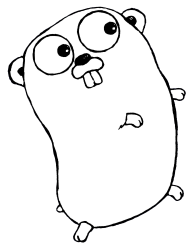


go
command

Proxy

Mirror


```
go get go.dog/breeds
```



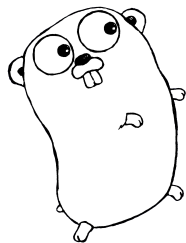
go
command

`$GOPROXY/go.dog/breeds/@v/list`

Proxy

Mirror

```
go get go.dog/breeds
```



go

command

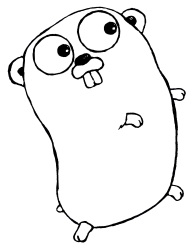
`$GOPROXY/go.dog/breeds/@v/list`

`v0.1.0, v0.2.0, v0.3.0, v0.3.1, v0.3.2`

Proxy

Mirror

```
go get go.dog/breeds
```



go

command

`$GOPROXY/go.dog/breeds/@v/list`

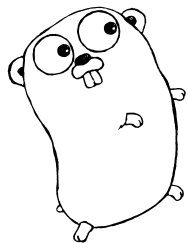
`v0.1.0, v0.2.0, v0.3.0, v0.3.1, v0.3.2`

`$GOPROXY/go.dog/breeds/@v/v0.3.2.info`

Proxy

Mirror

```
go get go.dog/breeds
```



go
command

```
$GOPROXY/go.dog/breeds/@v/list
```

```
v0.1.0, v0.2.0, v0.3.0, v0.3.1, v0.3.2
```

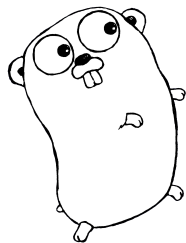
```
$GOPROXY/go.dog/breeds/@v/v0.3.2.info
```

```
{"Version": "v0.3.2", "Time": "2019..."}
```

Proxy

Mirror

```
go get go.dog/breeds
```



go
command

```
$GOPROXY/go.dog/breeds/@v/list
```

```
v0.1.0, v0.2.0, v0.3.0, v0.3.1, v0.3.2
```

```
$GOPROXY/go.dog/breeds/@v/v0.3.2.info
```

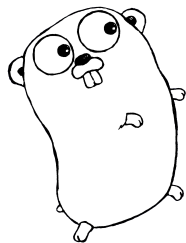
```
{"Version": "v0.3.2", "Time": "2019..."}
```

```
$GOPROXY/go.dog/breeds/@v/v0.3.2.mod
```

Proxy

Mirror

go get go.dog/breeds



go
command

`$GOPROXY/go.dog/breeds/@v/list`

`v0.1.0, v0.2.0, v0.3.0, v0.3.1, v0.3.2`

`$GOPROXY/go.dog/breeds/@v/v0.3.2.info`

`{"Version": "v0.3.2", "Time": "2019..."}`

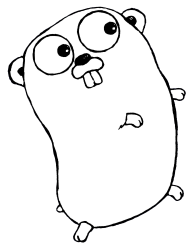
`$GOPROXY/go.dog/breeds/@v/v0.3.2.mod`

[Fetch .info and .mod files of
dependencies]

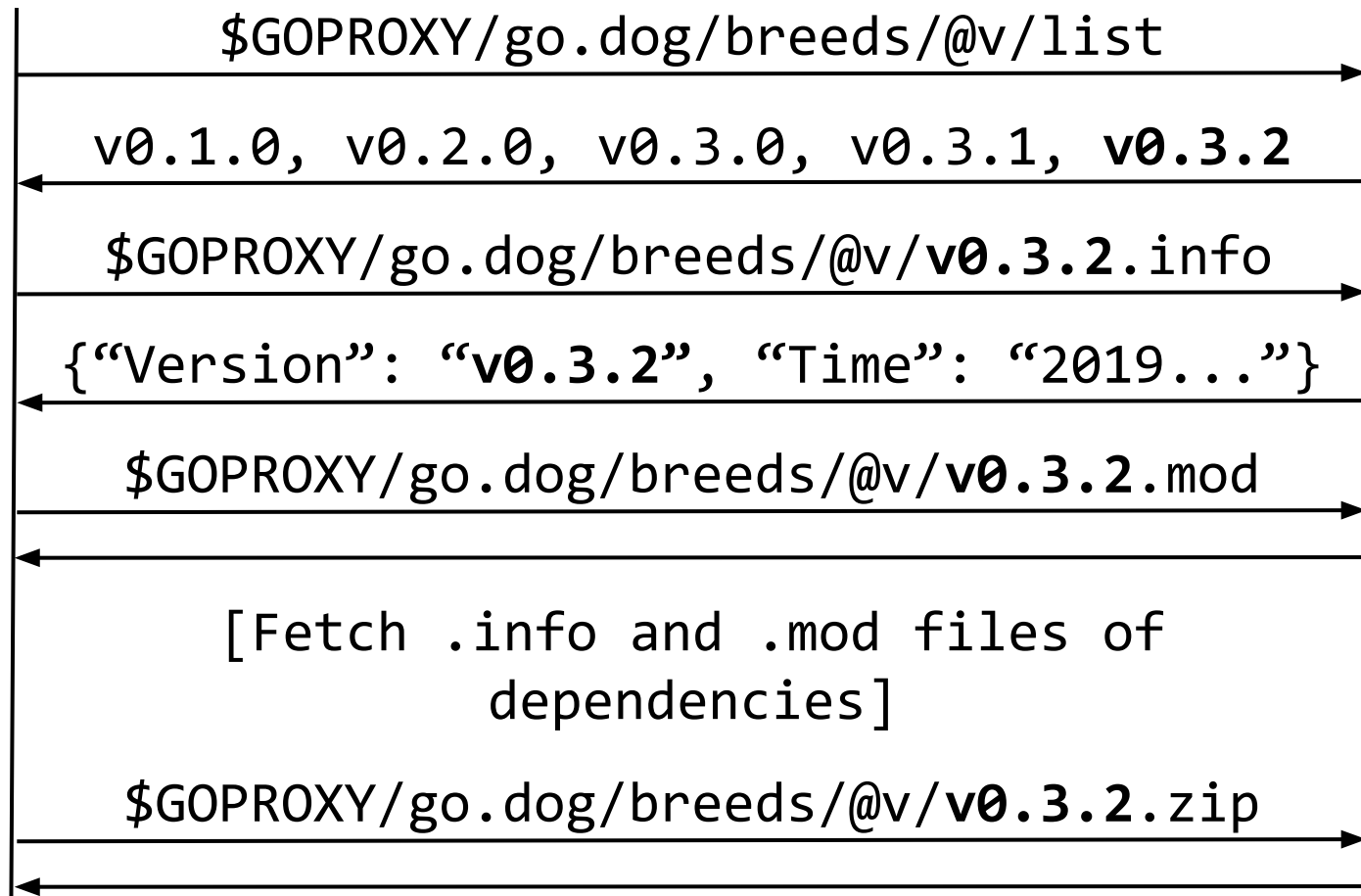
Proxy

Mirror

go get go.dog/breeds



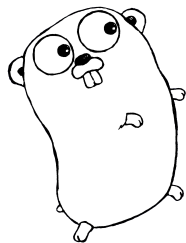
go
command



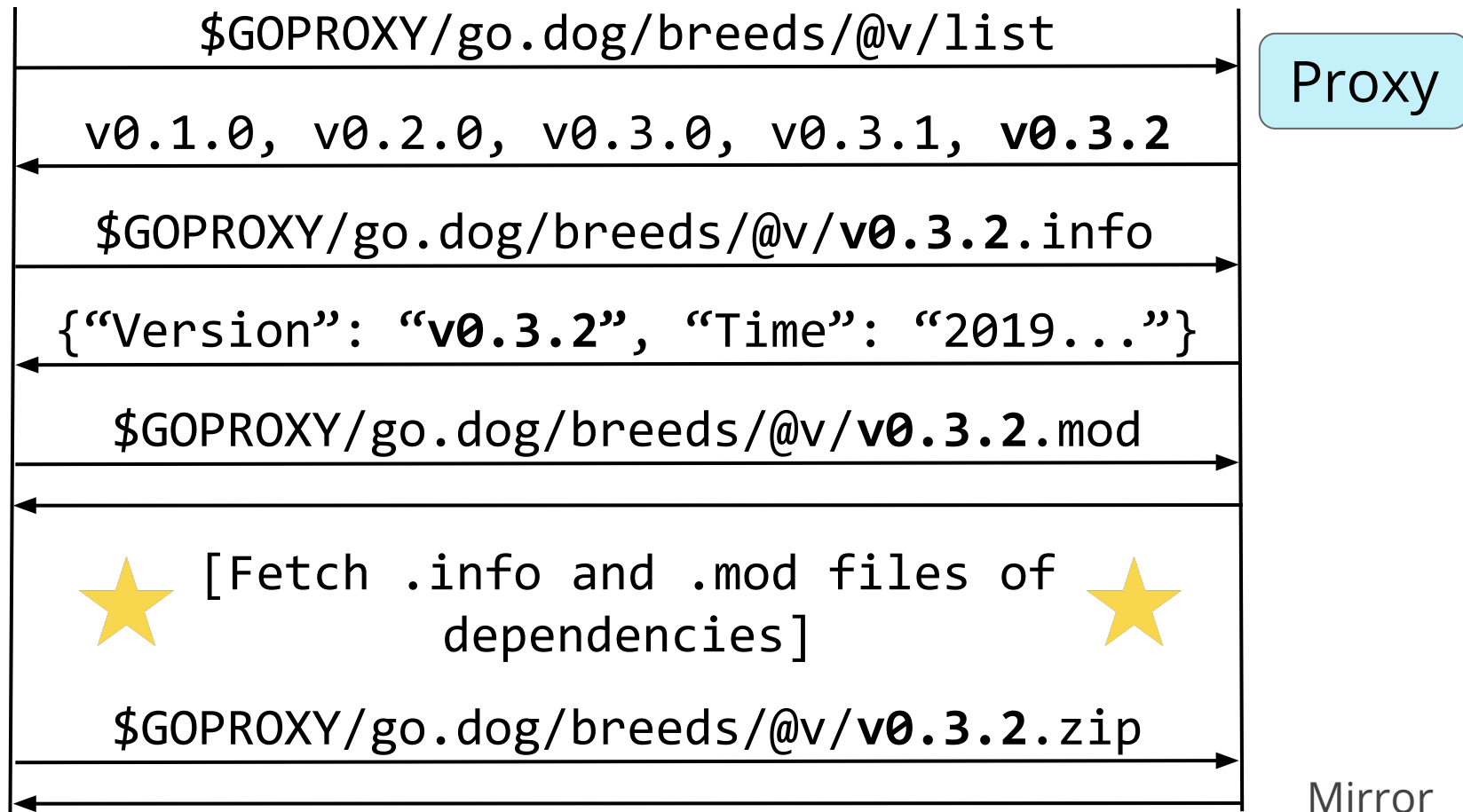
Proxy

Mirror

go get go.dog/breeds

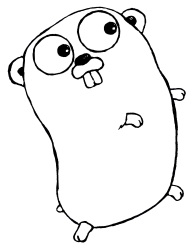


go
command



Mirror

go get go.dog/breeds



go

command

`$GOPROXY/go.dog/breeds/@v/list`

`v0.1.0, v0.2.0, v0.3.0, v0.3.1, v0.3.2`

`$GOPROXY/go.dog/breeds/@v/v0.3.2.info`

`{"Version": "v0.3.2", "Time": "2019..."}`

`$GOPROXY/go.dog/breeds/@v/v0.3.2.mod`

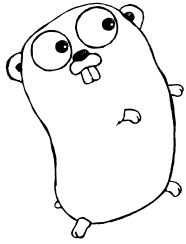
[Fetch .info and .mod files of dependencies]

`$GOPROXY/go.dog/breeds/@v/v0.3.2.zip`

Proxy

Mirror

```
go get go.dog/breeds@master
```

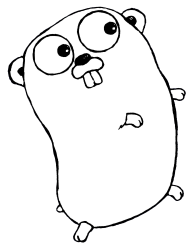


go
command

Proxy

Mirror

```
go get go.dog/breeds@master
```

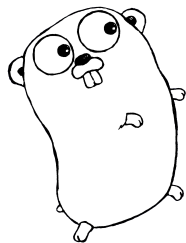


go
command

`$GOPROXY/go.dog/breeds/@v/master.info`

Proxy

```
go get go.dog/breeds@master
```



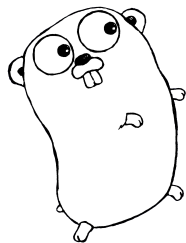
go
command

`$GOPROXY/go.dog/breeds/@v/master.info`

`{"Version": "v0.3.2-20190426-f86f4", ...}`

Proxy

```
go get go.dog/breeds@master
```



go
command

`$GOPROXY/go.dog/breeds/@v/master.info`

`{"Version": "v0.3.2-20190426-f86f4", ...}`

`$GOPROXY/go.dog/breeds/@v/v0.3.2-20...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`

Mirror = Proxy (+ caching)

Why use a mirror?

- ✓ No more disappearing dependencies

Why use a mirror?

