

Swirling liquids work similarly to bitcoin

April 23 2018



Credit: CC0 Public Domain

Fluid dynamics is not something that typically comes to mind when thinking about bitcoin. But for one Stanford physicist, the connection is as simple as stirring your coffee.

In a study published April 23 in *Proceedings of the National Academy of Sciences*, Stanford applied physics doctoral student William Gilpin

described how swirling liquids, such as coffee, follow the same principles as transactions with cryptocurrencies such as bitcoin. This parallel between the mathematical functions governing cryptocurrencies and natural, physical processes may help in developing more advanced digital security and in understanding [physical processes](#) in nature.

"Having an actual physical model and showing that this is a naturally occurring process might open up new ways to think about those functions," Gilpin said.

Tangible transformations

Cryptocurrencies like bitcoin work in mysterious ways on purpose. As a virtual currency, it isn't protected or controlled by any central group. Instead, cryptocurrencies exchange and secure information through a mathematical function called a cryptographic hash—a modern workhorse for cybersecurity. These functions mathematically transform digital information into a unique output that disguises the input.

Hash functions are deliberately designed to be complex, but they also remain consistent so that the same input always produces the same output. However, two similar inputs will likely produce very different outputs. These functions make it easy for computers to track cryptocurrencies but hard for hackers to do the same.

As a physicist, Gilpin said he saw similarities between the way [hash functions](#) work and the physical laws involved with stirring a liquid. "I figured there's probably some analogy there that was worth looking into," he said. And, with a few weeks free during a winter break he decided to explore his idea.

Gilpin focused on a principle called chaotic mixing, which describes the action of mixing a fluid. Imagine stirring coffee creamer into a mug of

black coffee and watching the creamer separate into a swirling pattern. If the creamer were stirred precisely the same way in the future, the same pattern would result. But even the smallest change in the location of the spoon or the speed of the stir results in a very different pattern. In other words, each initial stir produces a unique swirl signature.

Additionally, just looking at the resulting pattern of the creamer in the coffee doesn't reveal anything about the original action—where the spoon was, how fast it moved, or how many circles—similar to the way a hash function transforms information so that the input is impossible to identify.

Gilpin decided to put the chaotic-mixing-of-fluids example to the test as a hash function. He found that the equations involved in mixing a fluid fit the requirements for hash functions almost perfectly. "I wasn't expecting it to perform that well," he said. "When it looked like it satisfied every property of a hash function I started getting really excited. It suggests that there's something more fundamental going on with how chaotic math is acting."

Outside the box

Modern hash functions are an ongoing area of research, as cryptocurrencies and similar applications such as digital signatures are becoming increasingly common for credit card transactions and legal documents. Gilpin suspects the parallel between the fields of computer science and applied physics could help in creating even more secure ways of protecting [digital information](#).

This connection can also help validate precise procedures, such as those used in drug development, said Gilpin. Certain drug development methods require injecting various fluids at specific points in time, similar to the way a hash [function](#) performs a precise order of equations.

"If you don't form the correct arrangement when you're done, then you know that one of your processes didn't go right," he said. "The chaotic property ensures that you're not going to accidentally get a final product that looks correct."

The discovery also suggests that cryptographic, presumably human-devised computations are not unique to the digital realm. "Something as ordinary as a fluid is still performing computations," said Gilpin. "It's not something only humans tell computers to do. It's something that nature does and it shows up in the structure of how things form."

Gilpin isn't a computer scientist or drug developer himself. When he's not connecting the digital and physical fields, he studies the way fluids work in nature with Manu Prakash, an assistant professor of bioengineering. So for him, "the idea that we can start to use some of these ideas from computer science is pretty exciting."

More information: Cryptographic hashing using chaotic hydrodynamics, *Proceedings of the National Academy of Sciences* (2018). www.pnas.org/cgi/doi/10.1073/pnas.1721852115

Provided by Stanford University

Citation: Swirling liquids work similarly to bitcoin (2018, April 23) retrieved 21 September 2024 from <https://phys.org/news/2018-04-swirling-liquids-similarly-bitcoin.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.