CARDOZO LAW

BENJAMIN N. CARDOZO SCHOOL OF LAW • YESHIVA UNIVERSITY

Aaron Wright
Associate Clinical Professor of Law
Co-Director, Cardozo Blockchain Project

(212) 790-0420
aaron.wright@yu.edu

Testimony Before the Subcommittee on Oversight and
Subcommittee on Research and Technology

"*Beyond Bitcoin: Emerging Applications for Blockchain Technology*"

Aaron Wright
Associate Clinical Professor
Co-Director of Cardozo Blockchain Project
Wednesday, February 14, 2018

"Blockchain's Opportunities and Risks"

Chairman Abraham, Ranking Member Beyer, Chairwoman Comstock, Ranking Member Lipinski, Chairman Smith, Ranking Member Johnson, and members of the Oversight and Research and Technology Subcommittees, thank you for the opportunity to testify before you today. I hope my testimony will provide further insight on the potential and risks of blockchain technology, particularly with respect to next-generation public blockchains such as Ethereum. I also hope that my testimony will spur this Committee to increase funding for basic research of blockchain technology within the United States and encourage Congress to increase its exploration of the technology in line with the current efforts of other leading jurisdictions.

My name is Aaron Wright, and I am a law professor, writing and teaching primarily in the area of technology law. Over the past four years, I have dedicated my academic efforts to researching and developing blockchain technology, writing about policy issues associated with blockchain technology, and counseling blockchain technology projects. As part of those efforts, I am: (1) developing an academic project called OpenLaw, in conjunction with ConsenSys, which enables anyone to create "smart" legal agreements that leverage blockchain technology;[1] (2) serving as an advisor of a private blockchain company BlockApps;[2] (3) chairing the Legal Industry Working Group of the Enterprise Ethereum Alliance; and (4) helping to organize "The Brooklyn

[1] More specifically, OpenLaw enables anyone to model all or parts of a legal agreement using a domain specific language developed for lawyers. Any agreement created on OpenLaw is stored on the Ethereum blockchain and can call Ethereum-based smart contract. *See* OpenLaw.io, https://www.openlaw.io.

[2] BlockApps enables developers to build blockchain applications on top of a customized permissioned private blockchain or a public blockchain. *See* BlockApps, https://blockapps.net/.

Project," a collaborative industry effort to develop sensible regulatory standards for blockchain technology.[3]

Blockchains constitute a new infrastructure for the storage of data and the management of software applications, decreasing the need for centralized middlemen. While databases often sit invisibly behind online services, their significance cannot be understated. Databases serve as a backbone for every platform, website, app, or other online service. Up to this point, databases have been for the most part maintained by centralized intermediaries, such as large Internet companies or cloud computing operators. Blockchains are beginning to change this dynamic, powering a new generation of disintermediated peer-to-peer applications, which are less dependent on centralized control.

Blockchains blend together several existing technologies, including peer-to-peer networks, public-private key cryptography, and consensus mechanisms to create what can be thought of as a highly resilient and tamper-resistant database where people can store data in a transparent and non-repudiable manner and engage in a variety of economic transactions pseudonymously.[4]

More advanced blockchains, most notably Ethereum, also integrate decentralized computing systems enabling parties to write and deploy computer processes known as "smart contracts."[5] These programs are stored on a blockchain and are executed by multiple members of a blockchain's underlying peer-to-peer network, creating computer processes that are potentially autonomous and difficult to shut down once deployed.

While complex, public blockchains exhibit a set of core characteristics that differ from earlier data structures. Blockchains are disintermediated and often transnational. They are resilient and resistant to change and enable people to store non-repudiable data, pseudonymously, in a transparent manner. Most—if not all—blockchain-based networks feature market-based or game-theoretical mechanisms for reaching consensus, which can be used to coordinate people or machines. These characteristics, when combined, enable the deployment of autonomous software and explain why blockchains serve as a powerful new tool to facilitate economic and social activity that otherwise would be difficult to achieve.[6]

Importantly, for purposes of this hearing, blockchains are useful for more than just virtual currencies, like Bitcoin. They are underpinning an array of online services that seek to use the technology to store information and run computer processes in areas that could potentially impact a range of industries in the United States. I will highlight some use cases here:

As we have seen over the past two years, blockchains are poised to transform capital markets. Technologists are relying on blockchains to build genuinely global marketplaces—markets that are decentralized, geographically agnostic, and accessible to all. Blockchain technology is being explored to improve the efficiency of traditional financial services, creating