- ✓ No more disappearing dependencies

Why use a mirror? ✓ Faster downloads

- ✓ No more disappearing dependencies

Why use a mirror? ✓ Faster downloads

- ✓ Less storage use

- Why use a mirror?
- ✓ No more disappearing dependencies
 - ✓ Faster downloads
 - ✓ Less storage use
 - ✓ Easy to use

Better solutions

✓ Reproducible builds

Modules

✓ Persistent dependencies

Mirror

3. Trustworthy fetches

Checksum
Database

3. Checksum Database

The old way... direct HTTPS

The new way... go.sum files

go.sum for github.com/katiehockman/puppies

```
github.com/maps/neighborhood v1.4.1 h1:g24URVg00FbNUTx9qq...
```

```
github.com/maps/neighborhood v1.4.1/go.mod h1:zAC/RDZ24gD...
```

```
github.com/audio/dogs v0.19.2 h1:ZZpq6xI6kv/LuE/5s5UQvBU...
```

```
github.com/audio/dogs v0.19.2/go.mod h1:NO/8qkisMZLZ1FCs...
```

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

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

Check in your module's go.sum file!

My module's go.sum file

```
github.com/maps/neighborhood v1.4.1 h1:g24URVg00FbNUTx9...  
github.com/maps/neighborhood v1.4.1/go.mod h1:zAC/RDZ24g...  
github.com/audio/dogs v0.19.2 h1:ZZpq6xI6kvLuE5s5U...  
github.com/audio/dogs v0.19.2/go.mod h1:NO/8qkisMZ...
```

The generated go.sum lines

```
github.com/audio/dogs v0.19.2 h1:ABfk0xE3fdLeS8s3W...  
github.com/audio/dogs v0.19.2/go.mod h1:HI/0dfjwDS...
```

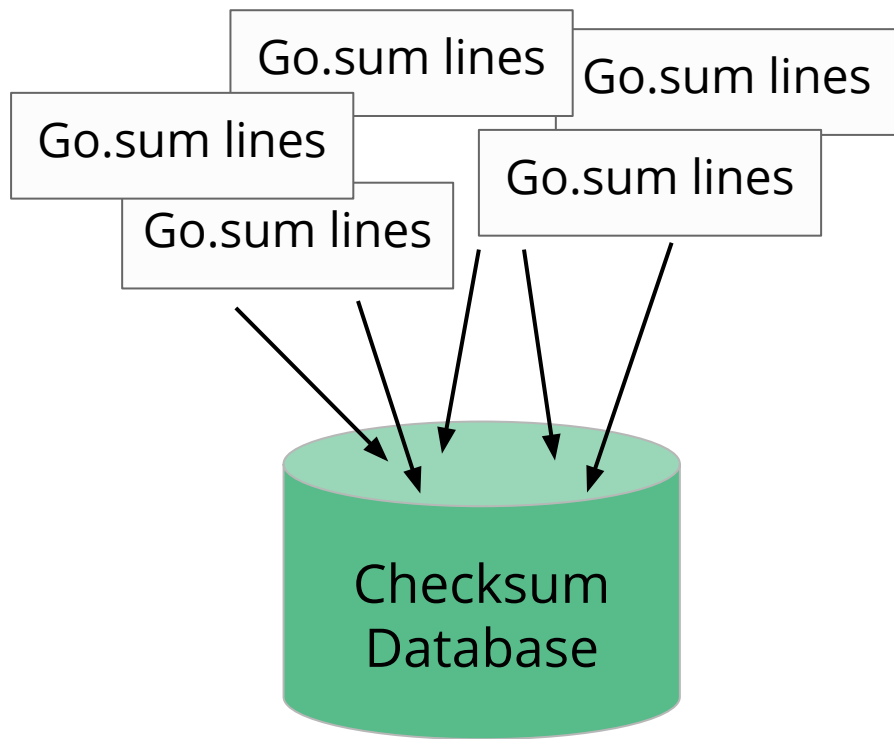
“Trust on *your* first use”

What about proxies?

The best possible scenario...

The **newest** way...

The newest way...

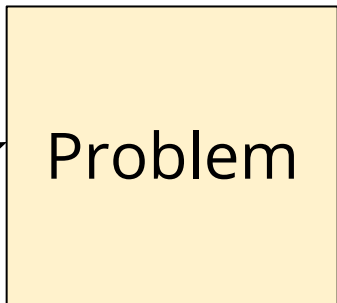
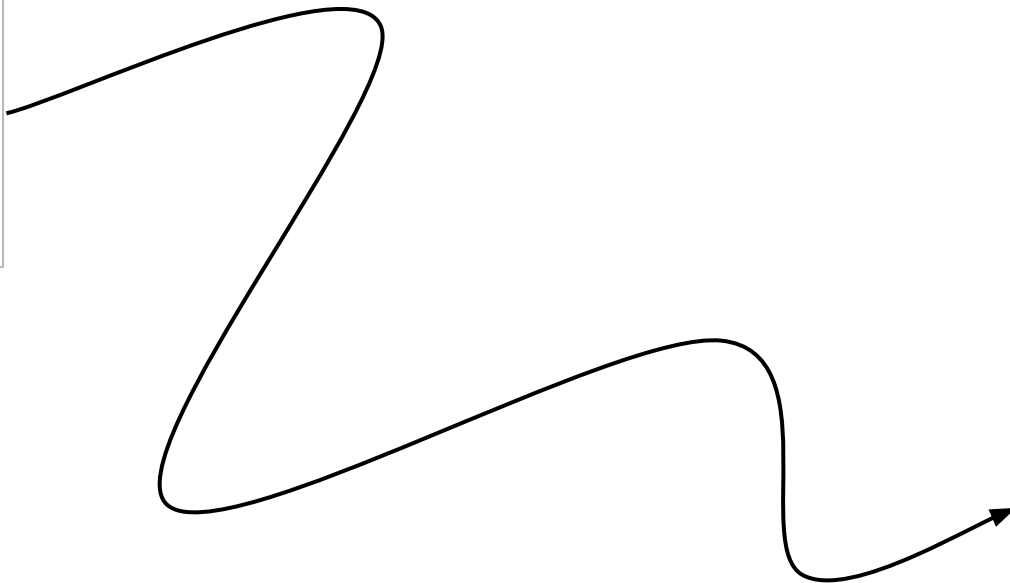
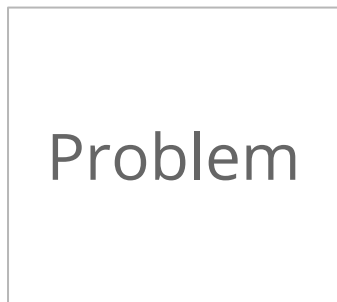


golang.org/design/25530-sumdb

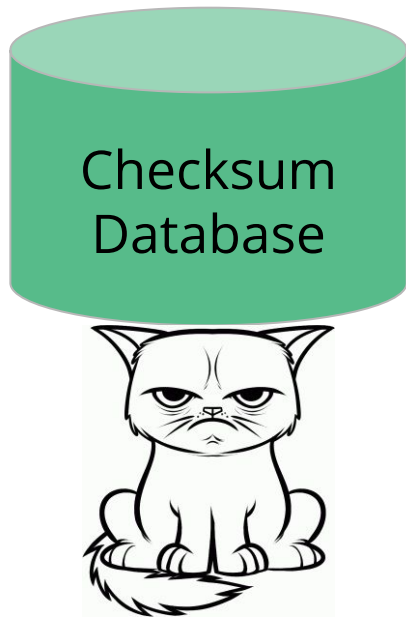
Checksum DB

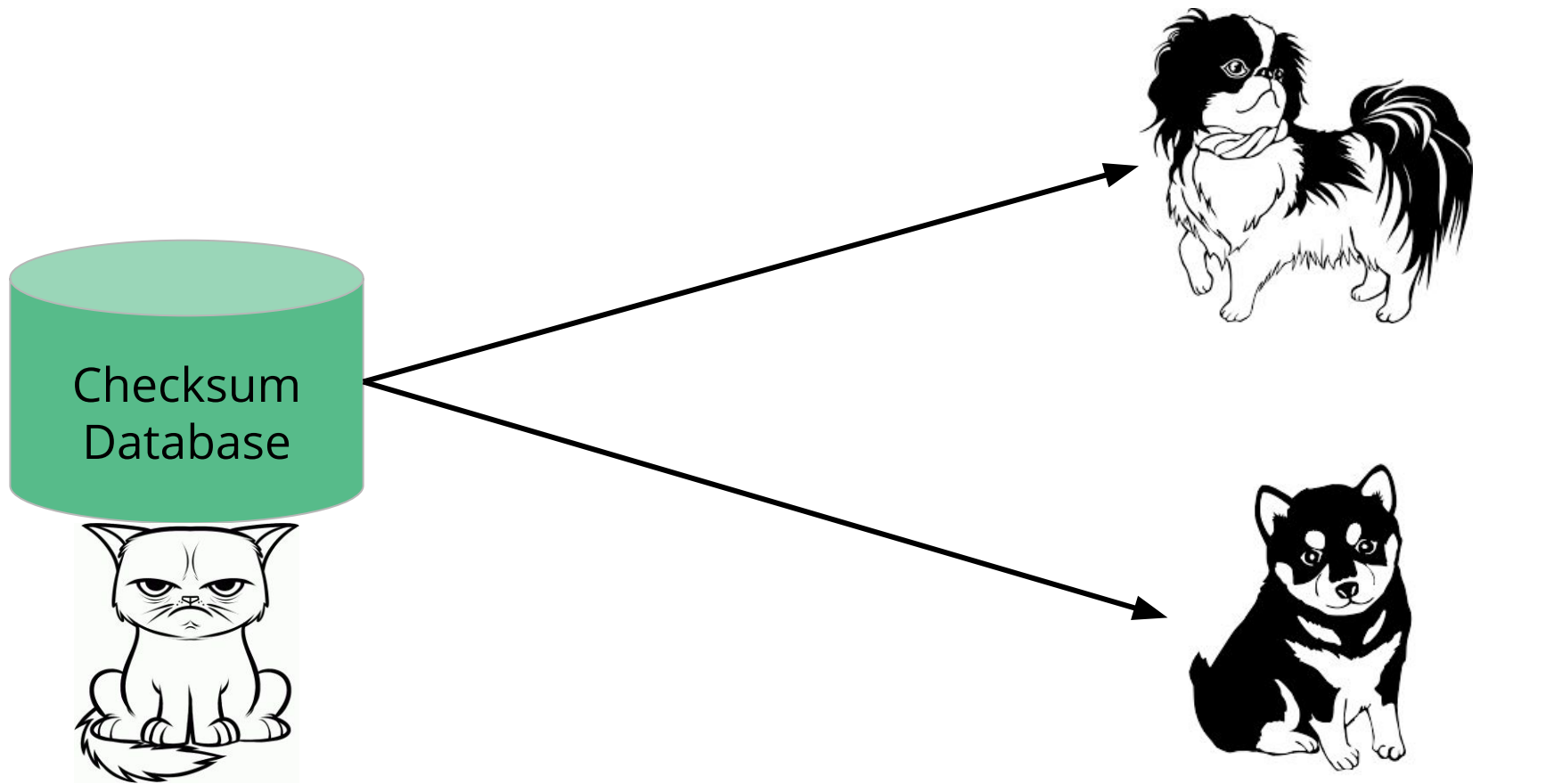
How about a database?

