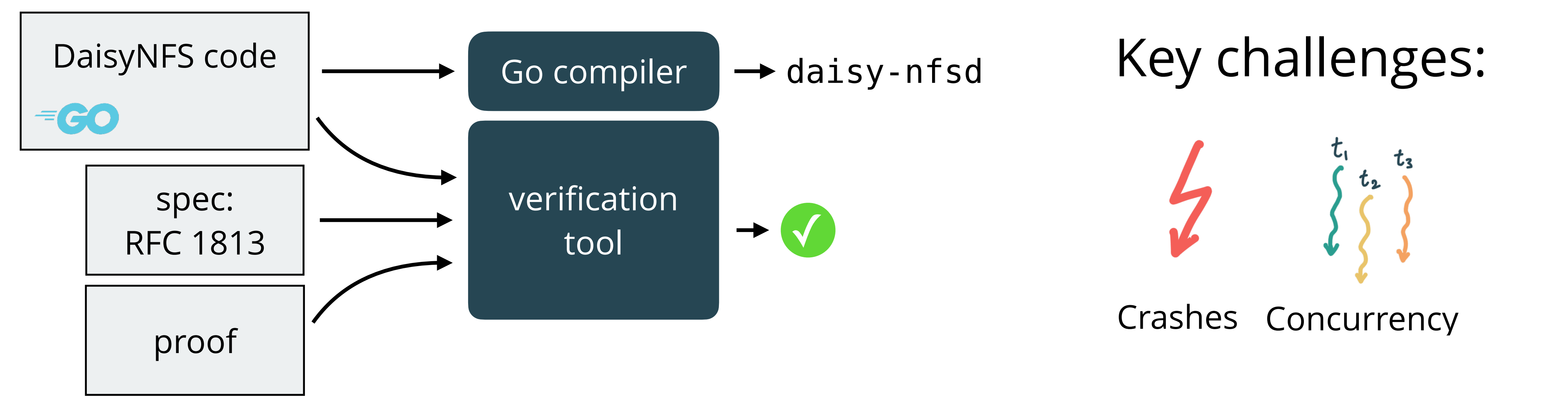


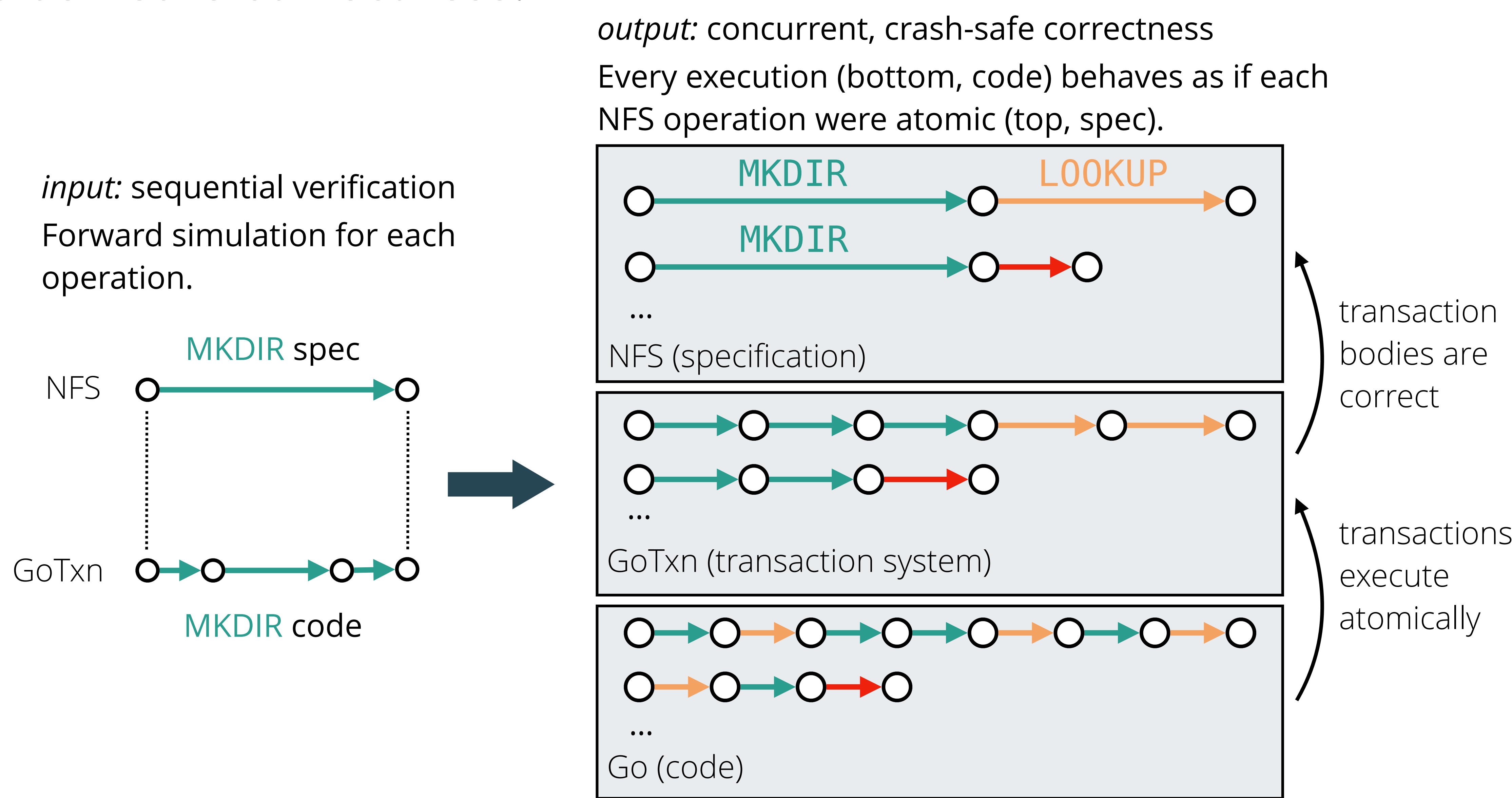
# Verifying the DaisyNFS concurrent and crash-safe file system with sequential reasoning

