Vitalik Buterin & Vlad Zamfir | The Ethereum Roadmap: Solving the Blockchain Scalability Problem

June 17, 2018

"We always overestimate the change that will occur in the next two years and underestimate the change that will occur in the next ten." — Bill Gates

INTRODUCTION

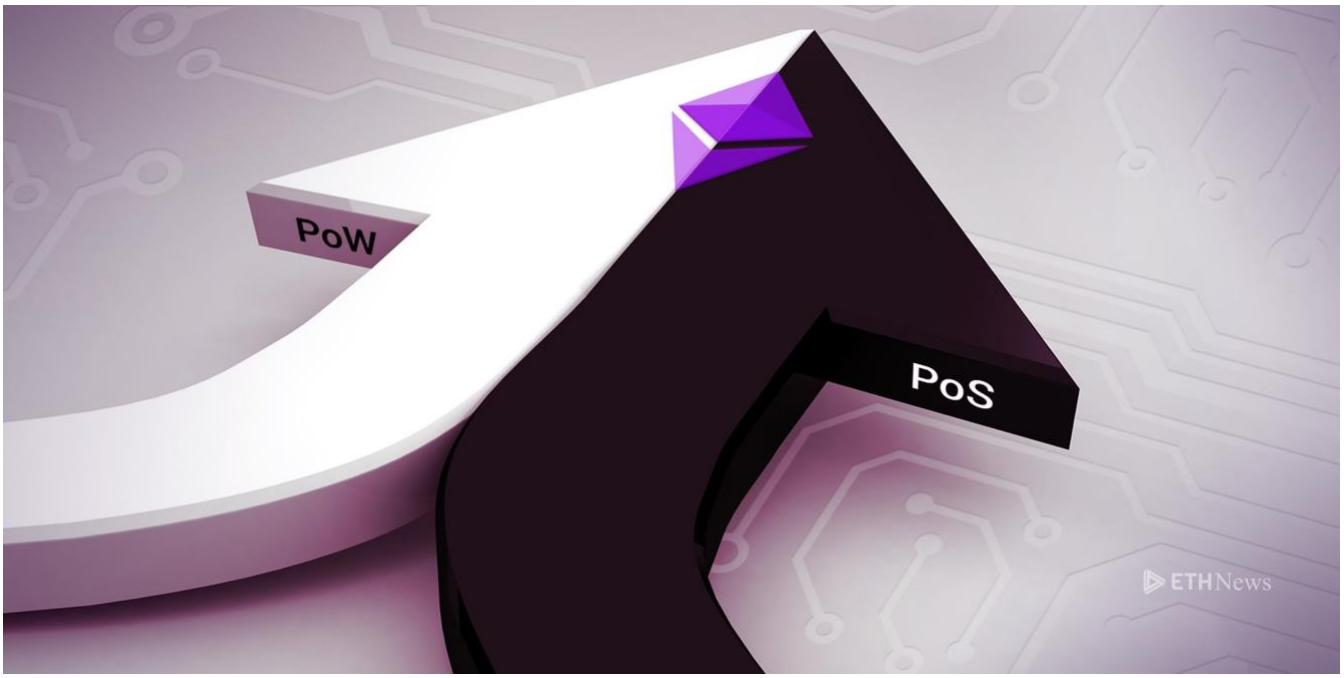
What's up everybody? Welcome this week's episode of Hidden Forces, with me Demetri Kofinas. My guests for this episode are Vitalik Buterin and Vlad Zamfir. Vitalik needs little introduction. He is the founder and inventor of Ethereum, the first cryptocurrency enabled, decentralized, Turing-complete machine ever created. Ethereum and Bitcoin combined make up nearly 60% of the entire market cap of all cryptocurrencies. Vlad is one of Ethereum's most prominent researchers and the leading figure in the development of Casper, a consensus mechanism that aims to enable the Ethereum platform to scale its existing architecture for use cases that reach beyond the network's current capacity like decentralized car sharing applications, stock markets, and online games. In this conversation, we focus our attention on the Ethereum roadmap, specifically Casper, Plasma, and the developer community's approach to sharding. I also get Vitalik and Vlad's reactions to the recent comments by SEC Director of Corporation Finance William Hinman, as well as their thoughts about governance models in open source, crypto economies. For more information about today's episode or if you want easy access to related programing in blockchain and cryptocurrencies, visit our website at HiddenForces.io and subscribe to our free email list. You can follow us on Twitter, Facebook, and Instagram at @hiddenforcespod for regular updates and audience feedback, including the latest information about futures episodes, topics, and guests. And now, let's get right to this week's conversation.

WHAT'S THE PROBLEM?

I've known about bitcoin since 2011 and began learning about the development ecosystem around blockchain around 2014/2015. I never found the offering compelling enough to get excited about, and my coverage of the technology has primarily been a consequence of my looking for alternative protocols. I have been frustrated by the lack of explanatory information that can help give me a clearer understanding of what Ethereum is, how it works, and what the prospects are for its application at scale. As I see it, there are two primary bottlenecks to scalability. The first is governance, and the second is architectural. I want to explore both in depth.