Problem

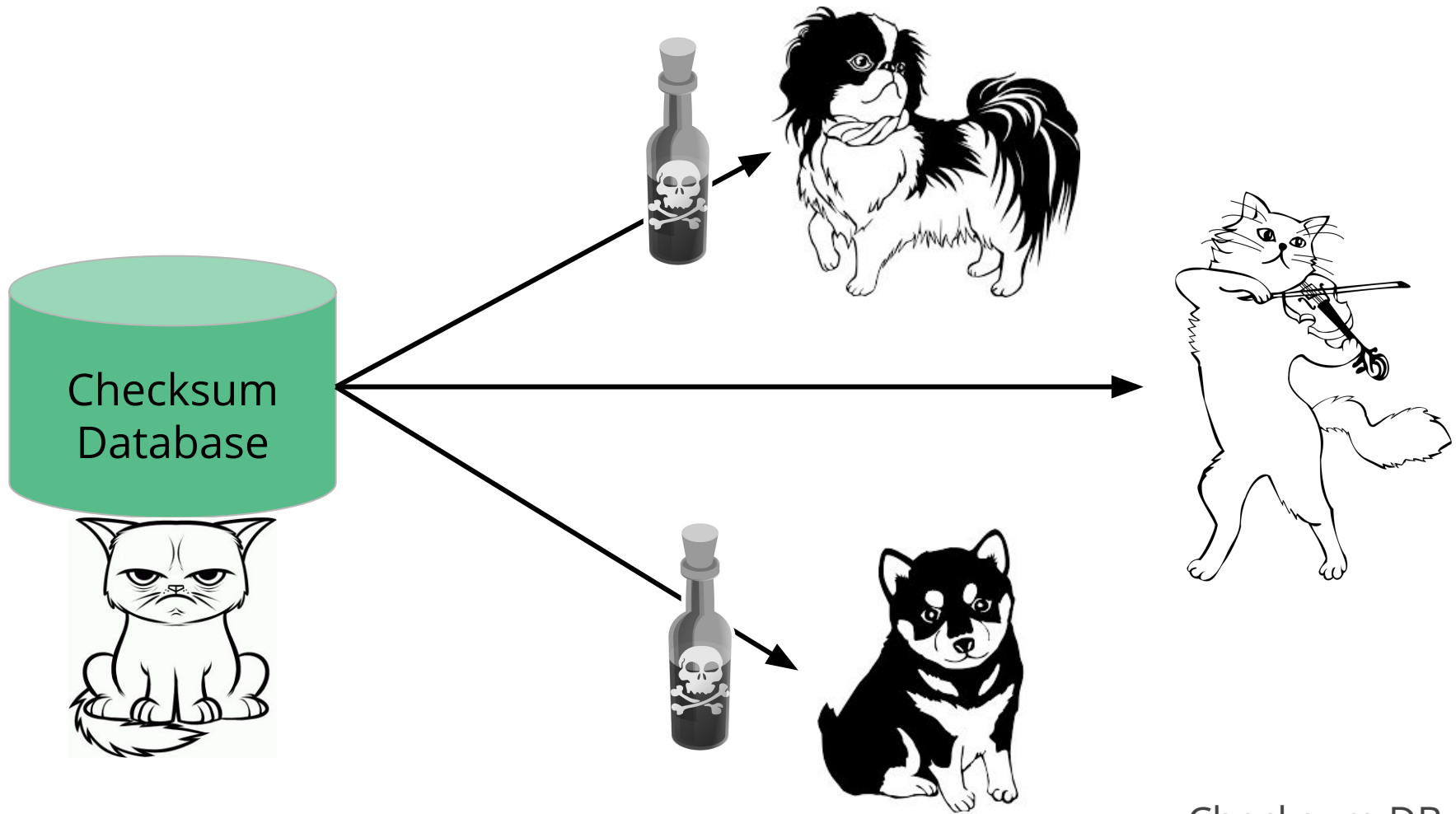


Checksum DB

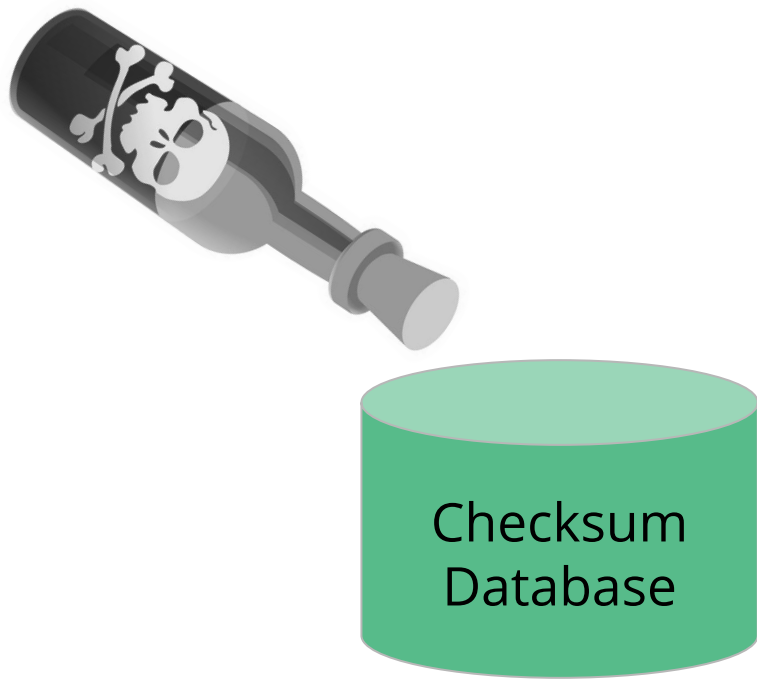


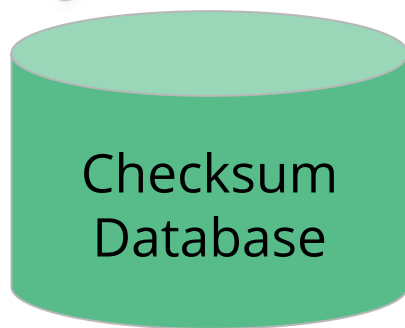
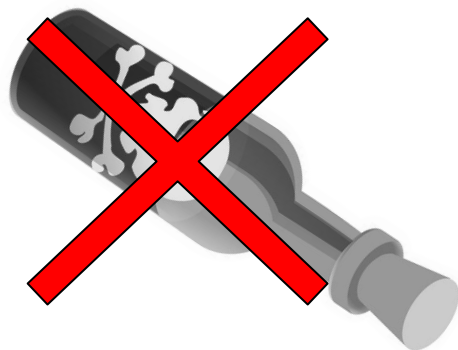


Checksum DB

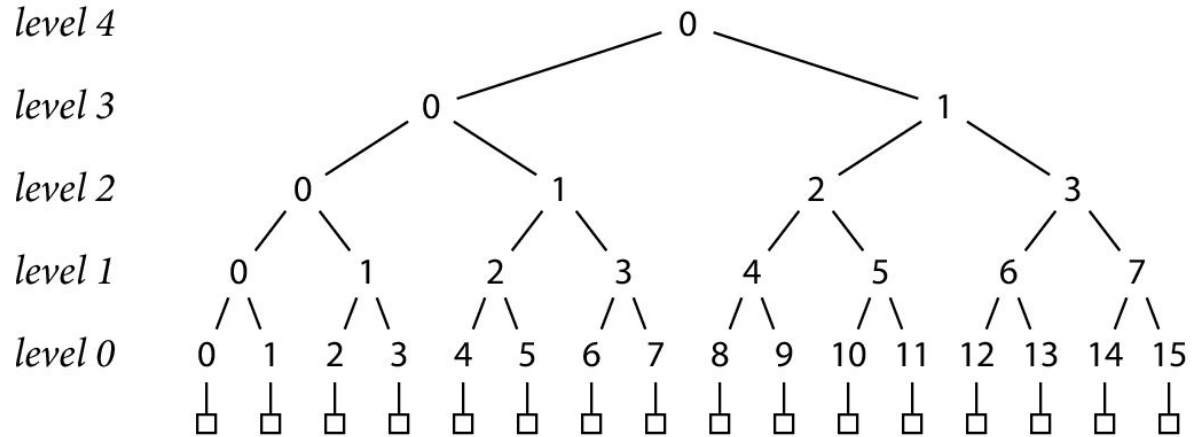


Checksum DB





Transparent Log

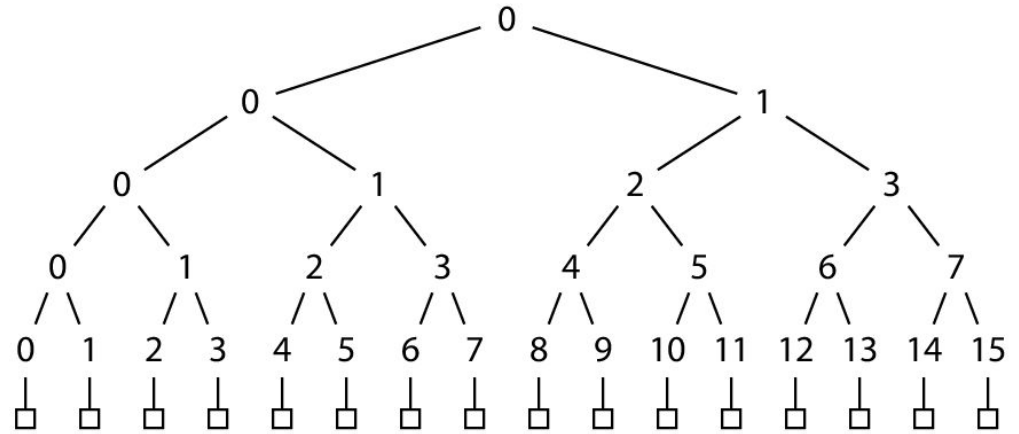


<https://research.swtch.com/tlog>

Checksum DB

Transparent Log (merkle tree)

level 4
level 3
level 2
level 1
level 0



What about a merkle tree?

