March 1, 2022 • www.atllp.com

CRYPTO AND BLOCKCHAIN'S SURGING WAVE OF DATA LAWS (PART I OF IV)

Just as Web3 is a catch-all term for digital assets and infrastructure – as highlighted at last month's Cryptopia pop-up – crypto is a catch-all for digital currencies used as a medium of exchange over the internet. This exchange occurs through technology that permits transactions to be gathered into blocks of data (i.e., blockchain technology).

While crypto and blockchain technology have spurred seemingly limitless amounts of innovative data use – total transaction volume grew to $15.8 trillion in 2021, up 567% from 2020's totals – crypto crime is also way up. Illicit addresses received an estimated $14 billion over the same time period. (*See The 2022 Crypto Crime Report by Chainalysis*.)

Part of the problem is, unlike traditional technologies, blockchain is not maintained by a single individual or centralized entity– anyone can download a copy of it – leading to numerous data innovation, privacy and security challenges. As to the latter, incidents that occurred last year were monstrous. For example:

- Poly Network (August 2021): $610 million – stemming from a security hole in the 'cross chain' smart contracts used by the platform company.
- Cream Finance (October 2021): $130 million – crypto hackers stole all liquid assets owned by this lending platform on the Ethereum blockchain.
- Vulcan Forged (December 2021): $140 million – play-to-earn blockchain platform's biggest users were hacked and had tokens stolen.
- BitMart (December 2021): $200 million – half of loss occurred via a "large-scale security breach" on the Ethereum blockchain.

These incidents highlight the severity of cybercrime in a dynamic industry. As crypto continues to grow and "comprise an expanding part of the U.S. financial system," cybercrime will follow suit unless there are laws and regulations to bolster the security and structure of crypto and blockchain technology.

States are trying. Last year, 33 states considered crypto and blockchain legislation. In prior years, Georgia, Tennessee, Delaware, Illinois and Wyoming adopted laws recognizing the legal authority to use blockchain technology for

PEOPLE

Jeffrey Schultz, CIPP/US

SERVICES AND INDUSTRIES

Data Innovation, Security and Privacy

White-Collar Criminal Defense and Government Investigations

Securities Regulation and Litigation

electronic transactions (i.e., smart contracts). As the frontrunner, Wyoming has more than 20 laws relating to blockchain. A bill pending in New York would recognize the use of blockchain technology and smart contracts in commerce. (AB 3760 and SB 1801 allow signatures, records and contracts secured through blockchain technology to be considered in an electronic form and to be an electronic record and signature; and allow smart contracts to exist in commerce. The Senate passed the bill on Feb. 10, 2021.)

Significantly, in 2017, Delaware amended the Delaware General Corporation Law to authorize the use of distributed ledgers or blockchain technology for the creation and maintenance of corporate records, including a Delaware corporations' stock ledger (8 Del. C. § 224). While arguably federal legislation already exists which legalizes smart contracts, these legislative efforts help to clarify and promote their use. (The fact that smart contracts are written in code without a physical signature does not prevent their enforceability due to the United States Electronic Signatures in Global and National Commerce (E-SIGN Act) and the Uniform Electronic Transaction Act (UETA). See 15 U.S.C.§ 7001, et seq.)

But ultimately, the federal government will have the most impact. As noted last August by the Chairman of the Securities and Exchange Commission (SEC), Gary Gensler, "right now, we don't have enough investor protection for crypto. Frankly, at this time, it's more like the Wild West." Last year, Congress introduced 35 bills targeting this technology including:

- The Consumer Safety Technology Act (H.R. 3723) – promoting the study of potential blockchain technology primarily by the Department of Commerce and the Federal Trade Commission (FTC).
- The Eliminate Barriers to Innovation Act (H.R. 1602) – creating an SEC and Commodity Futures Trading Commission 'Working Group on Digital Assets' to promote congressional comprehension of blockchain technology.
- The Securities Clarity Act (H.R. 4451) – providing clarification on how blockchain tokens would be regulated by the SEC.
- The Blockchain Promotion Act of 2021 (S. 1869) – establishing a working group to "recommend to Congress a definition of blockchain technology."
- The Blockchain Regulatory Certainty Act (H.R. 5045) – ensuring clarity for blockchain innovators and providing myriad blockchain-related services such as "a safe harbor for licensing and registration for certain non-controlling blockchain developers and providers of blockchain services."

The federal agencies vying to determine the most direct way forward for the laws and regulations governing crypto and blockchain technologies include:

- The Securities and Exchange Commission
- The Commodity Futures Trading Commission
- The Federal Trade Commission
- The Department of the Treasury
- The Office of the Comptroller of the Currency
- The Financial Crimes Enforcement Network

Not to be left out, a few weeks ago the United States Secret Service launched a cryptocurrency public awareness hub. On its hub the Secret Service highlights the "ongoing growth in decentralized financial ecosystems, peer-to-peer payment activity and obscured blockchain ledgers" that "are abused and used in illicit ways."

As noted by leading technology innovators at Cryptopia, laws, regulations and industry standards are coming, and that's not necessarily a bad thing. For further information about crypto and blockchain technology, contact the authoring attorneys at Armstrong Teasdale, or sign up for their upcoming webinar on March 16, 2022, titled "The Intersection of Blockchain, Crypto and DeFi with Data Innovation, Privacy, and Security."