

Are your Zones Resolvable?

Detecting DNS(SEC) Misconfigurations with Formal Reasoning

Felix Linker
ETH Zurich

Yue Huang
HKUST(GZ)

David Basin
ETH Zurich

Huayi Duan
HKUST(GZ)

DNS Zone Configuration Errors are a Problem

They even have names!

Lame Delegation

Rewrite Blackholing

DNS Zone Configuration Errors are a Problem

• Press Release

DENIC reports DNSSEC disruption affecting .de domains

👤 DENIC-Redaktion 📅 May 6, 2026 ⌚ 1 min read

Formal Reasoning has been suggested



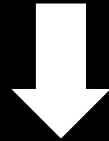
GRoot: Proactive Verification of DNS Configurations

Siva Kesava Reddy Kakarla UCLA sivakesava@cs.ucla.edu	Ryan Beckett Microsoft Research ryan.beckett@microsoft.com	Behnaz Arzani Microsoft Research bearzani@microsoft.com
Todd Millstein UCLA & Intentionet todd@cs.ucla.edu	George Varghese UCLA varghese@cs.ucla.edu	

Formal Reasoning has been suggested



Two problems with these approaches

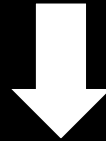


1. Verify absence of *some* errors
2. DNSSEC not supported

Formal Reasoning has been suggested



Two problems with these approaches

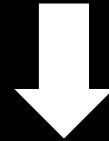


1. **Verify absence of *some* errors**
2. DNSSEC not supported

Formal Reasoning has been suggested



Two problems with these approaches



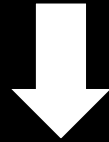
1. **Verify absence of *some* errors**
2. DNSSEC not supported

You have to know
what you're looking
for

Formal Reasoning has been suggested



Two problems with these approaches



1. Verify absence of *some* errors
2. **DNSSEC not supported**

Issues like DENIC
outage require
DNSSEC

A New Formal Model to Detect DNS Misconfigurations

1. Can detect errors without explicitly looking for them
2. Support for DNSSEC



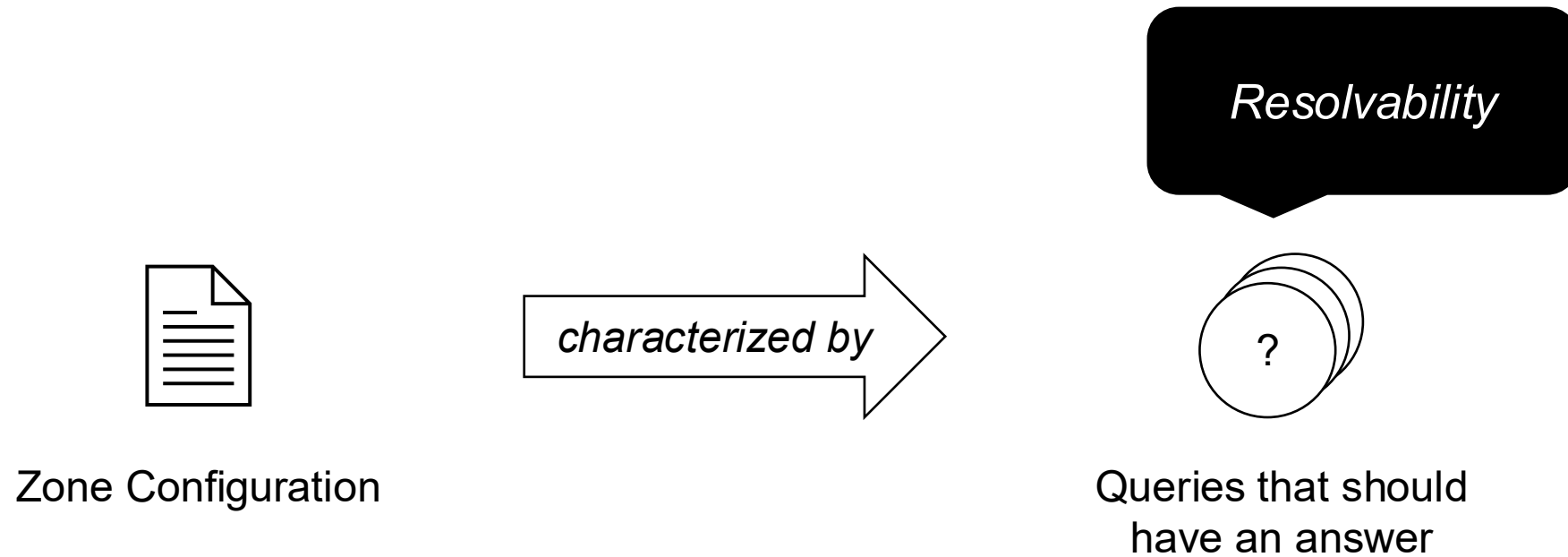
...more on this later...

Agenda

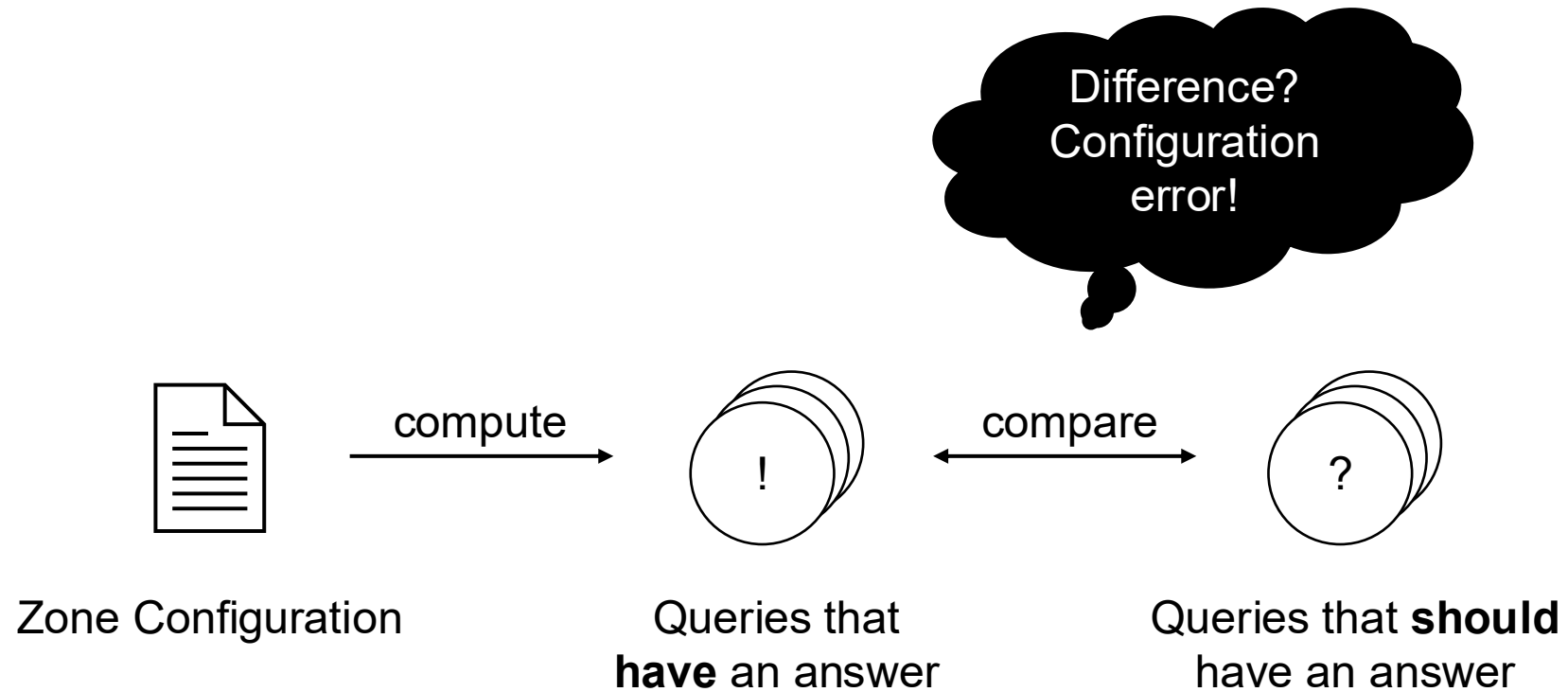
1. Which property do we target?
2. *How* does our model work?
3. How *well* does our model work?
4. How could our model be used?

Which property do we target?

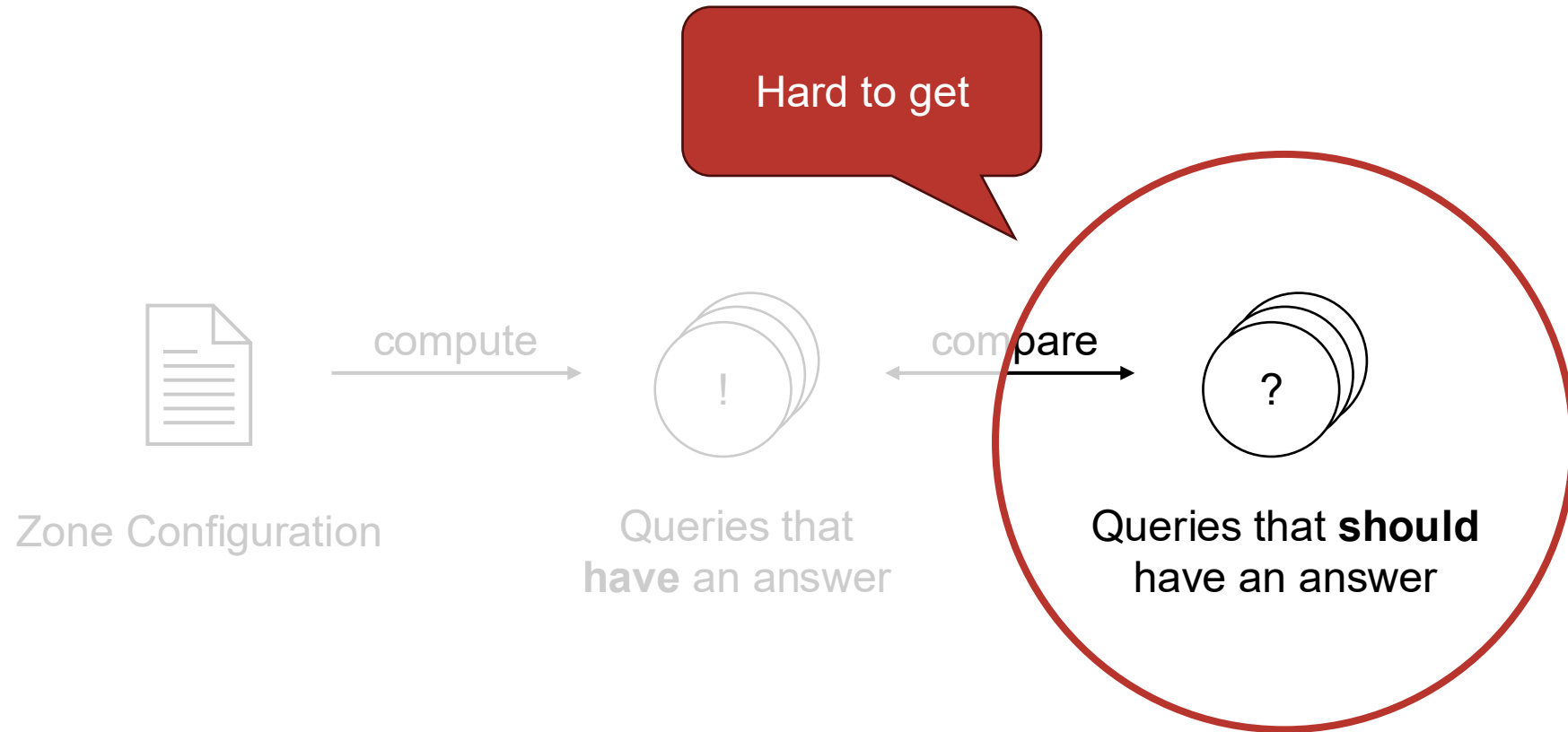
Which property do we target?



