Businesses will inevitably continue to explore opportunities to seek rent on top of Ethereum, which could yield in both positive and negative outcomes. Ethereum Serenity and the economics underlying its protocol opens the door to new FinTech opportunities which would grow as a market in tandem with the growth of the Ethereum ecosystem. Validating will be adopted into the “as-a-service” industry which would positively support maximizing the number of stakeholders participating in the network and enable non-technical holders to be more engaged in the network as a validator (i.e. higher degree of decentralization). However, businesses such as validating-as-a-service/staking-as-a-service (VaaS) pose new interesting dynamics and attack vectors. This topic is for awareness pertaining to certain economic-driven vulnerabilities, particularly involving VaaS and potential features that might be embedded on these platforms.

The Overpromise Attack

For holders who trust technology companies more than they trust themselves to custody and manage their Ether, VaaS would be a compelling opportunity for less technical holders (individuals or institutions) who want to earn a yield on their holdings. The VaaS industry could ultimately become a competitive industry driven by architectural commoditization (low barriers to entry due to limited upfront costs and few fixed costs). In this case, if transfer of funds from one VaaS to another becomes seamless, holders might seek the platform that would maximize their yield. This scenario could present a significantly cheaper method for maliciously attacking the network.

Suppose a VaaS business began marketing 15% or even 30% yields when realistically other validators offered 5%, boasting a ‘groundbreaking minimal cost architecture.’ That VaaS platform could gain traction across the industry fairly quickly. Without needing to purchase any Ether, and paying only the difference between the actual yield and the marketed yield, that VaaS business could custody enough Ether to control the network for a fraction of a cost it would take in the traditional method.

For example, assume the following variables:

- $5 million to build a VaaS system to production
- $5 million in marketing
- 20% marketed yield
- 5% actual yield
- Six months time to onboard enough ETH
- 20 million ETH at stake in the network
- 31% = minimal percent needed at stake to attack the network
- $240 ETH/USD price (representing current price at time of this writing)

Assuming 1:1 discouragement, the cost of successfully executing an Overpromise Attack on the network would be:

$5,000,000 + $5,000,000 + ((20% - 5%) / 2) * ((31% * 20,000,000) / 2)*$240 = $65.8 million

The cost of an attack the network was designed to withstand would equate to (31% * 20,000,000 * $240) or roughly $1.5 billion.

The Flash Crash Attack

Differentiation for VaaS might entail building out more robust functionality. This functionality could include proprietary levers or switches which lower risks and maximize profit. A feature that could mirror traditional trading platforms would be a ‘stop loss’ where a position would be immediately liquidated when a certain dollar amount or percent threshold below the current price is reached (e.g. a 10% stop loss on a $30 purchase would indicated automatic liquidation at $27).

Stop losses are viewed as the culprit of flash crashes because automated selling leads to steep declines, and steep declines lead to more automated selling. Flash crashes are not uncommon, even across broader markets. On May 6th, 2010, the S&P 500, Dow Jones Industrial Average and Nasdaq dropped by $1 trillion in a matter of 36 minutes. On June 21st, 2017, the price of ETH/USD briefly fell from $319 to 10 cents in about one second.

Price has a direct impact on validator yield. A lower ETH/Fiat price would lower the ratio of dollar-based rewards against fixed validator costs. At a certain price point, costs could exceed rewards forcing validators into a negative yield region. For VaaS providers, which are leveraging economies of scale to provide a decently competitive yield relative to the validators with a self-set up, reaching a price that result in negative yields would position the VaaS provider in an awkward situation. Does it (1) force its customers to pay the VaaS provider (due to negative yield), (2) eat its loses, or (3) form a policy to agree to pull their validating position when yields turn negative or near negative (a stop loss)? The first scenario is unlikely. Depending on the service provider, terms of the service would either implement two or three, with three being the most sustainable business model (what if yields turn negative for a significant amount of time?).

Reaching negative yields are difficult but not impossible. With 20 million total ETH at stake in the network, negative yields are not reached until about $60-80 ETH/USD range. However, suppose an ETH/Fiat flash crash occurred akin the event in

June 2017, and VaaS providers automatically force their clients out of their validating positions. Concurrently, this event could drive down the total Ether staked in the network significantly - flash crashing its network security. An adversary, which either forced the flash crash with a fat finger trade or not, would be able to subsequently accomplish a successful attack on the network with less Ether staked in the network by taking advantage of automated ‘stop loss’ VaaS positions.