Ethereum Security Lead Martin Holst Swende Publishes Thoughts On EIP 210

By
JORDAN
DANIELL
WRITER
ETHNEWS.COM

NEWS • ECOSYSTEM
April 27, 2018 3:45 PM

The security specialist published his thoughts on one of Ethereum's currently prominent improvement proposals. His thoughts on the matter provide insight into some new features coming with the next hard fork, Constantinople.

Today, Ethereum security lead, Martin Swende, published the first entry of a series focusing on features that are being considered for the forthcoming Ethereum hard fork, Constantinople.

The series begins with a thorough analysis of EIP 210, which was authored by Vitalik Buterin and intended to address blockhash refactoring.

Blockhash refactoring allows newer blocks in a blockchain to link directly to much older ones, helping to increase connections between blocks. This helps to streamline light client proofs, allowing them to verify subchain "key blocks" instead of requiring light clients to verify an entire header chain.

0

Building from Buterin's EIP, Swende explains how a blockhash refactoring update as part of Constantinople would be implemented via a peculiar three-part process. Per Swende:

1.) A contract is placed at the address `0xff` at `CONSTANTINOPLE` fork block. This is the contract which does storing and lookups of hashes.

2.) Upon every block, before executing any transactions, the contract is invoked with a special `SUPERUSER` sender: `0xfffffffffffffffffffffffffffffffffffffffe`. This call contains a blockhash to store, for the *previous* block.

3.) After `256` blocks have passed in `CONSTANTINOPLE`, any invocations of `BLOCKHASH` are replaced with a `CALL` to `0xff`, where the `b` is used as `CALLDATA`, and the call is provided with `1M` gas. However, the actual `gasCost` is `800`, a raise from the previous `20`.

Designed to "both replace and expand" the way pre-Constantinople contracts obtain blockhashes, EIP 210 proposes to update the way EDCCs (or smart contracts) access hashes. Swende said that this "enables improving the light client protocol," and Buterin believes it will make "the protocol more 'pure.'"

As noted by Buterin's EIP, these blockchash updates will save Ethereum client implementations from having to explicitly "look into historical block hashes," allowing a significant portion of the "implied state" (data that is technically apart of the state but not a part of the state tree) to be removed.

As the second part of Metropolis after Byzantium, the Constantinople fork received "meta" EIP 1013, which, in addition to EIP 210, contains EIP 145. The latter addresses bitwise shifting instructions in the Ethereum Virtual Machine.

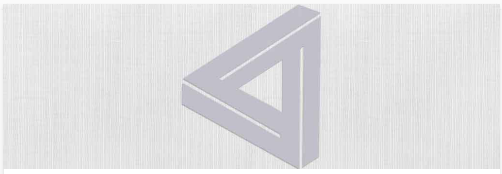
JORDAN DANIELL

Jordan Daniell is a full-time staff writer for ETHNews with a passionate interest in techno-social developments and cultural evolution. Jordan enjoys the outdoors, especially astronomy, and likes to play the bag pipes and explore southern California on foot in his spare time. Jordan lives in Los Angeles and holds value in Ether.

ETHNews is committed to its Editorial Policy

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

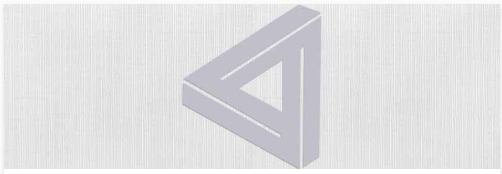
Ethereum | hard fork | Metropolis | Constantinople | Martin Swende | EIP 210 | blockhash refactoring | Vitalik Buterin



OPINION

Flexibility Is Strength: Evolving The 'Smart' Contract

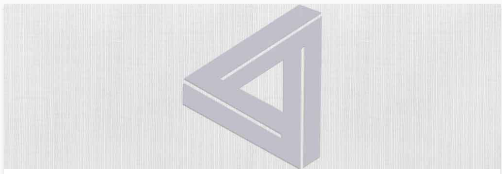
Lucinda Knapp
Apr 29th, 2018



BUSINESS AND FINANCE

Prominent Spanish Lender Issues Distributed Ledger

Jordan Daniell
Apr 26th, 2018



WALLETS AND EXCHANGES

Contract Exploits Spark ERC20 Token Suspensions

Jordan Daniell
Apr 25th, 2018