CrushCrypto

ICO Review: Quantstamp (QSP)

Protocol for Securing Smart Contracts

October 24, 2017

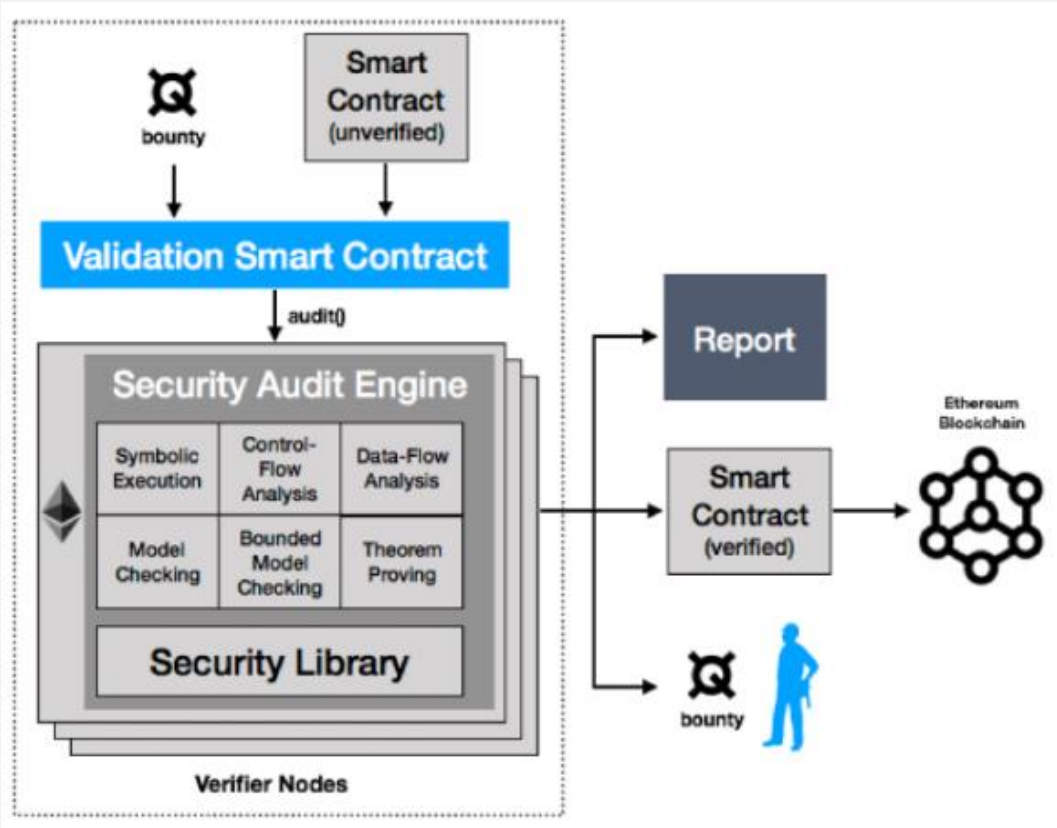
What is Quantstamp?

- Quantstamp is the first scalable security verification protocol for Ethereum smart contracts.
- Advantages include automation, trust, governance, and ability to compute hard problems over a distributed network.
- Quantstamp aims to lower the cost of smart contract auditing with reports delivered within minutes after submission.

