UNIVERSITY OF PITTSBURGH LAW REVIEW
Vol. 83 ● Summer 2022

TECHNOLOGY-ENABLED CO-REGULATION FOR BLOCKCHAIN IMPLEMENTATION

Jiang Jiaying

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

TECHNOLOGY-ENABLED CO-REGULATION FOR BLOCKCHAIN IMPLEMENTATION

Jiang Jiaying*

ABSTRACT

Blockchain technology has great potential to reshape the financial industry. However, the existing policy and regulatory regimes fail to provide a supportive environment for blockchain technology to fulfill its potential. In this Article, I propose technology-enabled co-regulation as a new approach to blockchain implementation, especially in the financial markets. This approach has two distinctive elements: a collaborative environment and a technology-enabled mechanism. A collaborative environment consists of regulatory and industry sandboxes in which regulators and industry representatives can experiment with novel ideas. A technology-enabled mechanism is empowered by regulatory technologies ("RegTech") and supervisory technologies ("SupTech") that support compliance with regulatory and reporting requirements and facilitate supervisory obligations. This technology-enabled co-regulation can help to achieve policy and regulatory goals: a fair and efficient market, financial stability, consumer and investor protection, law enforcement efficiency, and, most importantly, technology innovation. Technology-enabled co-regulation is preferable to traditional command-and-control regulation and self-regulation. Its collaborative and technological elements are also more advanced than a simple co-regulation is. To reach this conclusion, this Article conducts an impact assessment of proposed regulatory options. The impact assessment consists of five analytic steps, asking the following questions: (1) what problems have emerged from existing policies and regulations? (2) what are the objectives of the proposed regulations? (3) what are the regulatory options? (4) what are the possible impacts? (5) how do the options compare?

* Dr. Jiaying Jiang, Hauser Global Fellow at New York University School of Law. I greatly appreciate comments and feedback from faculty members and fellows at the NYU Hauser Program, NYU Information Law Institute, and Privacy Law Group. I also thank participants of the 2021 National Business Law Scholars Conference for their great questions and comments that shaped this project. Last but not least, I thank the editors of the Pittsburgh Law Review, especially Jean Yesudas, Jacob Dougherty, and Erin Napoleon, for reviewing and editing this piece.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

Table of Contents

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

INTRODUCTION

Blockchain technology, or blockchain, is a distributed database system. Supported by its consensus mechanism and cryptography, blockchain technology can provide tamper-proof, traceable, transparent, and secured data. This property enables parties worldwide to transfer value in a trustless environment and reshape various industries whose operations require a trusted environment. For example, blockchain has already had an impact on the financial industry. According to a KPMG analysis, blockchain can increase efficiency from transparent records for a single source of truth.[1] Its distributed databases can avoid reconciliation by creating one version of a ledger that is synchronized across computers.[2] Through these immutable records—which are permanent, unalterable, and visible to everyone involved—blockchain can enhance data integrity to reduce loss, potentially improving data accuracy and security, reducing the risk of fraud, and showing compliance through an audit trail.[3] Blockchain can also increase capital availability and lower business costs because its smart contracts and consensus mechanisms can trigger an automatic transfer of funds upon an agreed set of conditions and reduce reliance on third parties.[4]

However, blockchain technology's fulfillment of its potential faces many regulatory obstacles in China and the United States. In China, the regulatory environment is not always consistent. On the one hand, national and local policymakers and regulators have made a great effort to develop and adopt blockchain technology by calling for innovation. For instance, in March 2018, central and local governments issued more than 119 policies and regulations on blockchain technology—in 2018 alone, policymakers introduced thirty-five policies to support blockchain adoption.[5] During the Two Sessions[6] meetings in March 2019,

---

[1] BLOCKCHAIN AND THE FUTURE OF FINANCE, KPMG 1 (2019), https://assets.kpmg/content/dam/kpmg/ca/pdf/2019/05/blockchain-and-the-future-of-finance.pdf [https://perma.cc/UY7H-M245].

[2] *Id.* at 3.

[3] *Id.*

[4] *Id.*

[5] Ministry of Industry and Information Technology of China, 2018 Nian Zhongguo Qukuailian Chanye Baipishu (2018年中国区块链产业白皮书) [2018 Blockchain Technology and Application Development Whitepaper] 105 (2018), http://www.miit.gov.cn/n1146290/n1146402/n1146445/c6180238/part/6180297.pdf [https://perma.cc/Y83H-3BDS] [hereinafter 2018 Whitepaper].

