# Enigma

Privacy protocol for decentralized applications

Analyst: Vladimir Shamanov (@vshamanov)

Updated: June 5, 2018



Enigma is a privacy protocol that aims to enable private and scalable computation on data without revealing the data itself.

The protocol is intended to work with any blockchain by adding the ability to move private and computationally intensive processes off-chain. Currently, Enigma is focused on building out data-specific services including a data marketplace and complimentary distributed applications.

## Project Overview

| | |
|---|---|
| Name | Enigma Catalyst |
| Issuer | Enigma MPC, Inc. |
| Category | Utility token |
| Sector | Privacy |
| Sale Start | 09/11/2017 |
| Sale End | 09/16/2017 |

## Token Overview

| | |
|---|---|
| Name | Enigma |
| Symbol | ENG |
| Type | ERC20 token |
| Initial Distribution | 75,000,000 |
| Current Supply | 75,000,000 |
| Max Supply | 150,000,000 |
| Emission Type | Fixed |

## Resource Links

- Website
- GitHub
- Twitter
- Telegram
- Reddit
- Blog
- Whitepaper

## Project Background

Enigma is attempting to solve both privacy and scalability issues of existing blockchains. The protocol originated from CEO Guy Zyskind's research at MIT in 2015. Enigma acts as a second layer on top of existing blockchains, allowing for computationally intensive or private tasks to be transferred off-chain. Using this structure, nodes can prove they have completed a task without a need to see the underlying data. The team believes this will enable a type of smart contracts where data remains encrypted called "secret contracts."

The team believes that a range of use cases can emerge from the protocol including medical research and the ability to prove specific details like creditworthiness or age, without needing to reveal underlying specifics. Because privacy is enforced through a variety of mechanisms, including client-side encryption and distributed off-chain computing, details of individuals are never exposed.

The network uses three layers; a protocol layer for private data computation, a platform layer that enables the creation of data sharing marketplaces, and an application layer where decentralized applications are built.

Currently, the platform layer is focused on the Enigma Data Marketplace, which is a smart contract based decentralized infrastructure for buying and selling datasets. Information is stored off-chain by providers and can be purchased using the Enigma (ENG) token. The goal is to eventually allow anyone, including individual users, to offer data through the platform in return for tokens.

The first application built on Enigma was Catalyst, an algorithmic trading library for cryptoassets. The application allows users to backtest and analyze trading strategies to gain insight into performance. Catalyst links to the data marketplace, where traders can subscribe to datasets contributed by Enigma and third-party data providers. Traders use ENG tokens to pay for dataset subscriptions, and data providers receive ENG in return for making their data available.

## Technology

The Enigma protocol is designed to connect to any existing blockchain and transfer private and intensive computations to an off-chain network. While simple tasks can be completed on the blockchain more computationally intensive or private tasks are distributed across a network of nodes and processed off-chain. Only a subset of all nodes are assigned the task of processing data to reduce redundancy in storing data and computing tasks.

Data is managed through an off-chain distributed hash table (DHT) that stores references to the source of the information. This allows private data to be encrypted on the client side through APIs provided by Enigma. To increase privacy nodes are given only a subset of the overall data and never have access to the complete dataset.

Through a series of updates Enigma plans to integrate new features over time to expand the protocol and application functionalities.

The Discover release, scheduled for Q3 2018, aims to introduce a secret contracts engine that will execute all contract code inside trusted environments. Developing a secret contract would be similar to current smart contracts with the addition of specific logic to identify what needs to run privately in Enigma. The Voyager release planned for 2019 is set to introduce a distributed virtual machine to allow users to choose between general-purpose secure multi-party computations.

Enigma plans to finish their roadmap with the Defiant release in 2010, which will allow the Enigma network to operate its own blockchain independent from other networks. This could include moving to a native token from the current Ethereum based token. The Enigma token, ENG, is currently used to pay for data subscription services with plans to use tokens for compensating individual data providers and nodes that offer storage or computational resources.

## Distribution

On Sept. 12, 2017, Enigma completed a token sale raising $45 million from more than 5,000 contributors. A total of 150 million tokens were created with 50% of supply (75 million ENG) going to token sale participants and the remaining 50% (75 million ENG) split between the team and a reserve for community incentives such as trading competitions and data licensing.

## Team

### Guy Zyskind
CEO

- Recieved a MSc from MIT and taught MIT's first engineering class on blockchain
- Previously CTO of Athena Wisdom

### Can Kisagun
Co-founder

- Co-founder and CEO of Eximchain

### Tor Bair
Head of Growth and Marketing

- Previously data scientist at Snap

### Victor Grau Serrat
Director of Engineering

- Previously Founding Partner at Colorful Ventures

## Advisors

### Prof. Alex Pentland
Director at MIT Media Lab

### Jacob Gibson
Co-founder & COO at Nerdwallet

### Justin Lent
Frmr Director of Hedge Fund Development at Quantopian

### Matthew Falk
Former Software Engineer at Two Sigma

### Bill Baryhydt
CEO of Abra

### Josh Lim
Former VP of Treasury and Trading Operations at Circle

### Mael Barut
Co-founder of Galois Capital

### Kevin Zhou
Co-founder of Galois Capital

## Investors

Floodgate

Flybridge Capital Partners

Converge

Digital Currency Group

MIT

## Additional Resources

- Enigma Data Marketplace Documentation
- Catalyst Documentation
- Strategic Coin Report