QED-IT WINTER ’19
RELEASE NOTES

Overview

The QED-it Winter ’19 release delivers privacy-preserving asset management over Blockchain networks using zero-knowledge proofs. Using QED-it, customers can now issue and transfer ownership of fungible and non-fungible assets on the Blockchain without sharing who is the buyer, who is the seller, and what they are transferring. Blockchain participants approve the transactions and reach consensus by verifying zero-knowledge proofs that ensure the validity of every transaction. An enterprise deployment provides the resilience and robustness required for production usage, while native client SDKs enable easy integration with existing systems.

Release Highlights

Transfer asset ownership privately using ERC20-like and ERC721-like interfaces

Issue assets in private or publicly

Support for multiple asset types

Proof parallelization for scalability and robustness

Java, C#, JavaScript, and Go client SDKs

Enterprise deployment using industry standard components

Features

Private Asset Transfer

The QED-it Winter ’19 release introduces a new protocol family for transferring ownership of digital assets on the Blockchain privately using ERC20-like and ERC721-like interfaces. Instead of writing the details of the transactions on the Blockchain, QED-it generates a zero-knowledge proof that lets all Blockchain participants verify that the transaction was valid but without sharing who is the buyer, who is the seller, and what they are transferring.

Public or Private Asset Issuance

QED-it supports both public and private asset issuance. Publicly issued assets reveal who is the issuer and the total amount of the asset in circulation. This type of issuance is useful for representing stocks or bonds on the Blockchain, where this information is publicly known. On the other hand, privately issued assets do not divulge who is the issuer and the total amount in circulation. Both publicly or privately issued assets do not reveal who currently owns them and do not reveal details of the transaction when being transferred.

Multiple Asset Types

QED-it supports the issuance and transfer of multiple asset types on the same Blockchain network. The assets can be both publicly or privately issued.

Proof Parallelization

Asset transfer proofs are broken down to smaller proofs to be ran in parallel in order to provide greater efficiency and robustness, simpler update process in the future, and the ability to extend transactions with custom business logic.

Native client SDKs

QED-it offers Java, C#, JavaScript and Go native client SDKs making it simple to integrate existing products and projects with the QED-it solution. For more information on the native client SDKs see the QED-it API documentation.

REST API

In addition to the native client SDKs, the QED-it solution can also be used via a REST API. For more information on the REST API see the QED-it API documentation.

Enterprise Deployment

QED-it can be deployed on-premise or in the cloud. The solution architecture relies on enterprise-grade components such as PostgreSQL for an external database and RabbitMQ for queue management. QED-it solution is also compatible with enterprise hardware security modules (HSM) for secure signatures of transactions.

Blockchain agnostic solution

QED-it offers a Blockchain agnostic solution allowing integration with existing Blockchain stacks. An Ethereum connector and a Quorum connector are provided as part of the release. Additional connectors will be provided in the future.

Known Issues and Limitations

- Data encryption and failure mode testing in PostgreSQL are currently not supported.
- Smart contracts on the Ethereum and Quorum networks cannot interact with QED-it proofs and results.

About QED-it

Comprised of world-class entrepreneurs, researchers and developers, QED-it provides the industry’s first enterprise solution for preserving privacy over Blockchain networks. By applying advanced zero-knowledge proof cryptography, QED-it enables financial institutions to unlock the full potential of the Blockchain. QED-it provides several native language SDK’s for interacting with the QED-it solution accelerating Blockchain development and production roll-out for the world’s largest organizations.

www.qed-it.com | info@qed-it.com | Ehad Ha’am 54 Tel Aviv, Israel