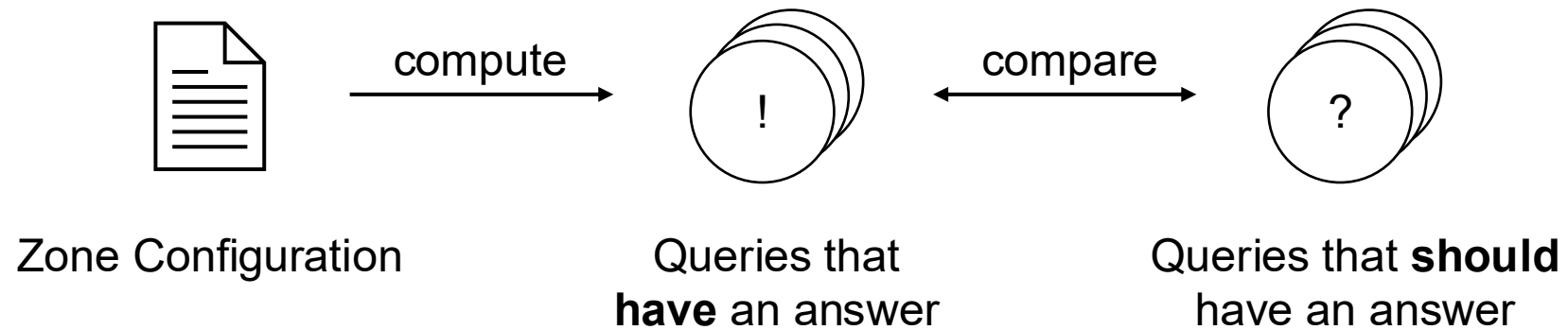
Which property do we target?



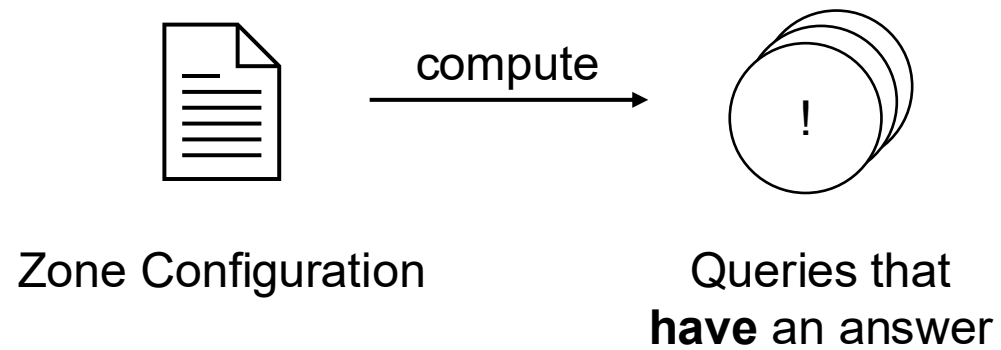
Which property do we target?



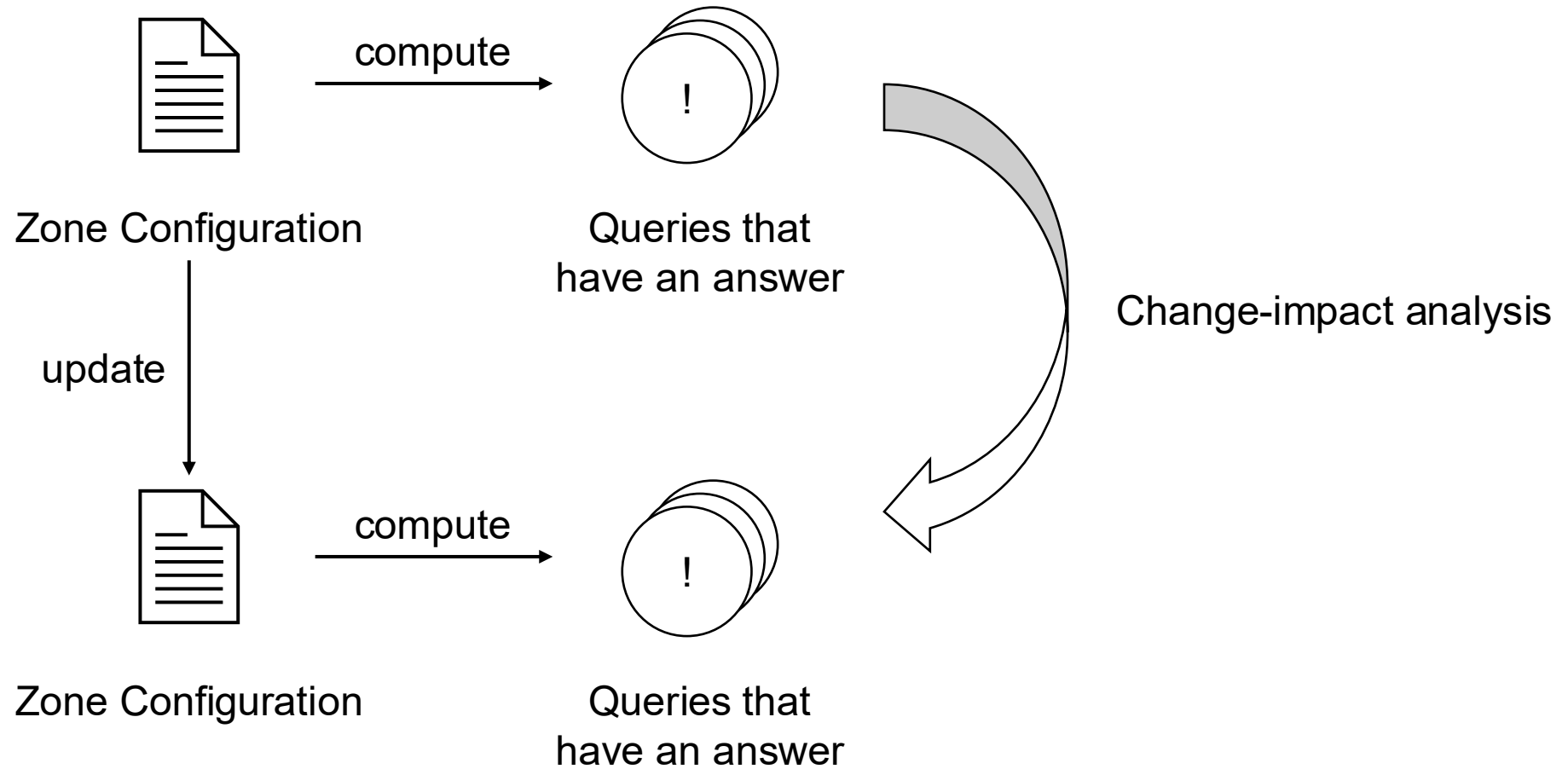
Which property do we target?



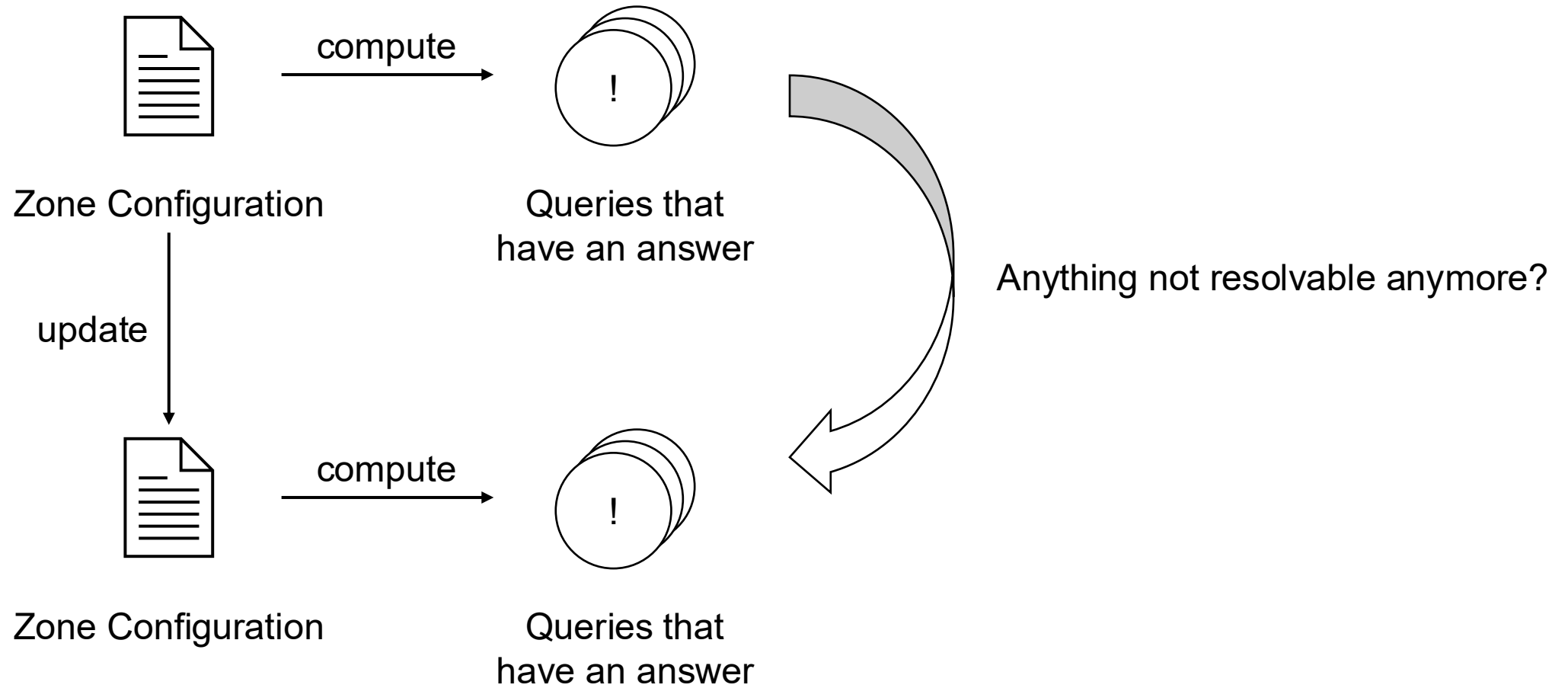
Which property do we target?