- ✓ Tamper-proof

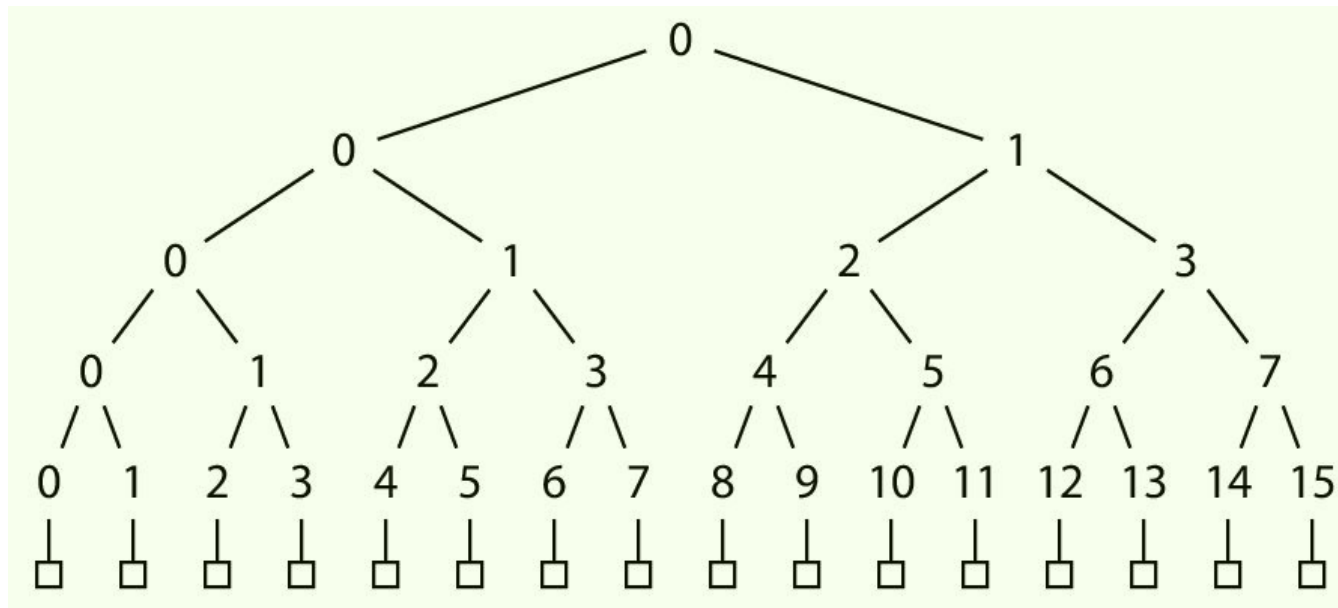
level 4

level 3

level 2

level 1

level 0



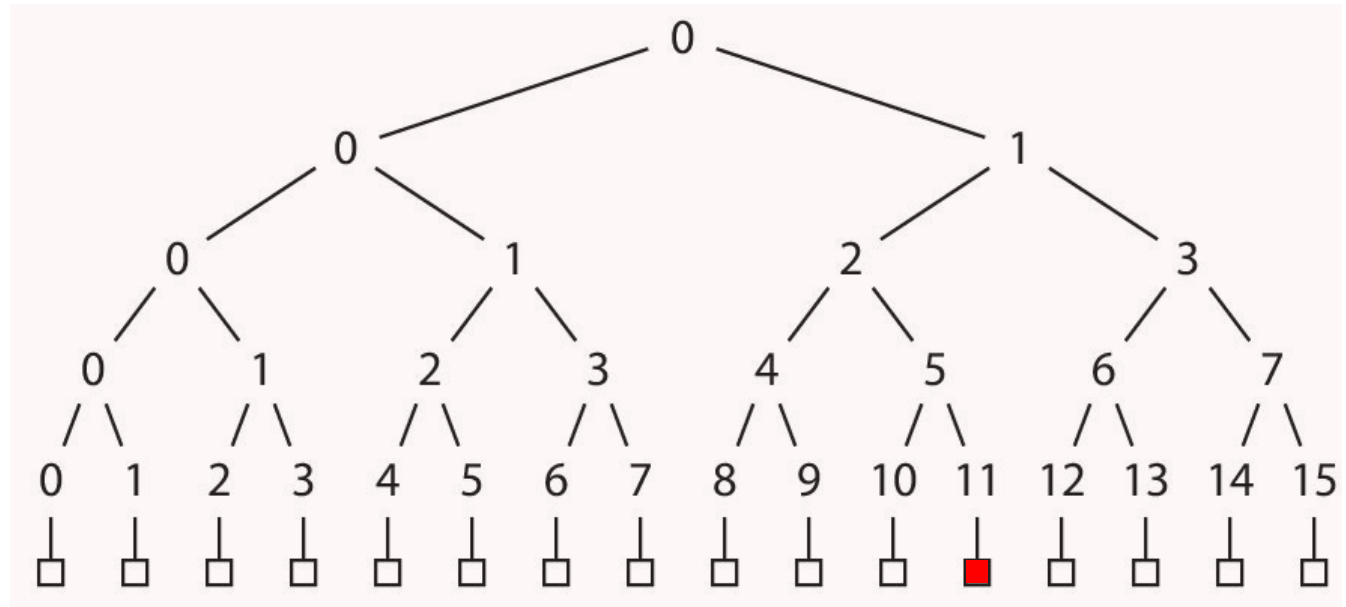
level 4

level 3

level 2

level 1

level 0





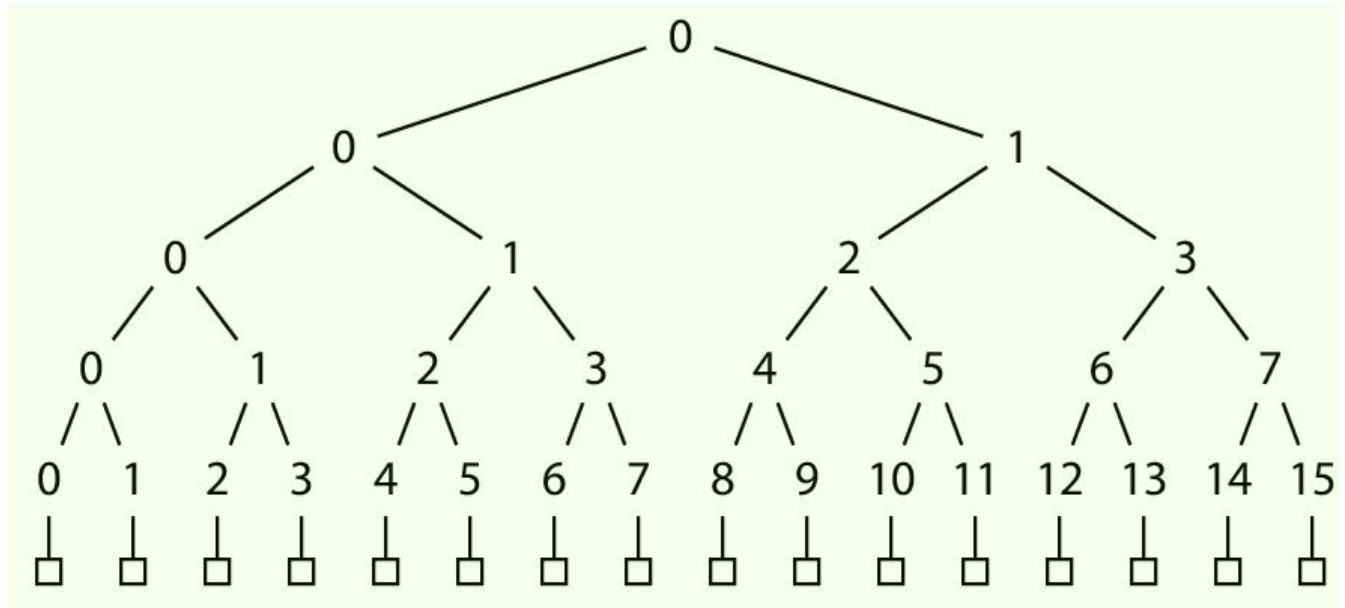
level 4

level 3

level 2

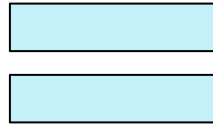
level 1

level 0



We all want the “correct” code

We all want the “correct” code



We all want the “same” code

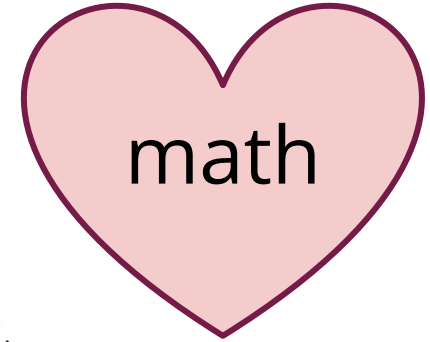
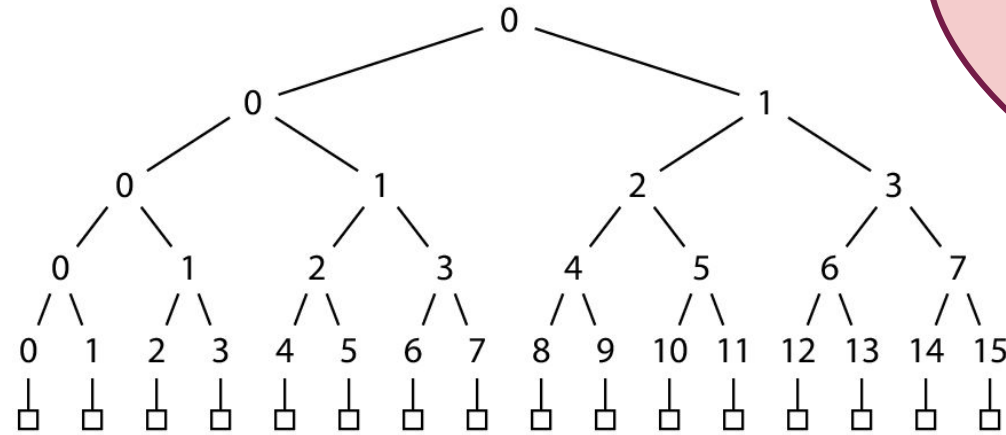
level 4