[6] The term Two Sessions, or in Chinese Lianghui, refers to the annual plenary sessions of two organizations that make national-level legislative and political decisions: the National People's Congress and the National Committee ("NPC") and the Chinese People's Political Consultative Conference

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

representatives from across China advanced more than thirty blockchain-related legislative and policy proposals.[7] By May 2019, more than thirty provinces and cities had published blockchain-related policy guidance.[8] On the other hand, the Chinese government takes a harsh stance against one of the biggest blockchain applications—cryptocurrencies. On September 4, 2017, China's central bank, along with six other departments, issued an all-out ban on initial coin offerings ("ICOs") and cryptocurrency trading.[9] This ban created turmoil in the blockchain space, resulting in substantial losses for many entrepreneurs and consumers.

In the United States, blockchain adoption also faces regulatory fragmentation and uncertainty.[10] U.S. regulation regards blockchain technology as a type of financial technology when it provides financial products or services—one of the most heavily regulated sectors of the economy.[11] Instead of advocating for new laws or issuing new regulations, regulatory agencies have adapted existing regulatory frameworks to blockchain-related business by interpreting existing requirements to yield guidance and enforcement actions. As a result, multiple regulatory agencies can have overlapping regulatory authority over the same blockchain activity, and

("CPPCC"). The NPC is China's legislature, and it meets in full session for roughly two weeks each year and votes on important pieces of legislation. The CPPCC is a political advisory body in the People's Republic of China. Two Sessions gathers thousands of the country's top decisionmakers in one place and discusses important local and national issues. A major goal of the Two Sessions is for China's leadership to set out its visions and plans for the next twelve months.

[7] China Academy of Information and Communications Technology, 2019 Nian Qukuailian Baipishu (2019年区块链白皮书) 17 (2019), http://www.caict.ac.cn/kxyj/qwfb/bps/201911/P020191108365460712077.pdf [https://perma.cc/77ZG-NTTC] [2019 Blockchain Whitepaper].

[8] *Id.*

[9] Chao Deng & Paul Vigna, *China to Shut Bitcoin Exchanges*, WALL ST. J. (Sept. 11, 2017, 8:16 PM), https://www.wsj.com/articles/china-to-shut-bitcoin-exchanges-sources-1505100862 [https://perma.cc/B9XQ-9WUG]; *see also* Greg Pilarowski & Lu Yue, *China Bans Initial Coin Offerings and Cryptocurrency Trading Platforms*, PILLAR LEGAL (Sept. 21, 2017), http://www.pillarlegalpc.com/en/legalupdates/2017/09/21/china-bans-initial-coin-offerings-and-cryptocurrency-trading-platforms/ [https://perma.cc/3VSR-AW2G].

[10] New America's India-U.S. Fellows, BLOCKCHAIN REGULATION IN THE UNITED STATES: EVALUATING THE OVERALL APPROACH TO VIRTUAL ASSET REGULATION, *in* THE PROMISE OF PUBLIC INTEREST TECHNOLOGY: IN INDIA AND THE UNITED STATES (Aug. 5, 2019), https://www.newamerica.org/fellows/reports/anthology-working-papers-new-americas-us-india-fellows/blockchain-regulation-in-the-united-states-evaluating-the-overall-approach-to-virtual-asset-regulation-tanvi-ratna/ [https://perma.cc/W82Y-L3BK].

[11] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

they may treat it differently.[12] Prospective regulated entities face unclear and diverse compliance rules. The fear of incompliance further results in ineffective blockchain experiments and innovations.

With an eye toward narrowing the gap between the existing regulatory regimes and blockchain implementation, this Article proposes a new regulatory approach—technology-enabled co-regulation—to not only fulfill blockchain's potential in the real economy, but also to help achieve policy and regulatory objectives. This approach has two distinctive elements: a collaborative environment and a technology-enabled mechanism. A collaborative environment consists of regulatory and industry sandboxes in which regulators and industry representatives can experiment with novel ideas. A technology-enabled mechanism is empowered by regulatory technologies ("RegTech") and supervisory technologies ("SupTech") that support compliance with regulatory and reporting requirements and facilitate supervisory obligations. This technology-enabled co-regulation can help to achieve policy and regulatory goals: a fair and efficient market, financial stability, consumer and investor protection, law enforcement efficiency, and, most importantly, technology innovation. Technology-enabled co-regulation is preferable to traditional command-and-control regulation and self-regulation. Its collaborative and technological elements are also more advanced than simple co-regulation.

