

# Treadwell Stanton DuPont today announced its researchers quietly broke the SHA-256 hashing algorithm over a year ago

*This cryptographic breakthrough will provide massive financial advantages to bitcoin investors and traders worldwide.*

NEW YORK, NEW YORK, UNITED STATES, September 3, 2019 /EINPresswire.com/ -- The Wall Street fintech [Treadwell Stanton DuPont](#) broke silence today as it [announced](#) its Research & Development and Science Teams successfully broke the SHA-256 hashing algorithm silently in controlled laboratory conditions over a year ago. The announcement aims to secure financial and technological platform superiority to its clients and investors worldwide.



"The era of decentralized, inflation-free digital currency is upon us," said CEO Mike Wallace. "These breakthrough advances in cryptanalytic research, amidst widespread economic recession fears, create incredible financial opportunities, but also come with huge responsibility to ensure the technology we build is secure and benefits everyone."

SHA-256, which stands for Secure Hash Algorithm – 256bit, is a one-way function that converts a text of any length into a string of 256 bits, known as a hashing function. SHA-256 is a member of the SHA-2 cryptographic hash functions designed by the NSA, with all major SSL certificate issuers using it to enable encrypted communication between a web browser and a web server, which is by all current standards deemed secure and trustworthy. Up to now, it was thought impossible to use the output of the hash function to reconstruct its given input. However, this now seems to have changed, although Treadwell Stanton DuPont's cryptanalysis does not work exactly this way. It should also be remembered that Bitcoin makes heavy use of the SHA-256 cryptographic hash function too, and so it is not very clear what impact the recently announced discovery may have on the cryptocurrency.

While the best public cryptanalysis has tried to break the hashing function since its inception in 2001, work on searching, developing and testing practical collision and pre-image vulnerabilities on the SHA-256 hashing algorithm began back in 2016 in Treadwell Stanton DuPont's R&D facilities, culminating 2 years later with the successful discovery of a structural weakness and the initial development of the first practical solution space of real world value by its researchers.

"While we have successfully broken all 64 rounds of pre-image resistance," said Seijiro Takamoto, Treadwell Stanton DuPont's director of newly formed Hardware Engineering Division, "it is not our intention to bring down Bitcoin, break SSL/TLS security or crack any financial sector security whatsoever."

In accordance with its disclosure policy, Treadwell Stanton DuPont won't be saying exactly how they did it — because once the proof-of-concept is out, anyone with enough computing power will be able to produce a SHA-256 collision, rendering the algorithm both insecure and obsolete. Cryptographers have long been predicting a collision like this would require at least 100 years before someone produced a smart enough algorithm which actually finds and exploits a structural weakness, given the mathematical laws that govern hash functions. And while it is inevitable that hash collisions should occur because the input data is potentially infinite but the output length is fixed, this prediction has been rendered very short. For a while back we've all known to some extent something like this would be possible and was bound to happen, albeit not so fast.

Treadwell Stanton DuPont revolutionized stock market forecasting technology with the introduction of the NeuroEvolution Based Unified Layer Architecture (NEBULA) Synaptic Synthesis Engine (SSE) online platform in 2017. Today, Treadwell Stanton DuPont leads the world in innovation with the use of quantum-inspired combinatorial optimization computing techniques, empowering investors with breakthrough stock market forecasting services.

Annabelle Wilson  
Treadwell Stanton DuPont  
+1 917-809-4370

[email us here](#)

Visit us on social media:

[Facebook](#)

[Twitter](#)

---

This press release can be viewed online at: <http://www.einpresswire.com>

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases. © 1995-2019 IPD Group, Inc. All Right Reserved.