

ETHEREUM • EVENTS • FEATURES • TECHNOLOGY

Ethereum Economics Gets Spotlight in Vitalik Buterin EDCON Keynote

Alyssa Hertig (@AlyssaHertig) | Published on February 22, 2017 at 13:30 GMT

FEATURE

 220





 12







In a new speech this week, ethereum creator Vitalik Buterin gave a spotlight to the study of so-called 'cryptoeconomics', the union of cryptography and economics at the heart of public blockchain R&D.

At the ethereum developer conference EDCON 2017, held over two days in Paris, [Buterin](#) used his talk to provide a big picture overview why he considers the study of the subject core to his work on ethereum, the [second-largest public blockchain](#) by market capitalization.

Topics included how cryptographic puzzle pieces (such as proof-of-work, hashes and more complicated tools like zk-SNARKS) can be paired with forms of economic engineering including incentives and privileges.

While the subject may have seemed educational at first, the talk served to highlight the intellectual backdrop for some of ethereum's more necessary (and contested) ideas for how to improve its protocol.

For example, Buterin noted that the field is likely to inform its highly-anticipated proof-of-stake protocol and possibly lead to the building safer oracle systems that feed ethereum smart

DON'T MISS A SINGLE STORY

Subscribe to our free newsletter and follow us

Email Address

SUBSCRIBE



consensus
2017

Registration Is Open!

REGISTER NOW

CONSTRUCT 2017 VIDEO

SPONSORED FINANCIAL CONTENT



We could see the end of Social Security in 2017...

Banyan Hill



Before Applying For A Credit Card, Check If You Pre-Qualify Citi

dianomi™

FEATURES



Who Broke the SHA1 Algorithm (And What Does It Mean for Bitcoin)?



After New Highs, Bitcoin Price Faces Uncertain Path Ahead

contracts outside data.

Before diving in, however, Buterin began the talk with his own definition of the emerging concept.

He told the audience:

"Cryptoeconomics is about using a collection of cryptographic and economic building blocks in order to build systems that have some desirable informational security properties."

The importance of punishment

Buterin went on to explore how he is using cryptoeconomics to analyze where blockchain-based systems can go wrong, often referring to bitcoin as a key example and reference point.

Though the main reason that ethereum is pursuing proof-of-stake is because it could prove to be a greener, fairer alternative to bitcoin's proof-of-work consensus mechanism, Buterin went as far as to argue that proof-of-stake might also be a more secure, at least in some ways.

Proof-of-work, he argued, is vulnerable to something along the lines of a [P + epsilon attack](#), a way that miners can fool the system.

"This is one of the reasons why people want to push over to proof-of-stake," he said.

The comments come months after ethereum first revealed its plans to switch to a new consensus mechanism, and an outstanding question remains whether this experimental R&D can [keep pace](#) with user and developer expectations.

Despite the claims that proof-of-stake works better, it's worth noting that proof-of-stake hasn't been deployed on a large-scale network, and some technical experts still [doubt](#) that it will work.

Still, Buterin's point was that cryptoeconomics can be the frame of mind for finding new solutions.

Together cryptography and economics can be used to goad actors to act the right way, he said. One way to do that is to punish actors who are doing wrong — to push them to act in a way that benefits everyone. Usually that means taking away their money.

"Notice that this is a deviation from Satoshi and the holy book," he said.

Awaiting use cases

Buterin went on to explain how ethereum researchers are applying the subject to invent new properties that [Casper](#), its planned proof-of-stake algorithm, needs.

Borrowing from traditional distributed systems theory, he calls one feature that it needs "auditable safety," which is to be able to prove that one-third of the validators are faulty.

Once it proves that, the system can "kick them again and again," as Buterin put it, referring to the negative incentives a protocol can establish.

In other words, the protocol can snatch up a ration of the security deposits that the misbehaving actors originally stored on the network.

The second property that it needs is "plausible liveness," or confidence that the protocol won't stall or come to a stop, he posited. In terms of ethereum, that means that the network needs to continue moving so that transactions and smart contracts can continue to go through.

Beyond that, there are other areas he highlighted for further research.

Ultimately, he ended his talk with a list of open technical problems, including censorship resistance and scalable validation, both of which could emerge as obstacles on its planned proof-of-stake rollout.

Image via Pete Rizzo for CoinDesk

Cryptoeconomics

Cryptography

Ethereum

Proof-of-Stake



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 QBLUE 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

PREVIOUS ARTICLE



Bitcoin Advocacy Group Coin Center Collects \$1 Million in...

NEXT ARTICLE



Major Banks Use Blockchain Prototype for Live Oil Trade

Don't miss a single story

Subscribe to our free newsletter and follow us

Email Address

SUBSCRIBE

SPONSORED FINANCIAL CONTENT

dianomi

A massive stock market rally is at our doorsteps, according to ...
Banyan Hill

Before Applying For A Credit Card, Check If You Pre-Qualify
Citi

Principle #2: Cash Isn't Always King
J.P. Morgan Funds

Donald Trump's latest order could save a 100% legal tax haven.
Money Map Press

Beginners Guide to Trading Options Shows How To Make \$59,590
Profits Run

Motley Fool issues buy alert on this "Millionaire-Maker" stock
The Motley Fool

Ron Paul: "Buying Gold Will Not Be Enough -- Here's Next Step To Take"
Stansberry Research

Top Bank Announces 1% Money Market w/ \$10K Deposit
smartasset

RELATED STORIES

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.

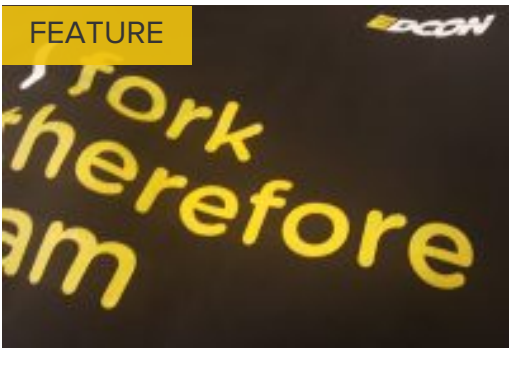
NEWS

Feb 21, 2017 at 15:30 | Michael del Castillo

New Ethereum Blockchain Consortium Could Run on Experimental Tech

Could the enterprise blockchain consortium use its own experimental technology to break away from the traditional top-down governance model?

FEATURE




Feb 20, 2017 at 16:10 | Alyssa Hertig

Rebranding The DAO: The Contentious Blockchain Concept is Back

It looks like we haven't seen the last of leaderless blockchain-based companies. Despite the spectacular demise of The DAO, developers are...

OPINION



Feb 20, 2017 at 12:36 | Olivier Rikken

3 Smart Contract Misconceptions

The smart contracts hype is creating new operational challenges, according to blockchain consultant Olivier Rikken.

