



ORIGIN

Whitepaper

The blockchain platform for building decentralized marketplaces

Matthew Liu

Joshua Fraser

Founders of originprotocol.com

Certain statements in this document constitute forward-looking statements. Such forward-looking statements, including the intended actions and performance objectives of the Company, involve known and unknown risks, uncertainties, and other important factors that could cause the actual results of the Company to differ materially from any future results expressed or implied by such forward-looking statements. Accordingly, readers should not place undue reliance on forward-looking statements. No representation or warranty is made as to future performance or such forward-looking statements. The Company expressly disclaims any obligation or undertaking to disseminate any updates or revisions to any forward-looking statement contained herein to reflect any change in its expectation with regard thereto or any change in events, conditions, or circumstances on which any such statement is based.

This document was last updated on June 20th, 2018.

For the most up to date information on our engineering architecture and implementation, please refer to our Github at github.com/originprotocol and developer documentation at docs.originprotocol.com.

Abstract

Origin Protocol intends to build the Origin Platform that allows developers and businesses to build decentralized marketplaces on the blockchain, with an initial focus on the sharing economy. The Origin Platform enables buyers and sellers of fractional use goods and services (car-sharing, service-based tasks, home-sharing, etc.) to transact on the distributed, open web. Using the Ethereum blockchain and Interplanetary File System (IPFS), the Platform and its community participants are decentralized, allowing for the creation and booking of services and goods without traditional intermediaries.

This whitepaper:

- Examines our intended technical proposals for designing the Origin decentralized application (DApp), the Origin developer libraries, and the Origin protocols that collectively power the Origin Platform
- Defines intended protocols for enabling buyers and sellers to transact in a trustless and distributed fashion.
- Introduces the Origin cryptographic token and its intended role in the smooth functioning of the Origin Platform

For a comprehensive examination of the intended market need and product features of the Origin Platform, please see our Product Brief. [→](#)

As our software is actively being developed, we highly recommend visiting our Github [→](#) and developer documentation [→](#) for the latest engineering architecture and implementation information.



Table of Contents

01 Introduction

- The decentralized sharing economy
- Technical design overview and philosophy

02 The Origin Platform

- Origin decentralized application
- Origin developer libraries
- Origin protocols

03 Engineering details

- Listing and transaction user flow
- Platform components interaction
- Supporting infrastructure
- Origin Token

04 Summary

Introduction

THE DECENTRALIZED SHARING ECONOMY

Sharing economy global bookings are expected to top \$335B by 2025¹, with buyers and suppliers meeting on marketplaces like Uber, Airbnb, Postmates, Doordash, GetAround, Fiverr, and TaskRabbit. These middlemen are expected to extract \$40B of platform fees annually by 2022².

22% of US adults have participated as suppliers of services and goods³ in the sharing economy, and this number is expected to rise. As value exchange becomes more distributed, these buyers and sellers need a decentralized way to match and meet without the middlemen. We propose cutting out these intermediaries with the Origin Platform and its new standards for buying and selling fractional usage assets and services.

¹ The sharing economy is estimated to grow from \$14 billion in 2014 to \$335 billion by 2025 - Brookings Institution →

² The new research, Sharing Economy: Opportunities, Impacts & Disruptors 2017-2022, forecasts that the sharing economy will reach \$40.2 billion in 2022, in terms of platform provider revenues, up from \$18.6 billion in 2017. - Juniper Research →

³ TIME's poll of 3,000 people, conducted by Penn Schoen Berland in late November, found that 22% of American adults, or 45 million people, have already offered some kind of good or service in this economy. - Time →

TECHNICAL DESIGN OVERVIEW AND PHILOSOPHY

Origin is built on top of several existing open-source libraries, protocols, and distributed systems. It is this prior work that makes Origin possible today.