To reach this conclusion, I conducted a regulatory impact assessment of proposed regulatory options. Colin Kirkpatrick and David Parker defined a regulatory impact assessment as "a method of policy analysis, which is intended to assist policymakers in the design, implementation, and monitoring of improvements to regulatory systems, by providing a methodology for assessing the likely consequences of the proposed regulation."[13] It is a critical tool for assessing policy or regulatory proposals.[14] The European Commission has established key analytical steps in impact assessments that involve understanding the problems to be addressed—identifying policy objectives, coming up with policy options, analyzing

[12] *Id.*

[13] COLIN H. KIRKPATRICK & DAVID PARKER, REGULATORY IMPACT ASSESSMENT: TOWARDS BETTER REGULATION? 2 (2007).

[14] *CEPA Strategy Guidance Note on Regulatory Impact Assessment*, UNITED NATIONS (Feb. 2021), https://unpan.un.org/sites/unpan.un.org/files/Strategy%20note%20regulatory%20impact%20assessment%20Mar%202021.pdf [https://perma.cc/L2PL-3WEV] [hereinafter *CEPA Strategy Guidance Note*].

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

their impacts, and comparing these options.[15] Similarly, this Article's assessment consists of five analytic steps, asking the following questions: (1) what problems have emerged from existing policies and regulations (2) what are the objectives of the proposed regulations? (3) what are the regulatory options? (4) what are the possible impacts? (5) how do the options compare?[16]

This series of questions support the structure of the Article. Part I identifies four major themes that have emerged from the existing policy and regulatory regimes in both China and the United States: the overwhelming scams and fraud in the blockchain market; insufficient innovation; the lack of investor and consumer protection; and the difficulties regulators face in catching up with the disruptive impacts of blockchain technology.

Part II explains two primary policy objectives that both countries seek to achieve—a fair and efficient market and technology innovation. Due to different policy and regulatory regimes, China and the United States may have slightly different interpretations and focuses when fulfilling the first goal—a fair and efficient market. Overall, "market safety and stability" has been an explicit goal in China's policy and regulatory guidance in the blockchain space. In contrast, the United States concentrates on protecting consumers and investors and strengthening criminal enforcement.

Part III proposes three regulatory options: command-and-control regulation; self-regulation; and technology-enabled co-regulation. Command-and-control regulation indicates that the state (i.e., the regulators) administers and enforces rules. The regulatory process generally consists of three stages: creating regulations; monitoring for compliance; and enforcing regulations. Self-regulation represents a shift away from state regulation. It delegates public policy tasks to private actors which can take place in the form of self-regulatory organizations. Under co-regulation, regulations are specified and enforced by a combination of the state and private actors (e.g., industry organizations). These organizations can be authorized by the state, agreed upon by industry participants, or both. The novel idea behind the co-regulation I propose is that technology (i.e., technology-enabled co-regulation) should supplement and augment it. This new approach represents a collaborative and technology-enabled paradigm.

Part IV is an assessment of the impacts of regulatory options to understand whether they can generate their intended effects—achieving blockchain's potential

---

[15] *Impact Assessments*, EUR. COMM'N, https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/impact-assessments_en [https://perma.cc/5PPX-H4QR].

[16] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

and regulatory objectives. Each approach has positive and negative impacts. Command-and-control can directly reduce blockchain- and cryptocurrency-related fraud and crimes. Regulators can also make monitoring and enforcement relatively easier. Enforcement backed by state authority can also effectively deter misconduct. However, this approach is less cost-effective, inflexible, and may lead to regulatory capture—a corruption of authority that occurs when a political entity, policymaker, or regulatory agency is co-opted to serve the interests of a minor constituency. The impacts of self-regulation are twofold. It benefits the blockchain industry by creating a flexible regulatory environment, providing industry expertise for effective rulemaking, and reducing information asymmetry in the blockchain industry. However, self-regulation presents governance and free-rider problems. In addition, the effectiveness of rule monitoring and enforcement may be controversial.

Technology-enabled co-regulation also presents significant merits. It can keep regulators well informed and help consumers and investors face less risk due to reduced information asymmetry. In addition, the industry can witness greater innovation, and the regulatory and supervisory process can expect an increase in operational efficiency and a decrease in costs and human errors. Moreover, a new blockchain infrastructure design can allow regulators to monitor and pursue enforcement actions in a timely manner, reduce identity theft and data breaches, and improve risk management. However, some negative impacts are hard to evade. Sandboxes can also subject regulators to a greater regulatory capture. The implementation of sandboxes is not cost-free and requires extensive work on assessments and talents. The use of RegTech and SupTech is unavoidably associated with some privacy and security concerns.

Part V compares these three options and provides justification for why technology-enabled co-regulation is the preferred option. In short, it outperforms the other two options in cost, flexibility, enforceability, regulators' up-to-date knowledge, and regulatory capture.

