SCAM Network

An autonomous network to fight scam

EDDRICK, T.; BRIAN, H.

Table of Contents

Abstract

In a constantly evolving scam landscape, SCAM token seeks to provide an anchor for victims to utilise to achieve retribution and remuneration for their losses. The SCAM network functions as a platform where victims without the ability to identify and locate their scammers are efficiently matched up with those with the ability to do so based on the financial impact of those scams.

Moreover, the SCAM network seeks to act as a beacon in the maelstrom of scamming by providing PSAs of confirmed scams. Users who report scams that are verified get rewarded with SCAM tokens, thus building a community based ecosystem within which uncovering scams and whistle blowing are rewarded.

Through such efforts, the SCAM network aims to:

1) Provide a useful platform upon which victims of scams can obtain help locating their scammers.
2) Cultivate an ecosystem where positive reinforcement in the form of financial rewards is given to successful Scam Hunters, thus promoting Scam Hunting.
3) Act as an active and effective stalwart against the burgeoning scam industry.

1. Introduction to the SCAM Network

The Scam Network is an ecosystem within which victims of scams and those with the ability to locate those scammers can be matched up, thus helping to negate many of the barriers to justice typical victims face. For instance, scammers are often difficult to track and utilise false identities, making it difficult for victims to seek any form of remuneration. By matching up victims with those proficient in tracking scammers down, the gulf in technical ability can thus be bridged.

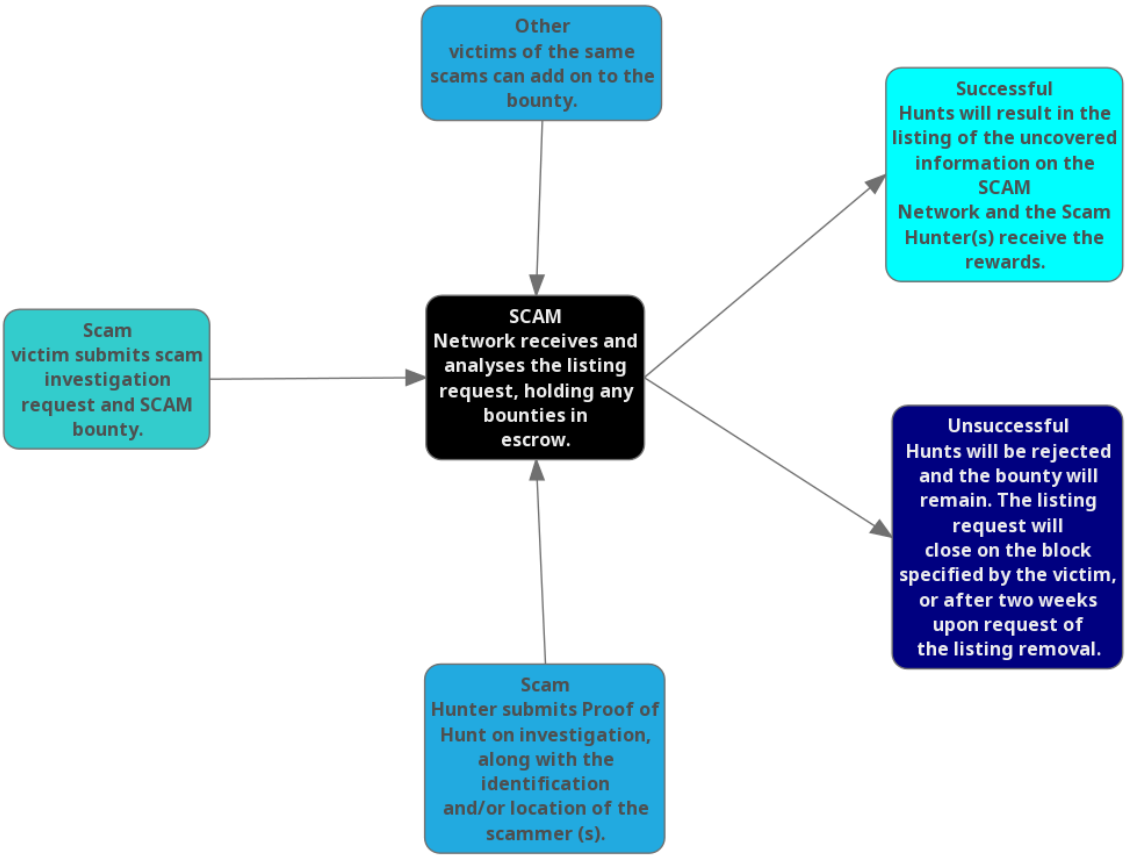
Beyond aiding victims, the Scam Network would also promote and reward Scam Hunting, where successful Scam Hunters would receive Scam tokens for their efforts. Scam Hunting can be in the form of aiding victims of scams, uncovering scams and even creating useful scam prevention information for the community. The provision of positive reinforcement for anti-scamming activities would aid in creating an ecosystem which directly counters the scam industry.