The Origin Platform is built on the Ethereum blockchain, the most widely-adopted cryptocurrency platform that enables smart contracts to execute on the blockchain at this time. Critical transactional data such as pricing and availability are stored directly on the blockchain. Other metadata such as descriptions, images, reputation, and reviews are stored on the Interplanetary File System (IPFS) and cryptographically linked to the contract. This allows for better scaling and minimizes the expensive computing and storage costs associated with doing everything on chain. When a data object is created in the frontend decentralized application (e.g. a freelance engineering listing object or a customer profile object) and stored on IPFS, a unique IPFS content hash is created to reference this data. This hash is then stored on the Ethereum blockchain.

IPFS is a content-addressable, distributed file system, allowing us to trust the integrity of the data even though it is stored outside of the Ethereum network. Storage on the IPFS network is also expected to be significantly cheaper than on the blockchain at the time of this writing. The expected future launch of Filecoin will add an important incentive system to ensure the longevity of this data on the IPFS network.

We anticipate several intended major advances in both Ethereum (e.g. Plasma and sharding) and IPFS (e.g. use of Filecoin as incentive to increase network speeds and reliability) that will improve our Platform's scalability and usability over time.

We have three overarching goals in our architecture design. First, we intend to keep everything as distributed and trustless as possible while balancing the need for performance and scalability. We intend to avoid single points of failure of our architecture like relying on a single centralized provider like Amazon Web Services. Second, we intend to stand on the shoulders of giants and avoid reinventing the wheel whenever possible. Lastly, we intend to always carefully balance performance and computation efficiency with user experience. Having the best architecture in the world is pointless if no one uses it.

The Origin Platform

The Origin Platform consists of the Origin decentralized application, the Origin developer libraries, and the Origin protocols.

ORIGIN DECENTRALIZED APPLICATION

The Origin decentralized application (DApp) is an open-source HTML and JavaScript application that enables buyers and sellers to meet, communicate, and transact with each other. The DApp further allows sellers a user-friendly way to create, manage, validate and publish listings. The DApp will use [js-ipfs⁴](https://github.com/ipfs/js-ipfs) for connecting to the IPFS network and [web3.js⁵](https://github.com/ethereum/web3.js/) for smooth integrations with popular browser clients like [Mist⁶](https://github.com/ethereum/mist), [MetaMask⁷](https://metamask.io/), and [Toshi⁸](https://www.toshi.org/). The Origin DApp will be the first DApp that interacts with the Origin developer libraries and protocols, but we expect developers to create alternative DApps which offer differentiated user experiences for specific use cases or verticals. While we envision competing frontend applications, it's important to remember they will all be interacting with the Origin protocols on the Ethereum blockchain and IPFS.

The Github repository for the Origin DApp can be found here: <https://github.com/OriginProtocol/demo-dapp>.

⁴ <https://github.com/ipfs/js-ipfs> →

⁵ <https://github.com/ethereum/web3.js/> →

⁶ <https://github.com/ethereum/mist> →

⁷ <https://metamask.io/> →

⁸ <https://www.toshi.org/> →

ORIGIN DEVELOPER LIBRARIES

There has been a dramatic increase in the number of projects pursuing blockchain development in recent times. However, the vast majority of software engineers across the world are still unfamiliar with the specific technical challenges of building on the blockchain. Solidity, the preferred language for developing on Ethereum currently, is actively being developed and consequently changes frequently. There are unique architecture and security issues that come along with building on the Ethereum blockchain.

To make the Origin Platform easier to use, we intend to release the Origin developer libraries that will abstract away much of this complexity. These will be open-source libraries that are designed to be much easier to use than directly interfacing with the blockchain and IPFS. We intend to release Origin.js, a Javascript library designed to enable web application developers to get started with the Origin Platform in a much shorter time frame.

The Github repository for Origin.js can be found here: <https://github.com/OriginProtocol/origin-js>.

Over time, we expect third-party developers to develop additional libraries in different programming languages to interface with the Origin protocols and shared data layer.

ORIGIN PROTOCOLS

The Origin Platform includes a series of open-source protocols that define standards for marketplace functionalities like user identity, user reputation, listing creation and publishing, representation of booking intervals and rules, and transaction stages.

