Paradigm

October 19, 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: Justin Slaughter's Reponses to Additional Questions for the Record

Dear Ms. Herron,

I'd like to thank the Subcommittee for inviting me to appear before it on September 20, 2023 to testify at the hearing entitled "Mapping America's Supply Chains: Solutions to Unleash Innovation, Boost Economic Resilience, and Beat China."

Per the request of the Subcommittee and in compliance with the Rules of the Committee on Energy and Commerce, I am attaching my responses to the additional questions for the record.

Thank you again for your help, and please let me know if you have any questions.

Sincerely,

DocuSigned by:
Justin Slaughter
FA13BF791BC7429...

Justin Slaughter
Policy Director, Paradigm

Attachment—Additional Questions for the Record

The Honorable Russ Fulcher

In the past, large American car manufacturers could take dirt in one end, and on the other end would roll out a completed car. Today's products are no longer completed by one manufacturer at one plant but are instead manufactured across a complicated array of suppliers often around the globe. Each stop along a supply chain is a silo of information which may or may not be effectively passed on to the next step in a process.

1. **Mr. Slaughter, how can blockchains be used to ensure increased interoperability through a supply chain?**

In a world where many companies work across city, state, and even international lines to produce one car, one computer, or one appliance, there is a greater need than ever for all the constituent participants in production to be able to track the provenance and validity of both components and production processes. This is where blockchains can provide utility in supply chains – they can provide this provenance assurance, as well as data sharing interoperability between varied manufacturing companies and participants. But it must be noted that the benefits of blockchains do not only apply to the manufacturer: they also accrue to ordinary consumers. While an end stage manufacturer might be able to keep track of supply chain information in a private database, there is no straightforward way for the other members of supply production to confirm the validity of materials, and also no way for consumers to confirm that their goods were properly sourced and ethically or correctly produced at each step. Public blockchains solve that issue by making all parts of the supply chain accessible to everyone in the network, even consumers.

Supply chains can often be thought of as a giant game of telephone – the more steps in a process, the more likely noise or distortions enter. One way to ensure our supply chains are effectively mapped and understood is to have clean, clear data about the state of our supply chains.

2. **Mr. Slaughter, how can blockchains ensure that information is effectively transmitted between nodes in a supply chain?**

As I mentioned in my testimony, "blockchains are a special type of shared database that enable the creation of unique, non-duplicable digital items. Blockchains do this by maintaining records of digital information ownership and replicating those records across multiple computers called nodes. Fixed rules, known as protocols, define activity, incentives, and updates—with the nodes on the network all having to agree on each addition of information to this shared database. Technological primitives, like cryptography and peer-to-peer messaging, ensure that the entire system functions according to those protocols.

These webs of nodes, protocols, and primitives give rise to systems that can be used for a variety of functions—from the creation of truly digital, peer-to-peer money to the formation of new online communities with their own embedded governance mechanisms. Whereas the laws of physics define scarcity in the world of atoms, the world of bits was previously unconstrained, making it nearly impossible to *trustlessly* enforce digital property rights. While cheap reproduction and distribution is helpful for certain uses, like sharing photographs and written documents, unique items require mechanisms that limit supply. With crypto, it's now possible to own and control scarce digital objects and track their provenance across time and space without the need for a centralized entity. This includes money, art, and digital representations of physical items."

There are numerous mechanisms that help ensure information is shared across a blockchain, from consensus mechanisms to tokens and even the size of the network. Generally speaking, the larger a blockchain network and greater the number of nodes, the more resilient and accurate a network. The difficulty of a malicious actor's ability to compromise a blockchain network and its data increases proportionately as a network scales and decentralizes – in other words, the larger the network, the more entities validating the information on it, and the harder it is for that information to be falsified.

In the digital space, blockchains make a lot of sense. A digital item whose ownership is tracked digitally using a blockchain. However, the intersection of the real world and a digital system creates new avenues for disconnect. While blockchains are a trusted ledger, they're only as good as the data humans give them. People could always lie.

And given Smart Contracts can automatically execute on transactions, deliveries are being done with the banks accounts of buyers and sellers getting hit.

3. **Mr. Slaughter, what solutions have you seen to address the challenges of connecting real world assets to the blockchain? Is this something that would help or hinder security at America's ports?**

The world that we live in increasingly straddles the line between physical and digital, with the time we spend in digital interactions continuing to grow. There have been a number of recent announcements of major financial institutions experimenting with tokenizing real-world assets (i.e. allowing for their exchange) on blockchains. Citigroup recently announced a pilot with Maersk and a canal authority to expedite shipping processes via tokenized cash management and finance.