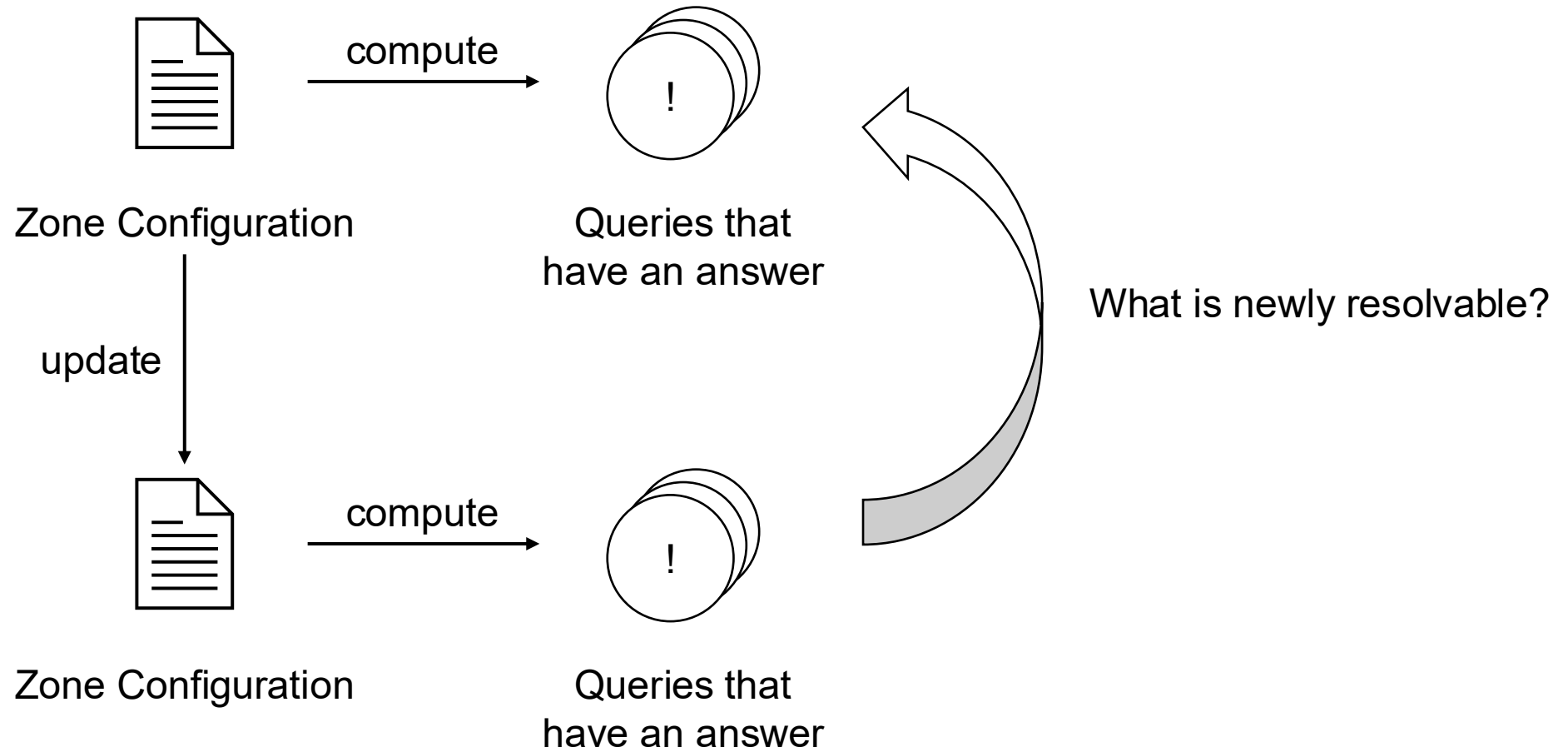
Which property do we target?



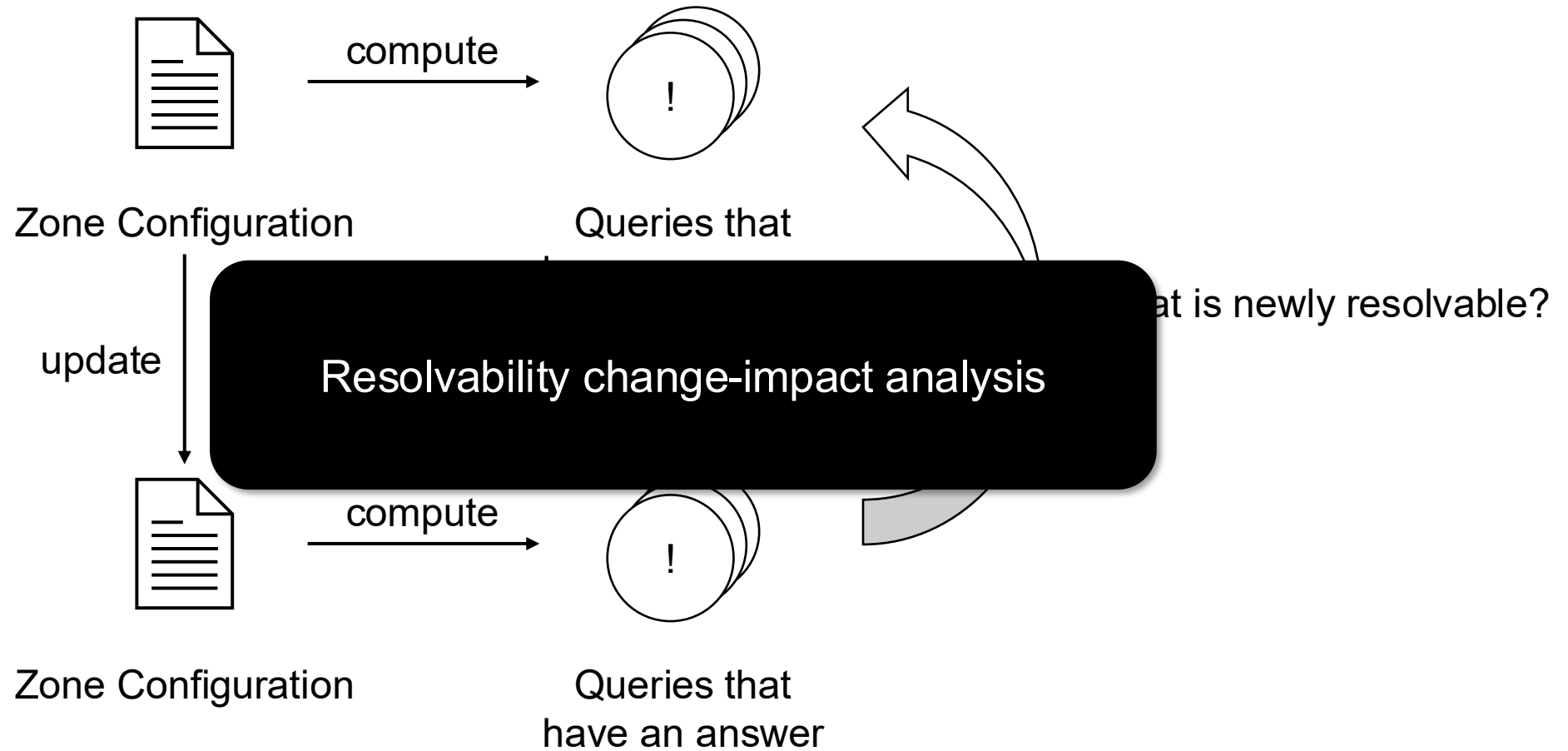
Which property do we target?



Which property do we target?



Which property do we target?



Which property do we target?

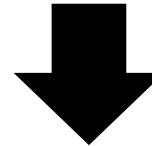
Resolvability change-impact analysis

Requires
interpretation

Which property do we target?

Resolvability change-impact analysis

Requires interpretation



Could have detected

• Press Release

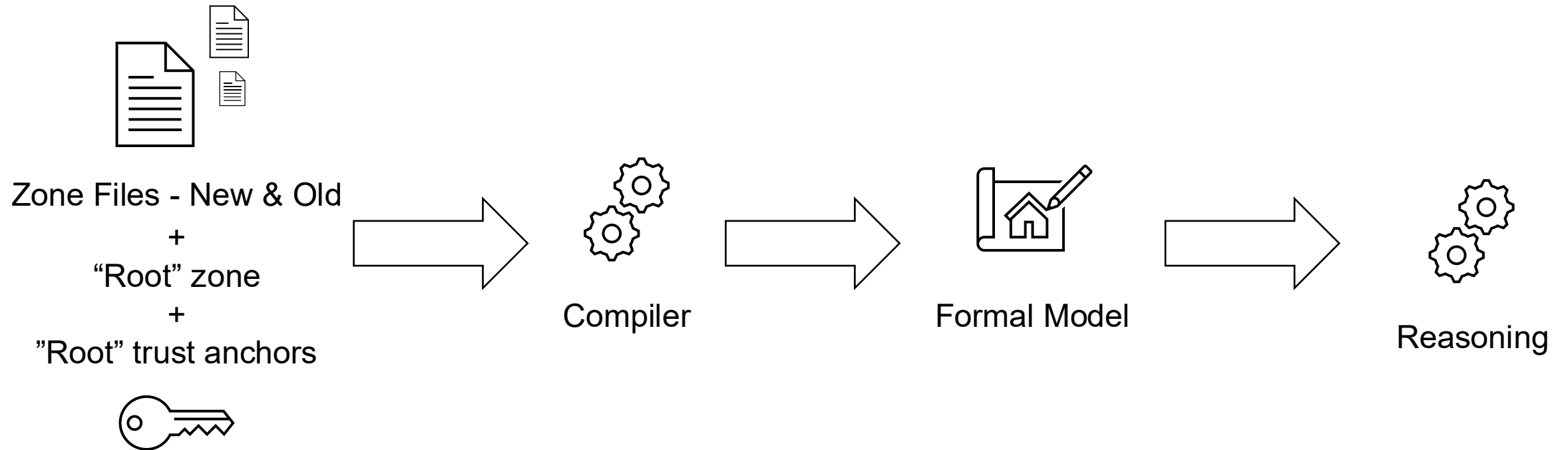
DENIC reports DNSSEC disruption affecting .de domains