level 3

level 2

level 1

level 0



Inclusion proof ✓

Consistency proof ✓

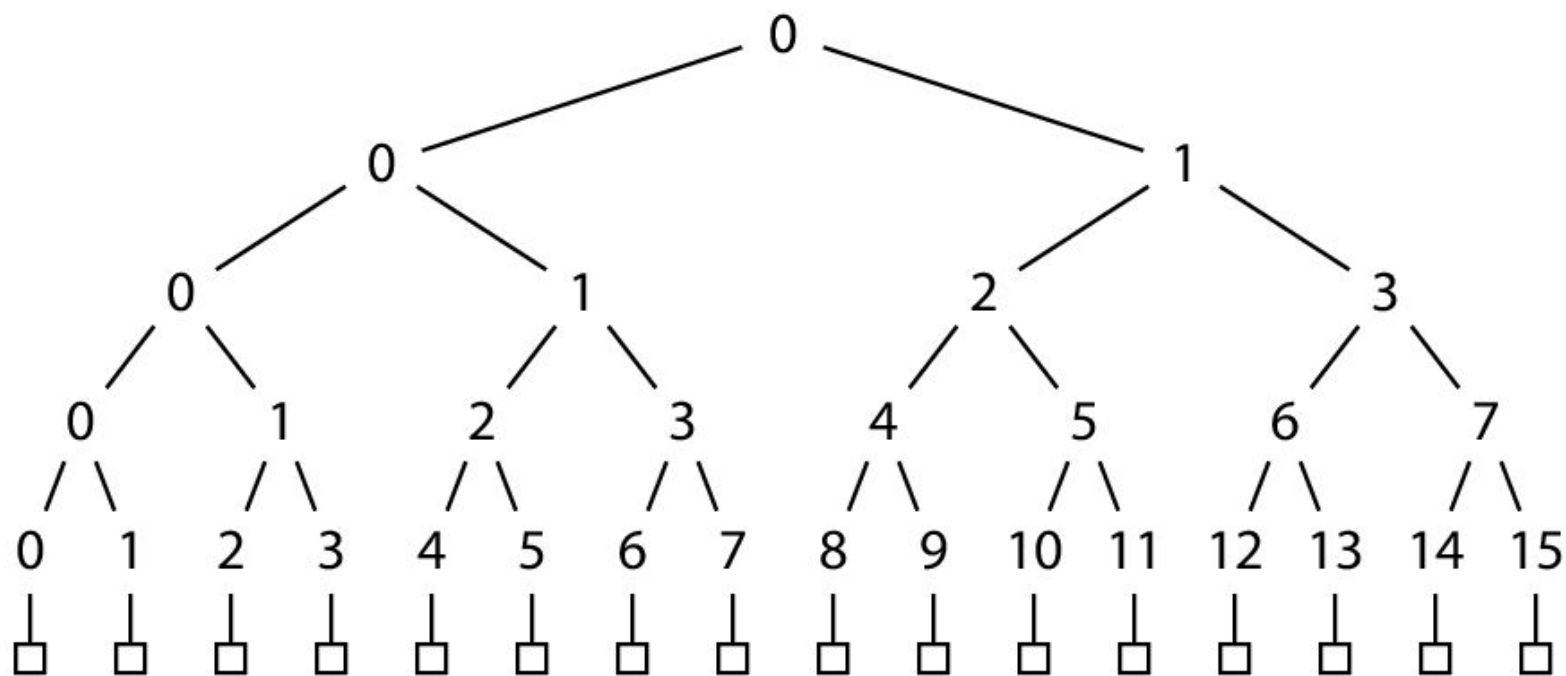
level 4

level 3

level 2

level 1

level 0



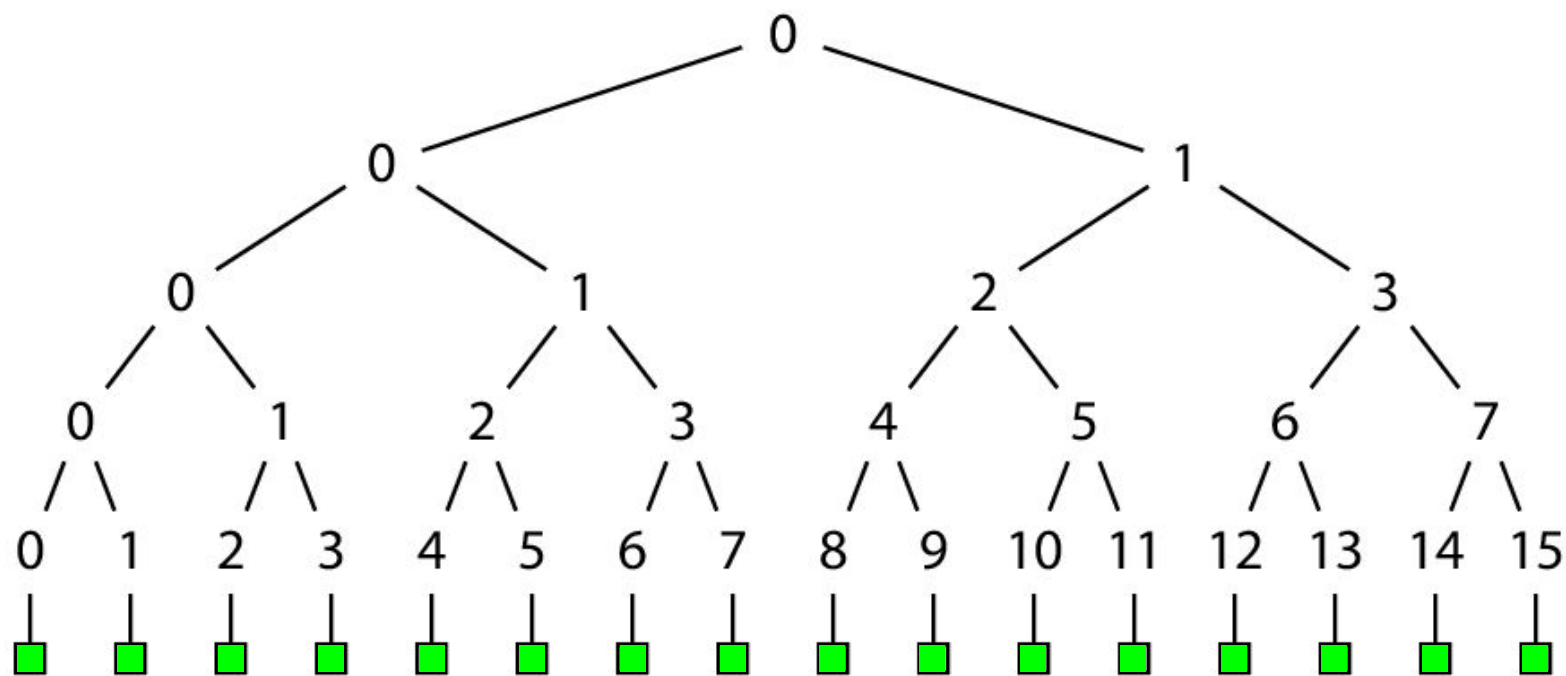
level 4

level 3

level 2

level 1

level 0



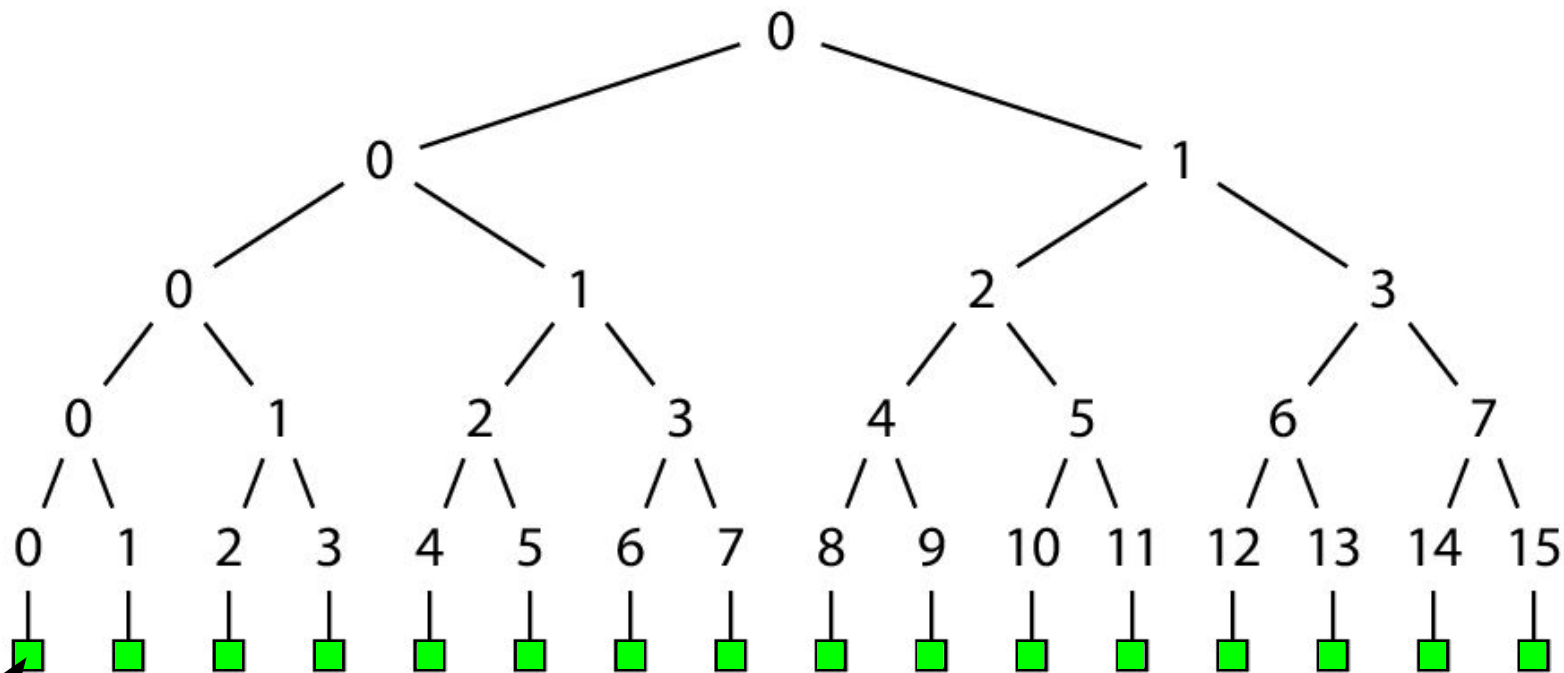
level 4

level 3

level 2

level 1

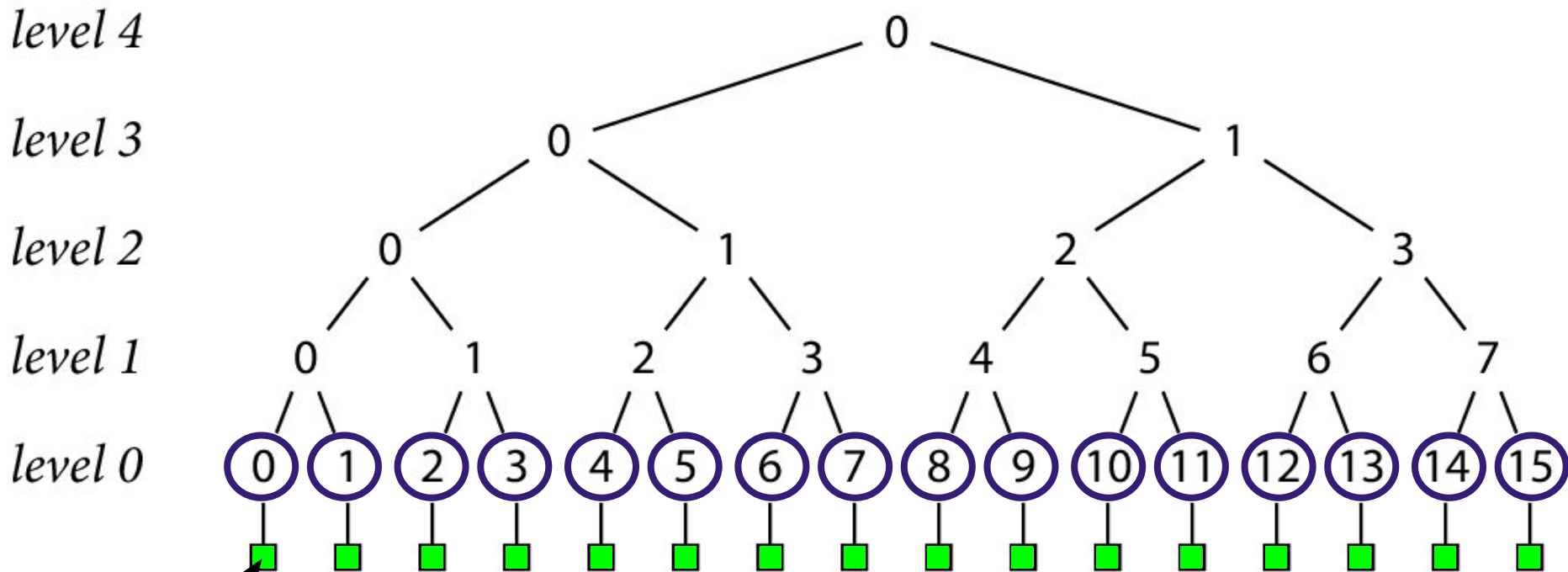
level 0



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

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

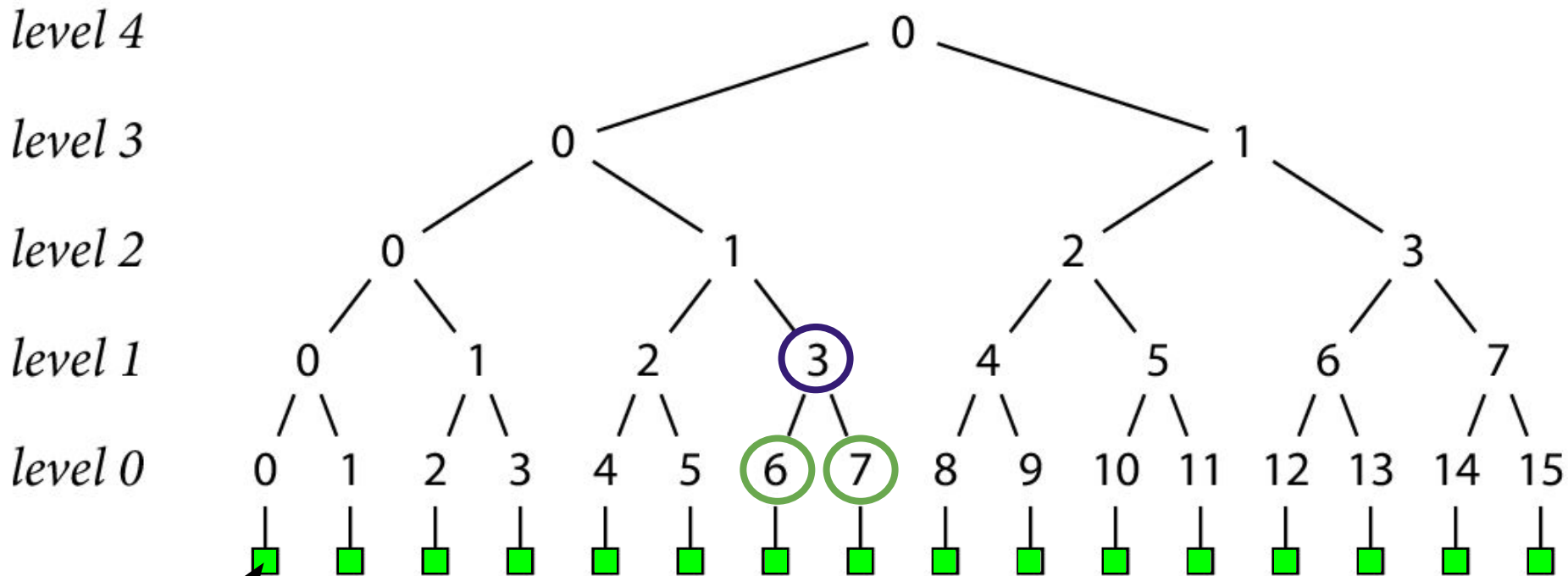
Checksum DB



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

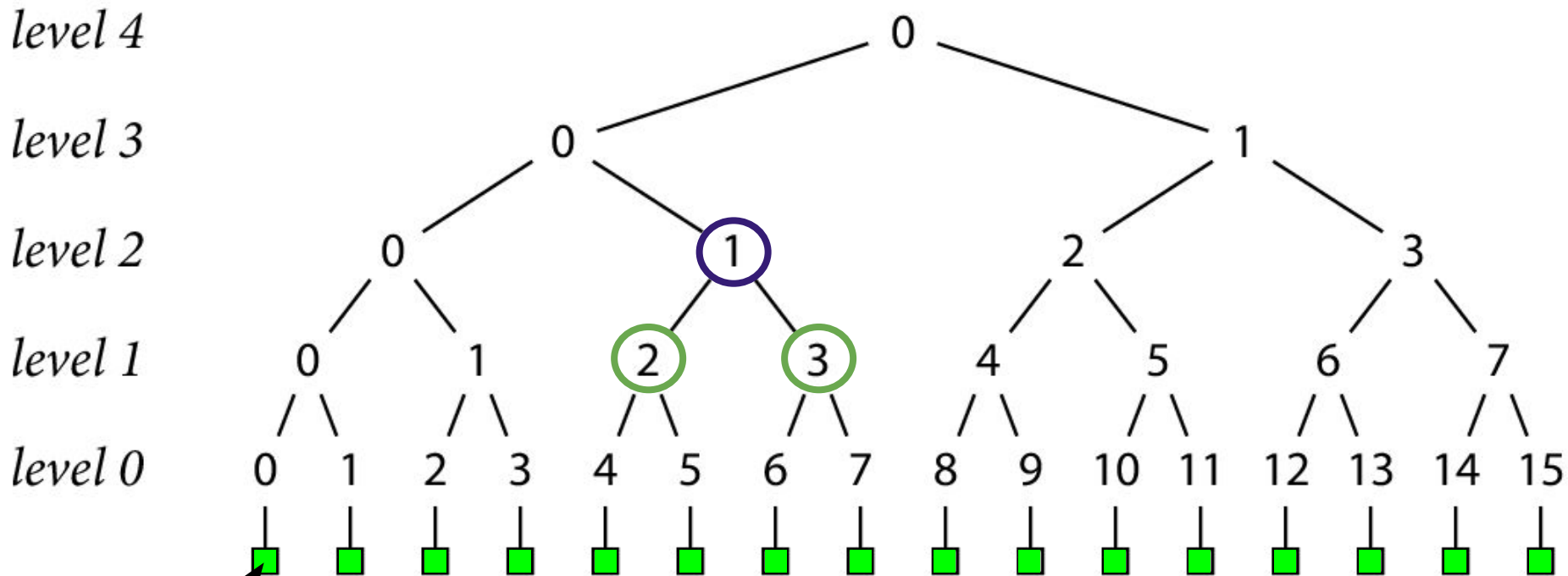
go.opencensus.io v0.19.2/go.mod h1:N0/8qkisMZLZ1FC...

Checksum DB



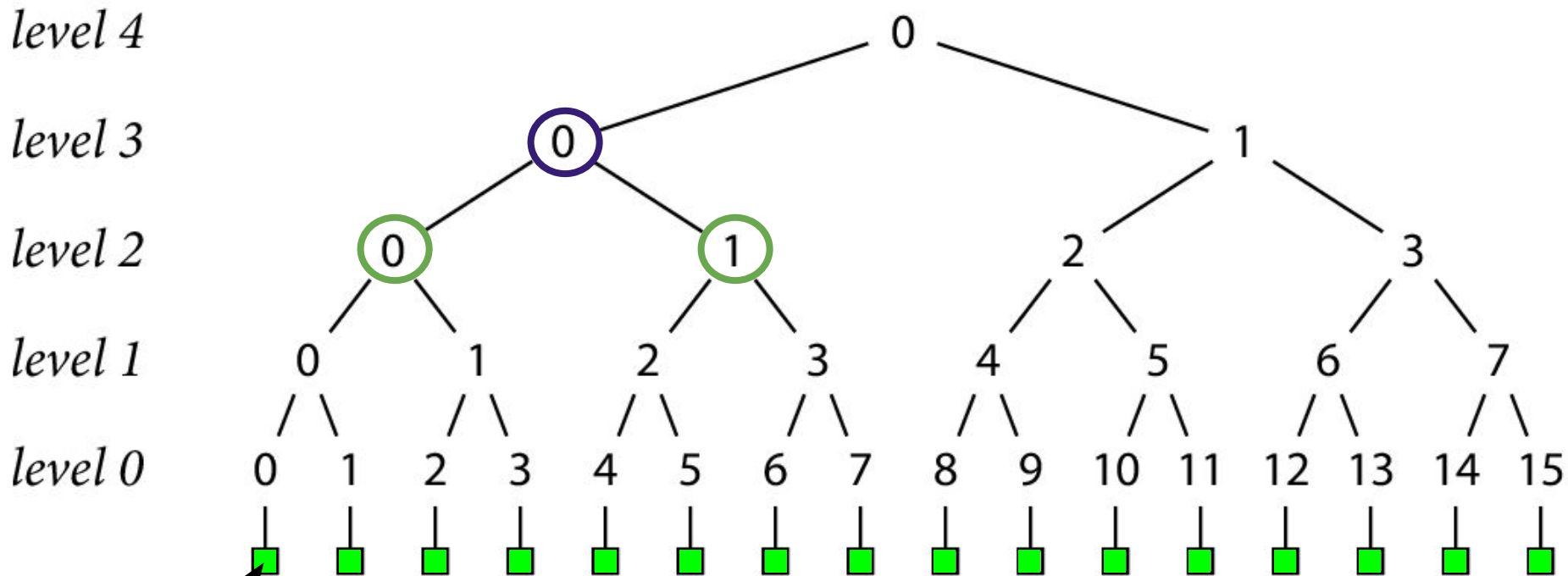
go.opencensus.io v0.19.2 h1:ZZpq6xI6kv/LuE/5s5UQvB...

