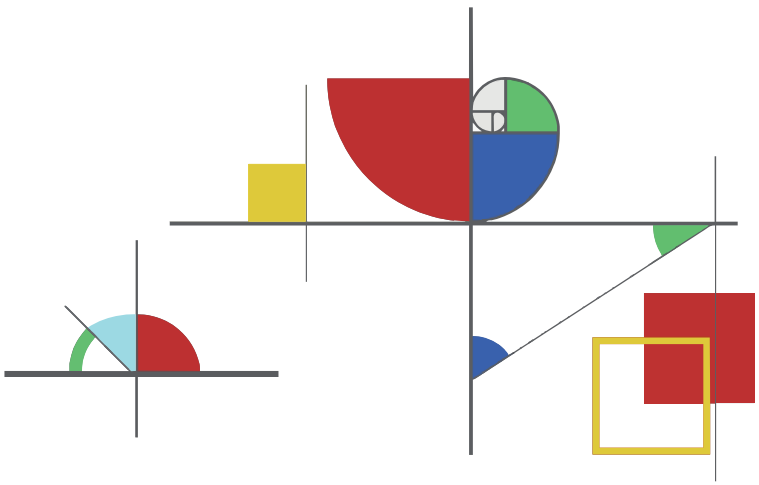
RAIR Protocol
Case Study



OnPath

What is Web3?

Many in the tech community believe that the decentralized web, also known as **Web3**, is the next evolution of the internet. Users have more control over their data and activities, and unlike the current internet, where centralized entities (ex. Google) control user data, **Web3** leverages blockchain technology, smart contracts, and decentralized applications (dApps) to create a more open, secure, and user-centric web.

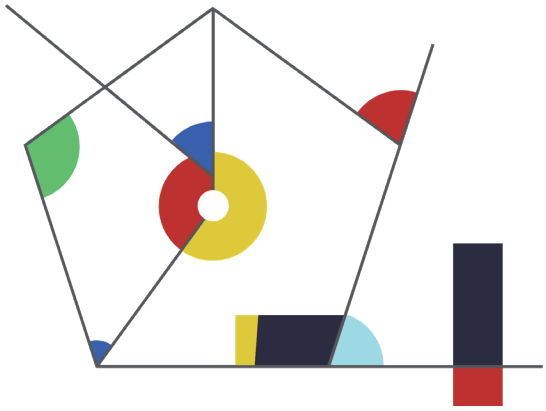
Web3 relies on deployment layers to handle the complexity of dApps, ensuring scalability, security, and efficiency. These layers make **Web3** more practical by improving performance, flexibility, and lowering costs.

Client: RAIR Protocol

RAIR Protocol (RP) is a distributed application with a decentralized backend that is easily deployed in the cloud. There are no centralized API keys, and all aspects of the front and backend are completely configurable.

The main features of the platform include:

- Token marketplace application
- Media streaming engine with built-in DRM
- Syncing engine across 8+ blockchains
- Integrations with Metamask, Filebase, Hashicorp, and more
- Authentication via Web3Auth, Yoti, and Metamask



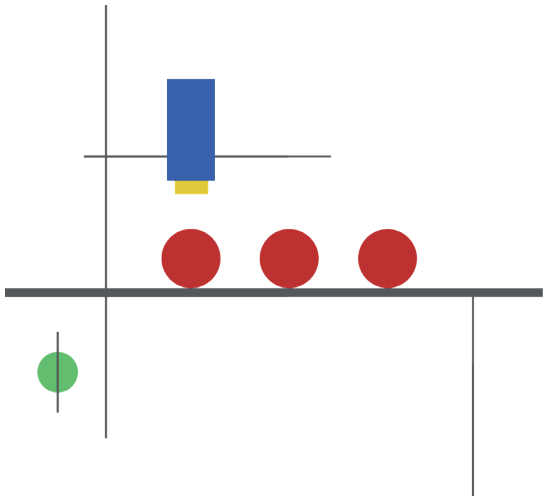
Users can mint NFTs, create collections, stream video NFTs, set prices and royalties, and more. Metadata for the NFTs are easily managed via csv upload.