1.1 SCAM Network motivation

With the rise in ICO funding, scamming is now, more than ever a burgeoning industry. In order for there to be widespread adoption and utilisation of various cryptocurrencies, there should exist some form of self-regulation in the blockchain space, where an autonomous organisation created and sustained by the blockchain community polices and cracks down on scamming. By helping to foster a safer and more legitimate environment for the blockchain community, the SCAM Network hopes to utilise this as a spring board to target scams in all communities.

2. SCAM Network model

2.1 Scam Investigation and Auditing Main net system (SIA)



2.2 Purpose and function of the SIA system

The focus of the network is to directly combat the scam industry by facilitating the ability of victims to find remuneration for their losses. Traditional sources of remuneration such as legal means of seeking compensation for losses or punishment for the perpetrators through prosecution struggle to provide the traditional safety net for victims in a digitalised world. Since victims do not necessarily have the ability to easily locate their scammers, they have difficulty seeking any form of justice, thus allowing scammers to escape scot free. This rewards further scamming behaviour and encourages the growth of the scamming industry, thus creating a vicious cycle that consistently rewards the efforts of scammers.

Hence, the focus of the SCAM Network is to break such a cycle by providing negative reinforcement to scamming by making the locating of scammers a rewarding experience. Beyond just helping victims by seeking justice through the already well-established, traditional means, the SCAM Network also hopes to discredit the reputation of scammers. Through the utilisation of social

exclusion and punishment, the SCAM Network seeks not only to help victims, but also to deter the perpetrators with the extensive and longstanding impacts of reputation loss.

Some argue that this may create a separate enclave of society, where scammers band together, creating an us-them false dichotomy of social separation. This is true of the traditional systems of prosecution, where there is no place for the technical prowess of the scammer to be rewarded in a constructive manner. The SCAM Network solves this elegantly by allowing anyone with the technical ability to accurately locate scammers collect bounties for their efforts, thus providing a financial reward for scammers to turn against each other and use their abilities in constructive manners. Moreover, since bounty hunters can remain anonymous, whistle blowing is hence actively rewarded as well.

The negative reinforcements that the SCAM Network provides against scamming thus also provides positive reinforcements for those within the scamming industry to support the SCAM Network instead of continuing to scam, allowing for the smooth transition of skilled labour away from the destructive scamming industry to the constructive SCAM Network.

2.3 SIA system mechanics

2.3.1 Submission process

Victims who desire help or those who would like to support them would need to submit a request form via the main platform. The platform would require the submission of user and scam details, as well as the bounty that the victims would like to post and the bounty release details that suit them. There would be a minimum of 0.05 ETH worth of SCAM as per the market rate, or 25 USD worth of SCAM as per the market rate, for the bounty, so as to prevent spamming of the submission process (or any malicious attempt to overwhelm this system of review). Since bounties are only payable in SCAM tokens, other cryptocurrencies paid by the user would be converted to SCAM through third parties such as shape shift or through the foundation itself at a fee. The fee earned would then be used to pay for the foundation upkeep as well as the purchasing and burning of SCAM tokens.

2.3.2 Listing process

Details of the scam investigation request would be posted on the Main net, where users can vote on the validity of the request as well as to contribute to the bounty pool. The same rules apply for the submission of bounties, aside from the minimum sum. The foundation would also review the application to ensure that the investigation report is non-malicious in nature.

