Claims

FM@Scale Today:

- Fast Proofs for HyperScale Verification
- Hard Puzzles by HyperScale Computing
- Big Proofs for High value software (crypto)

FM@Scale Directions:

- HyperScale for Learning Hard Puzzles
- Provers for Managing HyperScale
- Big Proofs for API boundaries

A Prover and Proofs

Z3

- Enormous trusted base
- A backend
- Basic SMT/SAT formalisms
- For “big” combinatorics

Contrast with small kernel proof assistants based on expressive logics.

Proofs	Usage
Natural Deduction “proof” objects	For Tactic replay
DRAT proofs	DNN training + DRAT-trim checking
SMT clausal proofs	
Axiom Profiler	Debugging Quantifiers
Models	Proof of feasibility Most useful
Cores	Diagnosis

Process: Scale Scope Service

Big Proof

Cube&Conquer

Azure workers, queues

Many Proofs

Azure Policies

Web Service

Many Biggish Proofs

Everest proofs (crypto)

Distributed Web Service

Users

Broad Set of Apps

GitHub

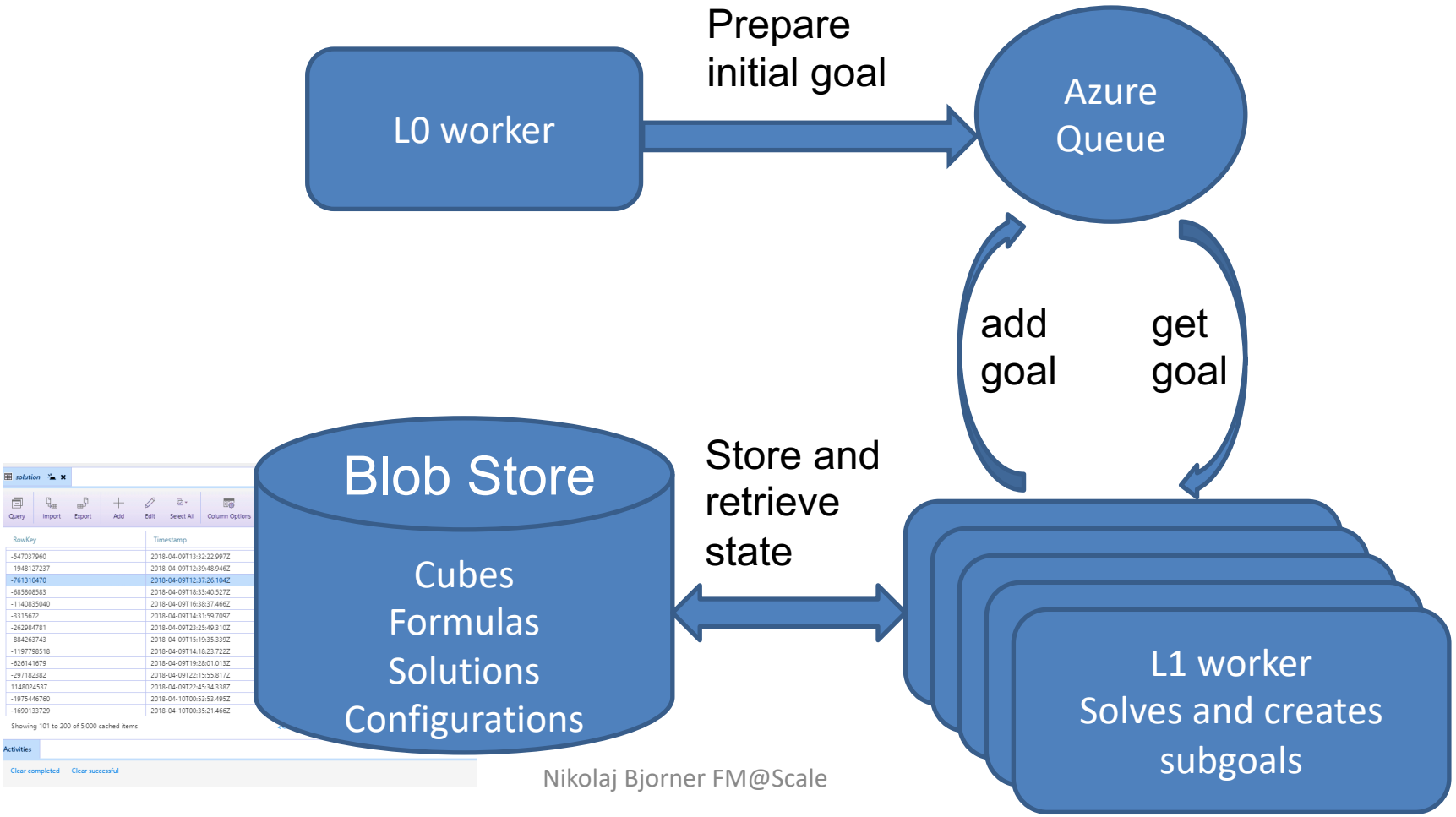
Some Background

Driving Scenarios

- Symbolic Execution
- Symbolic Model Checking
- Program Verification
- **Configuration Validation**
  - **E.g. routing in Azure DCs**
  - **50+ DCs, 100Ks routers, 10^{10} routes**
  - **With local techniques: minutes to verify**

Service
=
Software
+
Hardware
+
Configurations
+
Monitoring &
Optimization

Scaling Puzzle solving
The Cube, the Cloud and Z3



Scaling Dev through GitHub

cmake/travis

Dan Liew
delcypher

Follow

Block or report user

Student
http://www.danliew.co.uk

Organizations

SPACER Horn

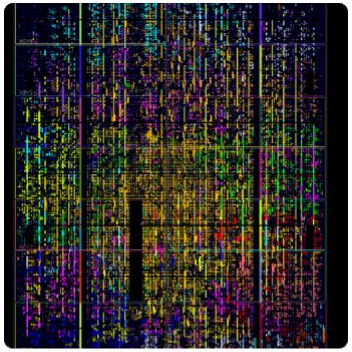
Arie Gurfinkel
agurfinkel

Follow

Block or report user

University of Waterloo
Canada
https://arieg.bitbucket.io

z3str3



Murphy Berzish
mtrberzi

Follow

Block or report user

University of Waterloo
Waterloo, Ontario

sequences

trinhmt

Follow

Block or report user

MIP

Nuno Lopes
nunoplopes

Follow

Block or report user

nuno.lopes@ist.utl.pt
http://web.ist.utl.pt/nuno.lopes/