How can you scale enterprise-grade privacy solutions 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.

Use case – Nightfall

Nightfall is an 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.

Your business needs

Privacy on a public blockchain without overly compromising decentralization, and staying compliant with regulations, is a difficult problem to solve. This makes it hard for enterprises to use public blockchains in spite of their advantages in terms of speed and error reduction.

Using Nightfall, you can enable a transfer of blockchain tokens privately at a low cost with counterparties.

Your specific challenges

Public blockchains do not provide privacy and suffer from centralization and value-capture. With blockchain transactions, businesses must also comply with regulations which is more difficult when blockchain transactions are private.

How Nightfall can help (with what?)

Using Nightfall, enterprise-grade privacy solutions are here now for public Ethereum. Businesses can now perform blockchain transactions with their customers and suppliers in privacy, while having high confidence that their counterparty is a bona fide organization. Users can now transfer tokens privately on a public blockchain through autonomous, decentralized identification and authorization of participants.

Potential business benefits

Businesses can privately transfer ERCx tokens between themselves,
their customers and suppliers. As Nighfall uses an x509 certificate for validation, counterparty risk may be alleviated.

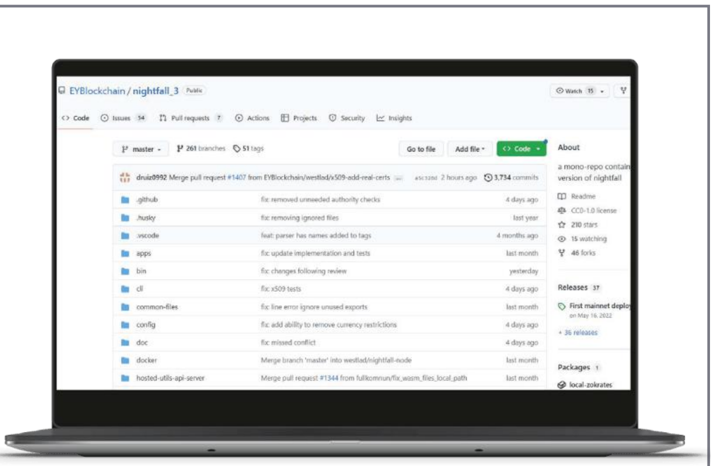
- Lower gas cost (estimated to be 6500 gas per Transaction).
- Expectation of a peak throughput of approximately 100 transaction per second (TPS).

Supports ERC20, ERC721 and ERC1155 tokens.

Nightfall* features and functionality

Nightfall code is in the public-domain which we hope will facilitate the development and adoption of privacy-focused enterprise solutions among companies seeking to enter Ethereum and the improve the ability to conduct business activities on the network.

- Private token transfers on a public blockchain
- Decentralized, autonomous validation of an x509 certificate
- Expected Cost reduction (estimated at x10 for ERCx token transfers).
- Reduced counterparty risk
- No out-of-band communication – all data for synchronization is available on-chain
- Public-domain code.



druiz0992 Merge pull request #1407 from EYBlockchain/westlad/x509-add-real-certs … a5c320d 2 hours ago 3,734 commits

.github	fix: removed unneeded authority checks	4 days ago
.husky	fix: removing ignored files	last year
.vscode	feat: parser has names added to tags	4 months ago
apps	fix: update implementation and tests	last month
bin	fix: changes following review	yesterday
cli	fix: x509 tests	4 days ago
common-files	fix: line error ignore unused exports	last month
config	fix: add ability to remove currency restrictions	4 days ago
doc	fix: missed conflict	4 days ago
docker	Merge branch 'master' into westlad/nightfall-node	last month
hosted-utils-api-server	Merge pull request #1344 from fullkomnun/fix_wasm_files_local_path	last month

About

a mono-repo contain
version of nightfall

Readme
CC0-1.0 license
210 stars
15 watching
46 forks

Releases 37

First mainnet deplo
on May 16, 2022

+ 36 releases

Packages 1

local-zokrates

Why EY

Nightfall's code is in the public-domain. Accordingly, it is available for use without restrictions, and we expect that the community will contribute to the code and related innovation. If you require assistance with zero-knowledge based privacy implementation for your blockchain transactions, no one is more qualified to help you than the team that created the original nightfall code.

Continuing the conversation

For more information about Nightfall, 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. 003828-23Gbl
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