How are you using blockchain to re-imagine your industry?

Starlight *
Zero-knowledge-proof (ZKP) compiler

* **Starlight is an internal project name at EY for code related to privacy/ZKP on a blockchain.** This code is not owned by EY teams and EY teams provide no warranty, and disclaims any and all liability for use of this code. Users must conduct their own diligence with respect to use for their purposes, and any and all usage is on an as-is basis and at your own risk.

FAQs

Starlight is a compiler which helps a developer turn a smart contract code into a privacy- preserving one using zero-knowledge. Starlight allows blockchain developers to help create a framework for customized zero-knowledge-proof (ZKP) smart contracts without any need for deep mathematical knowledge or months-long development timelines.

How do I use Starlight?

Take a clone of the npm from the GitHub repository, following the instructions in the read me section.

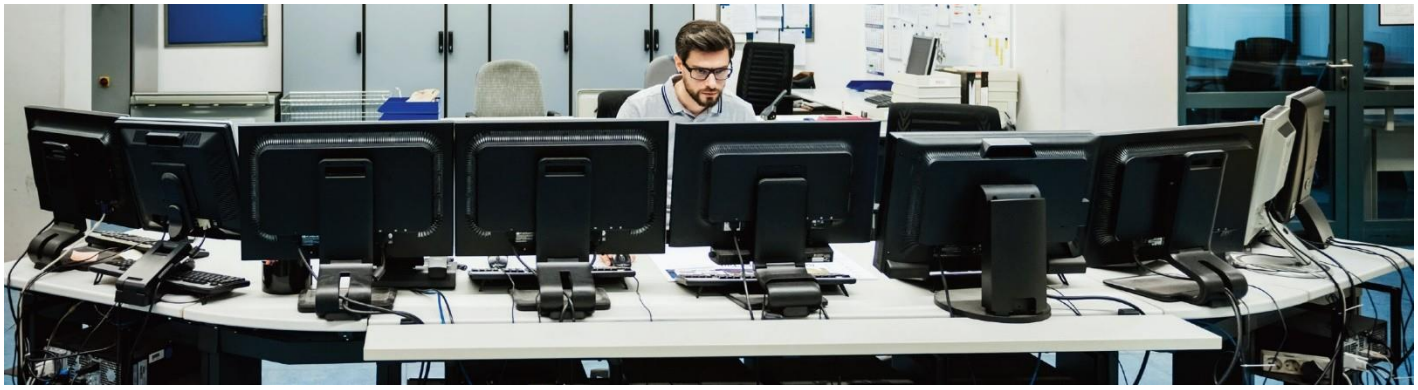
From there: Take your smart contract and write 'secret' in front of each variable declaration, including parameters, you would like kept private:

- Save this file as a .zol and run 'zappify -I <myFile.zol>'.
- And you're done!

How does it keep my information private?

Starlight creates a privacy preserving commitment system which not only hides your data but proves correctness of it using zero-knowledge.

One way of thinking about privacy here is that state is 'wrapped' inside an owned hash-based commitment. That hash cannot be edited, viewed, or removed without a valid zero-knowledge proof that shows the user is the owner of the commitment. And, being a compiled smart contract, the commitment can only be edited under the same logical rules as the input smart contract.



How do I run the output smart contract?

The output smart contract can be used easily without experience in cryptography — any complex logic is automatically completed. The user can either use the built-in
mocha tests or provided API endpoints to run Starlight with the exact same inputs as their original smart contract.

The steps are simple, just follow the instructions in the read me to run a setup, then start up the Starlight and use it just as you would with the smart contract.

How do I link my existing API-based application to this one?

Starlight maintains all original function, state, and parameter names and handles proof generation, data storage, membership witnesses, and shield contract transactions in the background so the user doesn't have to worry about them. Simply send the same parameters you normally would to the endpoint with the same original function name to use it.

Continuing the conversation

If you would like to learn more, please contact the team below.

Duncan Westland
Director,
Innovation-Emerging Technology
duncan.westland@uk.ey.com

Paul R Brody Global
Blockchain Leader
paul.brody@ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

BMC Agency
GA 17247139

EYG no. 003386-23Gbl
ED None

ey.com