I. WHAT PROBLEMS HAVE EMERGED FROM THE EXISTING POLICY AND REGULATORY REGIMES?

Blockchain applications and implementations have been troubling the financial markets in China and the United States over the past few years.[17] Policymakers and regulators have adopted various policies and regulations to tackle these issues.

[17] New America's India-U.S. Fellows, *supra* note 10.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

China's State Council put blockchain developments on its agenda in the 13th Five-Year Plan for the Development of Information Technology as the major policy guidance.[18] Following the guidance, the Cyberspace Administration of China ("CAC") detailed steps to accelerate developments of blockchain standards[19] and issued regulation to emphasize the duty of blockchain information service providers.[20] The Ministry of Industry and Information Technology issued blockchain whitepapers in 2016 and 2018 addressing several major areas of concern—such as standard setting, ecological structure of blockchain, and technical features[21]—exploring blockchain use cases in finance and the real economy,[22] and enumerating six goals of blockchain developments.[23] In terms of cryptocurrencies—one of the biggest blockchain applications—policymakers and regulators took a hard stance. The People's Bank of China ("China's central bank"), along with six other departments, banned ICO activities in September 2017.[24] They defined ICOs as unauthorized fundraising activities, subject to several financial crimes.[25]

In the United States, regulatory agencies oversee blockchain-related activities within their respective regulatory powers. They have been interpreting existing regulations, publishing official guidance, piloting relevant initiatives, and taking enforcement actions to exercise their regulatory power. For instance, the Securities

[18] Jiaying Jiang, *Regulating Blockchain? A Retrospective Assessment of China's Blockchain Policies and Regulations*, 12 TSINGHUA CHINA L. REV. 313, 319–21; *see also* "Shisanwu" Guojia Xinxihua Guihua ("十三五"国家信息化规划) [National Informationization Plan for the "13th Five-Year Plan"] (promulgated by St. Council, Dec. 27, 2016), http://www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm [https://perma.cc/45FW-CM2B].

[19] Jiang, *supra* note 18, at 319–21; *see also Jiakuai Yanzhi Qukuailian Xiangguan Biaozhun* (加快研制区块链相关标准) [*Accelerate the Development of Relevant Standards for Blockchain*], CHINA DAILY (Nov. 12, 2018), http://cn.chinadaily.com.cn/2018qklfnzl/2018-11/21/content_37293931.htm [https://perma.cc/QE6T-WF2F].

[20] Qukuailian Xinxi Fuwu Guanli Guiding (区块链信息服务管理规定) [Provisions on the Administration of Blockchain Information Services] (promulgated by the Office of the Cent. Cyberspace Affairs Comm'n and Cyberspace Admin. of China, Jan. 10, 2019, effective Feb. 15, 2019).

[21] *Zhongguo Qukuailian Jishu he Yingyong Fazhan Baipishu (2016)* (中国区块链技术和应用发展白皮书(2016)) [*The Blockchain Technology and Application Development Whitepaper (2016)*], http://ec.whu.edu.cn/a/37.html [https://perma.cc/8KFD-SVHQ].

[22] 2018 Whitepaper, *supra* note 5.

[23] *Id.*

[24] Deng & Vigna, *supra* note 9.

[25] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

and Exchange Commission ("SEC") released the report on The DAO investigation in 2017 and applied securities law to ICOs.[26] The Commodity Futures Trading Commission ("CFTC") treats cryptocurrencies as commodities under certain circumstances.[27] The Department of Treasury's Financial Crimes Enforcement Network, ("FinCEN") and the Federal Bureau of Investigation ("FBI") take enforcement actions against financial crimes such as money laundering and terrorist financing with the use of cryptocurrencies.[28] The Internal Revenue Service ("IRS") treats some cryptocurrencies as property and thus levies tax.[29]

As a result of these policy and regulatory actions, some of the problems in the blockchain industry have been solved, while some remain to be addressed. Additionally, new issues appear during the process of tackling existing problems. Due to unsolved problems and new issues which are quite diverse within these two jurisdictions, this Article singles out four of the most urgent problems both countries face and are eager to solve. These four issues take the perspective of the market and market participants, involving (1) overwhelming scams and fraud in the blockchain market; (2) insufficient innovation; (3) a lack of investor and consumer protection; and (4) regulators' difficulties in catching up with the interruptive impacts of blockchain.

A. Overwhelming Scams and Fraud in the Blockchain Market

Tackling scams and fraud has been the major target of existing policies and regulations.[30] Although there has been some progress, problems remain to be solved. And these issues have become even more severe in the blockchain market.