Fundamentally, any process with many different players and inputs, especially one that exists in a low-state of trust and in a quasi-public environment, is a potential use case for blockchains. Any system that involves scanning in deliveries at ports of entry and uploading that to a database, can be further enhanced by onboarding the different disparate scanning entities at each port of call into a shared blockchain database. Further, RFID chips embedded in goods, or attached to shipping containers, can add additional granularity and traceability within a supply chain, visible to all requisite parties participating in a distributed blockchain-based supply chain system. While I am not an expert on the port system, it would seem that a process that establishes the validity of different actions in a highly important area where you want to confirm consensus is what is desired, and that is what blockchains can provide.

Privacy has been a major focus of this committee. Last Congress we passed the American Data Privacy and Protection Act (ADPPA) out of committee and this Congress we've held six hearings which touched on the need for federal privacy standard. However, if data isn't secure, it can't be private.

4. **Mr. Slaughter, what concerns do you have that if supply chain data is put on chain it would no longer be private, or secure?**

The degree to which data on a blockchain is private depends ultimately on the specific blockchain in question. That said, it is possible to have information on a blockchain be as secure and private as exists in private databases, the latter being inherently susceptible to hacks and breaches like any other information system. This does not mean that companies must put all their most sensitive data on a blockchain, just as we do not expect companies to put all their most secure information in any one private database or system.

Additionally, data-minimizing cryptographic technologies such as Zero-Knowledge Proofs are increasingly being made of use. ZK-Proofs allow for the attestation to a certain query, and the querying party to be confident in the credibility of the response, without revealing the sensitive underlying data. An example would be a prospective buyer of alcohol using a ZK-Proof system to cryptographically attest to the store that they are, in fact, 21 years old (and the store having confidence in this attestation) – without revealing all of the sensitive personal information on their drivers' license (appearance, home address, license number) that they might otherwise not need or wish to reveal. ZK-Proof research is one of the most exciting and bleeding-edge corners of crypto development at the moment, with major US companies such as EY dedicating significant resources to its exploration.

Ultimately, I am confident that with good information security practices, increasingly robust cryptographically-supported data minimization techniques and a thoughtful decision making process for deciding which information to be put on chain, companies can ensure that supply chain data remains secure and private.

<u>The Honorable Jeff Duncan</u>

1. **In recent times, there have been highly publicized breaches within our mathematical encryption systems. These breaches have impacted well-known encryption methods such as AES, RSA, and even newer NIST Post-Quantum algorithms like SIKE and**

Crystals-Kiber. Considering these threats against our math-based encryption systems, what measures are we currently pursuing to investigate & adopt alternative approaches that guarantee security like quantum-secure, QuantaMorphic, physical-based data protection?

As I mentioned in my testimony, when it comes to cybersecurity, there has been a consistent advantage to the attacking side, as though we are in a soccer game where the score is 271 to 270. That said, this is an area where the only way forward is straight through: continued innovation and adoption of better information security practices. First, we need continued research and development into encryption so that America's encryption systems remain ahead of the curve. Additionally, there needs to be a layered approach to encryption such that there are redundancies in place to reduce the risk of a full breach. Relying on a single strong line of defense in encryption while allowing weak security practices is akin to putting an iron padlock on a cardboard box.

When it comes to cryptography, there has been an uptick in physical-based data protection in recent years, including the use of social key recovery, where a person can ask several friends to collectively control access to an account. If the user loses their password or it is compromised, access to the account can only be restored if a majority of the friends affirmatively approve granting access to it. The use of such social protection methods can add an additional layer of protective defense to traditional encryption systems.

2. **Winning the quantum race against Communist China is one of the greatest challenges of our time. Critical to winning this race is having a skilled American quantum workforce. Recently, the U.S. Department of Energy awarded a contract to Clemson University, a top R-1 national university, together with Winston-Salem State University, a respected HBCU to do just that. What can be done to build upon and replicate the Clemson-WSSU quantum workforce training model across the nation?**

As with so many aspects of emerging tech, there is no substitute for continued education and engagement. While I am not personally familiar with the Clemson-WSSU program, the rise of a host of programs at educational institutions across the country focused on emerging technologies like crypto, blockchain, AI, and quantum computing are a boon for both our economy and American national security interests. The best thing the government can do to build upon these programs is to increase its own focus on learning about emerging technologies across the executive and legislative branches. It is very hard for federal government workers to support higher education programs focused on new technologies if they themselves do not understand those new technologies.