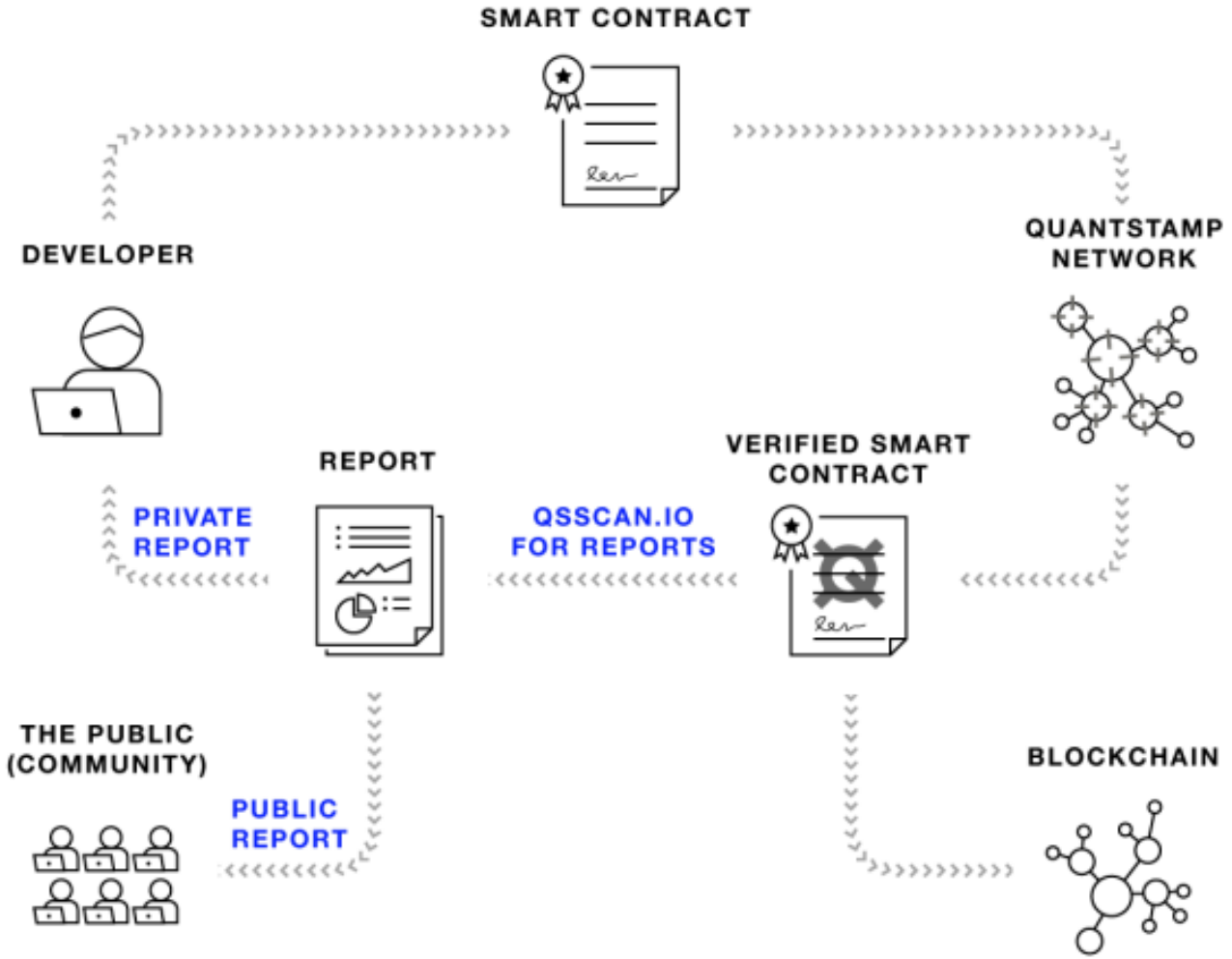
What is Quantstamp?

- Protocol components:
  - Upgradeable software verification system that checks Solidity programs.
  - Bounty system that rewards participants for finding errors in smart contracts.
- Quantstamp developments:
  - Quantstamp validation node.
  - Security library.
  - Validation smart contracts that handle bounty payment, voting mechanism and governance.

QUANTSTAMP SECURITY AUDIT ENGINE



How does Quantstamp work?



Development roadmap

Jun-Sep 2017

Quantstamp is founded by Richard Ma and Steven Stewart.

Built Solidity Static Analyzer prototype and automated truffle test generator.

Released first version of whitepaper and expanded team.

Oct-Dec 2017

Complete semi-automated audits for Request and three other companies.

Begin university partnerships, starting with the University of Waterloo.

