Ethereum Creator Vitalik Buterin Explores Zk-STARKs In New Blog Post

Adam Reese
November 11, 2017 2:23 AM

The creator of Ethereum has written a blog post that contrasts zk-SNARKs and zk-STARKs. In it, he begins to explore the features that may make zk-STARKs an attractive solution to various problems facing the blockchain platform, as well as potential future problems.

On November 9, Ethereum creator Vitalik Buterin published a blog post exploring the class of technology known as zero-knowledge Succinct Transparent ARguments of Knowledge (zk-STARKs) and how they differ from the related and better-known mechanisms that fit under the gloss of zero-knowledge Succinct Non-interactive ARguments of Knowledge (zk-SNARKs).

The concept for zk-SNARKs (which predates Ethereum, but in the Ethereum context could be used to verify transactions) caught the attention of several of that blockchain's developers as a result of its anonymity-enabling properties.

While currently the sending address, receiving address, and the amount of

Ether involved in every Ethereum transaction is a matter of public record, zk-SNARKs would effectively mask these three data points, potentially making the platform more attractive to privacy-focused users.

Among the features that enable greater anonymity is the use of a non-zero "random secret number." The prover of a transaction multiplies this number by the product of two mathematical functions, then sends the verifier the resulting value as well as the value of the random secret number. With this information, the recipient node can verify a transaction while knowing almost nothing about it.

As the ability to verify transactions faster has become a more central concern for Ethereum, several of the blockchain's developers have started looking at zk-SNARKs as a means to boost scalability. In addition to their potential to enhance privacy, zk-SNARKs offer the benefit of reducing transaction verification time relative to the capacity of the current protocol.

Zk-STARKs share this feature with their more famous SNARK "cousins," but according to Buterin, also address several shortcomings, including their "reliance on a 'trusted setup.'" Additionally, he claims that the technology is theoretically "secure even against attackers with quantum computers."

While he estimates zk-STARKs' proof sizes to be "a few hundred kilobytes" relative to zk-SNARKs' 288 bytes, he argues that the tradeoff may be worthwhile "in the context of public blockchain applications where the need for trust minimization is high," and most certainly will be "if elliptic curves break or quantum computers *do* come around."

According to a PowerPoint document by computer science professor Eli Ben-Sasson, who Buterin thanks by name in his zk-STARKs blog post, a "[computational integrity and privacy] system is *transparent* if setup and all verifier queries are public random coins." Unlike this technology, zk-SNARKS require a "*non-transparent* setup phase."

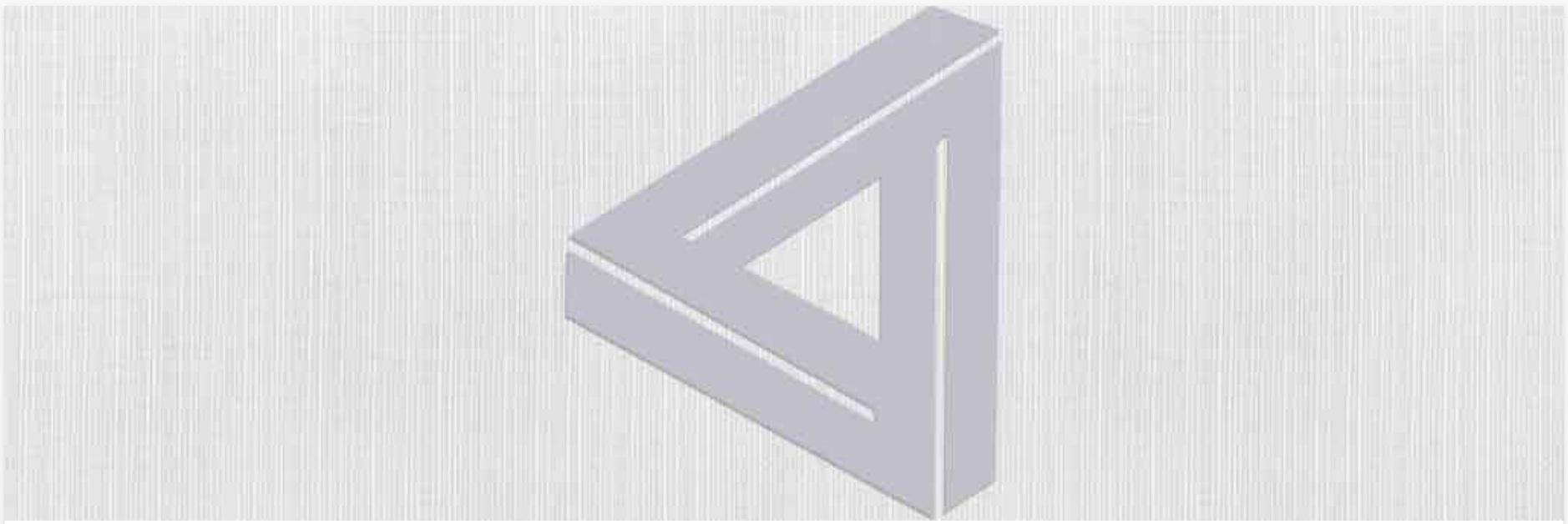
For further details, be sure to visit Buterin's blog post, here.

ADAM REESE

Adam Reese is a Los Angeles-based writer interested in technology, domestic and international politics, social issues, infrastructure and the arts. Adam is a full-time staff writer for ETHNews and holds value in Ether.