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



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

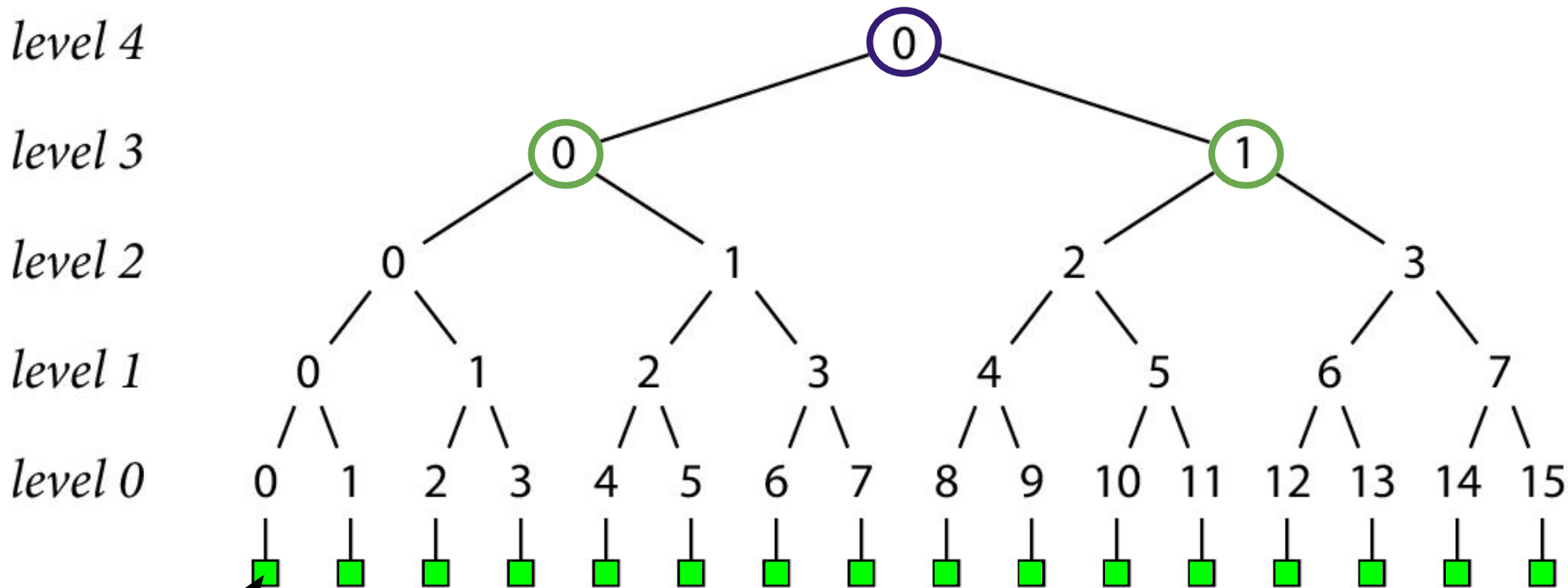
go.opencensus.io v0.19.2/go.mod h1:N0/8qkisMZLZ1FC...



