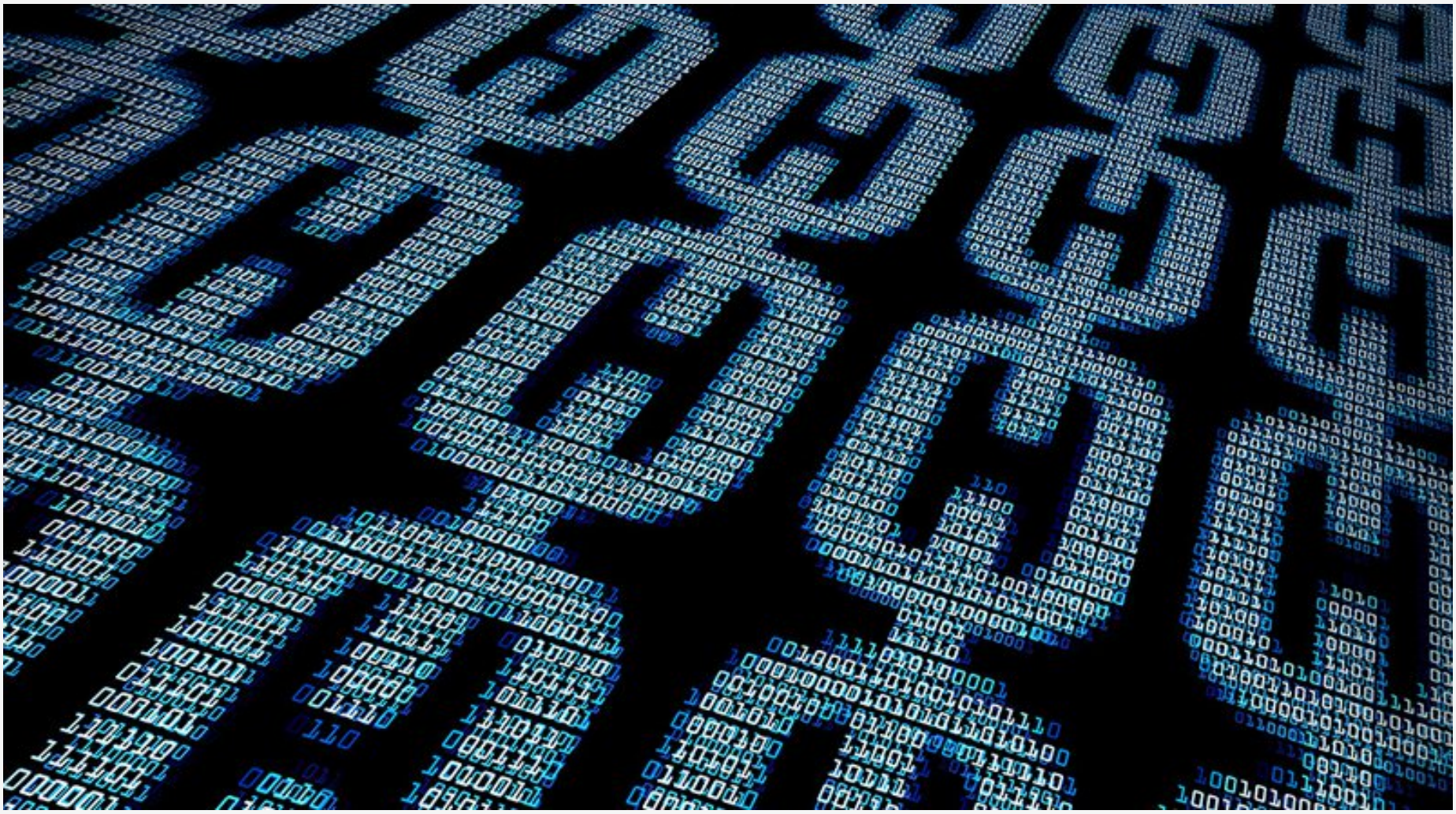
BASICS

Vitalik Buterin Reviews Chain Interoperability Schemes in New R3 Research Paper



In June *Bitcoin Magazine* reported that R3, the financial innovation consortium that includes many of the world's leading banks, commissioned Ethereum creator Vitalik Buterin to write a report on Ethereum design, upcoming technical developments and applications in private systems. R3 published both Buterin's

44-page report, which gives a detailed overview of Ethereum's overall architecture and technical design, current status and development roadmap; and an executive summary of Buterin's report, written by R3 former Senior Strategy Associate Kathleen Breitman and CTO Richard Gendal Brown, with a summary and R3's viewpoint.

Now, R3 has shared with *Distributed* a still unpublished R3 report written by Buterin in September, titled "Chain Interoperability." Buterin's new 24-page paper addresses the all-important interoperability issue with a thorough review of interoperability schemes that have been proposed and, in some cases, partly implemented. Chain interoperability is still a mostly theoretical effort since, as Buterin notes, "a live example of successful chain interoperability requires not one but two already existing, stable and sufficiently powerful blockchains to build off of." However, this is slowly starting to change as more distributed ledgers achieve critical power and stability, and interoperability can be expected to become a key requirement for new blockchains.

