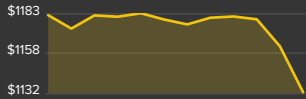


TRENDING

CoinDesk Research Releases 'Blockchains for Insurance' Report

BITCOIN PRICE INDEX (24H)



USD -4.08% ▼

**\$1,132.79**

EUR €1,072.47

CNY -4.38% ▼

**¥7,463.88**

GBP £908.93

NEWS ▾ PRICE & DATA ▾ GUIDES ▾ EVENTS ▾ RESEARCH ▾ ADVERTISING/PR ▾

FEATURES • TECHNOLOGY

# Who Broke the SHA1 Algorithm (And What Does It Mean for Bitcoin)?

Corin Faife (@corintxt) | Published on February 25, 2017 at 16:00 GMT

FEATURE



The cryptography world has been buzzing with the news that researchers at Google and CWI Amsterdam have succeeded in successfully [generating a 'hash collision'](#) for two different documents using the SHA1 encryption algorithm, rendering the algorithm 'broken' according to cryptographic standards.

But what does this mean in plain language, and what are the implications for the bitcoin network?

## Hash collisions

As laid out in a recent CoinDesk [explainer](#), a hash function (of which SHA1 is an example) is used to take a piece of data of any length, process it, and return another piece of data – the 'hash digest' – with a fixed length.

One way that hash functions are used in computing is to check whether the contents of files are identical: as long as a hash function is secure, then two files which hash to the same value will always have the same contents.

However, a hash collision occurs when two different files hash to the same value.

### DON'T MISS A SINGLE STORY

Subscribe to our free newsletter and follow us

SUBSCRIBE



**consensus**  
2017

**Registration Is Open!**

REGISTER NOW

### CONSTRUCT 2017 VIDEO

### SPONSORED FINANCIAL CONTENT



**We could see the end of Social Security in 2017...**

Banyan Hill



**Before Applying For A Credit Card, Check If You Pre-Qualify Citi**

dianomi

### FEATURES



**After New Highs, Bitcoin Price Faces Uncertain Path Ahead**

New Ethereum Proposal

Given the mathematical laws that govern hash functions, it is inevitable that hash collisions will occur for some values of input data (because the range of data you could put into the hash function is potentially infinite, but the output length is fixed).

For a secure hash function, the probability of this should be so small that, in practice, it is not possible to make a sufficient number of calculations to find it.

The significance of the Google/CWI team's results is in the fact that they were able to create a hash collision by finding a much more efficient method – 100,000 times more efficient in fact – than simply guessing every possible value of data.

It's the efficiency of this method that means SHA1 is now officially broken. (These results are outlined in more depth on [SHAttered.io](#), with an explanation of systems affected.)

## The SHA1 bounty

On 23rd February, a sharp-eyed Redditor on the [/r/bitcoin](#) page made a post pointing out that a long-standing bounty for discovering just such a SHA1 collision [has now been claimed](#).

The bounty – aimed to discover vulnerabilities in the algorithm – was originally announced by cryptography researcher Peter Todd in a [post on the Bitcoin Talk](#) forum in September 2013, but remained unclaimed until this week.

The challenge consisted of a script, written by Todd, which would allow anyone to move the bitcoins from the bounty address to an address of their choice if they could submit two messages which were not equal in value, but resulted in the same digest when hashed.

In addition to Todd, other contributors also donated to the bounty fund, raising a total of 2.5 bitcoins.

According to the researcher, the timing of the claim – slightly after publication of the collision attack – suggests that it was a third party who had read the Google team's research and made use of the results, rather than one of the original researchers, that took the reward.

Todd said:

*"If it was the authors themselves, we would have expected the bounty to be claimed just prior to the announcement being published. As it happened, that wasn't the case."*

## Ramifications for bitcoin




It's important to stress that the cryptography underpinning the bitcoin network, which makes use of the more secure SHA256 algorithm, is not directly affected by the discovery,

But, besides enriching the mystery bounty recipient, the SHA1 collision vulnerability does pose a concern for the bitcoin development community, since its Git version control system uses SHA1 to generate the hash digest for commits.

"The consequences aren't that we have to stop using Git immediately," Todd said, "but it will make it more important to review other people's work, because a third party could try to push a malicious commit in."

The vulnerability here is that an attacker could theoretically create two different versions of a code commit that would appear to be the same when hash values were compared – though for now, given the vast number of computations still needed to find a collision, it's highly unlikely that could happen.