Under the technical leadership of CTO Garrett Minks, **RP** has advanced Web3 by open-sourcing its deployment technology, a move essential for securing deals with large enterprises needing source code access. **RP's** open-source framework can increase application development speed by a factor of ten. According to the **RP** website, "Only a true open source deployment ecosystem can unlock the enterprise adoption our industry needs to scale to the next billion users."

As an experienced CTO, Minks understands that QA testing is essential to successful products. "A dev project without QA is like a soccer team without a goalie," he said. "It's critical to have functional testing that communicates well with developers, sending code back for review." There was no doubt that Minks would procure testing services — the question was who he would choose.

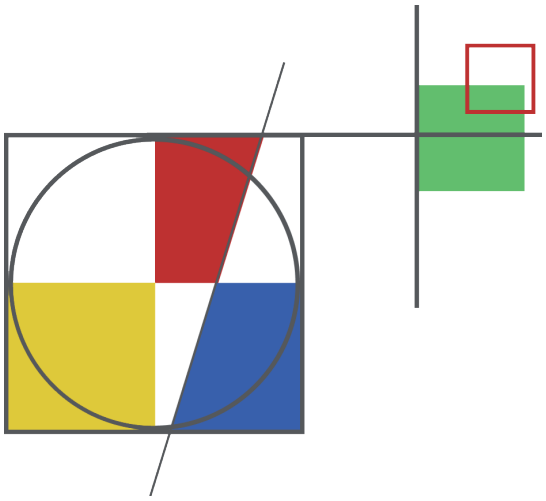
Why OnPath?

When asked why he chose OnPath, Minks explained that while he looked at Eastern-European providers, he preferred a US-based shop. Because of an offered trial engagement, Minks found OnPath to be an easy choice.



Onboarding

Minks reported that onboarding OnPath was drama-free and non-disruptive.



Mixed Onshore/Offshore Team

Minks said, "OnPath's offshore resources were sympathetic to our time zone and adapted to our work shifts. We had our daily catchup with no language issues at all. We ended up with what amounts to as surrogate employees, but without the management responsibilities — OnPath management was available at a moment's notice."

Minks added, "OnPath gave us high quality resources for offshore prices".

"OnPath's offshore resources were sympathetic to our time zone and adapted to our work shifts. We had our daily catchup with no language issues at all." -Garrett Minks

Solutions and Results

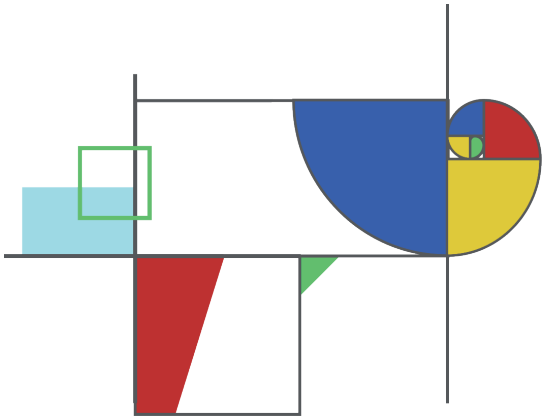
QAOps Solution

As the project developed, RP needed support for both testing and deployment. Minks reported that OnPath was able to ramp up on the DevOps side, evolving into a full QAOps engagement.

Critical Documentation

When publishing open source, meticulous documentation is essential to successful adaptation. OnPath engineers supported this effort. "OnPath tightened up our work," said Minks. On the security side, OnPath worked to protect RAIR's critical system to avoid exposure when they went open source.

OnPath CEO Brian Borg said, "Our original engagement was strictly functional testing, but we quickly realized that there was a critical security component that needed to be addressed. We brought in additional expertise to do a thorough security audit, point out risks in their smart contracts, blockchain approach, and overall infrastructure."



> **"OnPath tightened up our work. On the security side, OnPath worked to protect RAIR's critical system to avoid exposure when we went open source." -Garrett Minks**

Flexibility

Because OnPath scales QA services as needed, Minks was able to quickly expand or reduce testing activities without interrupting development. "This contributed to reducing resource costs when needed," said Minks.