According to Buterin, the concept of "one blockchain to rule them all" — a unique blockchain carrying a unique digital currency and used for all distributed-ledger applications — is obsolete. The future belongs, instead, to a network of interoperable blockchains, built on different distributed-ledger technologies and carrying different digital currencies, which can be federated to handle different aspects of distributed applications.

"One of the advantages of using platforms where cryptographic authentication is naturally baked into every single operation is that we can actually provide much tighter and more secure coupling between platforms than is possible with previously existing systems," notes Buterin. "Interoperable chains open up a

world where moving assets from one platform to another … becomes easy and even implementable by third parties without any additional effort required from the operators of the base blockchain protocols."

The Bitcoin Sidechains paper issued by Blockstream envisages an ecosystem of "sidechains" separate from the main Bitcoin blockchain but interoperable with it by means of two-way pegs, allowing for the transfer of assets between sidechains and the main blockchain. Though originally formulated assuming that the main blockchain is the Bitcoin blockchain, the concept of a sidechain can be generalized to sidechains pegged to other blockchains. In a sidechain, as defined by Buterin, "the functionality of a blockchain reading data from other blockchains is used to facilitate cross-chain asset portability." However, Buterin isn't too keen on the term "sidechain" because it implies a subservient relationship where a sidechain is subordinate to a master chain, which is usually assumed to be the Bitcoin blockchain.

In fact, though Ethereum is a peer blockchain fully independent of Bitcoin, it can be technically considered as a sidechain to Bitcoin thanks to BTCRelay, one of the first relays where one blockchain provides information to another. Using BTCRelay, a smart contract on Ethereum can read the Bitcoin blockchain, achieving one-way interoperability that allows users to pay for distributed Ethereum services and applications with bitcoin.

Natural use cases for relays include cross-chain oracles and atomic swaps, where an asset on one chain is exchanged for another asset on another chain. A first implementation of atomic swaps with BTCRelay and Ethereum is being developed by the Bitcoin–Token market project of the MakerDAO team. However, the Bitcoin protocol, without Ethereum-like smart contract capabilities, offers only limited relay capabilities.

Besides relays, other interoperability schemes analyzed by Buterin are centralized notary schemes and hash-locking schemes where the same condition triggers operations on two different blockchains. However, centralized notary schemes require trust, and hash-locking schemes are not flexible enough in some important cases.

Besides a review of the interoperability schemes proposed to date and a thorough discussion of their strengths and weaknesses, including security aspects, Buterin presents a gallery of use cases for chain interoperability. While the paper is mainly focused on public permissionless blockchains like Ethereum and Bitcoin, Buterin also addresses interoperability issues for permissioned blockchains and "Fedcoin" — digital currencies controlled by central banks.

Giulio Prisco

For *The Distributed Ledger*

LINKS FROM THIS ISSUE

Consortia Key To Blockchain's Success, Says Deloitte

Healthcare Rallies for Blockchains

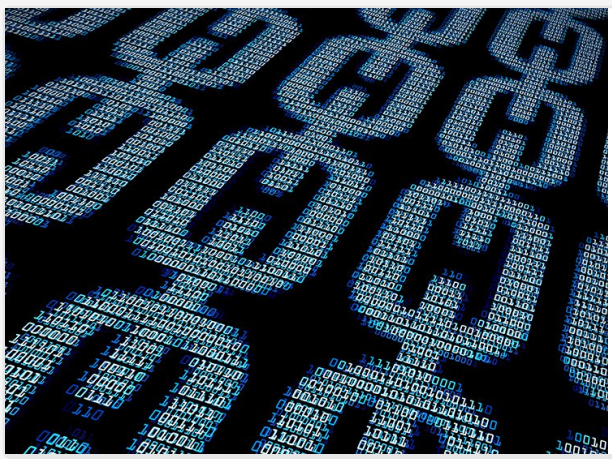
Blockchain: The Impact on the Real Estate Industry

How Blockchain Can Create the World's Biggest Supercomputer

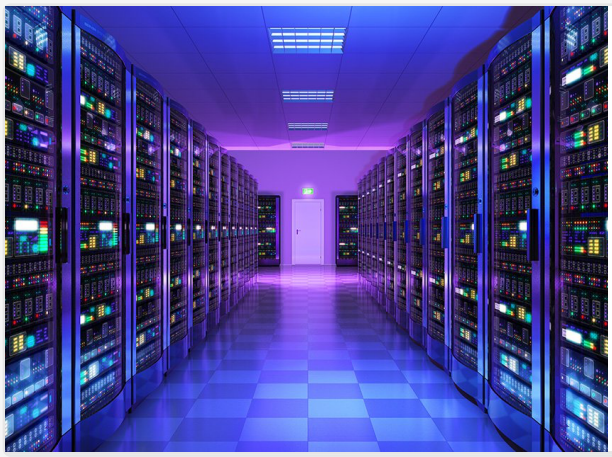
Private POCs, Permissioned Ledgers and Patents in Blockchain

The Truth About Blockchain

You might also Like



Vitalik Buterin Reviews Chain Interoperability Schemes in New R3 Research Paper



The Rise of the Enterprise Blockchain - How 2016 Signaled a Shift

Industry Updates: Ups and Downs for R3, A Blockchain Ecosystem for IBM, Hyperledger's Century, Quorum Quietly Opens Up