As well as SHA1, Todd has placed similar bounties on the [RIPE MD160](#) and SHA256 hash functions – both of which are necessary for the integrity of the bitcoin standard, and would

	<b>Aims to Supercharge Smart Contracts</b>
	<b>'Top 10' Blockchains Report Concludes: Now is the Time to Pivot</b>
	<b>Do You Believe in Blockchain Magic?</b>

### INDUSTRY PRESS RELEASES

Feb 23   14:20	<b>Press Release: BTC.com Mining Pool Announces New Settlement Mode Increasing Miners Revenue</b>
Feb 22   22:33	<b>Press Release: Blockchain Intelligence Group ("BIG") Launches QLU Version Codename Deep Cove</b>
Feb 17   14:49	<b>Press Release: CoinVert is becoming the preferred platform of instantly exchanging cryptocurrencies by offering the best rates in the market</b>
Feb 16   18:27	<b>Press Release: Active Year Ahead for Blockchain Solutions in Financial Services, says Corporate Insight</b>

[VIEW MORE](#)
[SUBMIT RELEASE](#)

 Got a news tip or guest feature?

### DON'T MISS A SINGLE STORY

Subscribe to our free newsletter and follow us

[SUBSCRIBE](#)

therefore be calamitous for the network if compromised.

Todd concluded:

"If you claim that bounty, you better go spend your bitcoins pretty quick."

Binary code image via Shutterstock

bug bounty cryptography hash functions Peter Todd SHA1



PREVIOUS ARTICLE



After New Highs, Bitcoin Price Faces Uncertain Path Ahead

NEXT ARTICLE

You are reading the most recent article in this section.

Don't miss a single story

Subscribe to our free newsletter and follow us

Email Address

SUBSCRIBE

SPONSORED FINANCIAL CONTENT

dianomi

A massive stock market rally is at our doorsteps, according to ...  
Banyan Hill

Before Applying For A Credit Card, Check If You Pre-Qualify  
Citi

Principle #2: Cash Isn't Always King  
J.P. Morgan Funds

Donald Trump's latest order could save a 100% legal tax haven.  
Money Map Press

Beginners Guide to Trading Options Shows How To Make \$59,590  
Profits Run

Motley Fool issues buy alert on this "Millionaire-Maker" stock  
The Motley Fool

Ron Paul: "Buying Gold Will Not Be Enough -- Here's Next Step To Take"  
Stansberry Research

Top Bank Announces 1% Money Market w/ \$10K Deposit  
smartasset

RELATED STORIES

ANNOUNCEMENT

INSURANCE

Feb 21, 2017 at 14:40 | CoinDesk

CoinDesk Research Releases 'Blockchains for Insurance' Report

CoinDesk Research has released its new 44-page research report on the intersection between blockchain tech and the insurance industry.

FEATURE

Feb 19, 2017 at 12:35 | Corin Falfe

Bitcoin Hash Functions Explained

Everything you always wanted to know about bitcoin hashing, but were afraid to ask.

Nov 14, 2016 at 13:38 | Michael del Castillo



FEATURE

## Zcash and the Art of Security Theater

As bitcoin core developer Peter Todd published his role in helping create the Zcash cryptocurrency doubt is cast on the system's "trustless setup."



NEWS

Apr 21, 2016 at 19:11 | Pete Rizzo

## MIT Responds to Bitcoin Developer Concerns Over 'ChainAnchor'

A blockchain project being developed by MIT researchers gained new attention this week following criticism of its alleged design elements.

0 Comments CoinDesk

1 Login ▾

♥ Recommend  Share

Sort by Best ▾



Start the discussion...

Be the first to comment.

### ALSO ON COINDESK

#### Blockchain Startup Storj Targets Enterprise Cloud With \$3 Million Raise

1 comment • 2 days ago\*

Adeniyi Abiodun — Bravo

#### Danish Police Claim Breakthrough in Bitcoin Tracking

10 comments • 3 days ago\*

Jean-Mouloud — Can they use it to track our coins from MtGox so we can finally receive our due?

#### Bitcoin Price Surges to Within \$30 of All-Time High

27 comments • 2 days ago\*

Sadhaka Padma — Bitcoin is going to rise if ETF go, or not go.. FIAT global ponzi scheme is collapsing..

#### Bitcoin Price Sets New All-Time High

26 comments • 2 days ago\*

Ixion — I think it might break downward a bit in the coming month. We might see 2k closer to the end of the year.

 Subscribe  Add Disqus to your site Add Disqus Add  Privacy

DISQUS