---

[26] SEC. & EXCH. COMM'N, NO. 81207, REPORT OF INVESTIGATION PURSUANT TO SECTION 21(A) OF THE SECURITIES EXCHANGE ACT OF 1934: THE DAO (2017).

[27] *Digital Assets*, COMMODITY FUTURES TRADING COMM'N, https://www.cftc.gov/digitalassets/index.htm [https://perma.cc/AFK5-LSHA].

[28] FinCen Advisory, *Advisory on Illicit Activity Involving Convertible Virtual Currency*, U.S. TREASURY (May 9, 2019), https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf [https://perma.cc/H7UV-5937]; *Virtual Ticket to Prison*, FED. BUREAU INVESTIGATION (May 3, 2017), https://www.fbi.gov/news/stories/fraud-scheme-leads-to-illegal-bitcoin-exchange [https://perma.cc/MJ5D-5AP4].

[29] *Digital Assets*, IRS, https://www.irs.gov/businesses/small-businesses-self-employed/virtual-currencies [https://perma.cc/CW8U-64M5].

[30] *What to Know About Cryptocurrency and Scam*, FED. TRADE COMM'N (May 2022), https://www.consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams [https://perma.cc/TW36-2364].

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

China outlawed ICO and cryptocurrency trading in 2017. But pyramid schemes and investment fraud using blockchain and cryptocurrency remain prevalent.[31] Fraudsters developed fraudulent schemes via diverse routes—creating more channels for fraudulent activities by moving their businesses to jurisdictions that allow ICOs, cryptocurrency trading, or Over-The-Counter ("OTC") transactions.[32] For instance, when bad actors recognized that users were copying and pasting the addresses of Bitcoin, they created malware, called CryptoCurrency Clipboard Hijackers, to take advantage of the Bitcoin addresses.[33] This malware works by monitoring the Windows clipboard for cryptocurrency addresses, and if a user does not double-check the address after they paste it, the sent coins will go to an address under the attacker's control instead of the intended recipient.[34] According to a website called Bleeping Computer, this malware could monitor over 2.3 million cryptocurrency addresses.[35] Thus, it could put many users at risk.

In the U.S. market, securities fraud, market manipulations, pump-and-dump schemes, cryptocurrency theft, and money laundering are still widespread.[36] Although law enforcement agencies have taken down some unlawful activities, such as Silk Road and Silk Road II, bad actors have developed a wider range of crypto-crimes such as SIM swapping, crypto dusting, sanction evasion, next-generation crypto mixers, shadow MSBs, datacenter-scale cryptojacking, lightning network transactions, decentralized stable coins, email extortion and bomb threats, and crypto-robbing ransomware.[37]

The underlying cause of these unceasing scams and fraud, from an economic perspective, is information asymmetry. Insiders or business owners of so-called blockchain projects usually hold more information regarding the projects than their consumers and investors. Information asymmetries in the blockchain market are usually not caused by a single factor but rather by a mix of various factors. The first

---

[31] Jiang, *supra* note 18, at 350.

[32] *Id.*

[33] Lawrence Abrams, *Clipboard Hijacker Malware Monitors 2.3 Million Bitcoin Addresses*, BLEEPING COMPUT. (June 30, 2018), https://www.bleepingcomputer.com/news/security/clipboard-hijacker-malware-monitors-23-million-bitcoin-addresses/ [https://perma.cc/9T5M-VWF6].

[34] *Id.*

[35] *Id.*

[36] Report of the Attorney General's Cyber Digital Task Force, *Cryptocurrency Enforcement Framework*, U.S. DEP'T JUST. (Oct. 2020), https://www.justice.gov/archives/ag/page/file/1326061/download [https://perma.cc/6NF5-3UNF].

[37] CIPHERTRACE, CRYPTOCURRENCY ANTI-MONEY LAUNDERING REP., 2018 Q4 5 (2019), https://ciphertrace.com/crypto-aml-report-2018q4/ [https://perma.cc/ALR8-E2M3].

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

is the complexity of blockchain itself. The complex technical aspect of blockchain prevents many laypeople or market participants from genuinely understanding what blockchain is and whether it could effectively and efficiently solve problems. Second, information dissemination is sometimes limited to the ownership structure. Many companies intending to initiate a blockchain product or service generally disseminate advantageous information regarding the project, company, team members, and expectations of future profits—while concealing information with adverse effects. Third, with the existing imbalanced information among market participants, regulators fail to improve the information flow, which further aggravates information asymmetry. Therefore, without access to sufficient information such as blockchain products or services, consumers are easily dragged into scams and fraud.