2.3.3 Proof of Hunt submission

Proof of Hunts can be submitted anonymously, but all submissions would not be accepted until all critical data points are filled in accurately. Along with CAPTCHAs, these would help bounty hunters keep their anonymity if so desired while still preventing malicious spam from clogging the system.

2.3.4 Proof of Hunt auditing process

Proof of Hunts would initially be audited solely by the foundation to ensure its legitimacy as well as to ensure that the information obtained would be sufficient for victims to mount a legal case against those who had scammed them. This process would be broken down into different portions for gradual automation. Processes which are the easiest to automate with bots and machine learning would be automated first, and the source code would be released to the public. Bug bounties would be set up to encourage and reward the community to contribute to the project and eventually take over much of the decision making for themselves. There would also be training processes which allows for individuals in the community who are interested in being involved in the auditing process to be verified and trained. They would act as a neutral third-party confirmation to eventually replace any remaining centralised foundation auditing.

This is designed so as to ensure a smooth transition from a centralised, but functioning audit process into a trust-less, decentralised and fully functioning audit process can occur, hence contributing to the self-sustainability of this system.

2.3.5 Bounty release process

The bounty release process would be in accordance with the settings which the original victim has configured the smart contract to have. That being said, there would be a grace period for further critical submissions to occur. This would be discussed in further detail in the section 2.3.6 about the NICE process.

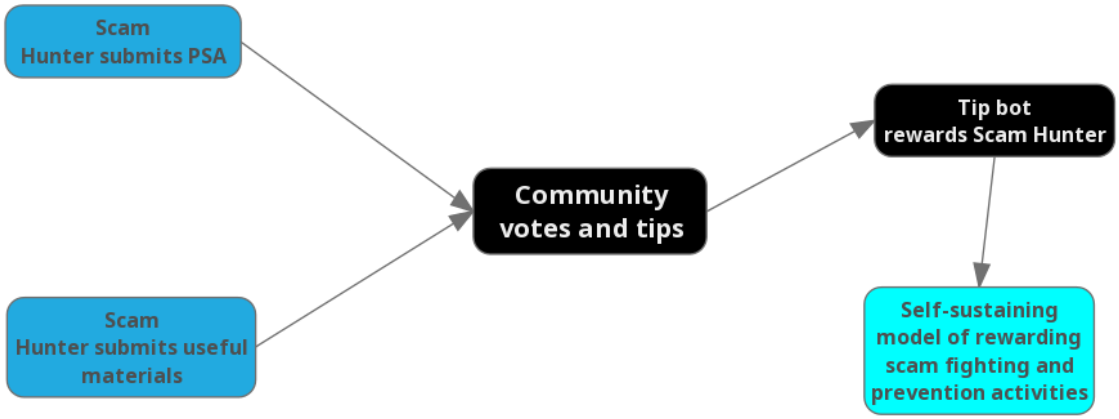
2.3.6 New Investigation Continuation Engine process (NICE)

This process is designed to ensure that critical information that happened to be missing in the original Proof of Hunt but happened to resurface or be discovered by other bounty hunters would not be excluded.

If this event occurs within the grace period mentioned within section 2.3.5, the main bounty would be split according to the extent of information that might be missing from the original Proof of Hunt. Since this process is inherently subjective, all users of the system must agree to the intervention of third party mediators such as the foundation at the point of usage of any of the products that the SCAM Foundation develops.

If this event occurs outside the grace period, the bounty hunter can choose to either allow the foundation to provide the information to the community without charge (relying on tips from the community to achieve profitability) or to decide on a minimum fee that they would want the community to raise before the information would be released. The SCAM Foundation would decide if it would like to help to raise said funds as per the foundation’s discretion.

2.4 Anti-scam Continuation Ecosystem (ACE)



2.5 Purpose and function of ACE

In times where scams have yet to surface, there must still be consistency in the rewarding the anti-scamming community to ensure the continued absence of scams. The shift in focus from rewarding Scam Hunters for helping victims seek justice to scam prevention helps to retain skilled labour within the anti-scamming ecosystem and continuously provide a financial incentive to work against the scamming industry.

This helps the SCAM Network attack the scam industry from multiple angles and maintain its ecosystem.

