How are you scaling your business in the world's biggest blockchain ecosystem?

Nightfall*

"Nightfall is an internal project names 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

Nightfall is a zero-knowledge (ZK) optimistic roll-up that helps enable private transactions on the public Ethereum blockchain. Using Nightfall, enterprises can orchestrate private transactions efficiently on Ethereum EVM-compatible blockchains without compromising the data immutability and security that Ethereum provides.

Are there instructions for using Nightfall?

Instructions in the Nightfall GitHub repository help with topics such as creating a Nightfall node to interact with other organizations. The instructions also address setup of a local instance and potentially scalability.

How does Nightfall validate identity?

Nightfall uses a x509 certificate and the digitally signed Ethereum address to check a submission and whitelist the Ethereum address, as part of the validation process.

Doesn't the use of x509 certificates break decentralization?

We don't believe that using x509 certificates in this way significantly impacts decentralization as there is no one authority that provides the certificates, instead there are several. With a certificate, the process is meant to be autonomous.

Doesn’t using an x509 certificate impact privacy?

The Nightfall code uses the x509 certificate as part of the validation process, which we believe may assist with regulatory compliance. The expectation is that the zero-knowledge technology will enable privacy for the transactions.

How much does it cost to use Nightfall?

We estimate that private transfers within Nightfall’s Layer 2 cost approximately 6,500 gas per transaction, assuming the Layer 2 block is sufficiently full (~50 or more transactions) to amortize the cost of making the block. This is estimated to be approximately one-tenth of the cost of an ERC20 transfer. The flat cost will depend on the gas price for the particular chain being used. The cost of moving funds into Nightfall from an ERCx contract is higher (~100,000 gas), but this may be a relatively less frequent. Similar considerations apply to withdrawals. Nightfall’s scaling uses an optimistic approach. Specific use cases may arrive at completely different economics.

Does a layer 2 mean waiting for a week for the transaction to be finalized?

No, this is generally a common misconception. We expect that deposits and transfers within Nightfall’s Layer 2 will have the same basic finality as the underlying blockchain. Only withdrawals normally require the one-week challenge window. However, these may be relatively rare events, and the delay may be mitigated for ERC20 tokens through providers who can process a withdrawal immediately for a small fee.

Is there a way for anonymous organizations or individuals to use Nightfall?

No. The Nightfall code uses the x509 certificate as part of the validation process, which we believe may assist with regulatory compliance.. Nightfall enables privacy, but is not meant to be anonymous.

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.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/ privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

BMC Agency
GA 17247139

EYG no. 003827-23Gbl
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com