---

[3] *See* The Brooklyn Project, https://thebrooklynproject.consensys.net/.
[4] *See* PRIMAVERA DEFILLIPI & AARON WRIGHT, BLOCKCHAIN & THE LAW: THE RULE OF CODE (forthcoming Harvard University Press 2018).
[5] *Ibid.*
[6] *Ibid.*

digitized financial agreements that are settled and cleared on a bilateral basis with less of a need for third party administration. Perhaps of greater long term importance, blockchains are securing scarce digital assets (often referred to as "tokens") and representations of digitized assets, which parties transfer using smart contracts in a secure and largely irreversible way, with less of a need for centralized intermediaries.[7]

Blockchain-based tokens are powering new forms of crowdfunding, often referred to as token sales, which have resulted in the sale of roughly $4 billion worth of assets last year alone. Token sales represent a potentially potent new tool for entrepreneurs to build powerful new technology platforms and hold the potential to democratize access to capital, helping to spur innovation throughout the United States.[8]

The impact of blockchain technology is spreading to the legal industry and other industries heavily reliant on contractual arrangements to structure business activity. Smart contracts are ushering in a renewed interest in "computable contracts," or contracts that can be processed and understood by machines. With blockchain technology, we soon may move beyond an era of agreements written predominantly or entirely in a natural language, replaced instead by agreements written, at least in part, in code.[9]

Outside of the private sector, governments across the globe, including China, Japan, and the European Union, are increasing experimentation with blockchain technology, exploring whether blockchains can secure and manage critical public records, including vital information, identity, and title or deeds to property, and whether blockchains can improve government procurement and taxation processes.[10] By leveraging the tamper-resistant, resilient, and non-repudiable nature of a blockchain, governments are looking to guarantee—with a high degree of probability—the integrity and authenticity of key governmental information and prevent cyber security attacks. They are also looking to streamline and automate basic government services.

Through these efforts, it is conceivable that blockchains could anchor new public digital infrastructure, and potentially even global and transnational systems, which are available to anyone with an Internet connection. Blockchains could underpin universally accessible, secure

---

[7] Jonathan Rohr and Aaron Wright, *Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets* (October 4, 2017), Cardozo Legal Studies Research Paper No. 527, University of Tennessee Legal Studies Research Paper No. 338, at https://ssrn.com/abstract=3048104.

[8] *Ibid.*

[9] DeFillipi & Wright, *supra* note 4.

[10] For example, the E.U. recently launched a "Blockchain Observatory and Forum," with the support of the European Parliament to "promote European actors and reinforce European engagement with multiple stakeholders involved in blockchain activities." *See* European Commission, Press Release: European Commission Launches the E.U. Blockchain Observatory, Feb. 1, 2018, http://europa.eu/rapid/press-release_IP-18-521_en.htm. China is experimenting with blockchain technology to collect taxes and issue invoices. *See* "China Will Experiment with Using Blockchain to Collect Taxes," MIT Technology Review, August 7, 2017, https://www.technologyreview.com/the-download/608570/china-will-experiment-with-using-blockchain-to-collect-taxes/. Japan is developing, in conjunction with shared ID systems for banks. *See* "Japan Developing Shared ID System For Banks," Nikkei Asia Review, Sept. 21, 2017, https://asia.nikkei.com/Tech-Science/Tech/Japan-developing-shared-ID-system-for-banks (noting that the initiative is being jointly developed by the Japanese Financial Services Agency and various financial institutions).

decentralized voting systems, transnational land and intellectual property registries, and global marketplaces available to all.

Extending beyond governmental services, blockchains are increasingly being explored to control devices and machines, with smart contracts defining the operations of Internet-connected devices. If these attempts prove successful, blockchains could foster a new era of machine-to-machine and machine-to-person interactions that could potentially change the very nature of our relationships with physical goods.[11]

Despite these opportunities, the disintermediated and transnational nature of blockchains makes the technology difficult to govern and makes it difficult to implement changes to a blockchain's underlying software protocol. Because public blockchains are pseudonymous, and because they have a tamper-resistant data structure, blockchains can be used to coordinate socially unacceptable or criminal conduct, including conduct facilitated through autonomous software programs.