These protocols are enabled by Solidity smart contracts and IPFS. For example, we intend to use the ERC-725⁹ identity standard in conjunction with the Origin User Registry to enable user identity on Origin-enabled marketplaces.

Our frequently updated developer documentation describe a full set of protocols that are used across the platform: <https://docs.originprotocol.com>.

The Github repository for our various smart contracts can be found within the /contracts directory in the same repository as Origin.js: <https://github.com/OriginProtocol/origin-js>.

⁹ <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-725.md> →

Engineering Details

LISTING AND TRANSACTION USER FLOW

Origin user “accounts” are Ethereum wallets that optionally have identity contracts associated with them. These identities adhere to the ERC-725 identity standard proposed by the Ethereum core team. Users are in control of their own identity data.

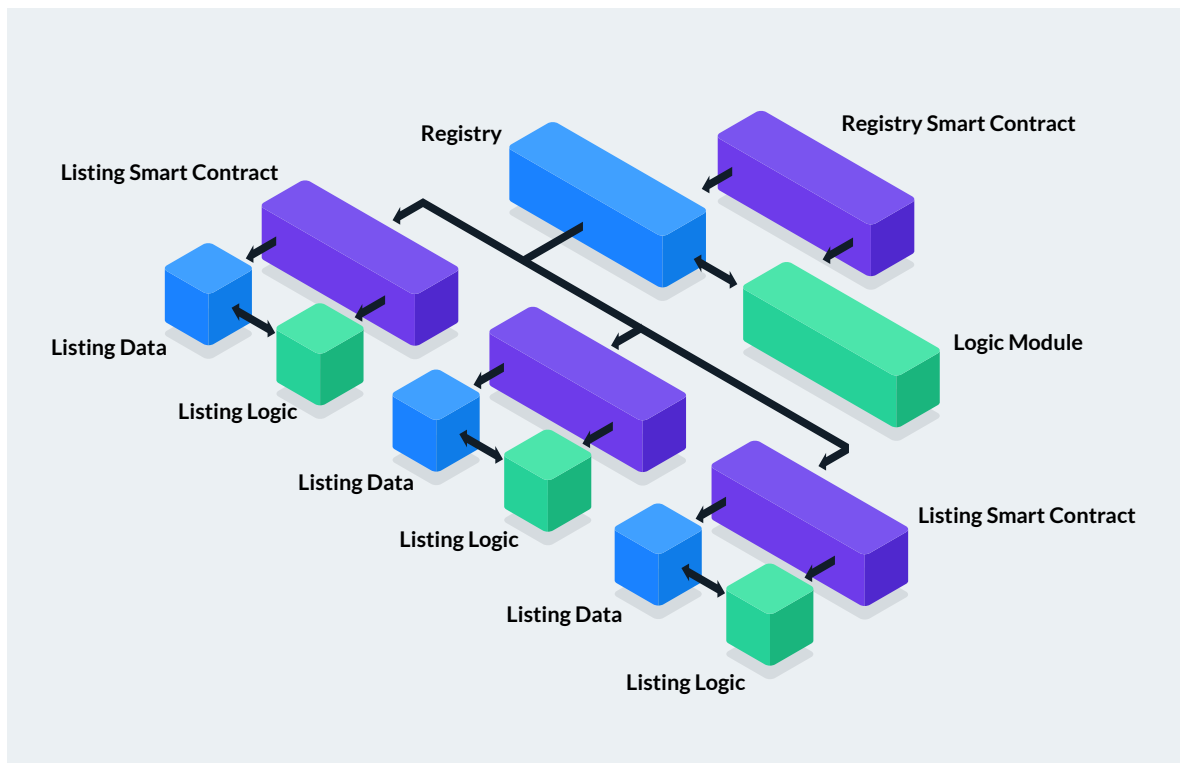
Origin listings can be created using a frontend DApp to publish a JSON data object to a publicly writable IPFS gateway. This JSON data object must conform to a set of standards and validation rules to be considered valid on the network. The IPFS node will publish the listing to the IPFS network making the listing available via distributed computers around the world to anyone who knows the content hash. The content hash of the listing is then sent to a smart contract which formally publishes the listing and also references pricing and availability information along with any specified booking rules and policies.