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

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

Checksum DB



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

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

Checksum DB

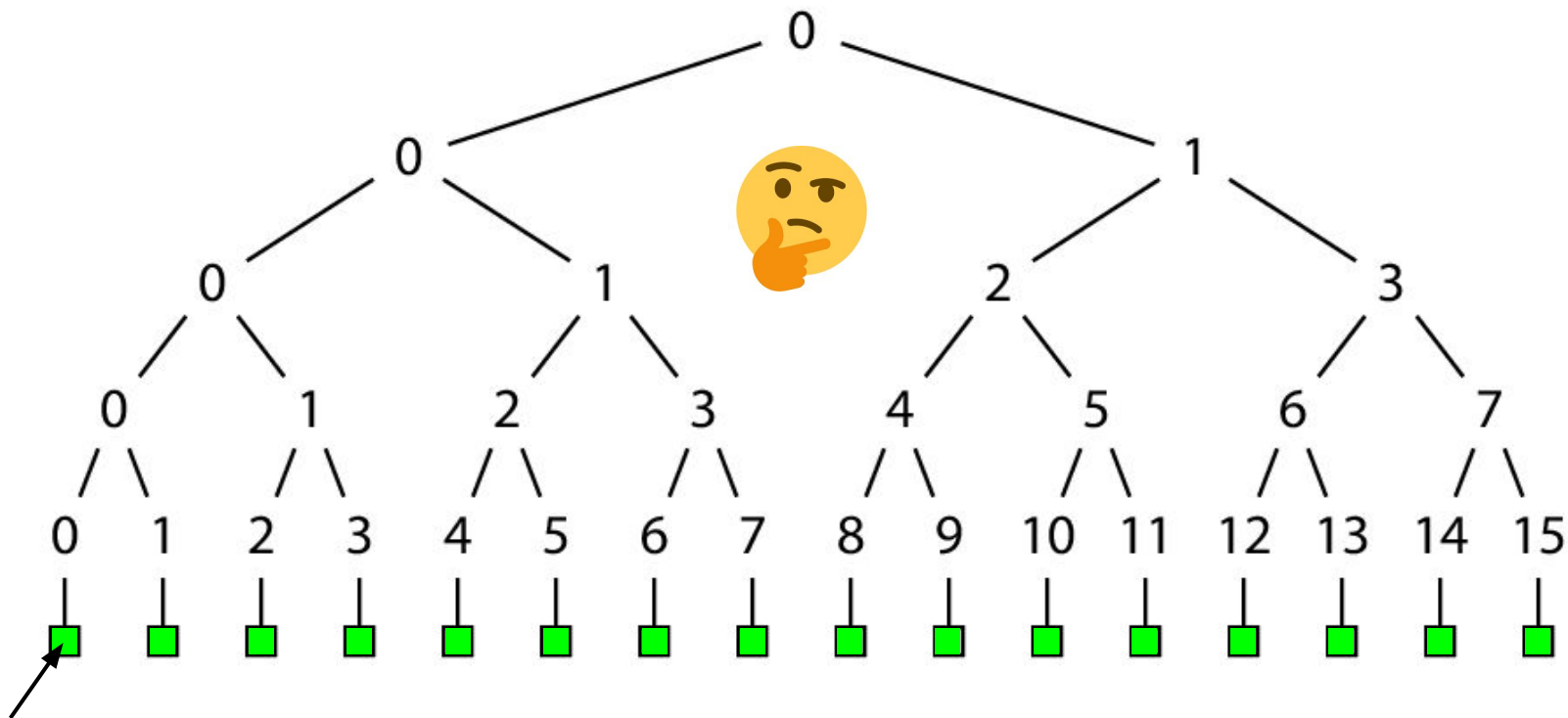
level 4

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 DB

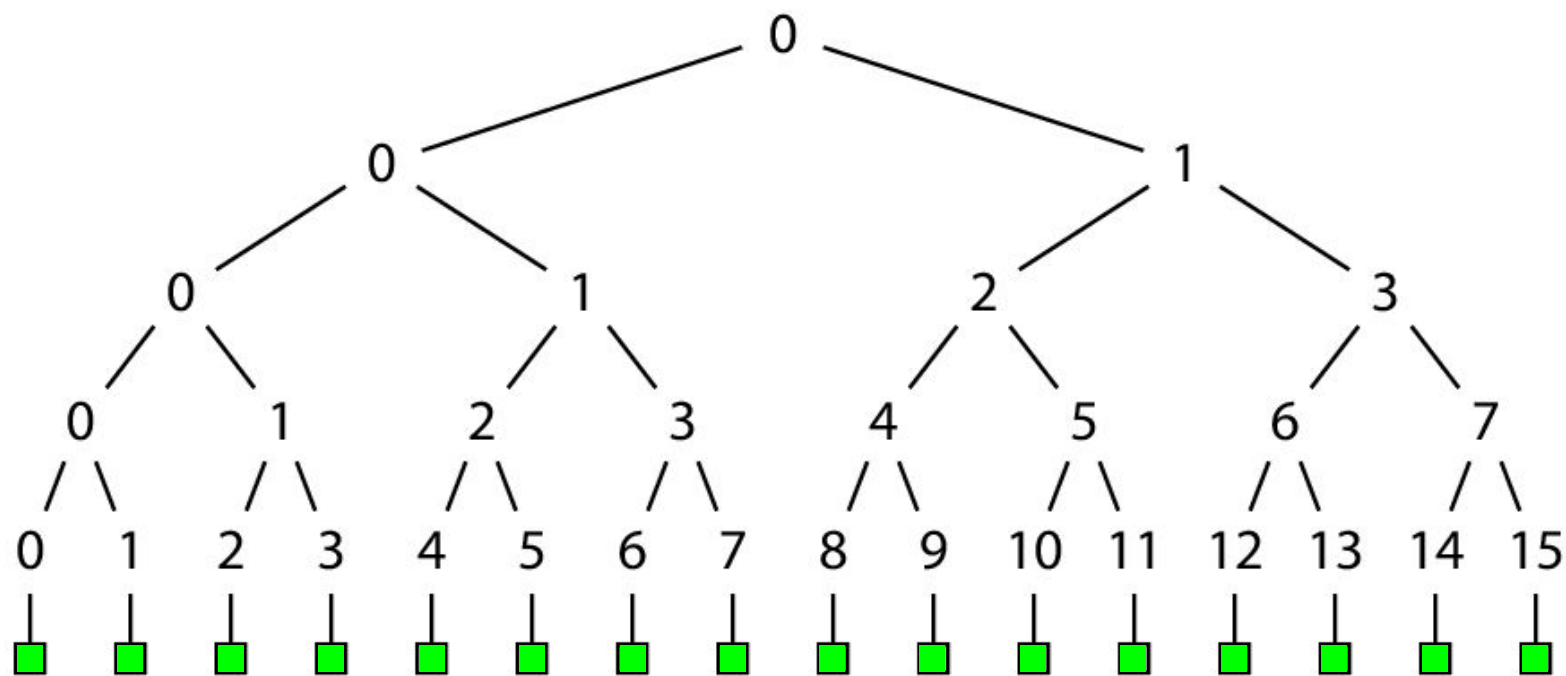
level 4

level 3

level 2

level 1

level 0



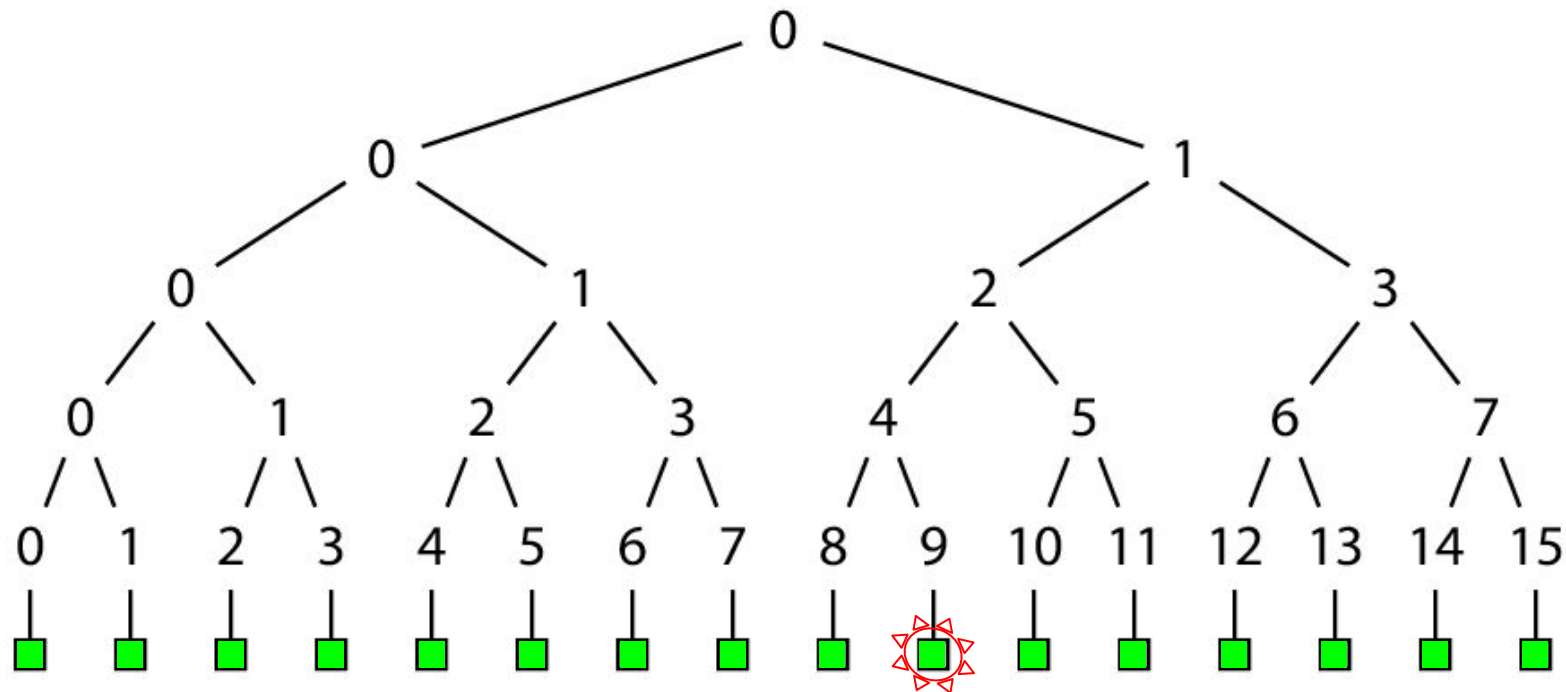
level 4

level 3

level 2

level 1

level 0



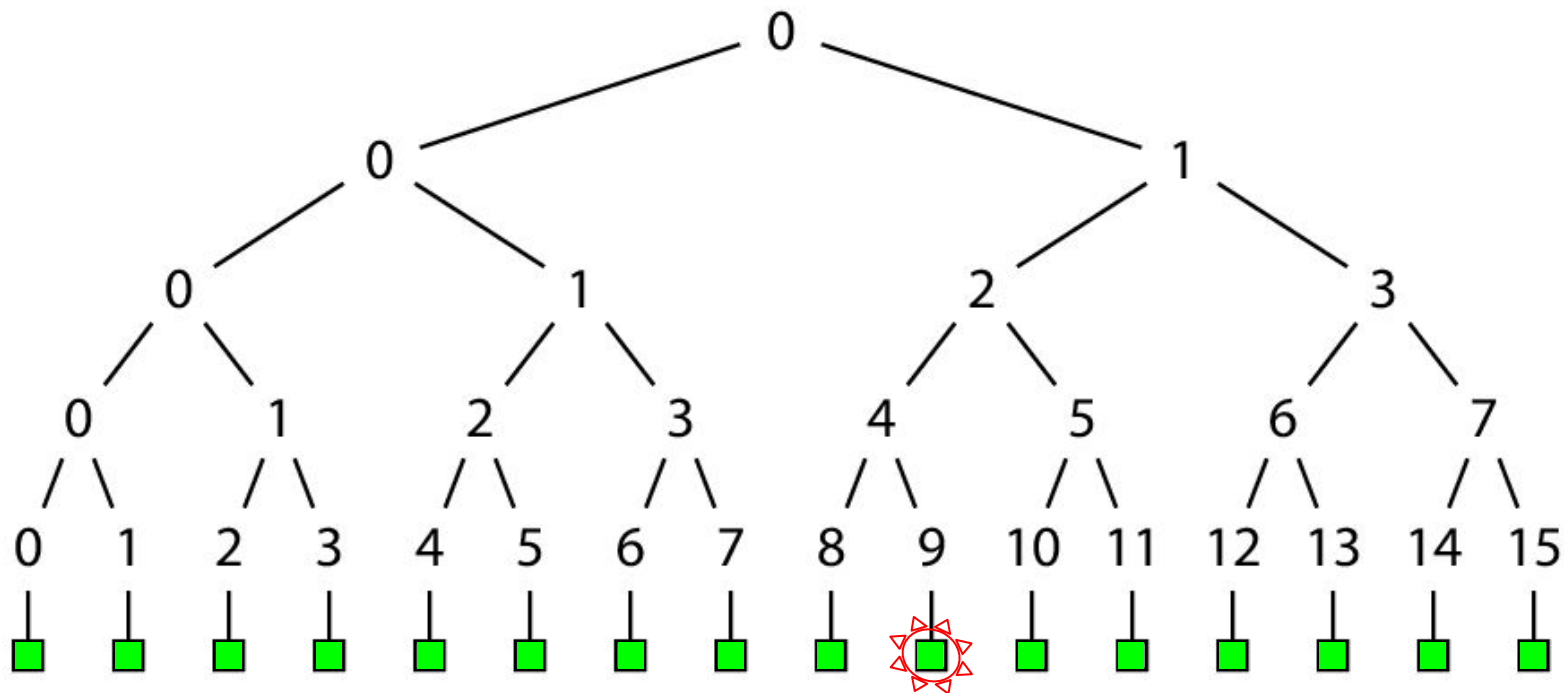
level 4

level 3

level 2

level 1

level 0



/lookup/go.dog/breeds@v0.3.2

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

Checksum DB

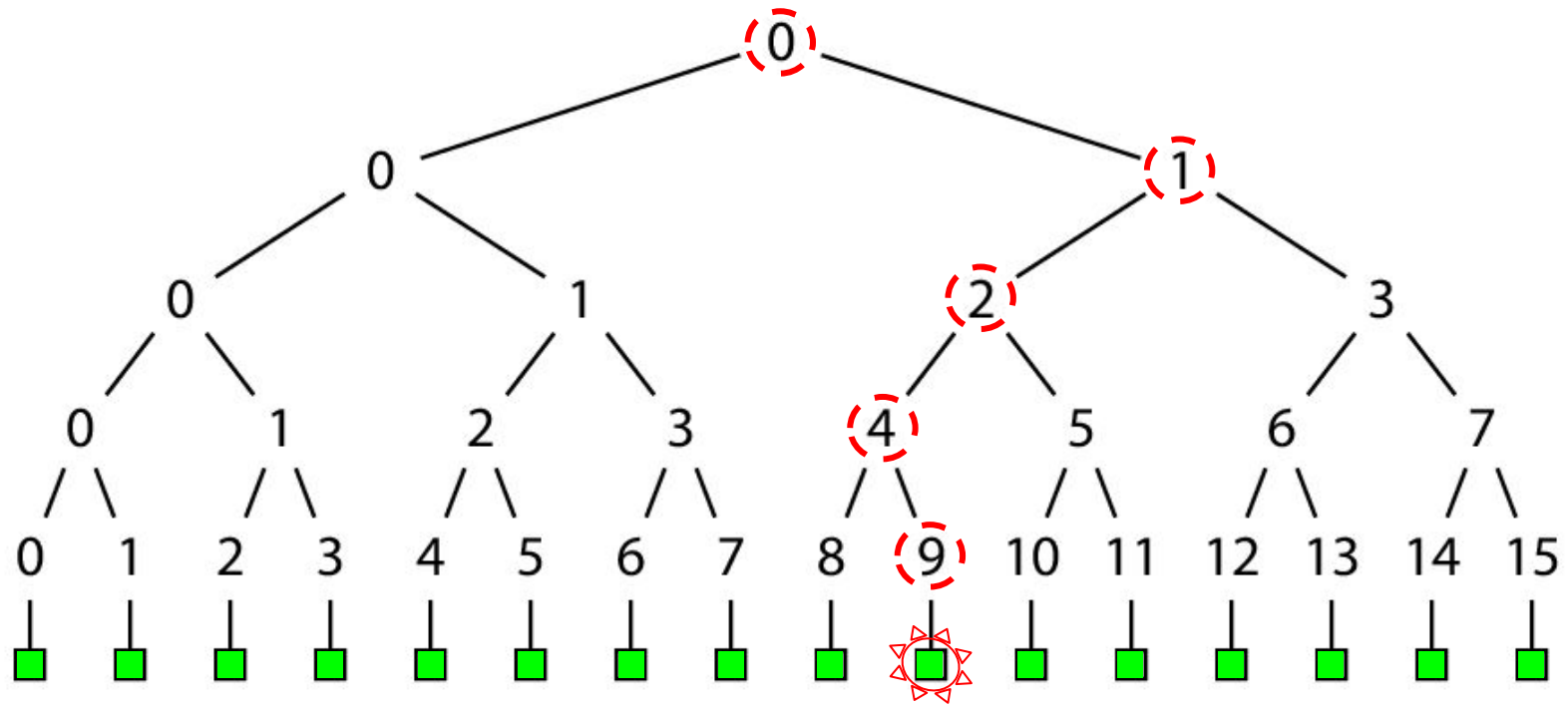
level 4

level 3

level 2

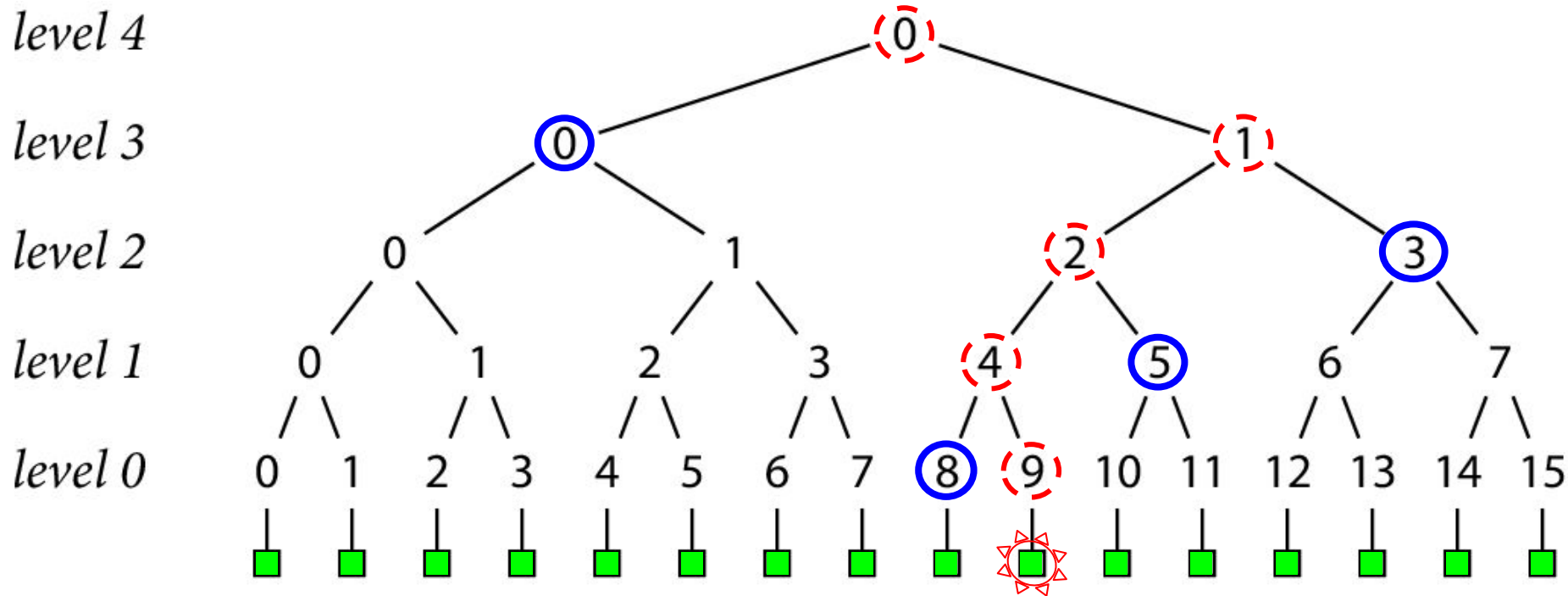
level 1

level 0



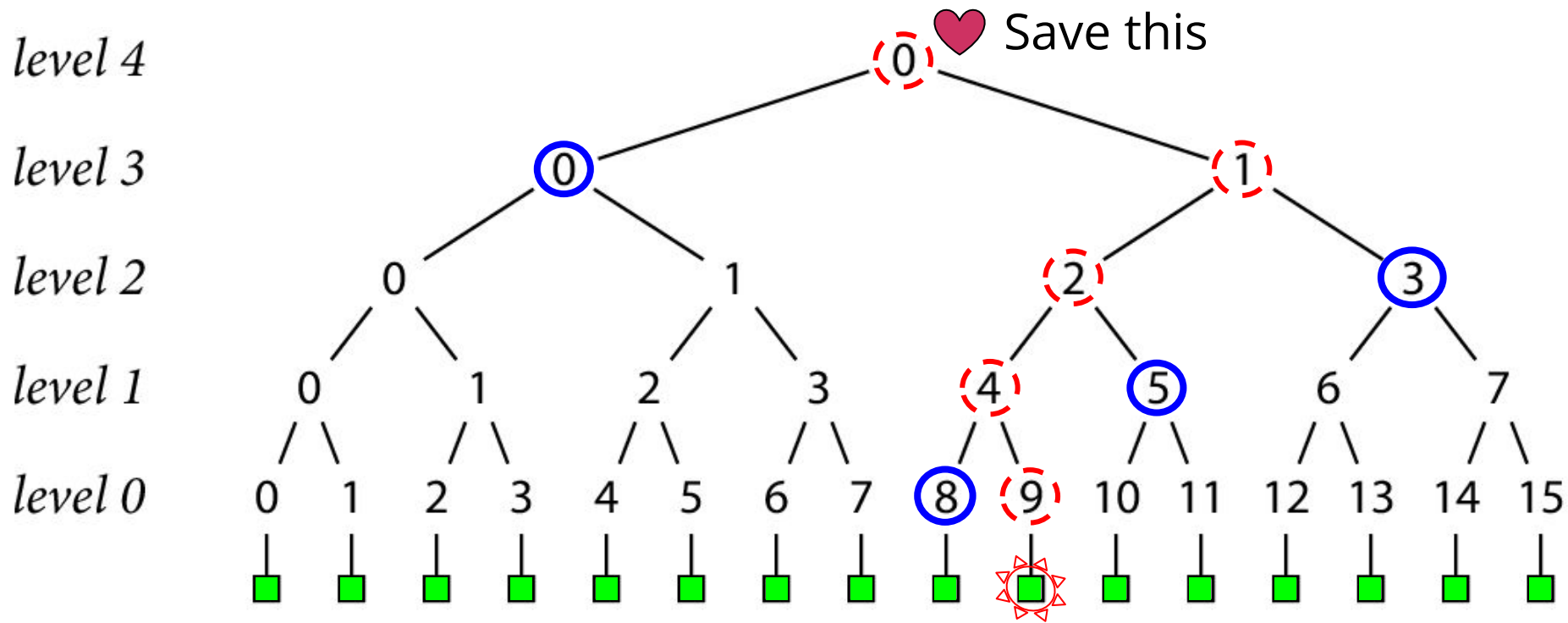
/lookup/go.dog/breeds@v0.3.2

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



/lookup/go.dog/breeds@v0.3.2

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



/lookup/go.dog/breeds@v0.3.2

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

Checksum DB

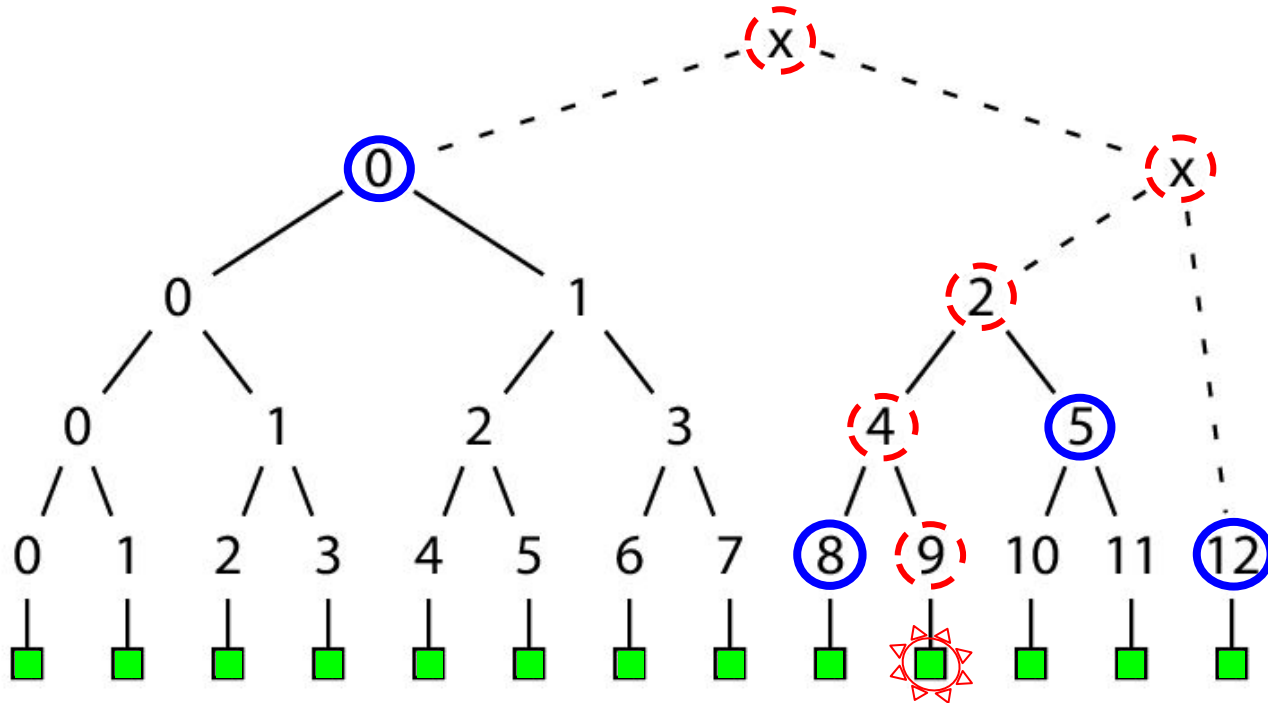
level 4

level 3

level 2

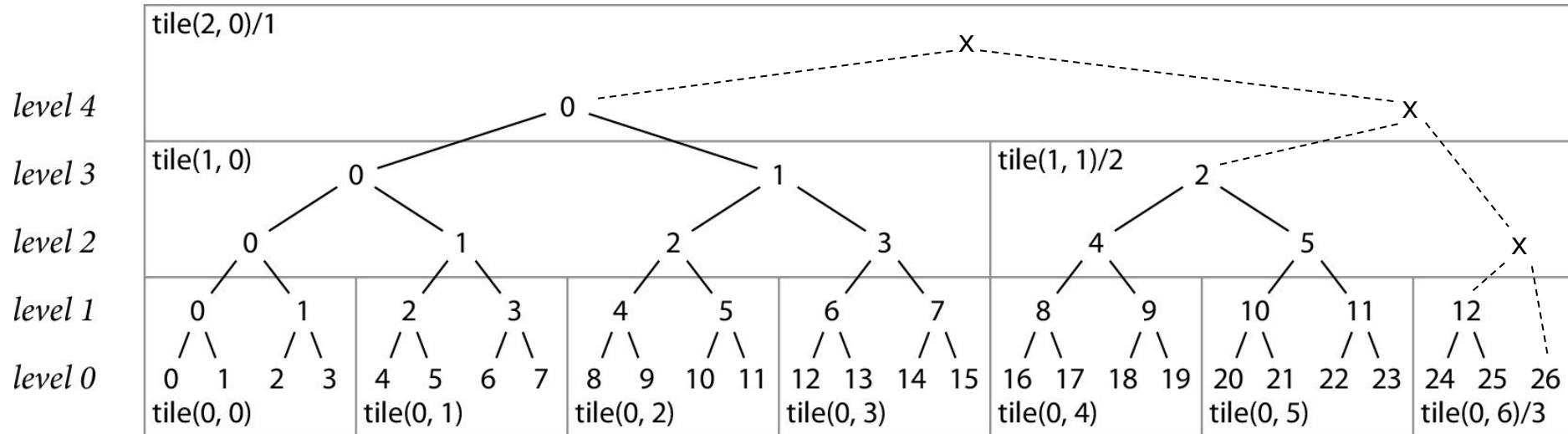
level 1

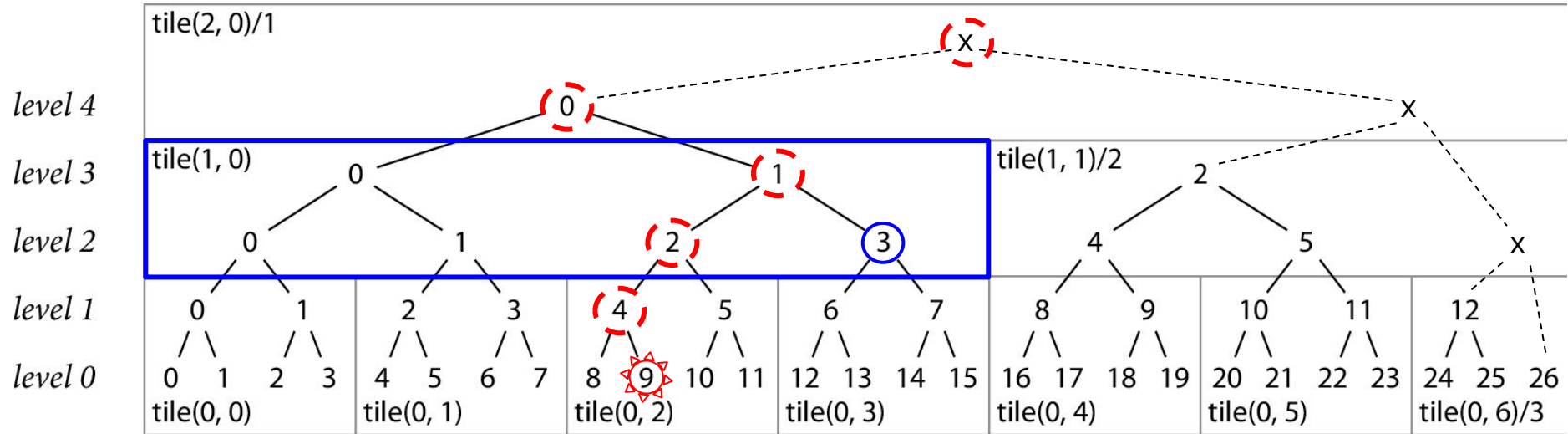
level 0

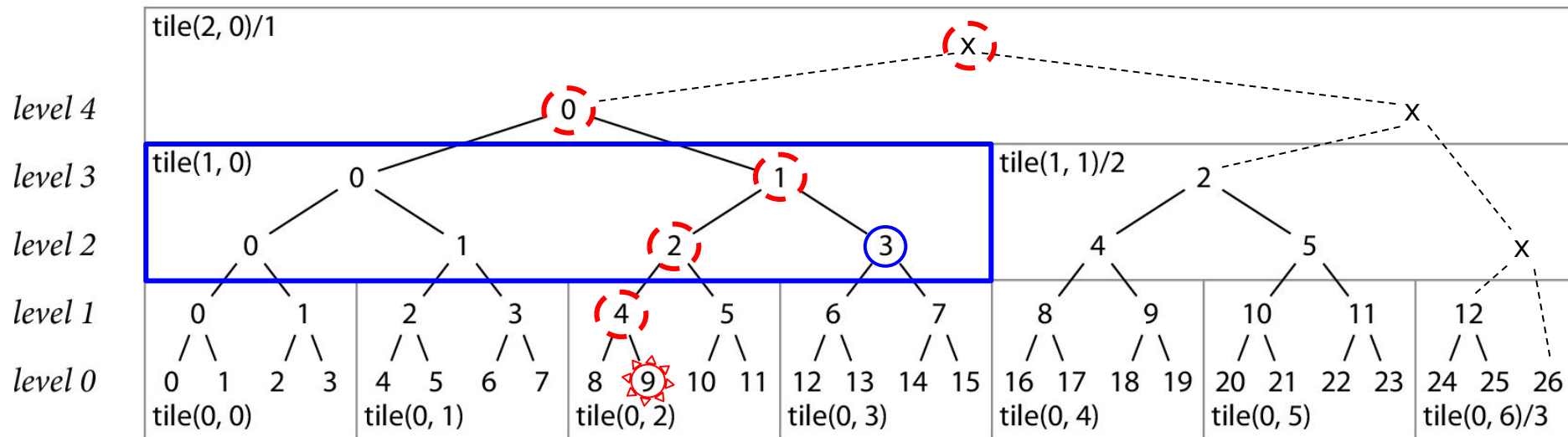


Tiles!









✓ Cache friendly

✓ Less storage

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

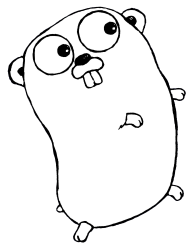
11131

uJ+UzAf0s0Gi22MuICyemMge4fp8gI3+5+wZF5t1aXU=

– sum.golang.org

Az3grjQmIfBoZv0eH1eRf4gu7VNSS8Lv sdfECddEnVIA1drPr
g29LDmVliD3dshfo9ZYr1Gq0HWyVWXJ96ZjDpiSvgY=

go get go.dog/breeds

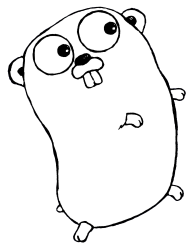


go
command

Checksum
database

Checksum DB

```
go get go.dog/breeds
```