Of greatest present concern, a slate of new more anonymous digital currencies, like Monero, are making it progressively easier to avoid anti-money laundering and other financial rules related to payment systems by emulating hard-to-track hand-to-hand money like cash and coins. These more anonymous digital currencies rely on advanced cryptographic techniques (such as zero-knowledge proofs and ring signatures) to obscure the origin, destination, and amount of every transaction facilitated by a blockchain. Entrepreneurs are using blockchain technology to avoid securities laws requirements, often with the aid of complicit lawyers and other advisors that emphasize form over substance. Cryptocurrency exchanges, particularly those located abroad, appear to have implemented weak measures to prevent abusive trading practices, and new decentralized marketplaces and exchanges are emerging which could operate without any centralized operator policing the network for illegal activity.

Blockchains also present a number of technological limitations. Existing blockchains are not as powerful and fast as other data management technologies and only can record a comparatively few number of transactions per day, as compared to current databases.[12] The encryption that these systems rely upon may be impacted by quantum computing.[13] And,

---

[11] DeFillipi & Wright, *supra* note 4.

[12] For instance, the Ethereum blockchain processes more transactions than any other blockchain and only processes roughly 800,000 transactions per day—far less than the trillions of messages sent across the Internet, or the 150 million daily transactions handled by credit card companies such as Visa. *See* Ethercan, "Ethereum Transaction Chart," https://etherscan.io/chart/tx (last accessed February 8, 2018). What's more, it takes approximately 15 seconds for an Ethereum transaction to be validated by the network and recorded to the shared data set, in contrast to the fraction of a second it typically takes a database to store and record information. *Id.*

[13] *See* Michael Crosby et al., *Blockchain Technology: Beyond Bitcoin*, 2 APPLIED INNOVATION 6 (2016) ("The basis of BlockChain technology relies on the very fact that it is mathematically impossible for a single party to game the system due to lack of needed compute power. But with the future advent of Quantum Computers, the cryptographic keys may be easy enough to crack within a reasonable time through a sheer brute force approach. This would bring the whole system to its knee."). Note that researchers at the Russian Quantum Center, the Steklov Mathematical Institute of Russian Academy, and the Institute for Quantum Science and Technology have proposed a possible solution to the quantum-era blockchain challenge. *See* E.O. Kiktenko et al., "Quantum Secured Blockchains," May 29, 2017, https://arxiv.org/pdf/1705.09258.pdf.

programming smart contracts has proved difficult, requiring research into formal verification and improved programming techniques.[14]

Due to the nascent nature of blockchains, and the fact that much of the innovation around blockchain technology is still occurring here, the U.S. government has the unique ability to shape the development of the technology by passing laws and regulations that will either constrain or promote the technology's growth and adoption. The United States could choose to implement regulations that make it expensive or difficult to develop or operate a blockchain-based service. Conversely, the U.S. could implement favorable regulatory frameworks to protect businesses experimenting with blockchains as part of pro-innovation policies.

Given the early stage of development, it still is possible to capture the benefits of blockchain technology, while limiting its downsides. The U.S. has the ability to rely on civil society, contractual negotiations, voluntary agreements, and ongoing marketplace experiments to solve blockchain-related regulatory problems. And, even where collective action is necessary, there are opportunities for industry self-regulation and private sector leadership.

As a guiding principle, however, it is my hope that the U.S. proceeds with thoughtful, technology-neutral regulation that:

- Permits the exchange of blockchain-based assets and scarce digital goods, particularly those used, purchased, and enjoyed by consumers;
- Enables parties to build new blockchain-based protocols, without fear of regulatory scrutiny to address the technical limitations outlined previously;
- Provides a predictable, minimalist, consistent, and simple legal environment that protects consumers without insulating entrenched market participants; and
- Re-examines existing laws and regulations that may hinder blockchain-based commerce.

To support these research and policy goals, I would encourage Congress to contemplate commissioning a National Blockchain Commission that would aim to cement America's technological standing and increase economic growth and innovation by exploring ways to invest in blockchain-based research—through prizes or otherwise—and to help ensure that blockchain-based innovation occurs here. The commission could: (i) help devise common principles to guide the federal approach for regulating blockchain technology, across a range of sectors, protecting values like financial privacy, personal autonomy, and consumer protection; and (ii) hold hearings, conduct research, and make recommendations for industry, the Executive Branch, and Congress.

Through the above approach, we can ensure that the United States remains the best place to develop, launch, and grow a blockchain-based project. The United States can maintain its lead

[14] *See* Karthikeyan Bhargavan et al., "Formal Verification of Smart Contracts," In Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security, pp. 91-96. ACM, 2016 (describing the challenges of creating secure smart contracts).

when it comes to Internet-based technologies and implement sensible guardrails to guide its development.

Thank you for your time and I look forward to your questions.