Removing Blockchain Adoption Barriers: Stabilizing Costs & Transparent Security

By Ben Stewart

I recently had the opportunity to lead a team that conducted a security audit of Metacash, a mobile wallet and set of smart contracts designed to improved UX when sending DAI, a stable cryptocurrency that is pegged to the US Dollar. Unlike other cryptocurrency wallets, Metacash simplifies new user onboarding by hiding the complex technical bits of the Ethereum blockchain by removing the need for the native Ether currency when covering transaction fees.

There's a lot I like about Metacash, but more than anything, I like that it solves a real adoption problem in a well-thought-out and secure way. The Ethereum blockchain (most popular public smart contract platform at the time of this blog) has many stable coins available on its network. Unfortunately, all transactions must pay a small transaction fee in the blockchain's native currency, Ether. This presents a challenge for mass adoption because people that want to use stable coins for blockchain payments are also required to purchase Ether to cover transaction fees. Metacash removes this complexity for the average user by abstracting out the need for Ether using a network of transaction relayers, so the users only need to worry about their stable currency, AKA their US dollar balance.

Making blockchain payments as simple and cost-effective as Venmo isn't going to happen overnight, but it also doesn't need to be a "someday" proposition. The first step for Metacash is to traverse the confidence hurdle, similar to the scrutiny emerging technologies need to go through before they are trusted by a mass audience. In the blockchain world, this means getting independent 3rd-party security audits, publishing the results, and demonstrating how you're fixing the problems that were identified during the audit(s.) Such open scrutiny helps build public and industry confidence in Blockchain and smart contracts as a viable platform.

As a technology advocate and experienced software security engineer, I'm constantly tracking new blockchain implementations and methods. Metacash caught my attention because it could solve the adoption problem of confusing transaction fees and price fluctuations. As an advocate for sensible blockchain applications (and well-thought-out security) I dug in a little deeper to learn more about the Metacash project. Initially, I discovered a potential man-in-the-middle/phishing vulnerability where a malicious app could trick a user into signing an unauthentic message compatible with Metacash. Once a user signs a message with their wallet, a malicious DApp could potentially steal all the funds from the user's Metacash wallet.

I found a couple of smaller issues as well and decided to reach out to the project team who was incredibly receptive to a deeper analysis. Security Innovation and Metacash had mutually compatible objectives. We want to help enable new tech that solves real problems, whilst learning more about blockchain and smart contacts in the process; they needed security expertise and were open to being… well, open.

Over 2 weeks, we looked at all 5 of the Metacash smart contracts and built an attack surface heat map. This allowed us to conduct risk-based testing, focusing on the most likely exploitation points of their attack surface. The resulting audit found 10 security problems, 2 of which were of high severity. As with all of our vulnerability reports, we provided the Metacash team detailed remediation guidance to fix the problems. They did so and agreed to publish both the audit report and an updated version of their platform.

Software development and deployment are very different in the blockchain world and that requires different skills and routine research to stay abreast of emerging trends. When it comes to blockchain, our expertise spans software analysis, blockchain code review, smart contract auditing, and a deep understanding of the various technologies used in this new world of distributed consensus and trustless automation. This is precisely why our blockchain CoE was established. Groups like Metacash help make our jobs easier and more impactful; and, I encourage others to follow suit.

At Security Innovation, we want to ensure that our research helps inventors secure the innovative solutions they bring to market. It's part of our commitment to technology advancing lives -- making things easier in a secure way.