



11 July 2023

Jessica Herron
Legislative Clerk
Subcommittee on Innovation, Data, and Commerce
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515-6115

Re: Ryan Wyatt's Responses to Additional Questions for the Record


Dear Ms. Herron:

I want to thank the Subcommittee for inviting me to appear before it on June 7th, 2023 to testify at the hearing entitled "Building Blockchains: Exploring Web3 and Other Applications for Distributed Ledger Technologies."

Pursuant to the Rules of the Committee on Energy and Commerce, I am attaching my answers to additional questions for the record, in the required format.

Thank you again for your help, and please reach out with any questions.

Sincerely,

DocuSigned by:

6487AB5C1414466...
Ryan Wyatt
President
Polygon Labs

Mr. Ryan Wyatt

Attachment - Additional Questions for the Record

The Honorable Greg Pence

- 1. As the President of Polygon Labs, your company is used by Fortune 500 companies like Starbucks, Nike, and Reddit. Can you tell me how and when I can get paid for *my* data using blockchain solutions?**

Polygon Labs is a software development company that builds blockchain scaling networks and complementary infrastructure. Anyone and any company can build their own web applications on top of the Polygon software without involvement or assistance from Polygon Labs.

To that end, Starbucks, Nike and Reddit have all built their own, independent applications on top of one of the software protocols created by Polygon Labs. These types of blockchain-based applications allow users to reclaim control over their internet experience: data, content, and following. Users do not relinquish their personal data; instead, when the user wants to engage with the Internet, they connect their personal, self-hosted wallet to any application. These self-hosted wallets are pseudonymous – meaning that they are identified only by a string of letter and numbers – and do not necessarily contain any personal data, unless the user intentionally has included a type of digital asset (*e.g.*, non-fungible tokens (“NFTs”)) with such information or which represents such information.

Autonomy over data in itself is a benefit to the users, but it also produces additional benefits, including monetary compensation. Certain blockchain applications have already been developed to allow for users to determine whether they want to get paid for or otherwise use their data for their own monetary benefit. For example, an application called DIMO creates a marketplace for personal vehicle data by connecting drivers with developers and manufacturers.¹ Through DIMO, drivers can sell their vehicle’s data for either payments or tailored insights into the health of their vehicle. Another example is Hivemapper, a blockchain-based application that allows for decentralized GPS mapping services. Drivers contribute dashcam footage to the Hivemapper Network and receive compensation in return,² giving users access to the most up-to-date GPS maps - especially around rural areas - while allowing drivers to earn passive income.

¹ <https://dimo.zone/>

² <https://hivemapper.com/>

Mr. Ryan Wyatt

2. Additionally, data breaches that leak personally identifiable information (PII) take place on both traditional platforms and blockchain platforms. What more is needed to limit hackers and bad actors from accessing information on blockchain and distributed ledger technologies (DLT) and Web3 platforms?

We agree that there have been data breaches that leak PII in web2 Internet applications; in these situations, centralized entities own user data. On the other hand, we are not aware of specific “data breaches that leak PII” in applications built on blockchain networks – this is because for truly web3 native applications built on top of a decentralized, permissionless blockchain network, centralized entities do not hold or maintain user data. Rather, to interact with blockchain-based applications, users must connect their self-hosted wallet, instead of providing personal data as is common for web2 applications. These wallets do not contain PII such as name, address, email, etc. and are identifiable only by a string of letters and numbers.

Although there have been hacks of blockchain-based software protocols, they typically take the form of the hacker “stealing” crypto-graphic assets, as highlighted in the Chainalysis 2023 Crypto Crime Report.³ For example, scams involve the user being tricked into surrendering their PII and function in the same way within blockchain networks as in traditional systems, meaning bad actors cannot “access” PII directly. Other types of cryptoasset “stealing” stems from vulnerabilities in the code and not the users personally.

To mitigate such risk, a number of practices can be implemented. For example, robust auditing procedures could be used to ensure the protocol (i) does not have loopholes or other weaknesses before launching publicly and opening the door for exploits as well as (ii) continues to function as expected once deployed, allowing for developers to find and address problems quickly and transparently. Other practices include “gated” or “guarded” launches, bug bounty programs, monitoring tools, among others depending on the stage of protocol development.

We are happy to provide more information upon request on any of the above answers.

³ <https://go.chainalysis.com/2023-crypto-crime-report.html>