ETHEREUM CASE STUDY

Security Assessment Reduces Attack Surface in Blockchain 2.0 Technology

"Freedom. The Ethereum platform boils down to this one word," stated Jeffrey Wilcke, Ethereum Director and Chief of the Mist and Go client projects. The road to freedom isn't easy, whether you follow the path of governmental, financial, or digital independence.

The group at Ethereum is the force behind Ethereum 1.0, second-generation blockchain technology that promises freedom. Some of the main properties of this system include the following:

- ***Decentralized.*** The public ledger provides an open platform for all to use and scrutinize—no central authority is needed to resolve conflicts by the design of the consensus protocol.
- ***Versatile***. Ethereum takes blockchain technology much further than any other project in the space, providing capabilities not present in Bitcoin or in other systems using blockchain technologies.
- ***Fair and incorruptible.*** Ethereum's virtual machine enables trustless transactions through so called smart contracts between its users—entirely deterministic and complete with audit trail.

Applications built upon this platform include, but are not limited to, financial products and derivatives, contract systems, health record systems, file storage applications, as well as voting and governance applications. As this is a nascent technology, many use cases may yet be undiscovered.

Problem

Two main challenges existed with the design and construction of the Ethereum platform:

- Security for applications perceived by the primary audience
- The underlying system that provides versatility for tracking digital assets and smart contracts

Transactions of potentially very high value require extremely robust security—systems that are free from bugs and resilient to attacks. Normal development processes simply did not provide the security in the system. In fact, Ethereum designed the project as a security-based project, not schedule based.

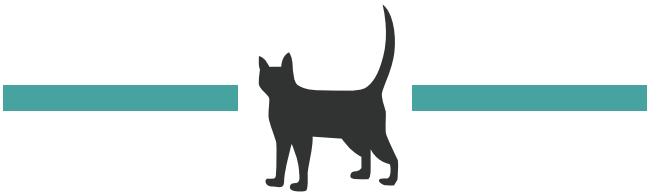
> *The system must stand up to the rigors of attacks from the moment of its launch.*

When released, the system must be "right the first time." With a system that people access for livelihoods, the consequences of mistakes become exceptionally harsh. Updates, while fixing issues, might not be accepted because the fixes can close opportunities presented in the unfixed version. The result is a security and risk-based project—a distant relative of a cost-based or schedule-based metering application or construction project.

The system must stand up to the rigors of attacks from the moment of its launch. The technical requirements for the project and its security assessment are stringent: Test the system. Test the mathematics underlying the system. Test the protocol. Test the architecture. Perform a security assessment across all components of the system, including

third-party libraries and the Ethereum virtual machine residing at the heart of the system.

Since the inception of Bitcoin, the financial world has been experimenting with blockchain technologies for financial markets, including banks, stock markets and insurers. Ethereum goes above and beyond financial applications, developing a versatile platform to represent ledgers of arbitrary transactions. Record keeping can provide reputation systems, provenance, and pedigrees in other application spaces.



Solution

The Ethereum development team started from scratch in an effort to have a superior foundation protocol and a superior decentralized blockchain platform for application development, incorporating the bleeding edge research in blockchain technology. According to Vitalik Buterin, Director, Co-creator and Original Inventor of Ethereum, no existing blockchain protocol existed that met the requirements. He had extensively researched systems using blockchain technologies and worked with various projects, the proven and the newcomers.

The organization formed a team, developed a mission statement, and began the project to build the system. A look at the team was impressive: high-powered and passionate individuals, computer scientists, mathematicians, and technology gurus who understand the components needed to build the system.

With security as the primary consideration, the Ethereum team decided on a three-prong solution for establishing security in the platform. They reached out to the following groups:

1. Academic and professional researchers in the security field
2. Security testing companies with in-depth experience with cryptocurrencies
3. Individuals that participated in a bounty program for bug discoveries

According to Dr. Jutta Steiner, Manager of Security Audits, Ethereum awarded Deja vu Security, LLC, a contract for several reasons:

- A company specializing in custom-made products that can provide an end-to-end security assessment
- Expertise in the project workspace, including blockchain technology and Bitcoin
- Enthusiasm in their work. Deja vu Security seeks and hires those with a penchant for security testing and solutions Members of the Deja vu Security team performed the following services:

Design reviews

The design reviews focused on the quasi-Turing-complete virtual machine of the clients, wire protocols, integrity of processing a blockchain, integrity of transaction processing, client implementation, and crypto- analysis.

Solution review

The solution review focused on the end-to-end process, with specific attention given to the blockchain, transactions, contracts and their internal state. The solution review also looked inside the implementation for incorrect usage of cryptographic primitives, including hashing, key strength, algorithm choices, timing attacks, padding, and more.

Protocol, P2P, and Network review

The protocol, peer-to-peer service and network were examined for susceptibility to vulnerabilities, including attacks such as Denial of Service, and the compromise and degradation of the Ethereum network.

Code review

The Go code review focused on issues, realized or potential, with data structures in the application and system, variables and pointers, threading, and network communication infrastructure.

Fuzz testing

The data items, protocols, scripting language, and Go client were fuzz tested using Peach Fuzzer®, a world- class fuzzing platform. The fuzzing system operates on any data consumer: applications, protocols, and entire systems, including SCADA systems.

Issues and risks were reported with weekly status reports, as well as a formal report bucketing the issues, identifying associated risks, recommending mitigation actions, and identifying the issues needing to be fixed before releasing the software. One issue involved a serialization parser in the Go client. Peach provided the details to identify and correct the issue. A formal final report with sign-off was issued, signifying acceptance of the deliverables and moving to a successful close of the project.

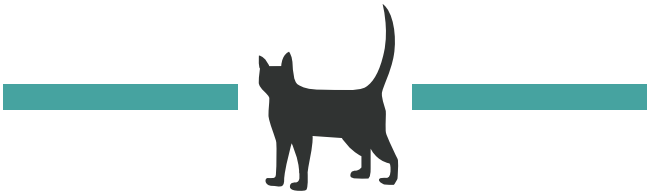
Value

Although the project findings meant additional work and schedule adjustments, the results were worth the effort. The platform is solid. Many development projects are using the Ethereum platform. The Ethereum platform is a productivity tool, offering shorter development times than a project with no platform. The Ethereum platform is robust and versatile. Its extensibility promises applications in other markets.

A security assessment performed by the security team at Deja vu Security confirmed the Ethereum design and implementation. Jeffrey Wilcke stated that the experience of Deja vu Security, in finding security issues and in having proper processes in place were invaluable. For example, Deja vu Security personnel identified missing detail in the formal specification. “It was like staring blindly at a piece of code, then having someone come up and immediately identify the issue. We were able to resolve severe issues only with your help for which we are incredibly grateful.”

Using tools that included design reviews, code reviews, reviews of the interactions among components, and a world-class fuzzing platform, Peach Fuzzer®, Deja vu Security evaluated the design and implementation, and isolated security bugs and vulnerabilities in the Go client and the blockchain protocol.

An outcome of this initial engagement has led Deja vu Security and Ethereum to continue to partner with a follow-up security assessment of the Python and C++ Ethereum clients. This project identifies and assesses unmitigated risks in the clients, and prescribes actions to mitigate the exposed vulnerabilities.



Whether your system is software, hardware, or a hybrid, Deja vu Security, LLC, has the expertise to make your system sound, secure, and vibrant. Founded and staffed by innovative thinkers, passionate security consultants, and leaders in their respective fields, Deja vu Security represents the best investment in device and application security that a sophisticated organization can make. Deja vu Security is a leader in security assessment and testing.

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