ETHNews is commited to its Editorial Policy

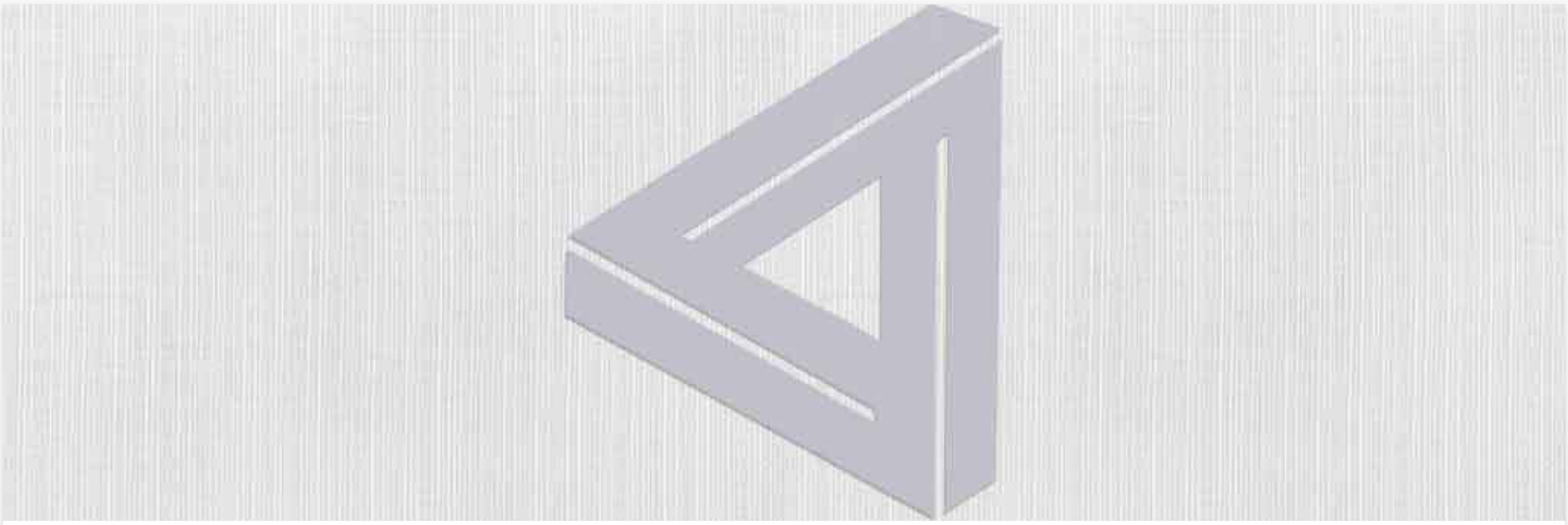
Like what you read? Follow us on Twitter @ETHNews_ to receive the latest Vitalik Buterin, Ethereum or other Ethereum ecosystem news.



LAW AND LEGISLATION

Chainalysis Inks Government Contracts Worth Over $700K

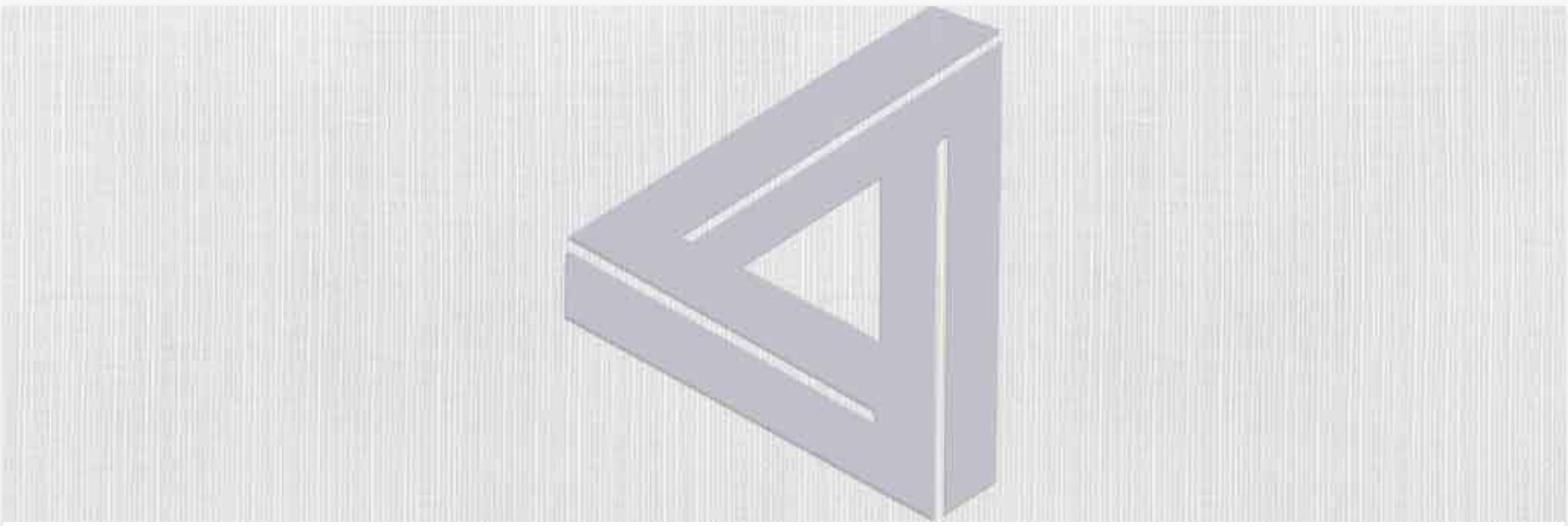
Matthew De Silva
Nov 10th, 2017



ECOSYSTEM

New Record: Over 100K Ethereum Addresses Registered On November 9

Adam Reese
Nov 10th, 2017



TECHNOLOGY

Blockchain Projects On GitHub Growing By About 100 Percent Annually, Suggests Report

Adam Reese
Nov 10th, 2017

Share

Facebook Twitter Reddit LinkedIn

CANCEL