2.6 ACE system mechanics

2.6.1 PSA compilation mechanics

PSAs are submitted by those who happen to discover scams or possible scams that may occur. This PSA appears on the PSA portion of ACE, allowing users to vote on its validity. These PSAs will be vetted and verified by the SCAM Foundation, but no submitted PSA would be censored. Verified PSAs would contain the verified tag from the SCAM Foundation. This verification process would also be subject to the same automation process mentioned in 2.3.4.

2.6.2 Useful material submission

The useful material submission section would be in the form of a forum-like platform moderated by community members. Tipping and voting bots would be available for tipping and voting purposes.

2.6.3 Whistle-blowing Temptation mechanism

This mechanism can function in the form of two different process flows, and is meant to tempt those who happen to be involved in scams or organisations attempting to perform or performing illicit activities to whistle-blow on their compatriots and superiors. The first means of encouragement is for the potential whistle-blower to submit the specifications of the evidence that he or she possesses, the amount of SCAM tokens desired and the time by which the bounty is required. If the bounty is achieved, the information is first released to the SCAM Foundation for analysis to ensure the validity of the information.

The second means of encouragement would be for whistle-blowers to release the information on ACE, allowing the community to vote and tip the whistle-blower. This would be subject to the same type of verification process mentioned in 2.6.1.

The way this mechanism was designed was with the intention to make whistle-blowing profitable and to prevent scams from being carried out in the first place. Naturally, this also acts as a means with which whistle-blowers can utilise in their advantage to absolve themselves from wrongdoing, on top of receiving a reward for their efforts in securing useful, anti-scam material for the community.

All verification processes would also be subject to the same automation process mentioned in 2.3.4.

2.7 Game theory behind how the SCAM Network can be self-sustaining

To function as a counter to the scamming ecosystem, a similarly rewarding, self-sustaining system must be put into place for anti-scamming activities. This creates a virtuous cycle where scammers are held liable, legally or otherwise, and where scam prevention is taken up. Assuming self-satisficing behaviour by all actors, the financial rewards of such anti-scam actions would create an ecosystem of autonomous policing, which is severely lacking in the current cryptocurrency landscape.

This particular model of direct scam opposition followed by scam prevention acts to neutralise two different instances where other models promoting anti-scamming behaviour will fail:

1. **The Red Queen event**
   Scammers will always stay one step ahead of scam policing because rewards are focused on punishing scammers rather than preventing scammers, which result in a system that requires the presence of scammers to survive. This thus results in autonomous systems which *allow scams to happen first* to be able to have something to punish and thus profit off.

   The SCAM Network targets this by providing an alternate stream of revenue in the form of rewarding the prevention of scams themselves – the exposing of code flaws and the sharing of security tips and tricks before any scams can happen. This creates a prisoner's dilemma situation for Scam Hunters, as those who find any room where scams can happen would not be incentivised to hide it from the community, since those who report said flaws would prevent anyone from profiting off scam victims.

2. **Mutually assured destruction event**
   Systems that are incentivised at destroying scamming activities at the cost of its own survivability will eventually allow itself to be destroyed, but the positive reinforcement that scamming gives would always revive it. To revive anti-scamming systems would, however, only provide negative reinforcement due to the cost of creating such ecosystems.

   The prisoner's dilemma that the SCAM Network creates for the actors in our ecosystem would prevent the premature death of itself by merely diverting funding from locating and punishing scammers to preventing scams themselves. Through this bi-directional, cohesive system, the SCAM Network prevents its premature capitulation to continue as a scam preventive mechanism even when scams do not exist.

3. Double crossing event

Since the SCAM Network functions by rewarding anti-scam behaviour, this creates the possibility where Bounty Hunters concoct scams in order to "uncover" the same scams they created. Hence, instead of eliminating scams, the SCAM Network might end up indirectly promoting scamming activities.

The winner takes all design of the SCAM Network thus helps to eliminate this possibility by appealing to the self-satisficing behaviour of potential scammers. Since only singular actors will receive any of the rewards, this deters any collusion between the scamming community, especially since the first person to claim the bounties for whistle blowing, scam investigation and PSA would get everything, leaving the rest to suffer the negative consequences. This multi-facetted system allows for many opportunities for singular actors to claim rewards for foiling scams or revealing perpetrators, thus creating a scamming ecosystem that, at every single juncture, would benefit every actor more to participate in anti-scamming activities.

