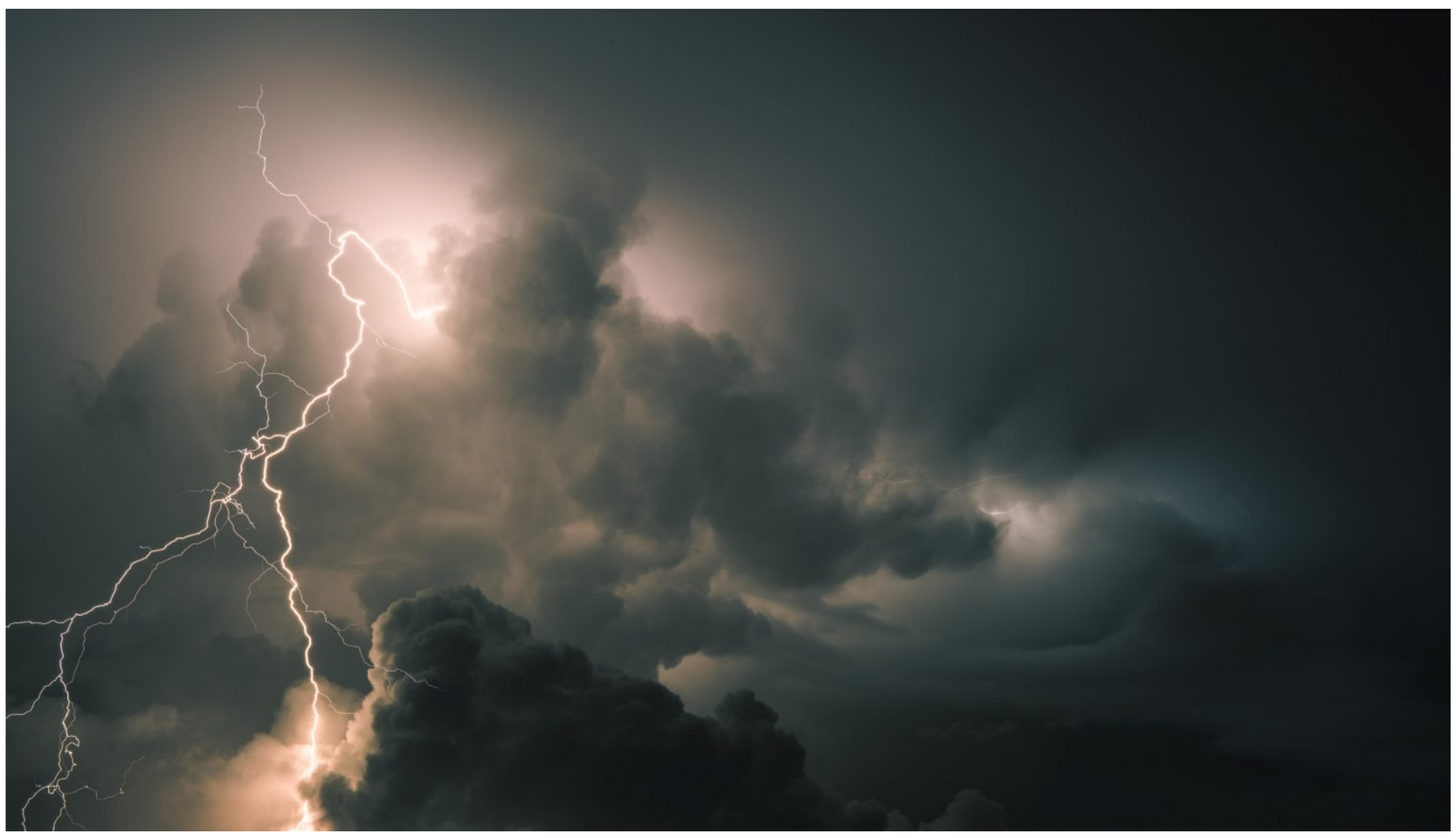
Faster Than Lightning? 'Sprite' Paper Envisions New Bitcoin Payments

Corin Faife (@corintxt) | Published on February 23, 2017 at 13:00 GMT

NEWS



Announced in early 2015, the Lightning Network, has been heralded as a promising solution to bitcoin's scaling challenges – one that, over the past year, has been inching closer to launch.

However, a new paper has laid out the framework for another payment system that researchers claim would be even faster.

Payment channels such as those proposed by the Lightning Network are one strand of the debate over scaling bitcoin which, although it often takes the form of arguments over block size, is ultimately about the volume of transactions the network can handle in a given length of time.

Larger block size is one way to improve transaction volume, but another strategy is to conduct payments 'off-chain', that is, in private payment channels between two or more parties where only the final balance is broadcast back to the main blockchain.

The authors of the new paper, titled "Sprites: Payment Channels that Go Faster than Lightning", claim that the Lightning Network's design is "more complicated than necessary" and assert that Sprite channels can reduce the maximum transaction time taken when each link in the transaction path suffers from a worst-case delay.

