Harnessing blockchain technology to transform global cybersecurity

By Colin Thornton

17 May 2018

In a digitally driven world, cybersecurity has become a highly lucrative sphere of modern business.

© monsit jangariyawong via 123RF

Today, experts around the world are clawing for a piece of the estimated $8.5bn cyberthreat intelligence industry pie, with innovative new products and solutions emerging almost every day.

Unsurprisingly, blockchain technology is being explored as a potential tool to combat increasingly sophisticated cyberthreats, and to provide experts and researchers with fresh incentives to fight cyber criminality in every shape and form.

Don't spend another cent on cybersecurity until real risks have been assessed

Charl Ueckermann 6 Apr 2018

According to Wikipedia, a blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography.

Recent reports have indicated that the global blockchain market size is expected to grow from $411.5m in 2017 to $7,683.7m by 2022, a truly startling figure.

Re-thinking ‘threat intelligence’

Arguably, today’s cybersecurity experts are not properly incentivised to keep scouring for the millions of potential cyberthreats that exist (or are being developed). As a result, malware often falls through the cracks in established anti-virus solutions – leaving companies and individuals vulnerable to attack.

With this in mind, US based Swarm Technology Inc. has created a decentralised IT security marketplace called PolySwarm. The marketplace is designed to bolster innovation and competition within the cyber intelligence community by rewarding the cyber experts who ‘are best able to protect users.’

According to PolySwarm, “this provides enterprises and consumers with unprecedented speed and accuracy in threat detection.”

It also addresses the all too common theme of the major, established anti virus-players failing to identify and correct emerging cybersecurity threats.

An anti-virus token…?

Importantly, blockchain lies at the heart of the pioneering PolySwarm marketplace.

Spinning out of the security firm Narf Industries, which recently completed a blockchain identity management project for the US Department of Homeland Security, Swarm Technologies believes that a crypto token could be used to close the insidious gaps in modern cybersecurity measures more efficiently.


How to avoid disaster in the wake of Spectre and Meltdown
Colin Thornton 23 Jan 2018

In late February 2018, the company launched an initial coin offering (ICO), with the public token sale running until 22 March 2018. Notably, PolySwarm raised an initial $15m in funding from backers, which included Science Blockchain.

The PolySwarm market runs on Nectar (“NCT”), an ERC20-compatible utility token that reportedly makes it easy to submit and classify potential threats on the PolySwarm market.

In a media statement, the company noted that Nectar essentially ‘replaces traditional, outdated antivirus and threat-scanning subscription payments.’

According to coindesk.com, proceeds raised during the token sale will initially go to building out PolySwarm, where Swarm hopes security researchers will come together to work on what it calls "micro-engines” - specialised software built to scan documents, files and websites that might hide vulnerabilities. Those ‘engines’, and the researchers behind them, will be rewarded by payment of the Swarm token.

Shared rewards system

While the Swarm/nectar tokens will be used to make all the payments on the platform, those payments will not just move

from Swarm to the researchers.

Importantly, the system also requires micro-engines to stake an amount of nectar tokens on its assessment of the digital products it is scanning. According to the company, the number of tokens backing each assessment indicates the researchers' confidence in that assertion. Then, every micro-engine (and in turn the researcher who built it) that makes the correct assessment gets a share of the fee paid for the scan, plus a share of any nectar that was staked by micro-engines that assessed the digital product incorrectly.

This smart system of shared rewards arguably incentivises researchers to find niche areas to scan – areas where many other researchers might not be bothering to look!

While it is still very early days, both the cybersecurity and blockchain communities will be keeping a hawk eye on the evolution of the PolySwarm marketplace and its novel system of incentivisation…

ABOUT COLIN THORNTON

Colin founded Dial a Nerd in 1998 as a consumer IT support company and in 2002 the business- focused division was founded. Supporting SME's is now its primary focus. In 2015 his company, merged with Turrito Networks who provided niche internet services outside of the local network. These two companies have created an end-to-end IT and Communication solution for SME's. Colin has subsequently become the managing director of Turrito. Contact him at info@dialanerd.co.za

- Understanding SA's 5G reality - 4 Apr 2019
- Why your business needs a cloud architect - 21 Feb 2019
- Privacy vs Profit: Will 2019 be the year of consumer paranoia? - 26 Nov 2018
- Why SMEs should be looking at cyber insurance - 28 Sep 2018
- Why your future digital ID should harness blockchain technology - 23 Aug 2018

View my profile and articles...