B. Insufficient Innovation

In addition to overwhelming scams and fraud, the blockchain market does not see well-developed innovation. Yet, both countries state that technology innovation is a major policy and regulatory goal. In China, policymakers and regulators seek to achieve technology innovation by building a blockchain ecosystem, standardizing the blockchain industry, and acquiring "world-leading innovation capacity in blockchain."[38] In that article, I studied the impacts of China's backchain policies and regulations.[39]

The blockchain ecosystem was initially formed as a result of a boom in blockchain entrepreneurship in 2018. Since then, blockchain startups have covered a wide range of industries. However, blockchain innovation in each industry has not yet become sophisticated and systematic.[40] While some progress has been in blockchain standardization, most key standards are still at the development stage or have not yet begun to be developed.[41] In terms of world-leading innovative capacity, China is a leader in the number of blockchain patents, the amount of capital invested and the number of deals in blockchain, and great policy support.[42] However,

[38] Jiang, *supra* note 18, at 356–63.

[39] *Id.*

[40] *Id.* at 356.

[41] *Id.* at 356–57.

[42] *Id.* at 358–62.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

blockchain research is not as robust as other indicators in the global rankings.[43] In addition, most domestic blockchain projects continue to be at the concept formation stage, lacking successful cases for large-scale applications and implementations.[44] Although blockchain applications have been expanding from finance to supply chain, social welfare, entertainment, and other fields, many of these applications are still immature.[45]

In the United States, blockchain innovation in the real economy is still lacking.[46] Some may suggest blockchain's innovation in the infrastructure for cross-border transactions could be seen as a success, because some new companies (Ripple and Stellar), or new projects under existing companies (IBM's World Wire, and J.P.Morgan's Coin), represent a new trend of cross-border transactions that allow for global reach, instant transition times, and low costs.[47] It is true many companies have explored blockchain use cases in the area of cross-border payment. However, regulatory uncertainty somehow slows down the innovation.[48]

Another innovation worth mentioning is the tokenization of assets as a class. Deloitte claims that "the tokenization of assets is disrupting the financial industry."[49] The tokenization of assets refers to the process of issuing a blockchain token (specifically, a security token) that digitally represents a real tradable asset—in many ways similar to the traditional process of securitization.[50] These tokenized assets,

[43] *Id.* at 362.

[44] *Id.* at 358.

[45] *Id.*

[46] Jiaying Jiang, *An Ex-Post Regulatory Impact Assessment of the U.S. Blockchain Regulatory Regime*, J.L. & CYBER WARFARE 48, 51 (Aug. 1, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3900283 [https://perma.cc/S6VF-KU46] [hereinafter *Regulatory Impact Assessment*].

[47] *Id.* at 58–61.

[48] Mike Orcutt, *Blockchain Boosters Warn That Regulatory Uncertainty Is Harming Innovation*, MIT TECH. REV. (Mar. 8, 2019), https://www.technologyreview.com/2019/03/08/136720/blockchain-boosters-warn-that-regulatory-uncertainty-is-harming-innovation/ [https://perma.cc/4U2D-H9TB] ("Regulatory uncertainty is one of the main reasons that while many traditional financial firms are interested in investing in crypto-assets, a good number have chosen to remain on the sidelines, Tom Jessop, president of Fidelity Digital Assets, told the DC crowd.").

[49] Patrick Laurent, Thibault Chollet, Michael Burke & Tobias Seers, *The Tokenization of Assets Is Disrupting the Financial Industry. Are You Ready?*, INSIDE MAG. 6 (Nov. 19, 2018).

[50] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

theoretically, can be bought and sold in a small amount of ownership, which lowers the barrier to enter the financial market and offers greater liquidity.

However, the idea of tokenized assets as a class was still at the stage of theoretical discussion. Progress of actual implementation would not be made in the short term because under the existing regulatory regime, the biggest hurdle preventing it from becoming a reality is the lack of policy guidance and specific regulation.

C. A Lack of Investor and Consumer Protection

Policymakers and regulators in both countries have been taking measures to protect investors and consumers in the blockchain market. However, the protection is still insufficient. In China, authorities outlawed ICOs and cryptocurrency trading, required blockchain service providers to register with the government and comply with disclosure rules, and began to work on standardizing the blockchain industry—intending to provide a safer blockchain market for investors and consumers.[51]

The results were unsatisfactory. Investors first suffered a great loss because their investments evaporated due to the delisting of cryptocurrencies and, furthermore, many other small and mid-size enterprises ("SMEs"), such as wallet providers and media services, were driven out of the market.[52] Second, to escape the law, some cryptocurrency trading companies moved businesses to other jurisdictions or used the OTC transaction while serving the same customers.[53] The creation of these new channels did not reduce fraudulent or investment risks consumers face. Third, protection through disclosure rules is limited.[54] As of February 15, 2019, 197 service providers had registered with the CAC to meet disclosure requirements.[55] This number means more than half of blockchain companies, which could be

[51] Jiang, *supra* note 18, at 338–39.