Stop and go

The idea of designing for worst-case scenarios is key to the Sprite proposal, which comes into its own in conditions such as disputes between parties in a payment channel.

Andrew Miller, assistant professor at the University of Illinois at Urbana-Champaign and co-author of the paper, said:

> *"In the case of a dispute ... the amount of time you might have to wait before getting the money back is determined by a timelock. In Lightning and Raiden, that timelock is longer the longer your payment path is. We've found a way of doing chained payments across multiple channels in a way that means the timelock is the same length regardless of how long the path is."*

Since the Lightning Network explicitly aims to facilitate cross-channel payments between parties who don't have a direct channel set up between them, a strategy to mitigate these kind of delays could be a significant advantage.

Extract from the paper: *"The worst-case delay scenario, in Lightning (left) and in Sprite (right). The two parties shown are "petty," dropping off-chain messages (red) after the initial open, and sending on-chain transactions (blue) only at the last minute. Disputes in Lightning may cascade, whereas in Sprite they are handled simultaneously."*

Soft fork barrier

However, for the time being, the mechanism needed to implement the Sprite micropayment channels makes use of functions that cannot currently be executed in bitcoin script (but could be run on the ethereum blockchain).

That means that implementing the system on the bitcoin network would require a soft fork to add new codes to the script, just as other proposals such as SegWit would do.

"It's straightforward to imagine how a soft fork to support this behavior would go, but at the moment that's not a soft fork that's been proposed yet," Miller said.

Still, with the paper now released, he did point out the possibility of other researchers finding a way to implement the Sprites system without requiring an extension to the bitcoin script.

Meanwhile, Miller confirmed that the authors of the paper are already in contact with the Lightning team, who have been providing feedback and analysis of the proposal.

At the same time, they have hopes that the Raiden network (the ethereum equivalent of Lightning) will be able to incorporate the Sprite technique in the near future.

Patrick McCorry, co-author of the Sprites paper and cryptocurrency researcher at Newcastle University, said:

> *"I'd be surprised if Raiden didn't implement this proposal: they won't have to deal with backwards compatibility issues [compared to bitcoin], so it's more likely they'll be able to do it because there's no soft fork requirement."*

In a final comment, Miller voiced the opinion that developing solutions for bitcoin first and then porting out to other crytocurrencies could hinder progress, since researchers have to contend with the quirks of bitcoin code.

"Our recommendation is that people try to express new ideas in either simple abstractions like pseudo code, or in ethereum because it's an easier example of what's possible, and then do the backward compatibility to fit with bitcoin today," he said, adding:

> *"If payment channels were invented for ethereum first, I think they would have immediately seen [our] way of doing it."*

Correction: *An early version of this article misstated when the Lightning project was announced.*

New Ethereum Proposal Aims to Supercharge Smart Contracts

'Top 10' Blockchains Report Concludes: Now is the Time to Pivot

INDUSTRY PRESS RELEASES

Feb 23 | 14:20 **Press Release: BTC.com Mining Pool Announces New Settlement Mode Increasing Miners Revenue**

Feb 22 | 22:33 **Press Release: Blockchain Intelligence Group ("BIG") Launches QLUE Version Codename Deep Cove**

Feb 17 | 14:49 **Press Release: CoinVert is becoming the preferred platform of instantly exchanging cryptocurrencies by offering the best rates in the market**

Feb 16 | 18:27 **Press Release: Active Year Ahead for Blockchain Solutions in Financial Services, says Corporate Insight**

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

Email Address SUBSCRIBE

Lightning image *via Shutterstock*

Academic Research | Lightning Network | payment channels | Scalability

PREVIOUS ARTICLE

Zcash Unveils Roadmap for 'Sapling' Blockchain Upgrade

NEXT ARTICLE

Blockchain Startup Storj Targets Enterprise Cloud With $3...

RELATED STORIES

NEWS

Feb 24, 2017 at 14:09 | Stan Higgins

Edinburgh University Partners with IOHK on Blockchain Research Hub

Scotland's University of Edinburgh is partnering with blockchain startup IOHK on a new research lab dedicated to the technology.

FEATURE

Feb 24, 2017 at 13:30 | Alyssa Hertig

New Ethereum Proposal Aims to Supercharge Smart Contracts

The creator of a new ethereum project says his ambitious off-chain networks, done right, could enable more complex applications of the technology.

FEATURE

Feb 8, 2017 at 10:44 | Alyssa Hertig

What Makes Bitcoin Great? One Scientist is On a Quest to Find Out

Academics still aren't sure why bitcoin is so robust, but one Cornell professor has made it her mission to find out.

NEWS

Feb 3, 2017 at 15:20 | Stan Higgins

Ethereum Payment Channels Could Enter Production in 2017

A project aiming to bring payment channels to ethereum is expected to become production-ready by the end of this year.