Listings can be searched, browsed, and booked via the frontend Origin or third-party DApp. Since we anticipate having too many listings to reasonably parse in a browser, the frontend DApp connects to an open-source contract indexing server (the bridge server) of the user’s choosing, making it possible to search and filter the entire public corpus of listings. Once a listing has been selected, a user can make a booking by sending payment to the booking smart contract along with the IPFS hash of the chosen listing and the desired interval to book. The smart contract will verify that the booking is valid and handle the transfer of funds between the buyer and the seller, including the escrow of funds when applicable.

Once a transaction is complete, users are encouraged to leave feedback about the transaction in the form of a rating and/or review. Once again, the content is stored on IPFS and only the content hash is stored on Ethereum. Users are able to establish their reputations over time with verified transactions, building a unified reputation across multiple listing verticals.

PLATFORM COMPONENTS INTERACTION

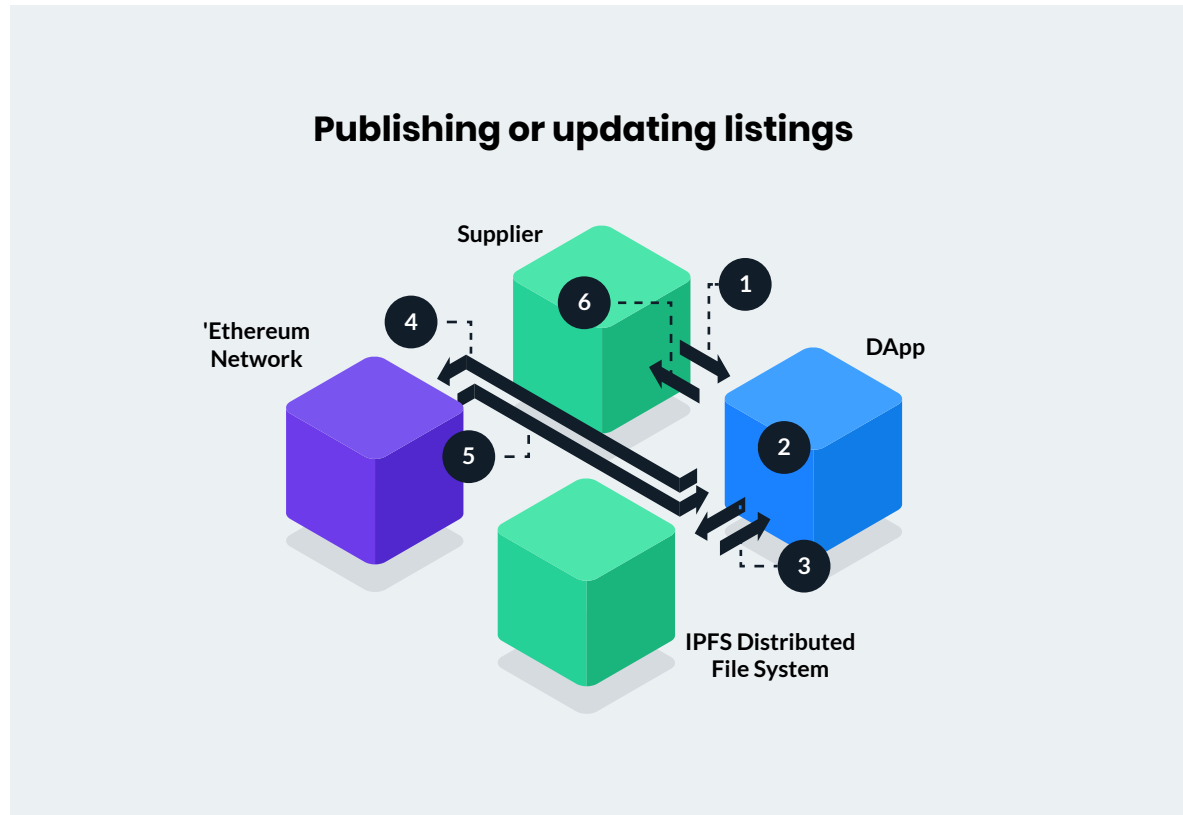
A series of smart contracts written in Solidity act as both the distributed database and the authoritative source of truth of all Origin listings.



