Starlight*

Zero-knowledge-proof (ZKP) compiler

Application brief

Enterprise transformation in privacy technology has faced an uphill climb. So much so, that many developers who have tried to develop privacy on the public blockchain have struggled, simply because it is a hard ask and there is lack of tooling available for each specific business case.

Starlight has been designed to bridge the knowledge and development gap by making it easier for developers to bring and use privacy features in the construction of decentralized applications.

Business challenges

B2B companies aim to keep contracts, customer, and supply chain information trackable and secure, so only they have access. They want to understand who's partnering with them and buying from them to maximize loyalty, satisfaction, and overall brand growth. This provides a competitive advantage, not to be seen by their competitors.

Having privacy while maintaining blockchain's trust and integrity is only possible with protocols such as zero-knowledge-
proof (ZKP). For the large majority of blockchain developers, ZKP is very complex, math heavy and time consuming to implement.

With Starlight, developers can migrate complex, B2B business agreements from private portals and point-to-point systems onto the public Ethereum network – all while retaining the privacy and security that enterprises require.

Starlight

Starlight bridges this gap by making an ordinary public blockchain smart contract a ZKP-enabled or privacy- preserving one.

Blockchain developers can simply input their existing smart contract and receive a customized and modified smart contract, , almost instantly.

It allows specific computations from the initial contract to be identified
and replaced with a ZKP protocol that proves correctness of the computation.

Unlike a zkEVM, Starlight creates a zero-knowledge protocol which replaces public variables with hash-based commitments and variable edits with irrefutable proofs. It maintains the logic from the original contract, so the transaction logic is maintained, but with privacy.

Key features

▸ Compiles blockchain smart contracts to zk-smart contracts
  (ZkApps).

▸ Requires no prior knowledge of ZKP mathematics or tooling.

▸ Available as a command line tool or hosted on node package manager (npm).

▸ Creates a zk-ready, easy to use smart contract.

▸ Includes deployment, orchestration and testing tools.
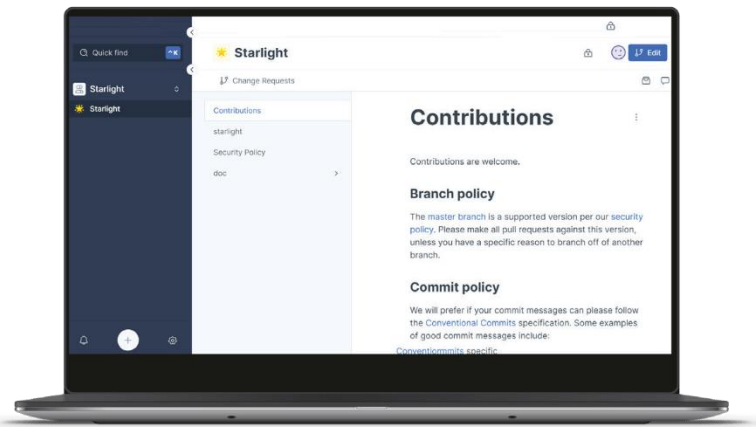
Application benefits

▸ **Public domain:** Starlight* is in the public domain and not code owned by EY. It is freely available for all to use and contribute to. .

▸ **Time or talent savings:** Because Starlight is easy to use, it allows any level of blockchain developer to easily add privacy to their existing use cases, saving both hours worked and costs to the business.

▸ **Fast:** Builds a full framework application instantly (vs. months of development time).

▸ **Educational:** By compiling from a user's input code, developers get a 'before and after'.

Continuing the conversation

To find out more 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.