[52] *Id.* at 349–50.

[53] *Id.* at 350.

[54] *Id.* at 351.

[55] Office of the Central Cyberspace Affairs Commission and Cyberspace Administration of China, *Guojia Hulianwang Xinxi Bangongshi Guanyu Fabu Diyipi Jingnei Qukuailian Xinxi Fuwu Beian Bianhao de Gonggao* (国家互联网信息办公室关于发布第一批境内区块链信息服务备案编号的公告) [*Announcement of the National Internet Information Office on the Publication of the First Batch of Domestic Blockchain Information Service Filing Numbers*] (2019), http://www.cac.gov.cn/1124305122_15539349948 111n.pdf [https://perma.cc/953R-UJYU].

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

categorized as service providers, had not yet registered with the CAC.[56] According to the data, as of October 31, 2018, the number of blockchain companies was 484.[57] Worse, few investor or consumer protections have come from the government's standardization effort because most of the standardizing work is at the beginning stage.[58]

In the United States, regulators take the approach of neoclassical economics, which assumes that potential investors are rational and can make informed decisions when they have enough information about a blockchain company.[59] Disclosure is the major tool that regulators use to protect investors and consumers. However, as of mid-April 2018, only thirty-nine companies had filed notices with the SEC,[60] which provided limited information to the public due to the exemption rules. Many other companies did not provide sufficient information because they sought to avoid the SEC's oversight.[61]

Additionally, entities' unfulfilled promises also leave consumers and investors somewhat unprotected. A survey studied fifty ICO projects to examine whether there was any difference between codes and contracts that have been made with investors.[62] It revealed that many ICOs fail to even promise that they would protect investors against insider self-dealing.[63] Fewer still manifested such promises in code.[64] As Boreiko and Shadev noted, "projects are making governance claims that

---

[56] Jiang, *supra* note 18, at 351.

[57] Lianta he Zhongguo Guoji Jingji Jishu Hezuo Cujinhui Qukuailian Jishu yu Yingyong Gongzuo Weiyuanhui (链塔和中国国家经济技术合作促进会区块链技术与应用工作委员会) [*Lianta Think Tank & Blockchain Technology and Application Working Committee of China Association for Promoting International Economic & Technical Cooperation*]; *2018 Nian Zhongguo Qukuailian Chanye Fazhan Lanpishu* (2018年中国区块链产业发展蓝皮书) [*2018 China Blockchain Industry Development Blue Book*] 1 (2018).

[58] Jiang, *supra* note 18, at 357.

[59] *Regulatory Impact Assessment*, *supra* note 46, at 51; *see also* Oren Bar-Gill, *The Behavioral Economics of Consumer Contracts*, 92 MINN. L. REV. 749, 749 (2008).

[60] *Rapid Increase in SEC Filings by Cryptocurrency and Blockchain Companies*, CRYPTOLAW (Apr. 24, 2018), https://www.cryptolaw.net/blog/2018/4/24/rapid-increase-in-sec-filings-by-cryptocurrency-and-blockchain-companies [https://perma.cc/UMG7-E68X].

[61] *Regulatory Impact Assessment*, *supra* note 46, at 51.

[62] Shaanan Cohney, David Hoffman, Jeremy Sklaroff & David Wishnick, *Coin-Operated Capitalism*, 119 COLUM. L. REV. 591, 637 (2019).

[63] *Id.*

[64] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

look to be modeled off of offline VC or traditional equity-based rules intended to reduce agency costs, but they are not encoding those promises into the sort of trustless, decentralized systems which undergird their networks' purported sky-high values."[65] Therefore, investor protection can hardly be seen as sufficient in these situations.

