

## Researchers tap AI in the fight against ICO scams

by [TRISTAN GREENE](#) — 3 days ago in [ARTIFICIAL INTELLIGENCE](#)



There's no definitive way to tell if an initial coin offering (ICO) is a scam, but a machine learning-based research method could make it easier to avoid the most obvious ones. And that's good for everyone except the scammers.

A Chinese startup called [Shannon.AI](#), working with researchers from Stanford, University of California Santa Barbara, and the University of Michigan, recently unveiled a white paper detailing an AI designed to sniff out cryptocurrency scams.

When it comes to cryptocurrency investing there's only one sure-fire way to avoid getting scammed: don't do it. Sure, the [Bitcoin bros and millennial millionaires](#) make it look like we can all drive our lambos to the moon if we invest, but the reality is the majority of ICOs last year were either [scams or failed](#).

As the researchers put it in their [white paper](#):

*Despite the fact that ICOs are able to provide fair and lawful investment opportunities, the ease of crowdfunding creates opportunities and incentives for unscrupulous businesses to use ICOs to execute “pump and dump” schemes, in which the ICO initiators drive up the value of the crowd-funded cryptocurrency and then quickly “dump” the coins for a profit.*

So how do you separate the scams from the legitimate contenders when they all seem like techno-babble to anyone who isn't well-versed in reading white papers?

There's no easy answer. An almost complete lack of any regulation makes it impossible to 'prove' a scam until [it's too late](#). This isn't about spreading fear, uncertainty, and doubt (FUD). It's simple facts.

Part of the reason for this is white papers and websites can be made to look legitimate with relative ease. Simply put, most scammers are counting on the fact that you won't dedicate as much time to researching their coin as they can to making it appear legitimate.

The problem is made even worse by the general toxicity and shill-like nature of the vast majority of cryptocurrency communities. When you have a large group of people whose common denominator is a mutual investment, coupled by bounty programs for spreading positive messages, it becomes impossible to get a clear picture of a coin's legitimacy by talking to the people involved with it.

The Shannon.AI team's white paper outlines a machine learning approach to separating the scams from legitimate projects:



*By analyzing 2,251 ICO projects, we correlate the life span and the price change of a digital currency with various levels of its ICO information, including its white papers, founding team, GitHub repository, website, etc. For the best setting, the proposed system is able to identify scam ICO projects with a precision of 0.83 and an F1 score of 0.80.*

Credit: [Shannon.AI](#)

 The number of ICOs has grown at a similar rate to the market cap. Most of them will fail within the first year.

And this is encouraging, even if it isn't revolutionary. This particular paper showcases an algorithm-based system that essentially automates what savvy investors are already doing by seeking out publicly available information that draws an overall picture of a coin. This is good for a couple of reasons, as the team points out:



*Compared against human-designed rating systems, ICORATING has two key advantages. (1) Objectivity: a machine learning model involves less prior knowledge about the world, instead learning the causality from the data, in contrast to humandesigned systems that require massive involvement of human experts, who inevitably introduce biases. (2) Difficulty of manipulation by unscrupulous actors: the credit rating result is output from a machine learning model through black-box training. This process requires minor human involvement and intervention.*

holders as “paid attacks” or FUD, even when they come from reputable news sites.

It’s easier for a company to attack the messenger than fix any problems pointed out by legitimate researchers and journalists.

But if an AI working in a black box comes to the same conclusions, based on the same readily available information, it could be considered more trustworthy. The Shannon.AI algorithms don’t do anything a person couldn’t do on their own, but they do it much, much faster — and with greater accuracy.

Unless you’re a journalist or researcher who has the luxury of spending days at a time poring over white papers, websites, and Github repositories, you’re probably missing key pieces of information. AI that does the same job in a fraction of the time could make scam ICOs a thing of the past, or at least the minority.

We’ve reached out to the research team to see if there’s any plans to go to market with this tool, or if they’ll be further developing it.

In the mean time, trade with care: for every person who made millions investing in altcoins there are thousands of people who wished they’d paid attention to the red flags before investing.

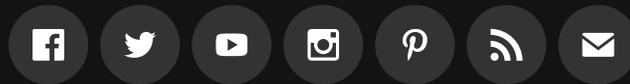
*Want to hear more about AI from the world’s leading experts? Join our Machine:Learners track at [TNW Conference 2018](#). Check out info and get your tickets [here](#).*

TECH

 SHARE ON FACEBOOK (274)

 SHARE ON TWITTER (287)





[EVENTS](#) [ABOUT](#) [TEAM](#) [ADVERTISE](#) [JOBS](#) [CONTACT](#)

**TNW** © 2006–2018 The Next Web B.V.  
Made with ♥ in Amsterdam.  
Powered by **maxCDN**