Quantstamp

A Visual Guide to Quantstamp

What is Quantstamp's mission?

Quantstamp is a Y Combinator backed security company that is developing a new protocol for smart contract verification that aims to help blockchain developers and projects around the world use its technology to perform cost-effective security audits on their contracts. Quantstamp's team boasts decades of combined experience in software security, formal verification, and static analysis, with over 500 Google scholar citations.

To date, Quantstamp has secured hundreds of millions of dollars of transaction value in smart contracts issued by leading blockchain projects around the world with our white glove security auditing services. As a proponent of the blockchain ecosystem, Quantstamp works with core infrastructure projects, community initiatives such as the Ethereum Community Fund, and funds blockchain research at leading universities such as the National University of Singapore.

What is the web product? And how is it different from the Quantstamp protocol?

Misconception: the current web product is the same thing as the Smart Contract Protocol that Quantstamp is building.

Reality: actually, the web product is the result of a separate effort by the Quantstamp Web Team. We built the web product as a demo for Y Combinator Demo Day.

Given that the protocol itself is a long-term endeavour, we wanted to demonstrate that a useful product could be delivered as an early proof-of-concept, and to help us find out what our customers want.

Since then, we have noticed that there are misunderstandings in the community about the web product, which some people seem to be confusing with the protocol or analyzers.

Analogy: you can think of the Protocol as an ocean liner: Massive, powerful, slow to turn. The Web Product is like a speed boat: Faster, agile, zipping around to explore different locations.

The various analyzer tools that we may use are like the engines that can power both ships. We are eventually building a multi-engine ocean liner, but while we're figuring out how make four engines sync together, we decided to make a little speedboat. That way, people can at least move across the water a little, and we can learn where people like to go when they're on the water.

What teams exist in the Quantstamp organization? What do they do?

There are three major teams in Quantstamp that contribute to revenue:

The Protocol Team comprises software engineers (including PhDs), research engineers, and blockchain researchers. This is the core of the company, and they are actively working on the protocol we described in the whitepaper.

The Web Team builds web products, including a demo version of the automated audit. This product was our first attempt at creating a user interface for customers to easily run audits. This team is not building the protocol.

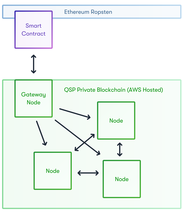
The Auditing Team consists of security and engineering experts (including PhDs). They perform manual audits for several reasons: to train our engineers about smart contract security, and to bring in revenue, which supports the Protocol and Web team. The audits increase our reach beyond the current runway.

How does the current Quantstamp web product work?

Under the hood, the web product is intended to include and build on Smart Contract analyzers, such as Oyente (an open-source tool).

Open-source tools are used by many tech companies. Open-source can be an essential aid for the innovation and creation of successful products.

Oyente is an expert tool that we made available to non experts. Oyente is hard to use on its own: you must download, compile, run, and interpret the results. We support Oyente by contributing to the project and donating to the research.



Our web product is a small part of our much larger decentralized goal. It's a UI/UX test that is giving us valuable information.
The infrastructure already allows for multiple analyzers to be added to the platform. A lot of the back-end here will one day be replaced by our protocol.

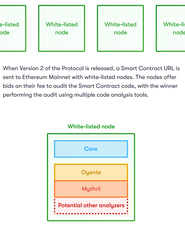
What is the Quantstamp protocol? How does it work?

The Quantstamp protocol solves the Smart Contract security problem by enabling a scalable and cost-effective system for smart contracts. Over time, we expect every Ethereum Smart Contract to use the Quantstamp protocol to perform a security audit because security is essential.

The protocol consists of two ports:

- An automated and upgradeable software verification system that checks Smart Contract code like Solidity programs. The conflict-driven distributed SAT solver requires a large amount of computer power, but it will be able to catch increasingly sophisticated attacks in time.
- An automated bounty payout system that rewards human participants for finding errors in Smart Contracts. The purpose of this system is to bridge the gap while moving towards the goal of full automation.

Protocol V1: (current)



In the current version of the protocol there is no connection to our web analyzer. Our Interface Smart Contract on Ropsten connects to a gateway node on the QSP Private Blockchain (hosted on AWS). The gateway node sends a user's submitted Smart Contract to various nodes in the network and each one checks the validation of the code.

Protocol V2: (currently being developed)

When Version 2 of the Protocol is released, a Smart Contract URL is sent to Ethereum Mainnet with white-listed nodes. The nodes offer bids on their fee to audit the Smart Contract code, with the winner performing the audit using multiple code analysis tools.

Interested in what we're building?
Follow our blog for updates:
medium.com/quantstamp