MELONPORT
CASE STUDY

Problem

Financial trading involves a mountain of paperwork and a frustrating amount of tedious logistics to ensure adherence to rules from regulators, trading groups, and professional organizations – mostly designed to protect the investor. Mona El Isa—originally of Goldman Sachs and Jabre Capital Partners—wanted to run her own hedge fund, but soon found that this tedious logistical work was keeping her from engaging in actual trading.

Her solution was to join forces with early blockchain developer Reto Trinkler and form Melonport, which would develop software called Melon that could manage the frustrating backend of trading; piggybacking on Ethereum's blockchain technology, Melon will be the software that operates and regulates the relationship between investors, managers and cryptocurrency exchanges. The protocol tracks asset prices in real time, handles the back-end of risk management and compliance, and the exchange happens on a blockchain which keeps costs lower for investors and investment managers. But before releasing Melon to the public, Melonport needed to implement efforts to ensure it was secure enough to begin responsibly handling people's sensitive financials.

> *"You know it's good work when you've got people challenging you..."*
>
> -Mona El Isa, Founder of Melonport

Solution

After shopping around, El Isa felt that some audits were lacking in specific technical analysis and eventually connected with Deja vu Security, who in turn assigned the project to two security consultants with concrete experience in blockchain and Ethereum technologies—Mitchell Harper and Dan Wessling.

Wessling said, Solidity, an Ethereum smart contract language, is "a new language, a new environment. Solidity contract developers don't have line-by-line debuggers... This made testing very difficult. There aren't a lot of stable and mature tools." To work around this bleeding-edge technology challenge, Harper wound up writing his own test environment, which made it possible for both consultants to step through the code line-by-line and see the behavior of data going through it. They teamed up, running separate testing environments to conduct a more complete test.

> Deja vu Security found a half-dozen critical vulnerabilities and eleven "yellow light" issues, all of which Melonport could address before launch.

The security consultants at Deja did find areas of concern, a half-dozen of which would have real impact on the software. There were also eleven smaller problems one might call "yellow lights," as well as general observations Harper and Wessling pointed out to Melonport in case the team had overlooked them during their own development process. To assist the Melonport team, Deja provided code snippets, as well as a lengthy and highly detailed report on the severity, complexity, risk, impact, and recommendations for the code at-issue.

Melonport's staff was impressed: "You know it's good work when you've got people challenging you in different areas that you and your team have not thought about before. It shows they've done a thorough analysis. An audit that doesn't challenge doesn't provide value."

Looking to the future

Melonport's next steps are to continue working on Melon's governance layer, and then test the code early next year with a small amount of real money before its full-blown launch. "...This technology is all very young. Even when we are ready to deploy live to main-net with real economic value at stake, I would emphasize that all of this is still very new and experimental."

The staff at Deja is equally aware that blockchain's evolution is just beginning, and that cryptocurrency is just one part of a broader change: "The hype [about blockchain] is above where we are in the technology, and we have to scale very slowly since we're talking about financial services."

Deja vu Security, however, can help make a secure future possible.

About Deja vu Security

Since 2011, Deja vu Security has been a trusted provider of information security research and consulting services to some of the world's largest and most-esteemed technology companies. Our expertise is in information security services where we provide our clients strategic insight, proactive advice, tactical assessment and outsourced development. For each client, we offer a full range of security services.

We balance an organization's business and security needs by helping clients build robust, secure solutions that represent the leading edge of computer security. We're more than a collection of expert security consultants: we spend our hours brainstorming, discovering, researching and developing every possible point of entry and vulnerability in software and systems. We work around the clock conceptualizing system architecture, devouring code, and testing theories. The result of that work is evident in each of our client-facing projects.

1415 10th Ave., Suite #1
Seattle, WA 98122
(855) 333 5288 | secure@dejavusecurity.com
www.dejavusecurity.com