3. Products

3.1 SIA Main net system

The primary objective of the SCAM Network is to incentivise the identification of scammers and thus be able to help victims hold them liable for their crimes. Hence, the main product would be the Scam Investigation platform, where victims can post bounties held in secure escrow through smart contract for Bounty Hunters to claim. Group victims can also pool their resources for huge bounties by simply contributing to the same bounty post.

3.2 Anti-scam Continuation Ecosystem

This secondary part of the SCAM Network is essential for its continued survival and promotion of anti-scam activities. It acts as a place where the community can interact, exchange security pointers and expose security flaws present in code or in hardware, all while being rewarded for it. Moreover, PSA of scams listed by the community on a platform would also be developed to help prevent more people from falling victim to known scams. This is also a place where whistle-blowers can go to obtain rewards for their troubles and thus stopping scams before they occur.

3.3 Bots

Bots to analyse community behaviour and participation for bounty rewards would be produced. Moreover, tipping bots and other community support bots would also be developed to encourage healthy, organic growth of the community. Auditing through bots would also be produced to reduce the amount of manual labour that due diligence incurs.

4. Product road map

Phase 0: Token listing (est. date from Q2 2018 onwards)

Focus on token listing on exchanges to encourage early adoption.

Phase 1: Main net launch (est. date Q2-3 2018, 10% reserve token burn)

The SCAM Network launches its main Scam Investigation platform for users to seek help and earn bounties. Vetting of Proof of Hunt would still be done completely manually at this stage, paid for by a small fee on the bounty and a joint payment from the proceeds of the token sale. All participants in the whitelisting would automatically become a member on the platform.

Phase 2: Anti-scam Ecosystem launch (est. date Q3-4 2018, 25% reserve token burn)

Launching of the Anti-scam ecosystem would act as the counter balance to the Scam Investigation platform and use game theory to reward continued anti-scam activities. A scam PSA platform and anti-scam forum would be the key instalments of this release. Bots for tipping, comment/thread linking and sharing would also be released.

Phase 3: Investigation and adoption of partial to full automation through code and smart contracts (est. date Q2-3 2019, 50% reserve token burn)

Vetting of Proofs of Hunt would require automation to reduce the cost incurred in verifying the accuracy of the data produced by Scam Hunters up to the necessary standards of due diligence. This inherently labour and time intensive endeavour can be made to be relatively trustless by elevating the role of the auditor to that of an arbiter, where the SCAM Network goes from being the independent reviewer to the independent professional judiciary over the results of the analysis by code.

5. Token sale

5.1 Terms of SCAM token sale

All SCAM tokens ever produced would be issued on the ETH blockchain through the ERC20 token standard. Total token supply ever to be minted would be 12 million tokens.

Only ETH would be accepted in this crowd sale, up to a $12,000,000 hard cap.

5.2 SCAM token distribution

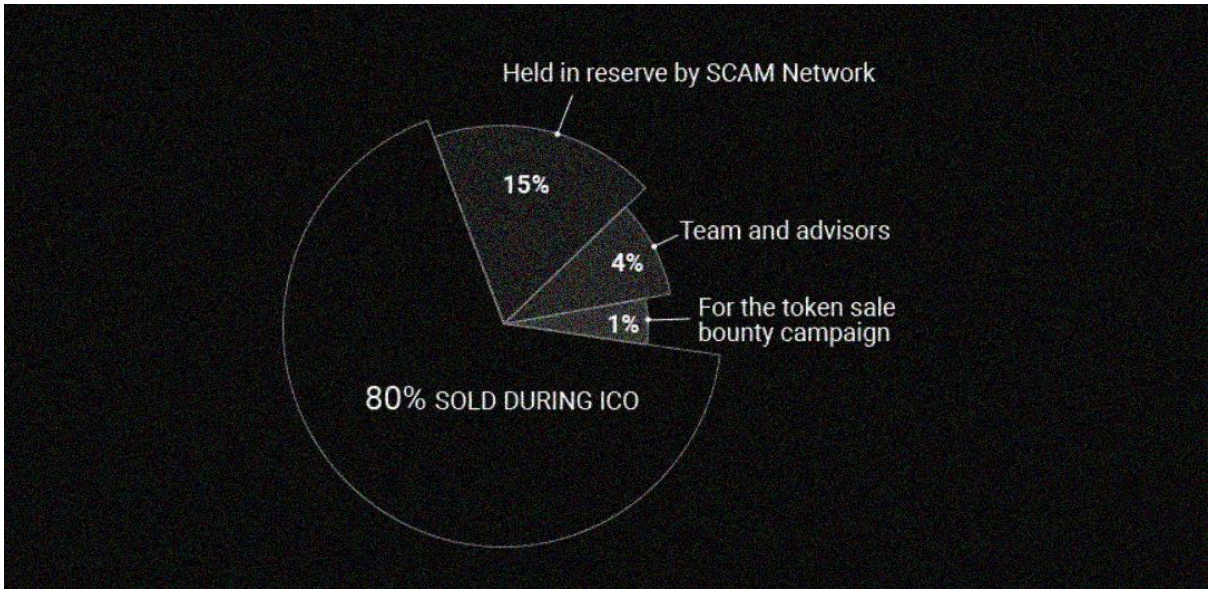
SCAM will be distributed as described below:

