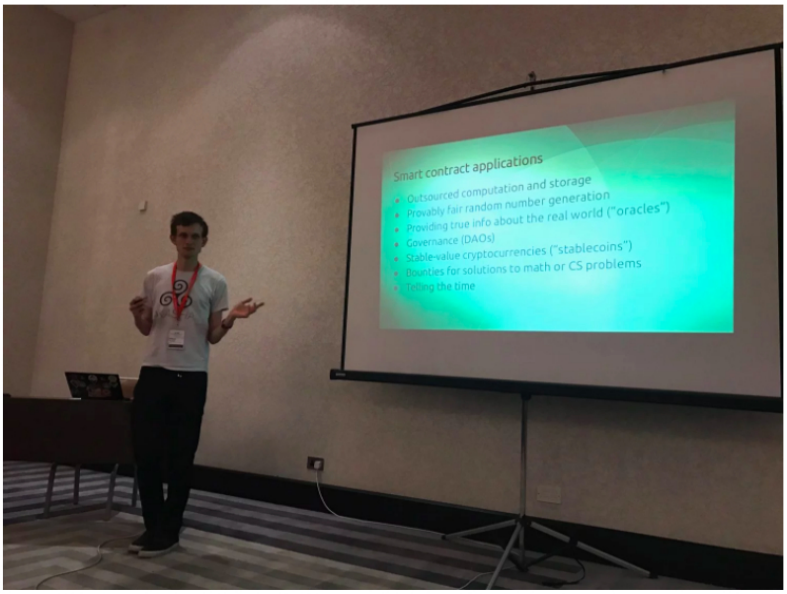
Vitalik Buterin Doubles Down on Ethereum Incentive Strategy

Amy Castor

Apr 10, 2017 at 12:00 UTC | Updated Apr 12, 2017 at 11:47 UTC

FEATURE



On the first day of the Financial Cryptography and Data Security conference in Malta, an academic with a cryptography career spanning three decades ended his keynote with a caution.

Incentives should be used as a last resort, said MIT professor of engineering Silvio Micali, pointing to bitcoin and its industrial mining pools as an example of what can go wrong when people find ways to make money that nobody could have predicted.

But not everyone shares that view on incentives.

Fast forward to the Workshop on Trusted Smart Contracts at the tail end of the conference, and another keynote address.

This time, the speaker is someone with no formal background in cryptography. Yet, his success in creating one of the world's largest blockchains, second only to bitcoin, is hard to ignore.

As he spoke to the audience, Vitalik Buterin, the creator of ethereum, argued that, not only do incentives play a key role in securing the blockchain, they are also the reason bitcoin soared to success when decades of previous attempts at peer-to-peer currency failed.

With that, he launched into a discussion on smart contracts and mechanism design that in some ways contrasted with, but in other ways built on, what Micali had said at the event.

Encouraging altruism

Simply put, mechanism design is a field at the crossroads of game theory and economics that looks at how incentives can be used to achieve favorable outcomes. In the blockchain world, that means getting people to play by the rules.

But, as anyone who has followed the discussions on consensus algorithms knows, this is an

But, as anyone who has followed the discussions on consensus algorithms knows, this is an incredibly difficult thing to do.

It also underscores the onerous job ethereum is up against as it designs a proof-of-stake system to replace the existing proof-of-work protocol that underlies its own blockchain.

So, it is no surprise Buterin is thinking so much about mechanism design and its impact on the stability of blockchains, and particularly on his smart contracts platform, ethereum.

One way to look at mechanism design, Buterin said, is through a framework of what he called 'crypto-economics', a term he credits his colleague Vlad Zamfir for coining. Buterin went on to explain how cryptography and economic incentives come together to play a critical role in keeping a blockchain secure.

Cryptography, he explained, allows users to prove properties of messages in the past. For example, digital signatures allow you to authorize messages, hash chains let you prove one message came before another and zero-knowledge proofs preserve privacy.

Buterin told attendees:

> *"You can use all of these [cryptographic] tools basically to prove things that happened in the past according to a certain set of rules."*

In contrast, economic incentives, he said, guarantee that the desired properties of a blockchain will continue into the future.

Further, the idea of combing cryptography with economic incentives was Satoshi Nakamoto's real stroke of genius, he said, and the reason why bitcoin has become so "large and successful".

Layers and gadgets

Buterin went on to describe the two "layers" of a blockchain: a bottom layer that consists of a consensus algorithm and an upper layer that includes things like smart contracts, gadgets and channels, like Lightning Network.

'Gadget' was another new term that Buterin defined as a "mechanism that gets used by other mechanisms". One example of a gadget would be an oracle, which a smart contract uses to access information from the outside world.

As the ethereum creator explained, there are two ways to look at the smart contract layer: one way is to assume the bottom consensus layer works fine and view both layers as separate; another way is to analyze attacks on both layers simultaneously.

And, it is entirely possible, Buterin said, for an attack in the smart contract layer to permeate down to the consensus layer.

The rest of Buterin's talk focused on the various attacks that can happen at the smart contracts layer and how incentives work to secure the blockchain.

A means to an end?

But while incentives, as Buterin argued, may have led to bitcoin's $20bn market cap, one has to wonder, if bitcoin's success is also leading it to a kind of slow demise.

Arguably, incentives in bitcoin have led to a non-stop arms race and turned the issue of scaling into a civil war that threatens to split the community.

It is clear Buterin and his team are working hard to get away from mining by planning a switch to proof of stake. But the question that comes to mind is, does proof of work present the danger – or does that threat lie more inherently in incentives, as Micali pointed to?

Because, if incentives are the problem, ethereum may be veering from one path, only to venture down the dark corridor of another.

And, if incentives are not the problem, than Algorand, the proof-of-stake system that Micali is designing to have no incentives (if he can pull it off), may stagnate and never get off the ground.

Chess game image via Shutterstock. Event image via Amy Castor for CoinDesk

Technology Ethereum Vitalik Buterin Events Algorand