STATUS CASE STUDY

> *“We believe in moving decentralization forward, full transparency, and self-sovereignty… our founders Jarrad and Carl encoded a meaning into the name Status: ‘the state of us.’”*
>
> –Nabil Naghdy, Status COO

Just as social prophets predicted the massive socio-economic upheaval of the internet, so too have they begun to herald the latest disruptive technology known as “blockchain.” Put simply, blockchain is a virtual system in which every step in a process is dialectically both nearly 100% documented and traceable, but also nearly 100% private and decentralized. The power of verification and disclosure is in the hands of not one central authority, such as a bank or government, but in the hands of potentially millions or even billions of computers, or “nodes,” with possibly just as many different people. In a truly decentralized blockchain system known as “proof of work,” fraud, corruption, or centralized power of any kind is theoretically possible but practically implausible.

The potential promise of a decentralized future with power in the hands of the many, and personhood in the hands of the self, is what led Jarrad Hope and Carl Bennetts to found Status, an ambitious blockchain-based mobile platform that allows users to conduct financial transactions, communicate, and ideally, do basically everything else they would ever need to do online, with safety and self-sovereignty. They encoded their beliefs into the name of their project: “Status” comes from “the State of Us,” and they envisioned a borderless, decentralized community (a “state”) that anyone can be a part of.

Along the way, Status has evolved from a platform for cryptocurrency transactions and messaging to an app that functions essentially as a mobile operating system, running on standard systems like iOS and Android. The idea is to have users download Status from their phone’s app store, and then through Status, they’ll be able to do everything they would normally do on their phone—manage their finances, communicate with others, and banal tasks like order food—but with the benefit of those actions being done on a decentralized, heavily-encrypted system where they own their data.

Unfortunately, just because something is run on a blockchain doesn’t make it inherently perfectly secure. To be sure, when implemented absolutely flawlessly, blockchain is, at least with current computing power, ***nearly*** functionally impregnable. But blockchain experts like the ones developing Status know better than to blindly trust in a technology, even if it’s touted as the most secure internet technology ever. Status COO Nabil Naghdy explains, “People are going to be trusting us with potentially their life-savings. It’s a precarious case when you’re handling people’s money…There are a lot of potential attack vectors we’re dealing with, so we wanted to make sure we’re covered for most if not all of those risks…Having someone audit [the platform] was pretty key.”

The developers at Status had three top security concerns they wanted audited, so they could have the confidence to launch the platform and protect their users: One, financial transaction integrity—making sure transactions were authenticated and truly authorized. Two, protection against data leakage outside the app. And third, that the app was protected against hacking and malicious actors.

But not just anyone can audit a blockchain project: The nascent technology is highly complex and for many, still shrouded in mystery. Luckily for Status, by the time they were ready for an audit, Deja vu Security (Deja) had already completed projects for both the Ethereum Foundation itself, as well as the blockchain-run financial management system Melonport. After a referral to Deja and discussions about Status' needs and the scope of the project, two Deja security consultants got down to brass tacks.

Dan Wessling, the lead consultant on the Status project, had just come off working on Melonport, and was in charge of managing the engagement's scope, overhead, and other logistics so the other consultants could focus solely on the code. Dan described the general flow of work for Status as starting with assessing its architecture, and then looking for attack surfaces. "The first [attack surface] we look for is, where does the user control data that the application is taking in? Another thing we look at is configurations of whatever services, frameworks, or libraries they're using... [We also look for] how sensitive data is stored, managed, and cleared. And especially when we're working with blockchain, one thing we need to look into is the implementation of the app's cryptography." Wessling explained that the team studied the entropy of Status' twelve-word backup phrases—a security measure that in practice is unlikely to be broken by an attacker but is—like with all of blockchain—not inherently foolproof. And Status wasn't interested in taking chances: COO Naghdy urged that "[The app's security] is very important for us; because of how cautious we are in holding people's funds, we had to make sure it was secure. It wasn't optional." Deja's team was satisfied with the backup phrase implementation, calling it "sound."

But Status still had some work to do: Deja found four highly critical vulnerabilities and a handful of vulnerabilities of medium-to-critical risk. Among the vulnerabilities were issues with API implementation and potentially malicious DApps taking advantage of the platform. Some companies might balk at security experts poking holes in their work, but Status was ready for it: Nabil explained, "We were prepared to put in the time to fix [any vulnerabilities]. They weren't simple to fix, but it didn't delay the project. We wanted to make sure we're covered for most if not all risks." Status' team was able to address every one of the vulnerabilities Deja found, and considered Deja's work so useful that they plan to book them again for another round of audits. On this first engagement: "Practically, we discovered vulnerabilities. But it also gave the team the confidence to launch the beta version of the app and gave them a lot of experience in discovering vulnerabilities for themselves. We'll be doing many more security audits internally, though we'll also continue to use external audits, like Deja's."

Deja found four highly critical vulnerabilities and a handful of vulnerabilities of medium-to-critical risk. Status' team was able to address every one of the vulnerabilities Deja found, and considered Deja's work so useful that they plan to book them again for another round of audits.

Deja's security consultants enjoyed the work too and spoke highly of Status: "This is cutting-edge technology—this is the first time we've seen an Ethereum client on a mobile device. They're using new technology in a new way."

Status plans to make the app available to the wider public later in 2018, but early access to the beta is currently available to coders who support an open-source, decentralized world. Deja vu Security continues to run security engagements for some of the world's largest companies and is always open to new opportunities. Contact the Status team at status.im, and Deja at dejavusecurity.com.

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