80% for token sale contributors

15% for the SCAM Network for testing and reserve purposes which would be systematically burnt as the team progresses through Phase 1-3

4% for advisors, partners and the team

1% for the token sale bounty campaigns



6. Disclaimers

THIS DOCUMENT DOES NOT CONSTITUTE AN OFFER TO SELL, AN INVITATION TO INDUCE AN OFFER, OR A SOLICITATION OF AN OFFER TO ACQUIRE SECURITIES. THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY AND DOES NOT CONSTITUTE INVESTMENT ADVICE.

THE SALE OF SCAM TOKENS CONSTITUTES THE SALE OF A LEGAL SOFTWARE PRODUCT UNDER SINGAPOREAN LAW. IT IS THE RESPONSIBILITY OF EACH POTENTIAL PURCHASER OF SCAM TOKENS TO DETERMINE IF THE PURCHASER CAN LEGALLY PURCHASE SCAM TOKENS IN THE PURCHASERS JURISDICTION AND WHETHER THE PURCHASER CAN THEN RESELL THE SCAM TOKENS TO ANOTHER PURCHASER IN ANY GIVEN JURISDICTION.

ALL POTENTIAL RISKS CAN BE ASSESSED HERE.

OUR WHITE PAPER MAY CONTAIN 'FORWARD LOOKING STATEMENTS' - THAT IS, STATEMENTS RELATED TO FUTURE, NOT PAST, EVENTS. IN THIS CONTEXT, FORWARD-LOOKING STATEMENTS OFTEN ADDRESS OUR EXPECTED FUTURE BUSINESS AND FINANCIAL PERFORMANCE, THE PERFORMANCE, AND ACCURACY OF SCAM NETWORK, AND OFTEN CONTAIN WORDS SUCH AS 'EXPECT', 'ANTICIPATE', 'INTEND', 'PLAN', 'BELIEVE', 'SEEK', 'SEE', 'WILL', 'WOULD', 'ESTIMATE', 'FORECAST' OR 'TARGET'. SUCH FORWARD LOOKING STATEMENTS BY THEIR NATURE ADDRESS MATTERS THAT ARE, TO DIFFERENT DEGREES, UNCERTAIN. WE CANNOT GUARANTEE THAT ANY FORWARD LOOKING STATEMENTS, BACKTESTS OR EXPERIMENTS MADE BY US OR EXPECTED RESULTS OF OPERATION OF THE SCAM NETWORK WILL CORRELATE WITH THE ACTUAL FUTURE FACTS OR RESULTS.

FOR THE CONVENIENCE OF OUR USERS, SCAM TOKEN WHITE PAPER, WEBSITE AND OTHER RELATED DOCUMENTS ARE AVAILABLE IN A NUMBER OF LANGUAGES. IN THE EVENT THERE IS ANY CONFLICT BETWEEN THE ENGLISH LANGUAGE VERSION AND A FOREIGN LANGUAGE VERSION, THE ENGLISH LANGUAGE VERSION SHALL GOVERN.