Tej Chajed (VMware Research & UW-Madison), Joseph Tassarotti (NYU), Mark Theng, Frans Kaashoek, Nickolai Zeldovich (MIT CSAIL)

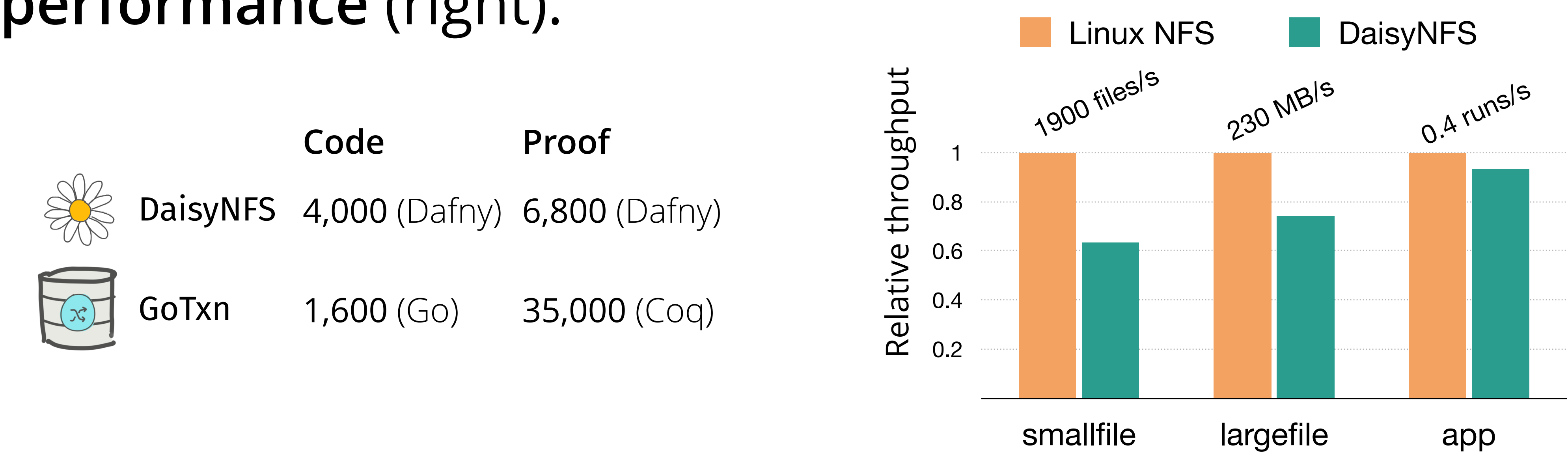
File systems are important, but have bugs. DaisyNFS is a file system with a proof that it correctly implements the Network File System (NFS) protocol.



**Simulation-transfer theorem** captures the verification benefit of transactions: turning sequential reasoning into concurrent, crash-safe correctness.



DaisyNFS has **low proof overhead** (left) and achieves **good performance** (right).



We built **DaisyNFS**: a verified, concurrent file system.

To make this feasible, DaisyNFS is built using transactions. A **simulation-transfer theorem** for the transaction system turns *sequential reasoning* into concurrent, crash-safe correctness.



[chajed.io/daisy-nfs](https://chajed.io/daisy-nfs)