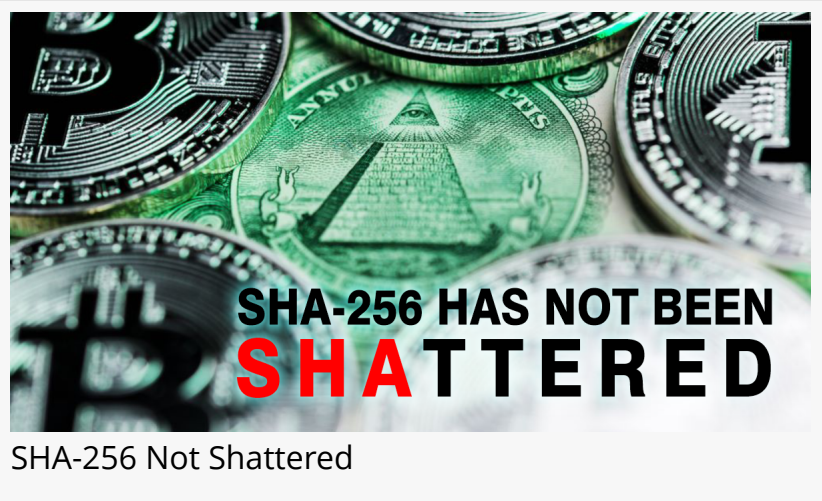


Treadwell Stanton DuPont today announced its R&D Team discovered a flaw in their own SHA-256 laboratory research

Further laboratory controlled trials led its researchers to identify an equipment flaw which was discovered to be rendering incorrect, ambiguous results.

NEW YORK, NEW YORK, UNITED STATES, September 12, 2019 /EINPresswire.com/ -- The Wall Street fintech [Treadwell Stanton DuPont](#) again broke silence today as it [announced](#) its Research & Development and Science Teams discovered a hidden laboratory equipment flaw which led to incorrect, ambiguous results during third and fourth tier trials concerning their attempt to break the SHA-256 hashing algorithm. The firm had previously announced it had succeeded silently over a year ago. The announcement aims to assure financial and security sectors the hashing algorithm is still secure.



"Rest assured all sectors can still sleep quietly tonight," said CEO Mike Wallace. "Our preliminary results in this cryptanalytic research led us to believe we were successful, but this flaw finally proved otherwise."

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. With this news, it is still confirmed impossible to use the output of the hash function to reconstruct its given input, even though Treadwell Stanton DuPont's cryptanalysis did not work exactly this way. It should also be remembered that Bitcoin makes heavy use of the SHA-256 cryptographic hash function too. Crypto investors can now relax as there is no impact from the previously announced (flawed) discovery.

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 preimage vulnerabilities on the SHA-256 hashing algorithm began back in 2016 in Treadwell Stanton DuPont's R&D facilities. It was thought to have culminated 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. This is not so anymore.

"We are being forced back to the drawing board," said Seiji Takamoto, Treadwell Stanton DuPont's director of newly formed Hardware Engineering Division. "We will be tightly testing, validating and confirming our advances with support from specially appointed cryptographers

and observers before making any such announcements in the future."

In accordance with its disclosure policy, Treadwell Stanton DuPont still won't be saying exactly how their advances progressed nor reveal any of their research just yet. Cryptographers have long been predicting a SHA-256 collision 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 is still holding its ground as of today.

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](#)

[LinkedIn](#)

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.