👤 DENIC-Redaktion 📅 May 6, 2026 ⌚ 1 min read

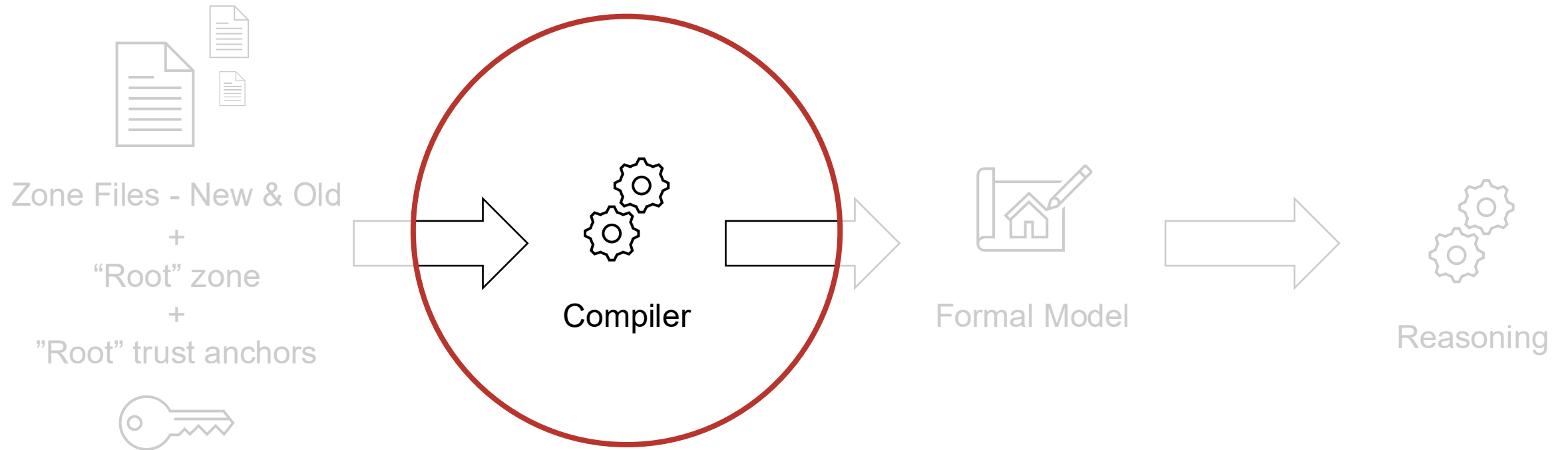
...changes which should preserve resolvability

How does our model work?

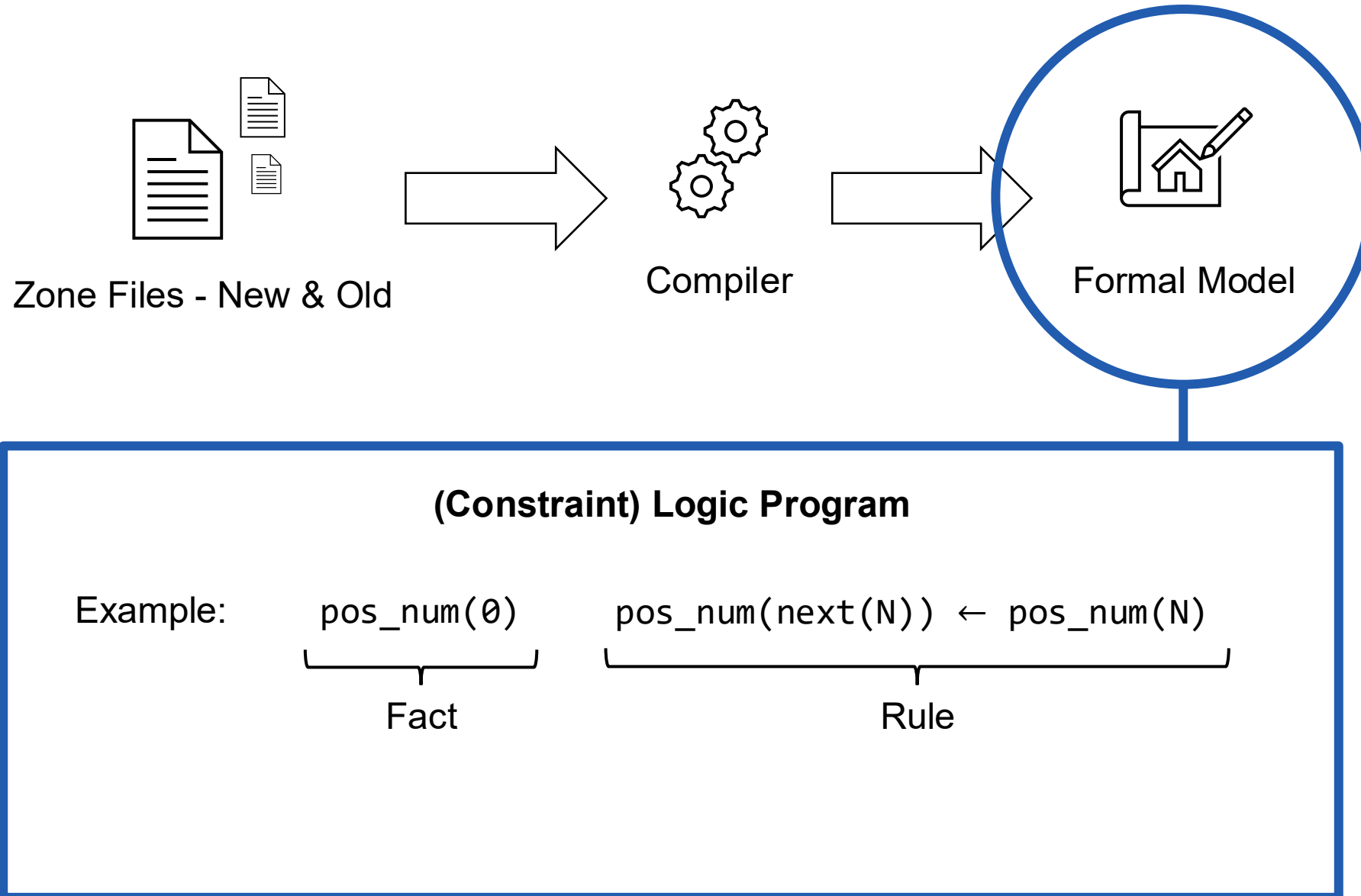
How does our model work?



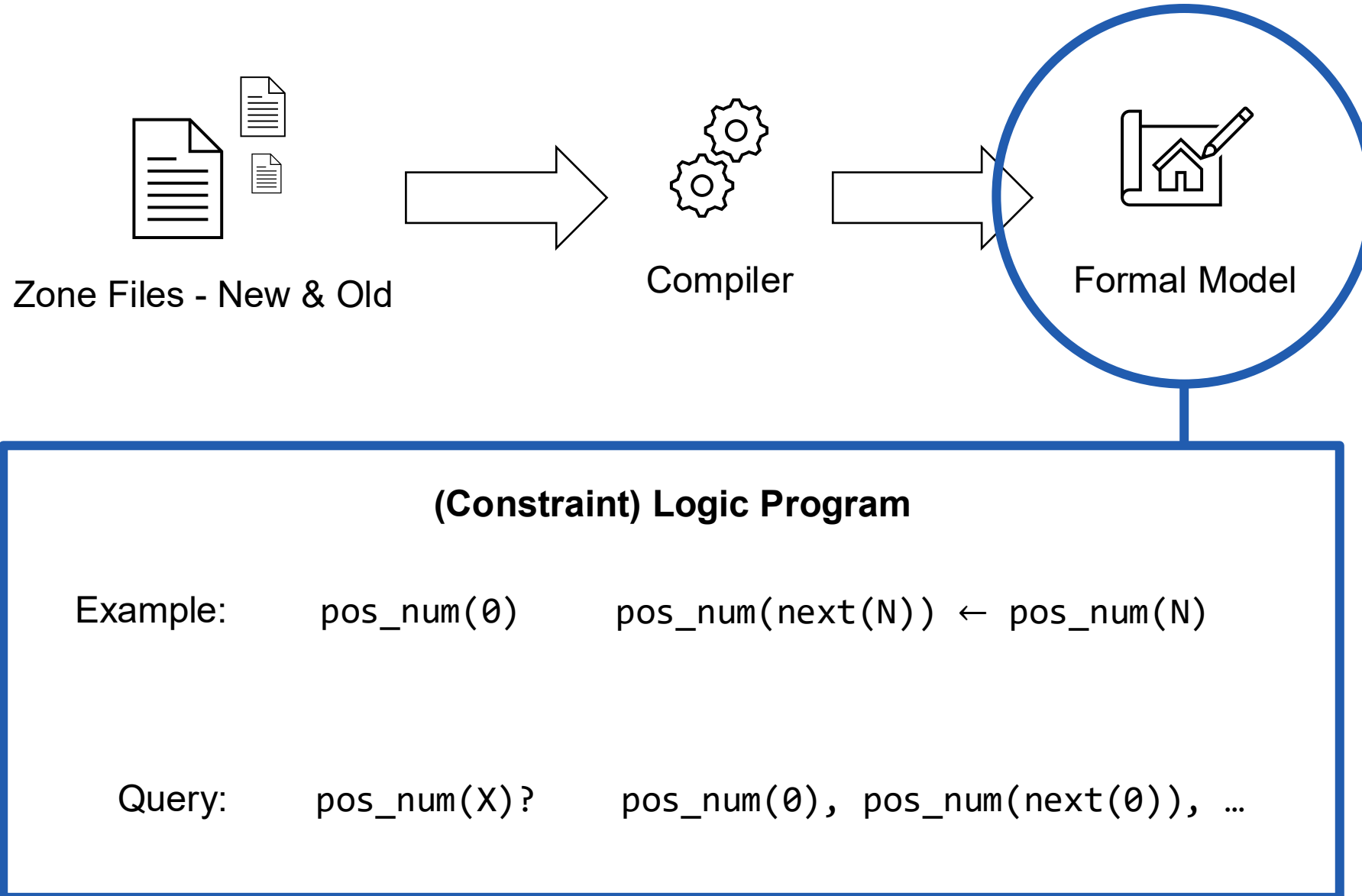
How does our model work?