Build Quantstamp validation/payment smart contract on Ethereum.

1H 2018

Build Quantstamp validation node and add analysis software.

Implement token holder governance.

Deploy to test network and begin academic review.

Begin work on smart contract insurance with partners.

2H 2018

Hold token holder vote for mainnet.

Release mainnet v1.

Begin work on distributed SAT consensus with BFT for mainnet v2.

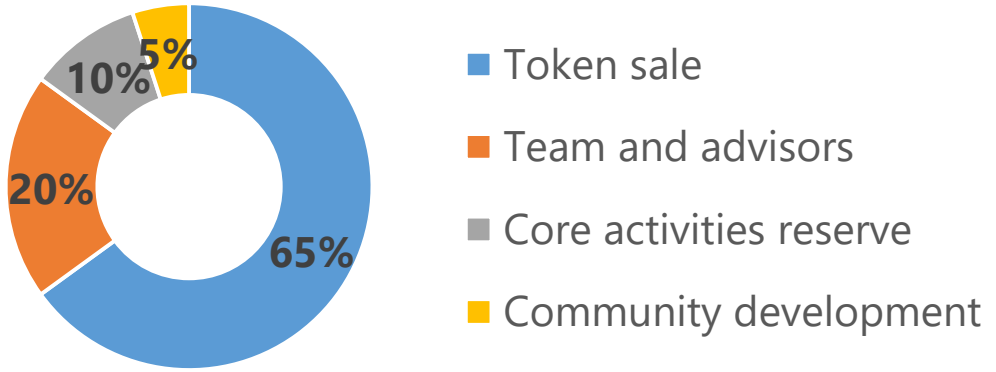
Add smart contract insurance alpha product on Mainnet smart contracts.

QSP token sale summary

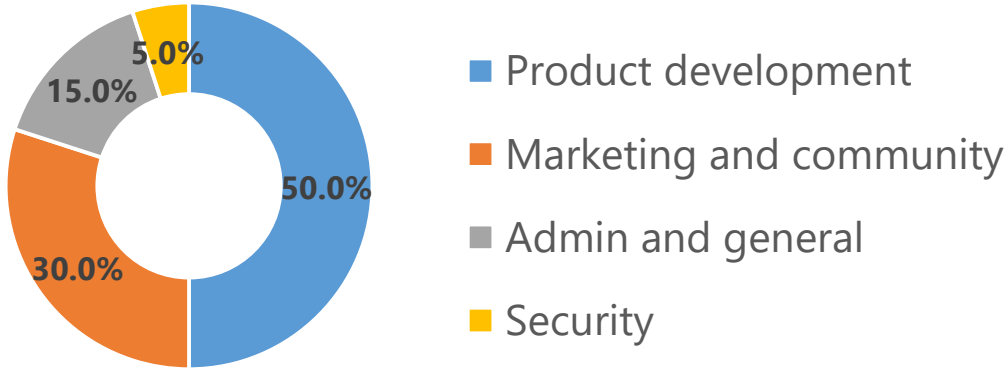
ICO SUMMARY

- **Project name**: Quantstamp
- **Token symbol**: QSP
- **Website**: https://quantstamp.com/
- **Hard cap**: US$30M (ICO contributors own 65% of total token supply if hard cap is reached)
- **Conversion rate**: 1 ETH = 5,000 QSP
- **Total supply**: 1 billion QSP
- **Max market cap at ICO (fully diluted)**: US$46M
- **Presale**: Presale is based on proof-of-caring
- **ERC20 token**: Yes
- **Bonus structure**: 3 tiers of bonuses (20% to 100%)
- **Crowdsale date**: Presale from October 4 to November 7, 2017 / crowdsale in November 2017
- **Token distribution**: 7 days after the end of ICO

TOKEN ALLOCATION



USE OF PROCEEDS



Use of QSP tokens

- QSP tokens are used to pay for, receive, or improve upon verification services.
  - **Contributors** receive tokens as an invoice for contributing software for verifying Solidity programs. Most contributors will be security experts. Contributions are voted in via the governance mechanism.
  - **Validators** receive tokens for running the Quantstamp validation node in the Ethereum network. Validators only need to contribute computing resources and do not need security expertise.
  - **Bug Finders** receive tokens as a bounty for submitting bugs which break smart contracts.
  - **Contract Creators** pay tokens to get their smart contracts verified.
  - **Contract Users** will have access to results of the smart contract security audits.

