In smart contracts, zero-knowledge is being used to prove properties/execution of the code after it has been executed.

It would be much more useful to provide proofs of properties of the code before executing the smart contract: before entering into any contractual arrangement, before irreversibly sending ether to any smart contract, it would be very helpful to first obtain and check proofs providing guarantees about the smart contract (termination and correctness; pre-conditions, post-conditions and invariants; economic like fairness, double-entry consistency, equity; self-enforcement of regulations).

The following paper describes a technical solution to this problem:https://eprint.iacr.org/2017/878 (see section 5).

What properties about a smart contract would you like to check before executing it?