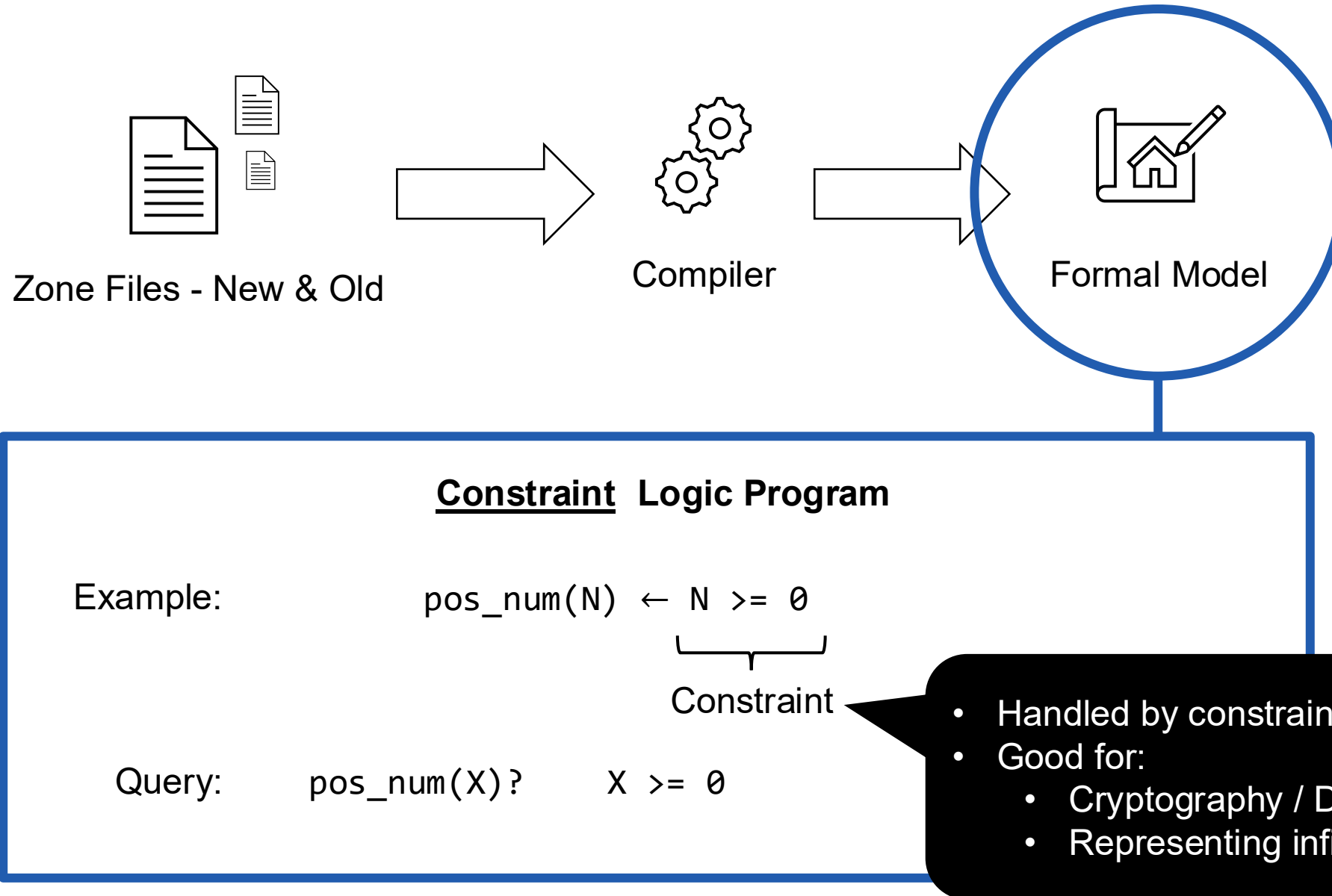
How does our model work?



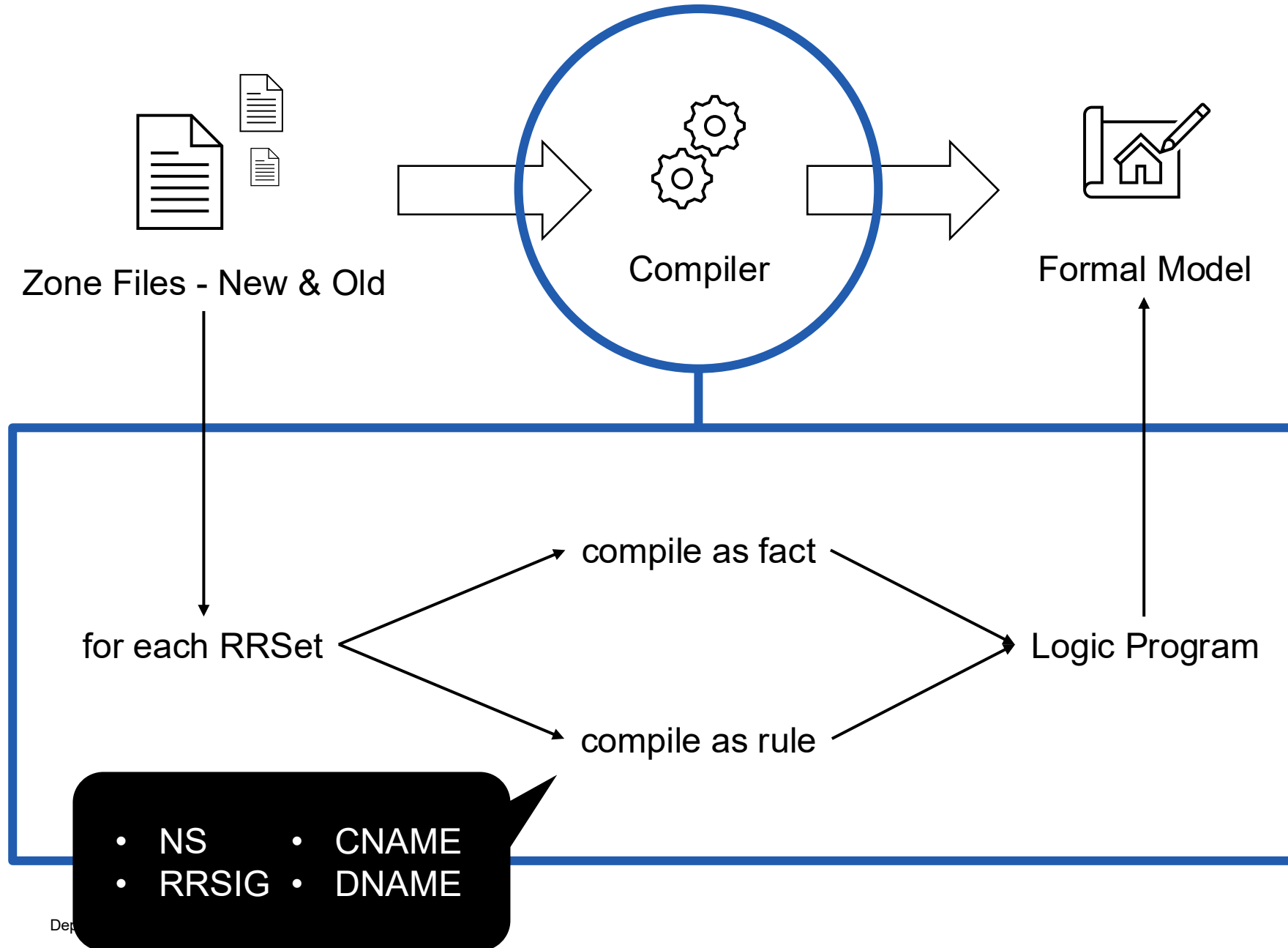
How does our model work?



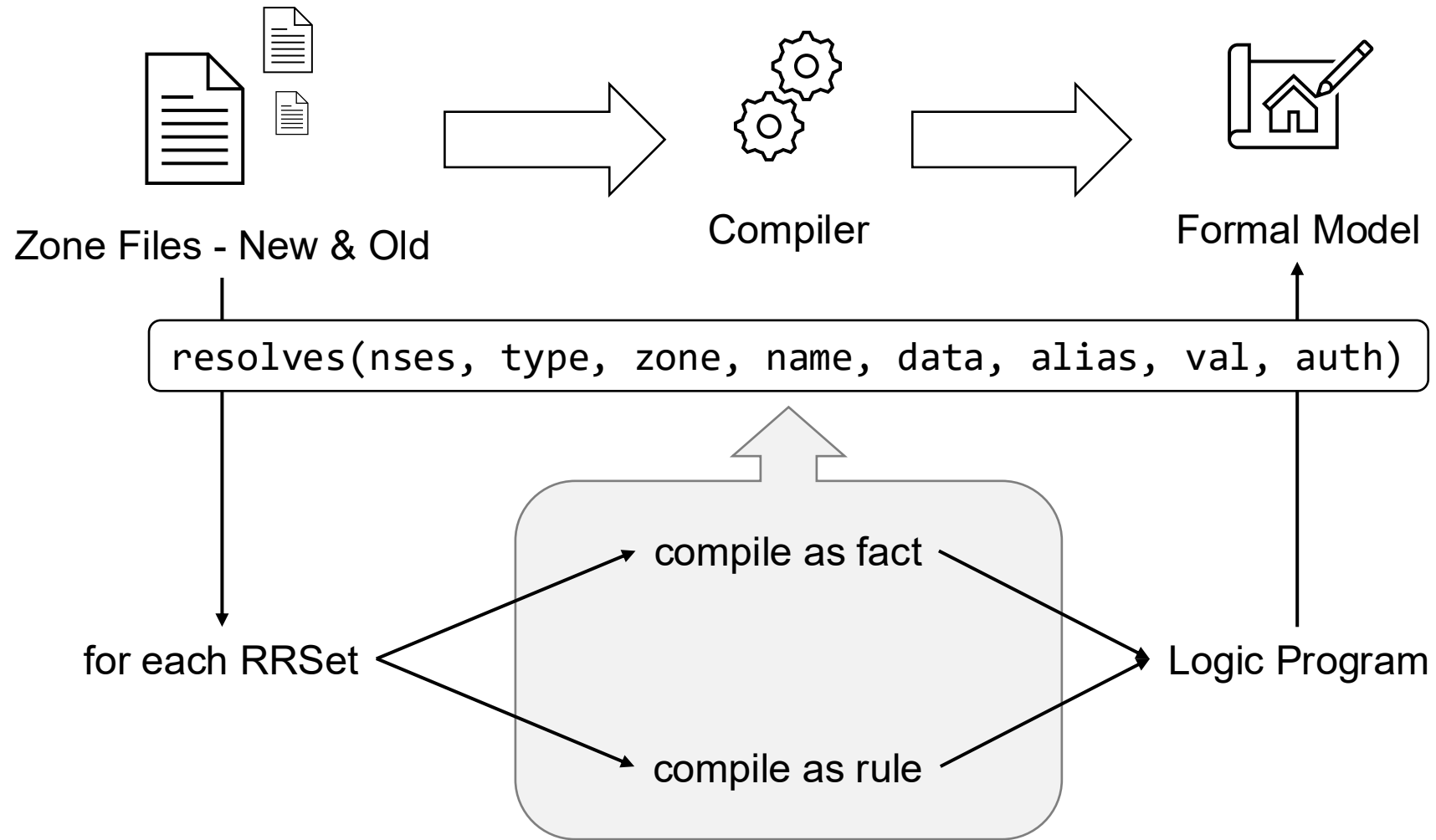
How does our model work?



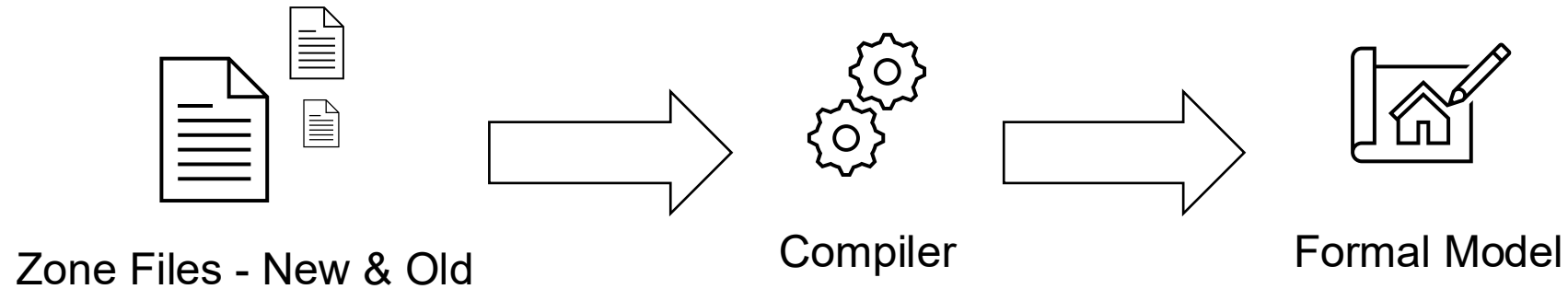
How does our model work?