These smart contracts will be used to publish and manage supplier listings, make bookings, leave reviews, and perform other interactions. We intend to use smart contract abstraction layers to enable continuous integration for deploying code updates.

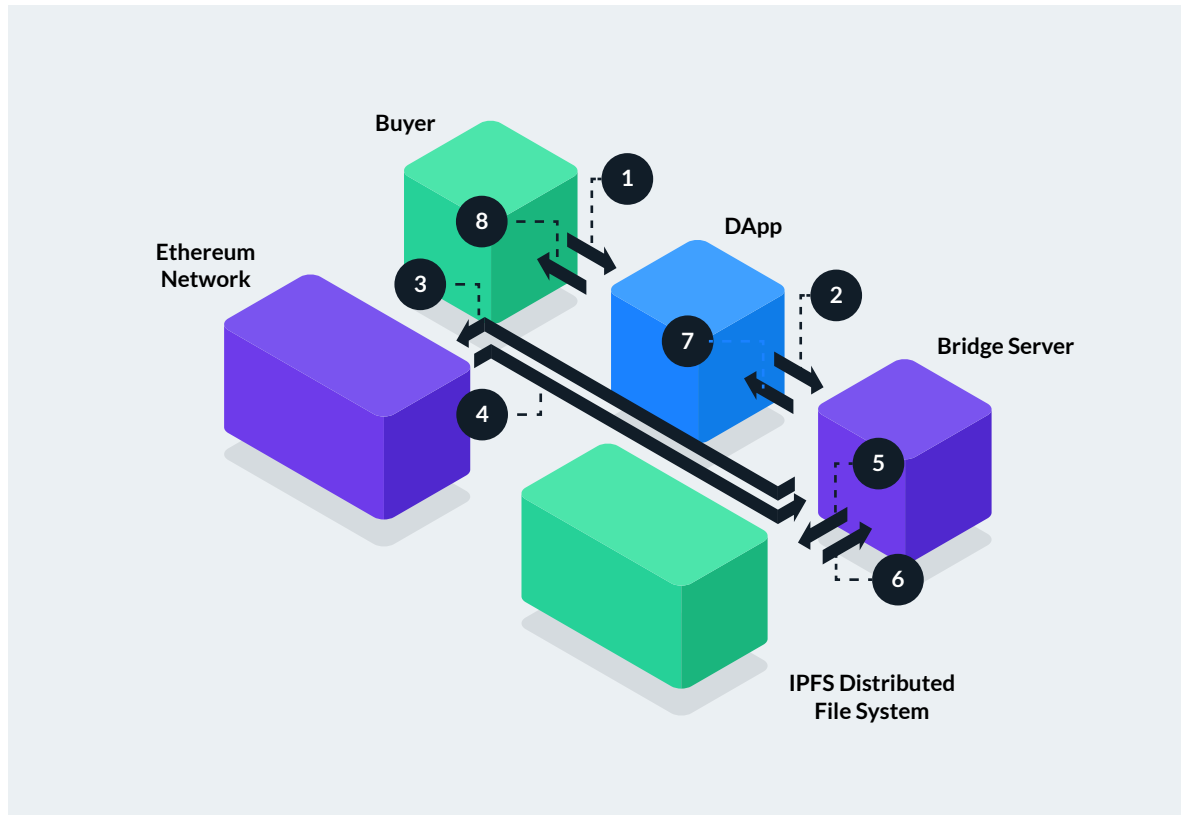
When a supplier creates or updates a listing:

1. A supplier connects to any Origin-enabled DApp.
2. The DApp enables the supplier to create or update a JSON object that represents their listing. The DApp validates that the submitted JSON object conforms to all of the validation rules of the selected JSON schema and then pushes the listing object to the IPFS network.
3. The IPFS network publishes the listing and returns the content hash.
4. The DApp sends this content hash to the smart contract on Ethereum along with pricing, availability, and booking rules.
5. The smart contract returns an Ethereum transaction hash.
6. The DApp monitors the pending Ethereum transaction and notifies the user of whether or not their posting submission has been successful.



