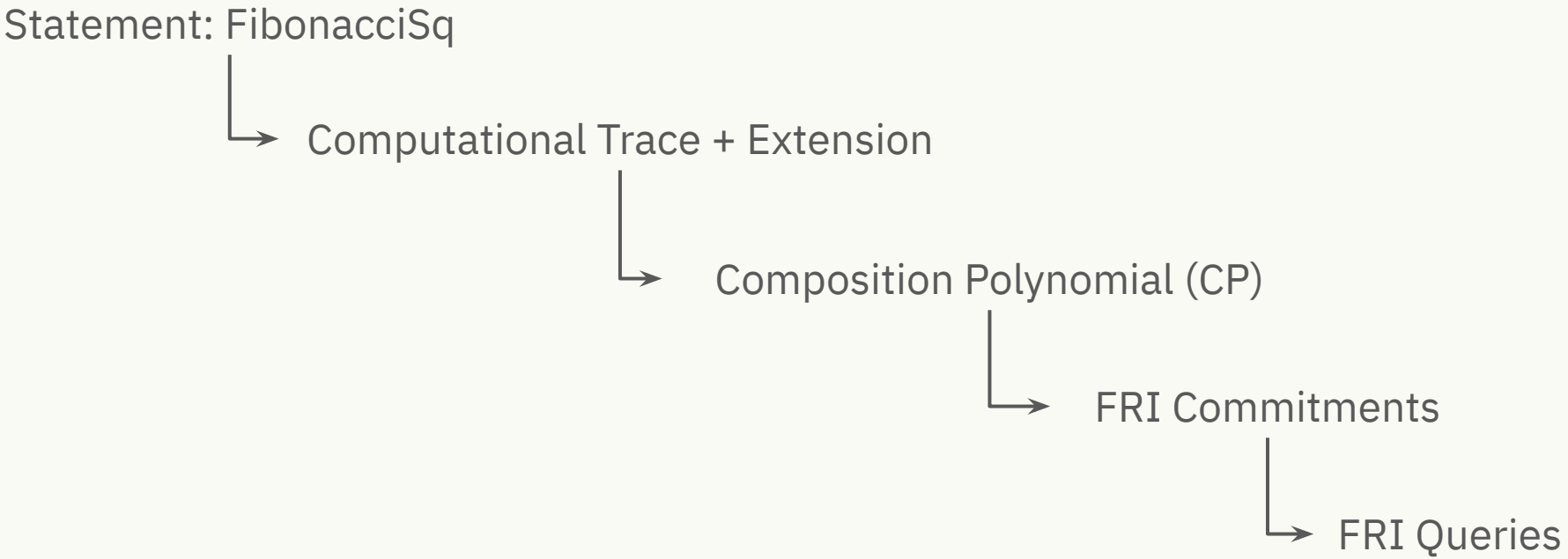
STARKWARE STARK 101

STARK 101: Finale

Finale

- Review
- Food for Thought
- What's Next
- Resources

Review


Statement: FibonacciSq
Computational Trace + Extension
Composition Polynomial (CP)
FRI Commitments
FRI Queries

Food for Thought

- Most of the proof was Merkle authentication paths
- The number of queries is basically constant so:
  - Larger trace -> $\log^2$ increase in proof size
  - Larger trace -> $\log^2$ increase in verifier time
- The prover needs to evaluate CP on all the evaluation domain
- Proving time grows quasi linearly (~ n log n)

The verifier is succinct

The prover is quasilinear

What's Next?

- Write a verifier
- Prove a different recurrence rule
- Prove a completely different computational statement
- Optimize performance

Resources

- All the material is online
- To better understand the math - read our blog posts
- Follow us @StarkWareLtd
- We'll be presenting a STARK-based VDF at SBC, this Wednesday
- Thank you

http://bit.ly/stark101sf

5 Questions, 1 Minute