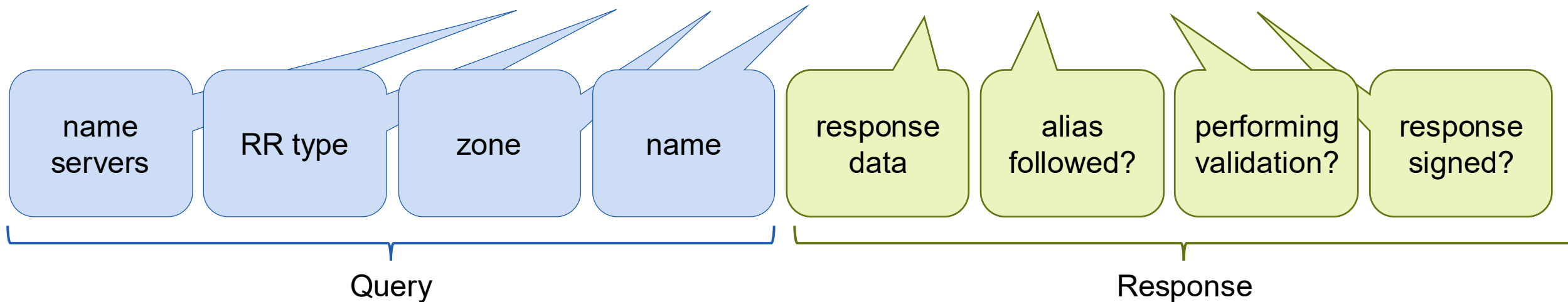
How does our model work?



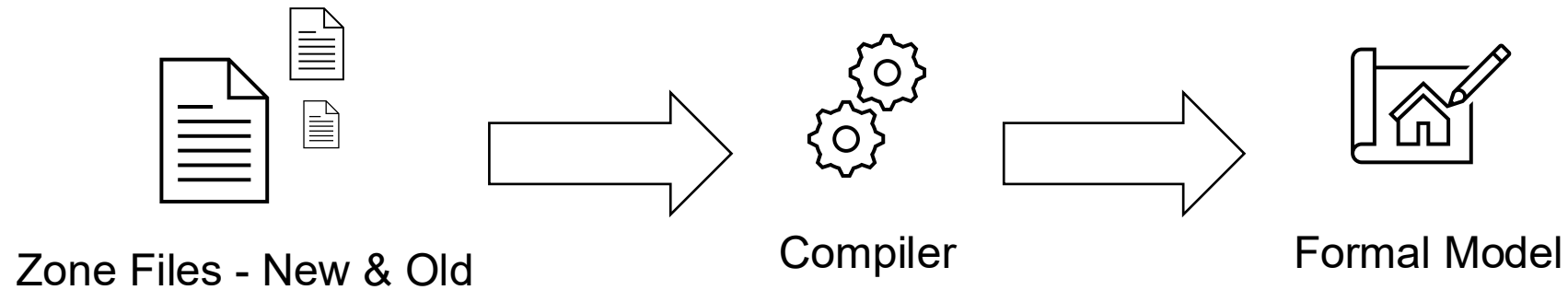
How does our model work?



```
resolves(nses, type, zone, name, data, alias, val, auth)
```



How does our model work?

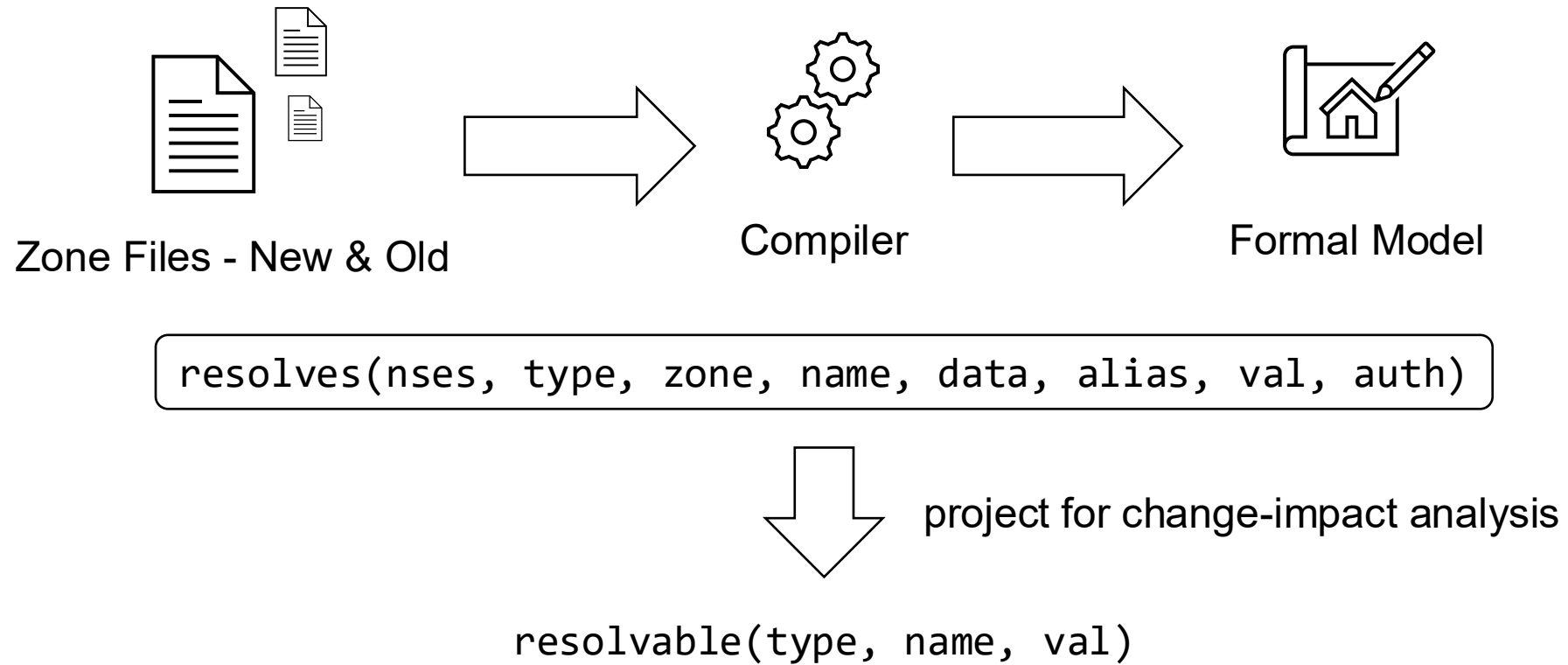


```
resolves(nses, type, zone, name, data, alias, val, auth)
```

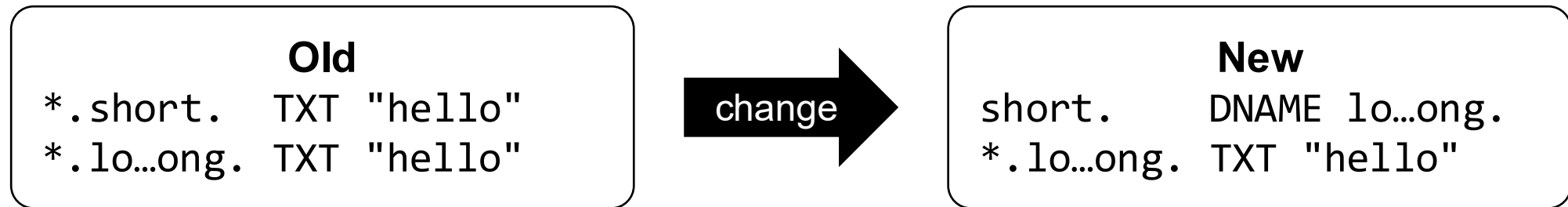
Scope of Model

- Abstract from:
 - Transport, headers, etc.
 - NSes serving inconsistent data
 - Cache
- Goal: What would resolvers conclude given input data?

How does our model work?



How does our model work? – Example



Impact?

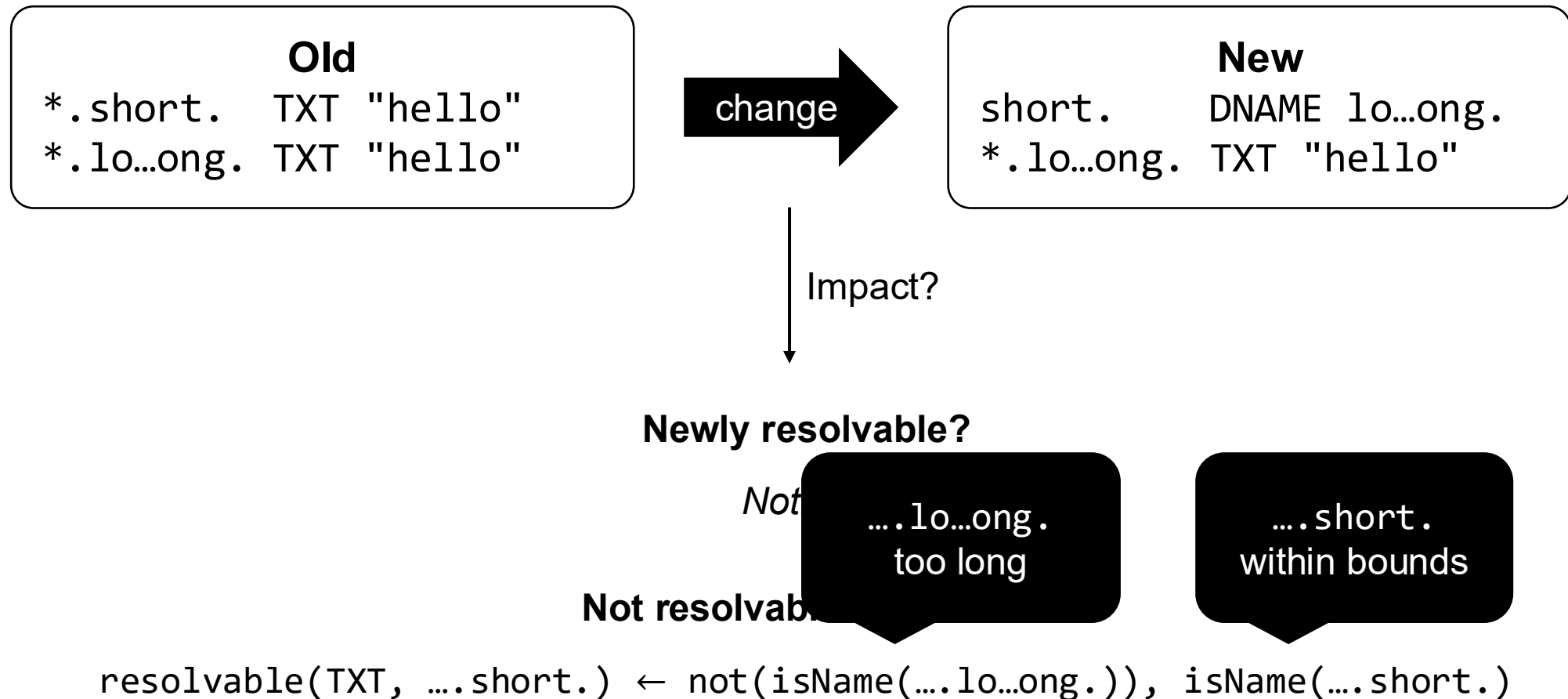
Newly resolvable?