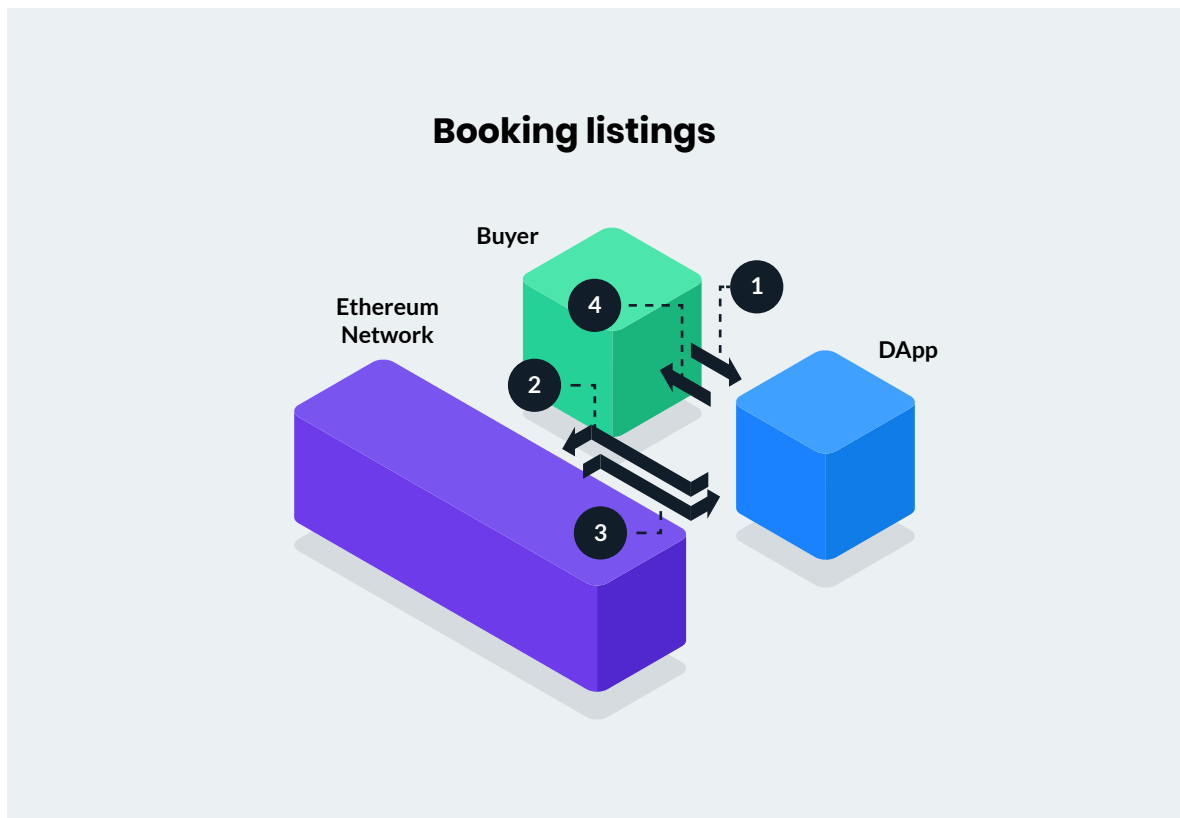
In a similar manner, buyers can search and browse listings with the addition of an open-source bridge server for faster performance:

1. A buyer connects to any Origin-enabled DApp.
2. The DApp connects to a selected bridge server (either Origin-hosted or a third-party alternative).
3. The indexing server requests the contents of the listings registry.
4. The smart contract returns a list of IPFS content hashes.
5. The bridge server requests each of those content hashes from the IPFS network.
6. The bridge server stores the results in a cache for future requests.
7. The bridge server returns listing results to the DApp.
8. The buyer can then browse all listing results.