Question: How would you rate the quality of OnPath's engineering?

Minks: "Ten out of ten. OnPath's support in going open source was invaluable," he said.

What types of testing were needed?

OnPath began with manual and automated functional testing to ensure immediate platform stability. Authentication, blockchain functionality and accessibility, security testing, performance testing, user acceptance testing, microservices and API testing all entered the picture over time.

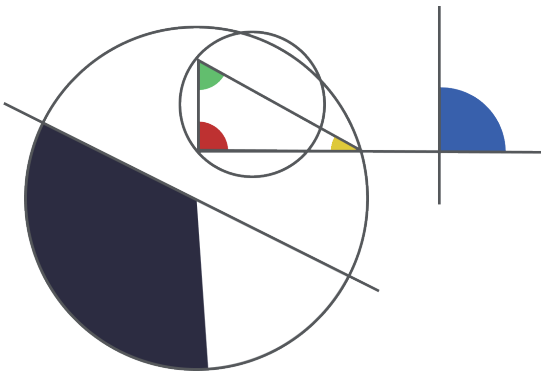
Additional challenges/goals

OnPath was engaged with RP when the decision was made to go open source. Because OnPath was brought in early, they were able to consult on good quality practices from the start — a fundamental principle of QAOps. RP and OnPath were aligned from the beginning. With open source, anyone can submit changes but it still needs to be tested and integrated. The world is now your dev team.

When the open-source decision was made, OnPath was able to quickly adapt a QA strategy to meet the new paradigm. There were also process changes — code testing was in progress, now with a much larger dev team.

DevOps management

As the team evolved and shifted, the OnPath QA team took on more responsibility, including setting up and managing the Google Cloud Platform (GCP) infrastructure and other devops responsibilities. OnPath also assisted in migrating to the distributed Akash cloud, and once the platform went open source, helped build a turnkey solution to automate the setup on the cloud of the user's choice.



Security testing

Security testing was approached with thorough diligence given the digital rights management and financial aspects of the platform. From architectural reviews to source code analysis and cloud security audits to web scans, every aspect of the platform was checked for solid security performance.

An Evolving Project Scope

The move to open-source had many new implications for testing from both a tools and process perspective. Borg said, "We pivoted often, as the project scope changed with each shift. Whenever RP identified a new market fit with added functionality, we adapted to meet their testing needs. As RP evolved, OnPath consistently adapted."

"Whenever RP identified a new market fit with added functionality, we adapted to meet their testing needs. As RP evolved, OnPath consistently adapted." -Garrett Minks

Technology and tools

QA tools

Jira, Xray, Confluence
Selenium - functional and health check automation
Postman - API automation
Locust - performance automation
Jest - integration automation
Browserstack - cross platform testing
Jenkins - CI/CD pipeline

Security testing

OWASP ZAP - passive scanning
Burp Suite - active scanning
Clair - container testing
SonarCube - source code static analysis
Shodan - OSINT
HTTP Header MDN - OSINT

Tech Stack

Front end:
JavaScript React

Middle / Logic
Javascript, Typescript, Alchemy
Solidity - Smart contracts

Back end
Docker and Docker Compose
Kubernetes - production deployment

Storage
MongoDB - data
GCS (Google Cloud Storage) - video
Filebase (IPFS storage) - media
Hashicorp - Secret keys

Integrations
Blockchains
Metamask - wallet authentication
Web3Auth - authentication
Yoti - facial age estimation
Cloud agnostic - AWS, Azure, GCP, Akash

Results

500
functional tests

60
Selenium automations*

286
Xray automated tests

80
Postman API automation tests*

12
scripts on Locust Performance Tool

25
Jest Tool tests for SDK and integration automation testing

100s
of automation tests, covering: functional, API, SDK, and performance testing."

763
Minimum of bugs opened in Jira — 729 closed

6
QA team members through the life of the project - manual, automation, security, management

**Ongoing Selenium use for health checks*
**Ongoing Postman API automation tests*