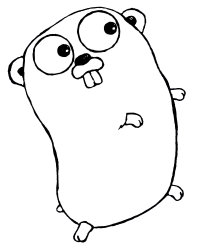
go
command

`$GOSUMDB/lookup/go.dog/breeds@v0.3.2`

Checksum
database

Checksum DB

go get go.dog/breeds



go
command

\$GOSUMDB/lookup/go.dog/breeds@v0.3.2

9

go.dog/breeds v0.3.2 <hash>

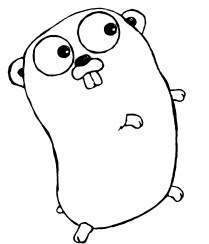
go.dog/breeds v0.3.2/go.mod <hash>

<STH>

Checksum
database

Checksum DB

go get go.dog/breeds



go
command

\$GOSUMDB/lookup/go.dog/breeds@v0.3.2

9

go.dog/breeds v0.3.2 <hash>

go.dog/breeds v0.3.2/go.mod <hash>

<STH>

Checksum
database

\$GOSUMDB/tile/8/0/005

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

[... more tiles]

Checksum DB

“Trust on ~~your~~ first use”
anyone’s

Why use the
checksum
database?

- ✓ Validates untrusted
proxies

Why use the checksum database?

- ✓ Validates untrusted proxies
- ✓ Mitigates hacked origins

Why use the checksum database?

- ✓ Validates untrusted proxies
- ✓ Mitigates hacked origins
- ✓ Prevents author error

Why use the checksum database?

- ✓ Validates untrusted proxies
- ✓ Mitigates hacked origins
- ✓ Prevents author error
- ✓ Easy to use

Better solutions

- ✓ Reproducible builds Modules
- ✓ Persistent dependencies Mirror
- ✓ Trustworthy fetches Checksum Database



Setting up your environment



On by default in Go 1.13

Environment variables

- **GO111MODULE**
 - `GO111MODULE="on"`
- **GOPROXY**
 - `GOPROXY="https://proxy.golang.org,direct"`

For private modules

- GOPRIVATE
 - GOPRIVATE="*.corp.google.com,rsc.io/private"

Trillian

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

A transparent, highly scalable and
cryptographically verifiable data store.



One more cool thing



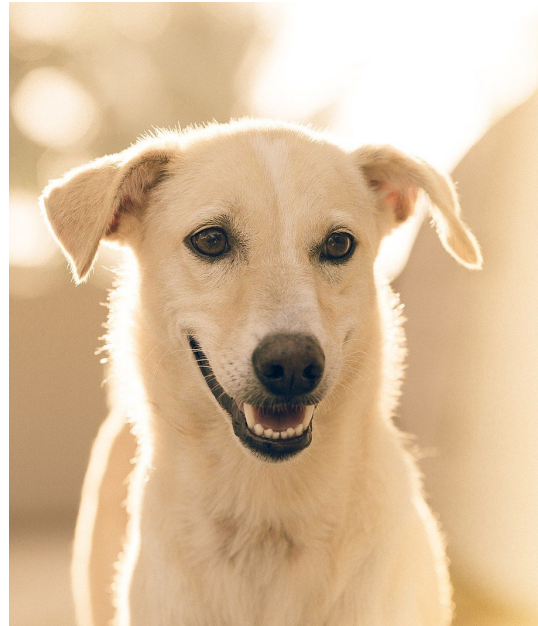
index.golang.org/index

- 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

The future of Go



Katie Hockman

github.com/katiehockman

Twitter: @katie_hockman