Nothing

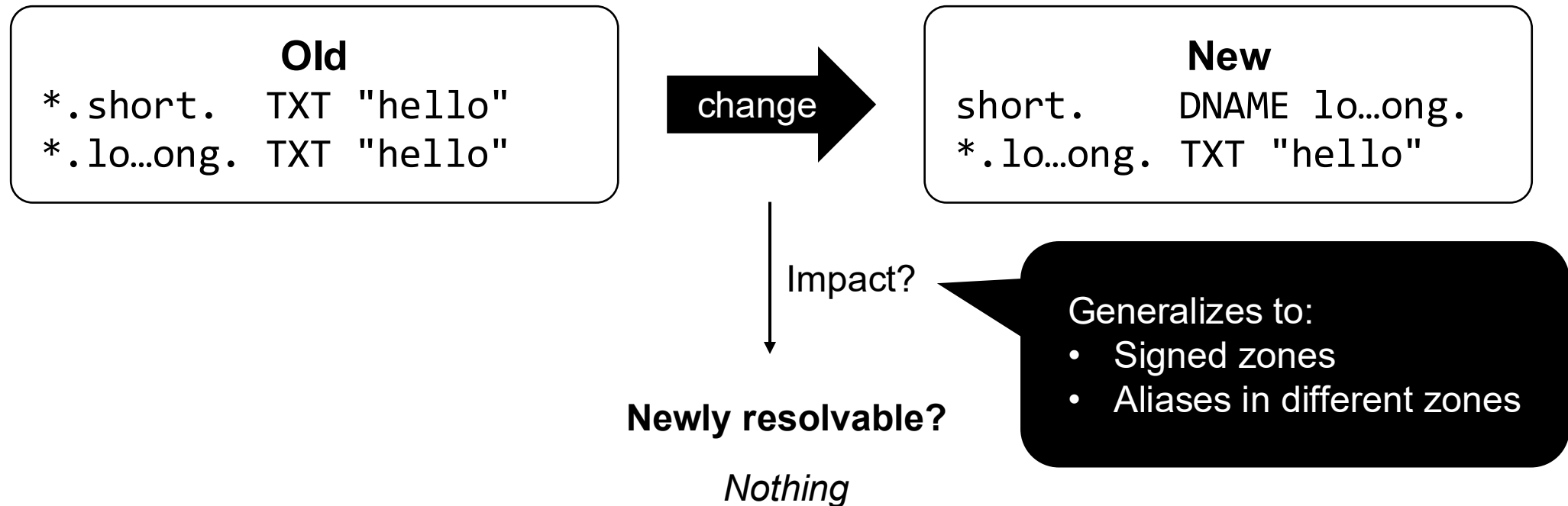
Not resolvable anymore?

`resolvable(TXT, ...short.) ← not(isName(...lo...ong.)), isName(...short.)`

How does our model work? – Example



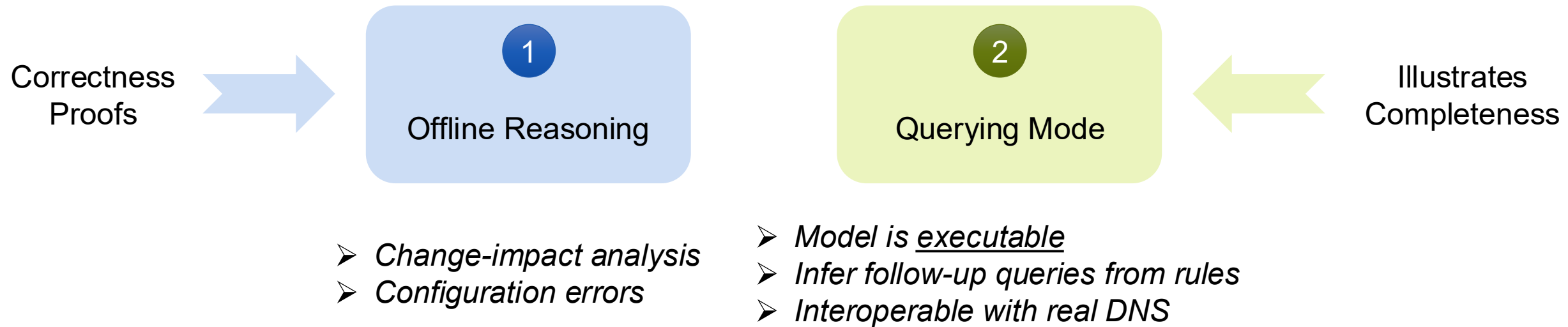
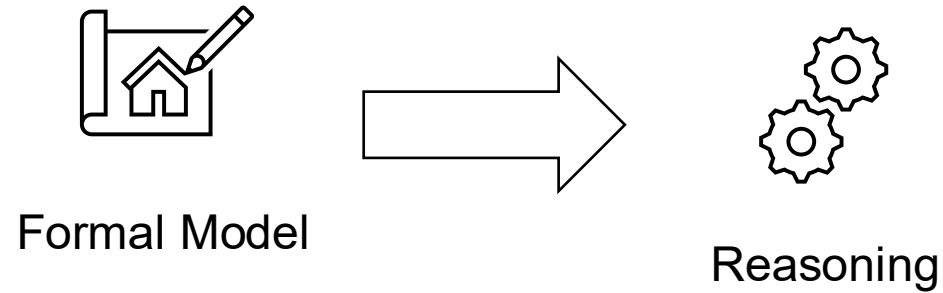
How does our model work? – Example



Not resolvable anymore?

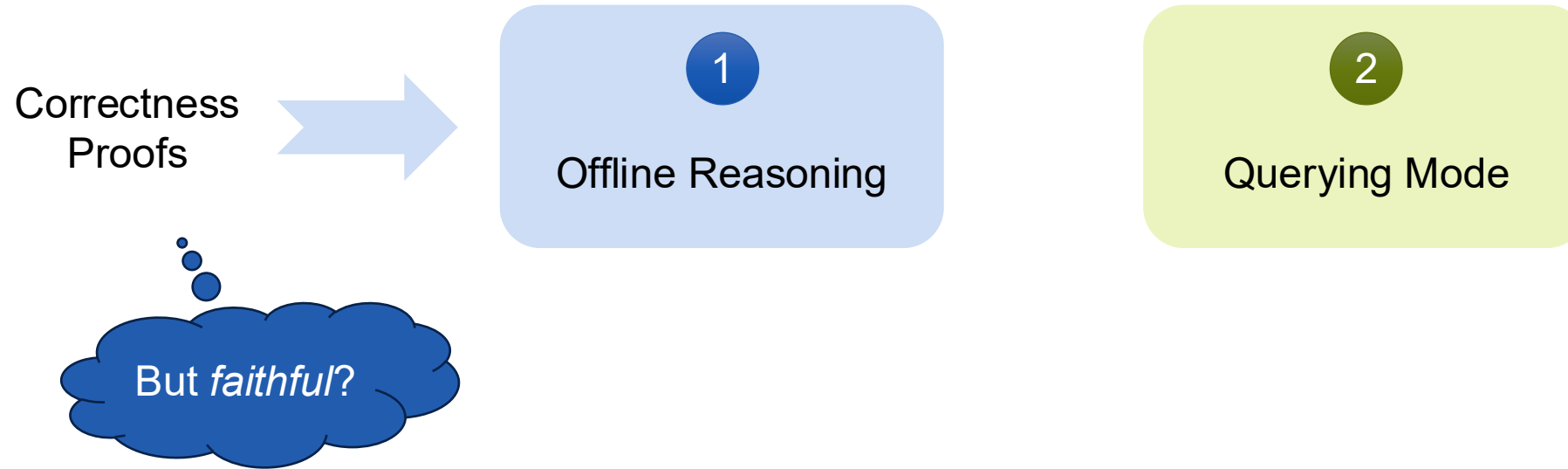
`resolvable(TXT, ...short.) ← not(isName(...lo...ong.)), isName(...short.)`

How does our model work?

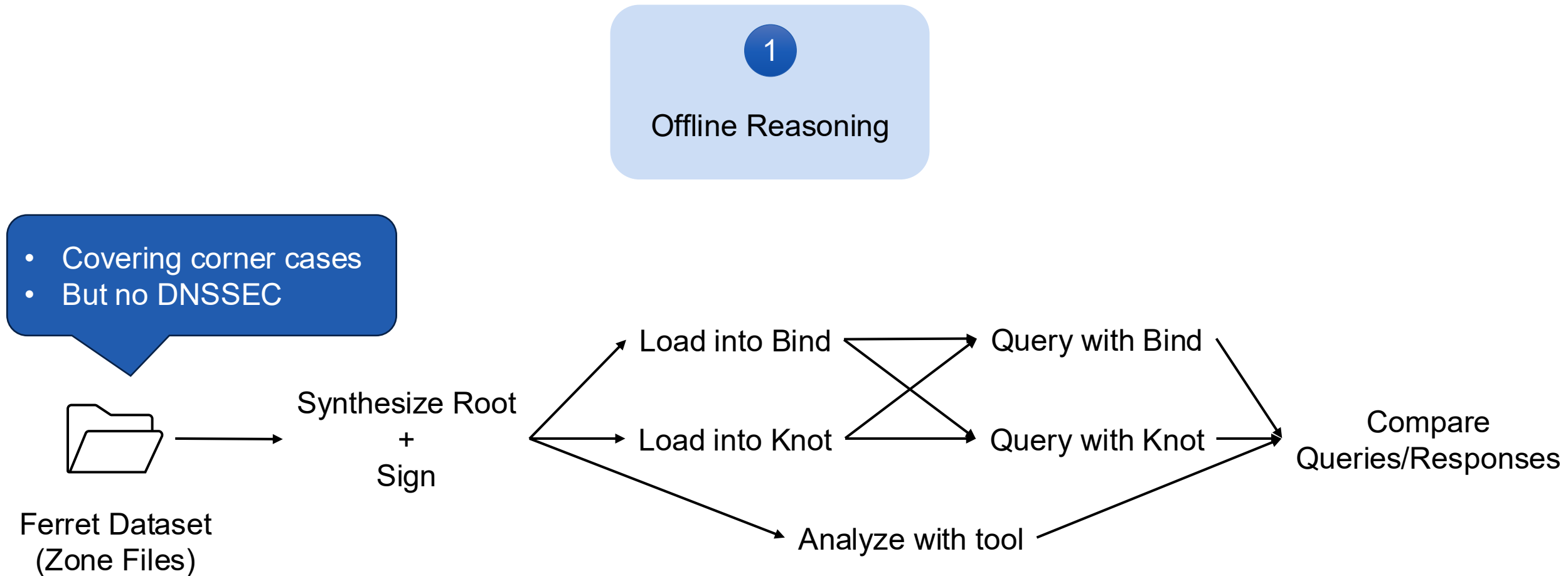


How *well* does our model work?