THE TEAM

Who are the people behind Quantstamp?

Richard Ma
Co-founder & CEO

Steven Stewart
Co-founder & CTO

Edward Zulkoski
Senior Security Engineer

Vajih Montaghami
Senior Security Engineer

Prit Sheth
Lead Backend Engineer

ADVISORS

Evan Cheng	**Dr. Vijay Ganesh**	**Dr. Derek Rayside**	**Dr. Sveinn Valfells**	**Tom Graham**	**Min Kim**	**David Drake**	**Parr Business Law**
Engineering Advisor	Security Advisor	Security Advisor	Blockchain Advisor	Marketing Advisor	Blockchain Advisor	Blockchain Advisor	Legal Counsel

The opportunities

- Quantstamp already had a successful audit with Request. This speaks to the team's capability in blockchain development/audit.
- This is one of the projects that can help drive blockchain adoption and the potential is significant. Quantstamp is a good candidate to tackle some of the problems currently facing blockchain adoption.
- Even if the software only has limited functionalities in the beginning, it can be a good first step in a manual audit because it can potentially save a lot of time for the auditor.
- In the Telegram, Quantstamp has indicated that they will buyback if token prices drop below ICO price, indicating that the team is confident in the project.

Our concerns

- The project is still at an early stage. The mainnet release is scheduled for August 2018, which is 9 months after the end of ICO.
- Presale participants receive up to 100% bonus which may create selling pressure after the ICO.
    - Example: If QSP tokens drop to 25% below the ICO price, those who received a 100% bonus could still generate a 50% return.
- We believe that smart contract audits cannot be fully automated because human judgment is required to understand the logic and intent of the smart contract.

Our concerns

- Since the problem that Quantstamp is trying to solve is large, there are other competitors – Etherparty, BlockCat, ZeeplinOS, and Agrello. All of these projects aim to lower the cost of smart contract development.

	Quantstamp	Etherparty	Blockcat	Agrello
Website	https://quantstamp.com	https://etherparty.io	https://blockcat.io	https://www.agrello.org
Focus	Scalable and cost effective smart contract security auditing	Enterprise contracts, securely audited and update, multi-chain publishing	Small independent contracts, individual use cases.	Multi-party legal agreements such as rent agreements.
Circulating market cap*	$30M	$48M	$4.5M	$14.7M
Fully diluted market cap*	$46M	$62M	$5.7M	$22.3M

* Based on ETH price of $280 for Etherparty, and market caps for Blockcat (CAT) and Agrello (DLT) from Coinmarketcap.com on October 24, 2017.

What do we recommend?

For flipping: **Neutral**.

- Even though public crowdsale participants are contributing 63% of the hard cap, they are only receiving 54% out of all the tokens allocated to ICO participants.

	$ allocation	$ allocation (%)	Bonus	Bonus-adjusted $ allocation	Token allocation (%)
POC tier 1 tokens	$3M	10.0%	100%	$6M	16.9%
POC tier 2 tokens	$4M	13.3%	40%	$5.6M	15.8%
POC tier 3 tokens	$4M	13.3%	20%	$4.8M	13.6%
Crowdsale tokens	$19M	63.3%		$19M	53.7%

- Unless participants get in during the presale, it is not attractive for short-term holders to contribute into the ICO.

What do we recommend?

For long-term holding: **Positive**.

- There is a lot of potential for this project, and if successful, it can really lower the cost of using smart contracts.
- With the team showing their competency by successfully auditing the Request ICO, we believe the project has a good chance to gain traction when the protocol rolls out.

CrushCrypto