THE ROADMAP

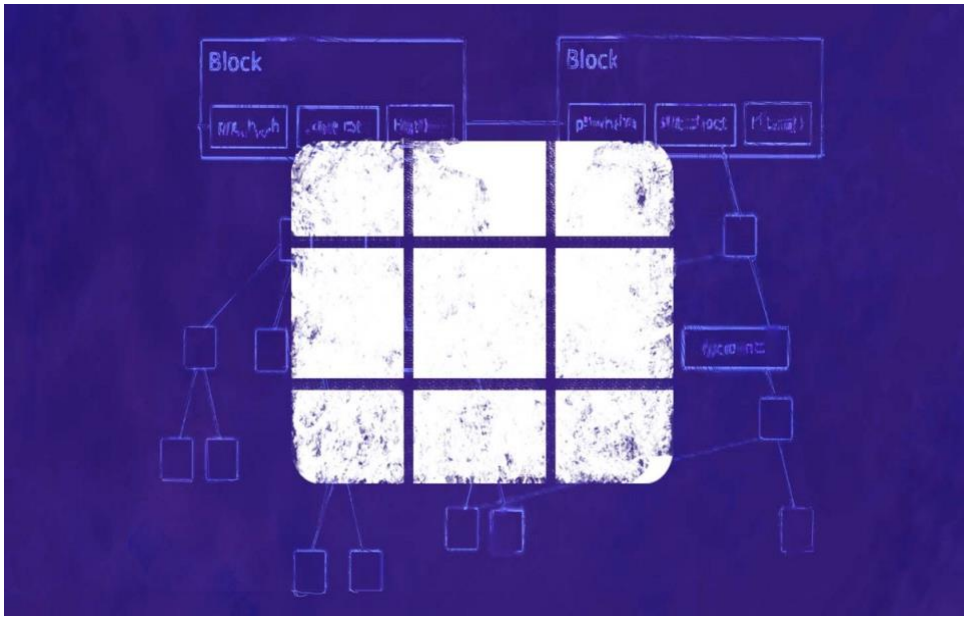
1. **Proof-of-Stake (PoS)** — Ethereum currently uses PoW in order secure the network and drive probabilistic consensus. What is your motivation for developing a PoS model for Ethereum? Is it driven mainly by the deficiencies in PoW (energy sucks & consolidation of hashing power via economies of scale)? How long have you been working on this? How does you staking solution differ from some of these competing systems like EoS (delegated proof of stake) or Hedera Hashgraph (proxy staking)?



   a. **Casper FFG (Friendly Finality Gadget)** — As I understand it, FFG is a compromise between a PoS system and a PoW system. Is this compromise a political one (i.e. appeasing the miners) or is it a technical one (test parameters of the new system without losing the safety of the old one). How does FFG work? How do you get consensus? When do you get consensus? What security guarantees do you have? Do you have a timeline for deployment?
   b. **Casper CBC (Correct by Construction)** — Let's do our best to explore the thinking behind this architecture. How far along is it? Let's start high-level and drill down as far as we can go. How do you manage timestamping? How quickly can you get consensus? What would the best-case scenario of a fully implemented PoS system like Casper look like for Ethereum? What are the most ambitious applications you believe can be built if Casper is implemented? Do you have a timeline for deployment?

***I've heard you reference game theory a bunch when describing the assumptions that are being made in the architecture for Casper. How can you get security proofs when you are relying on game theory? Is it satisfactory to build a system that rests on economic incentives in order to generate consensus?

2. **Database Sharding** — Is it possible to shard a database without achieving finality in each shard? If it is possible, how much more complicated is it? What are the biggest challenges facing the Ethereum developer community on this issue? How do you manage inter-shard communication?
3. **Plasma (State Channels)** — As I understand Plasma, it is an implementation of state channels. How does it work? What are the biggest challenges you are facing here? What are the differences between Plasma and Lightning Network? How do you implement state channels when smart contracts are concerned, and how much more complicated does this become? Does dispute resolution become a problem when you are using state channels where it would not be in cases where every transaction is happening/being verified on the main chain?



GOVERNANCE

Ethereum does what is known as "off-chain" governance, which differs markedly from EOS, which does something known as "on-chain." How does governance work for the Ethereum community?

4. **Benevolent Dictator** — How powerful is Vitalik? Does he have the role of the British monarch during the 19th century? The 20th? Is he just a figurehead? If we were to compare bitcoin to Ethereum, what would be a difference in governance that arises from the fact that Satoshi is unknow to the public whereas Vitalik is present?
5. **Developers** — Who are the key developers in this ecosystem? How powerful and organized is this community?

Miners — Who are the key miners in this ecosystem? How powerful and organized is this community? Let's take the example of Casper, which threatens to put the miners out of business. How do the various centers of power in this ecosystem come together in order to move the network forward? Are the miners in a position to just filibuster anything?

ALTERNATIVE LEDGERS

6. **EOS** — What are your thoughts on EOS? What are your biggest criticisms? What is the proper amount of centralization? Is 21 nodes not enough? Is 1000 too many? How can we come to a determination? Is this just a trial and error situation? What do you think about delegated proof-of-stake?
7. **Hedera Hashgraph** — What are your thoughts on Hedera Hashgraph? What do you think of their governance model? What do you think of their consensus protocol? What about their proxy staking?