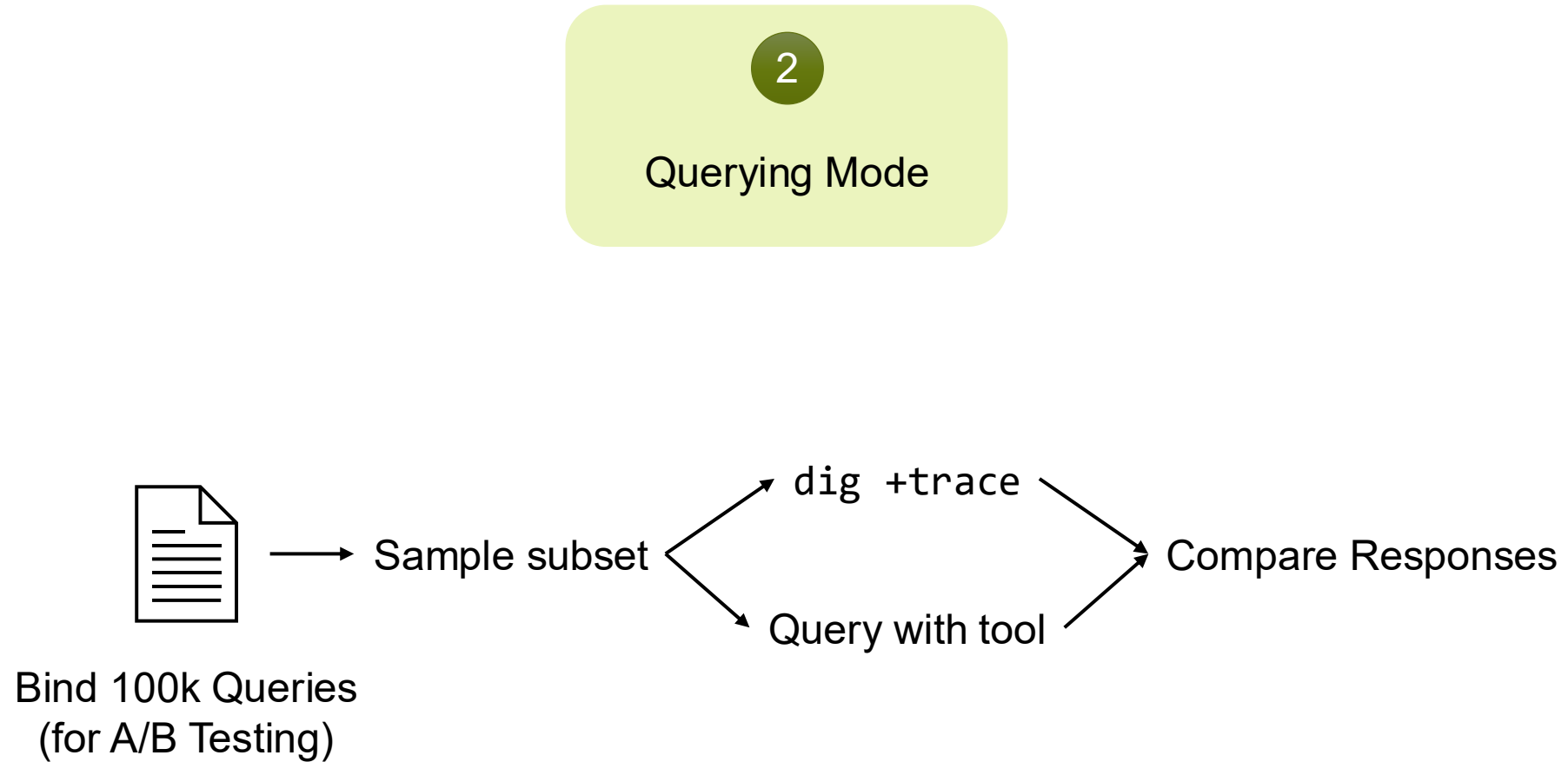
How well does our model work?



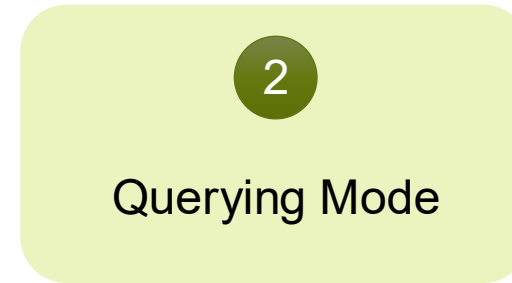
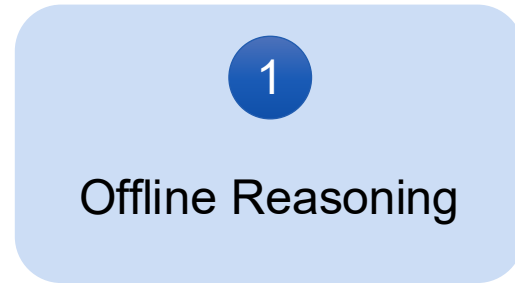
How well does our model work?



How well does our model work?



How well does our model work?



Results

- Compilation + reasoning work
- Faithful* model of the DNS

How well does our model work?

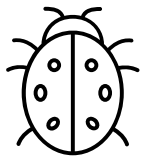
1

Offline Reasoning

2

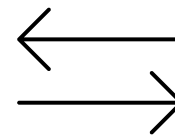
Querying Mode

Results



Many fixed bugs

- Handling of referral data
- DNAME and NS interactions
- ...and more...



Some accepted inconsistencies

- Data below delegations
- No CNAME synthesis
- ...and more...

How well does our model work?

Can we identify configuration errors? **Yes!**

Cyclic Zone
Dependency

Inconsistent
Delegations

Wildcard
Shadowing

Incomplete New
Zone Cut

Lame Delegation

Missing NS
Addresses

Rewrite
Blackholing

Rewrite Loop

How well does our model work?

Can we identify configuration errors? **Yes!**

Cyclic Zone
Dependency

Inconsistent
Delegations

Wildcard
Shadowing

Incomplete New
Zone Cut

Lame Delegation

Missing NS
Addresses

Rewrite
Blackholing

Rewrite Loop

• Press Release

DENIC reports DNSSEC disruption affecting .de domains

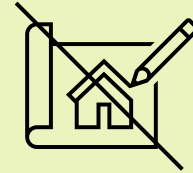
👤 DENIC-Redaktion 📅 May 6, 2026 ⌚ 1 min read

How well does our model work? – Limitations



Performance Limitations

- Some DNAME rewrites
- Querying times out
- Examples
 - Root zone: infeasible
 - google.com: 1.77 s
- But: Reasoning naïve



Model

- Limited denial of existence
 - Yes: Unsigned children
 - No: Signed wildcards
- Weak DNSSEC coverage

Next focus

How could our model be used?

How could our model be used?

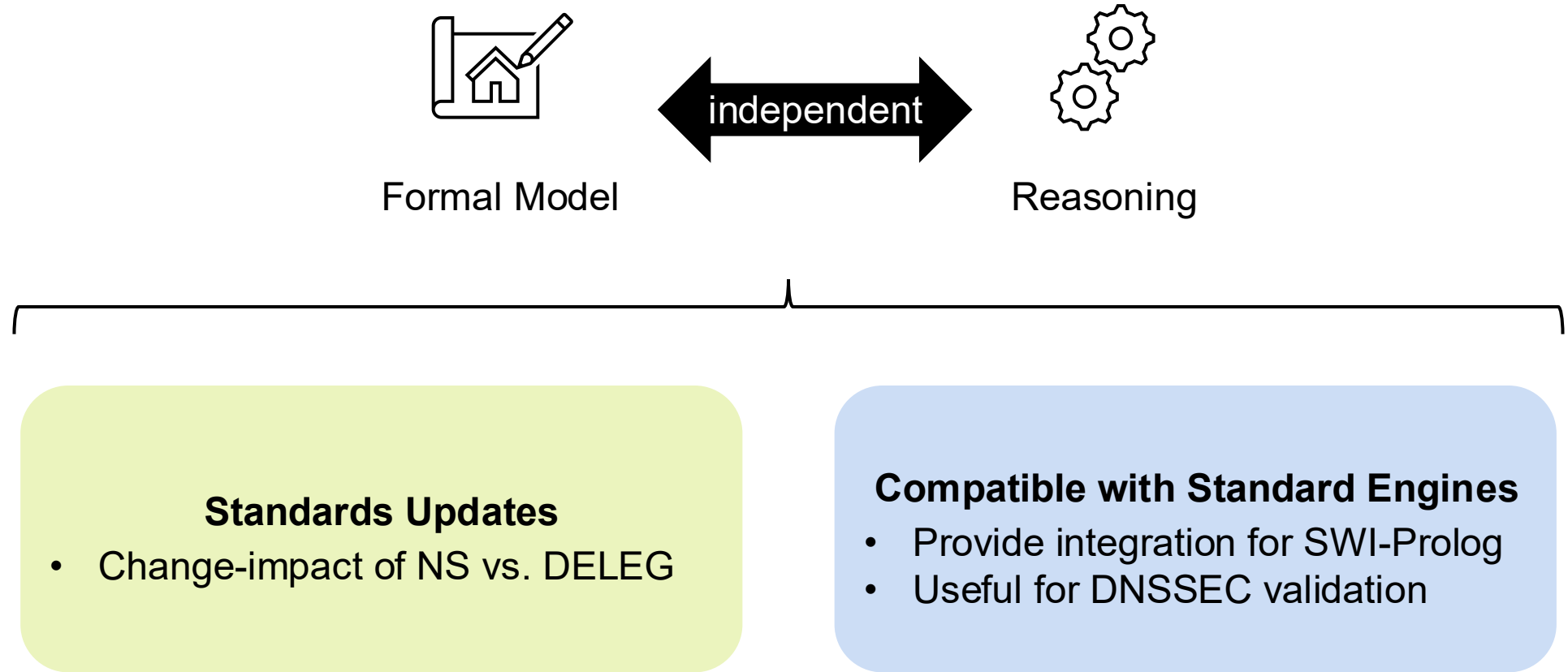
Regression Testing

- For updates that preserve resolvability

New Zone Cuts

Key Rollover

How could our model be used?



...exploring prototype with ISC

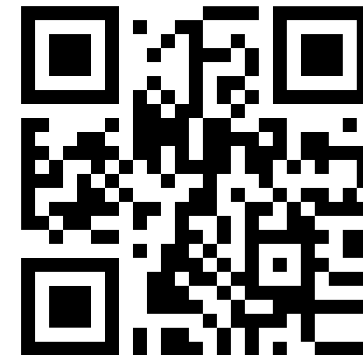
A New Formal Model to Detect DNS Misconfigurations

Resolvability Change-Impact Analysis

1. Can detect errors without explicitly looking for them
2. Support for DNSSEC



- Highly advanced but ongoing work
- Invite feedback & experiments



felixlinker.de