Buyers can book listings as well:

1. A buyer connects to any Origin-enabled DApp along with the content hash of the desired listing and usage interval.
2. The DApp sends the booking request to the smart contract.
3. The smart contract checks with the same oracles to make sure the correct amount of tokens were sent.
4. Assuming availability and the correct amount was sent, the smart contract will send confirmation of the booking to the DApp and reserve that interval for the buyer.
5. The DApp will inform the buyer of the successful purchase or display any errors.



A similar architecture is intended for less common operations such as cancellations, requesting a refund, or involving an arbitrator.

SUPPORTING INFRASTRUCTURE

The Origin team envisions a future where the entire Platform is decentralized. However, at the time of writing, there are still limitations with the underlying infrastructure we are using. For example, there are no great engineering solutions to conduct decentralized search of blockchain data. In these instances, the team is currently bootstrapping the network with supporting infrastructure that is considered more centralized. It is our intention that over time the Origin team or third-party developers will create the appropriate solutions to make the Platform completely decentralized.

Bridge server

The bridge server is an open-source, server-side application that fetches the list of content hashes from relevant smart contracts that host data (e.g. our Listings Registry and User Registry contracts). It then fetches those listings from IPFS and indexes them so they can be quickly searched and filtered by DApps. The Origin or expected third-party bridge servers play an important role in providing scalability to the network. The Origin bridge server intends to offer basic search and filtering capabilities across the entire public corpus of listings. We also envision custom DApps connecting to forked versions of our bridge server which specialize in offering custom functionality for specific verticals. For example, a marketplace for sporting event tickets would likely have very different needs from a regional car-sharing service.

The Github repository for Origin.js can be found here: <https://github.com/OriginProtocol/bridge-server>.

Public IPFS gateway

Origin currently runs a public IPFS gateway¹⁰ as a community service and intends to continue doing so to help bootstrap the network. Our frontend DApp will connect to this company-serviced gateway by default, but it is expected that users can choose to use any IPFS gateway they wish. Our sponsored gateway automatically pins all valid Origin listings that it discovers (regardless of whether it was originally published on our gateway or not) to help seed the network.

¹⁰ Our public IPFS gateway is currently hosted at <http://gateway.originprotocol.com> →

ORIGIN TOKEN

As an ERC20 token, the Origin Token will take full advantage of the Ethereum network's built-in wallets, developer tools, and resulting ease of use.

Origin Tokens are intended to be used for governance of the Origin Platform. It is intended that Origin Token holders will be able to influence the direction of software development and business policies on the Origin Platform.

Origin Tokens may also be used to incentivize various forms of participation from the Platform's ecosystem participants. Origin Tokens may be used to reward users, developers, marketplace operators, and/or other participants to perform actions and services that are beneficial to the health and growth of the Platform. In other instances, participants may need to acquire and use Origin Tokens for taking actions on the Platform, with the goal of creating disincentives for malicious or fraudulent behavior.

SUMMARY

With the emergence of the Ethereum platform and IPFS, the fundamental building blocks are now in place to enable decentralized commerce in the sharing economy. Origin is launching the Origin DApp, the Origin developer libraries, and the Origin protocols to allow buyers and sellers to connect without rent-seeking middlemen.

Our initial approach is to use IPFS as a distributed data store of user profiles, listings, reputation information, etc. IPFS content hashes are then referenced in Ethereum smart contracts that allow for actual transactions and transfer of value.

The Origin Token is being introduced as a utility token that serves multiple purposes. Both positive and negative incentives will be created by the token to ensure platform security, data validity, engagement, and growth. Further, we allow the community to participate in network governance through the Origin Token.

Origin is focused on bringing change and innovation to the sharing economy. We're excited by the opportunity to lower fees, increase innovation, free customer and transaction data, and decrease censorship and unnecessary regulation.

We are building a platform that invites other interested parties including developers, entrepreneurs and early believers to build this technology and community with us, altogether working to create the sharing economy of tomorrow. We hope you'll join us on this exciting journey.