Both countries somehow treat disclosure as a way to reduce information asymmetry, along with *ex-post* law enforcement of any violation to protect investors and consumers.[66] Outcomes are not satisfactory because the disclosure rule does not reach a sufficient scale.[67] Disclosure failure is further caused by a lack of a cooperative environment between regulators and the regulated entities.[68] Meeting the requirements of disclosure costs the regulated entities time and money, which become additional burdens for newly incorporated startups without consistent cash flow.[69] Some startups thus seek ways to avoid disclosing information to regulators. In some other cases, the disclosure guidance is not clear, so the regulated entities face difficulties to meet the requirements.[70] Therefore, only limited information is disclosed. Consumers and investors as decision makers do not get fair access to fair and sufficient information.[71] What's more, in the cryptocurrency space, even provided with information of a cryptocurrency project, investors or consumers may lack either the incentive, or capability, or both, to investigate the truthfulness of the information with which they are presented.[72] Their imperfect rationality and inability to make utility-maximizing decisions exposes them to the very risky cryptocurrency space.[73]

Another reason for insufficient investor and consumer protection is a lack of law enforcement infrastructure.[74] Tackling blockchain-related crimes should

[65] *Id.* at 639.

[66] Jiang, *supra* note 18, at 349–52; *see also Regulatory Impact Assessment*, *supra* note 46, at 51–56.

[67] *Regulatory Impact Assessment*, *supra* note 46, at 51, 71.

[68] *Id.*

[69] *Id.* at 51.

[70] *Id.*

[71] *Id.* at 48.

[72] *Id.* at 51.

[73] *Id.*

[74] Simon Dyson, William J. Buchanan & Liam Bell, *The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime*, ARXIV (July 29, 2019), https://arxiv.org/pdf/1907.12221.pdf [https://perma.cc/YUX6-QYHJ].

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

consider the distinctive characteristics of blockchain that criminals are taking advantage of. Blockchain's anonymous and decentralized characteristics makes identification and traceability difficult. Its support for borderless and encrypted transactions could obfuscate the use of legal and legitimate surveillance. Traditional technologies or methods may not be sufficient and effective to spot and ascertain crimes and further prosecute criminals. Corresponding infrastructure to effectively tackle crimes occurring out of the peer-to-peer technology are still absent and wanting.

D. Regulators' Difficulties in Catching up with Interruptive Impacts of Blockchain

Regulators play a critical role in the blockchain industry. Their knowledge, decisions, and actions greatly affect how blockchain is going to develop. The major problem with regulators is that they face difficulties in catching up with the disruptive impacts that blockchain can bring to society, which can further result in ineffective decision-making. Regulators in both China and the United States—even worldwide—face the same problem.

The difficulties in catching up with technology interruption do not stem from the technical aspects of blockchain, but instead from the unpredictable effects of blockchain applications. Understanding the complex technical aspects of blockchain is easier than predicting its effects. A technical understanding of blockchain could be easily gained through consulting experts or studying relevant research and reports. On the other hand, predicting the effects of blockchain applications—including which industries blockchain can be effectively integrated into, what problems in the existing industries blockchain could solve or ameliorate and to what extent, and what new problems blockchain would create when implemented to deal with existing problems—is difficult. One reason is that blockchain has not seen large-scale implementations. Existing cases and their data are insufficient to analyze its effects.

Another reason is that regulators' attitudes toward blockchain implementation are very conservative when confronting the need to regulate the blockchain industry. They are reluctant to proactively experiment with blockchain applications to understand what true impacts blockchain could bring. Regulators serve as gatekeepers, not as entrepreneurs who are enthusiastic about inventing new technologies or carrying out their innovative thinking. Additionally, regulators do not want to be blamed if things go wrong. It is fair to say that regulators should be neutral in terms of technology's implementations to avoid adverse results brought about by progressive innovation. But continuously taking the "wait and see" approach could result in a "too late to regulate" dilemma. By then, the blockchain market could have experienced tremendous turmoil and market participants may have suffered a great loss.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

Although regulators have taken actions to understand blockchain, their efforts are not sufficient to issue effective and efficient blockchain policies and regulations. Some of regulators' responses are too hasty, which could result in investors or consumers' greater loss. The all-out ban on ICOs and cryptocurrency trading is illustrative.[75] Some rules are too strict to operate blockchain innovations. In an interview with the biggest cryptocurrency trading platform in the United States—Coinbase—their legal team complained that the strict securities laws and financial regulations prevent them from listing more cryptocurrencies and conducting fundraising via cryptocurrencies.[76] The unclear guidance regarding cryptocurrency escrow services further limits the business they can do. As a result, the U.S. cryptocurrency market shrinks, and many related businesses flow to other jurisdictions.

Regulators play a critical role in fixing problems in the market. Without properly overseeing the market and reacting to problems in a timely manner, regulators contribute to regulatory failure. As Coglianese suggests, a way to think of excellence lies in the types of actions a regulator takes in the course of regulating.[77] The failure to take effective actions sometimes results in unpleasant outcomes. The goal of implementing regulation is to yield publicly valued outcomes, such as reduced risks or improved outcomes. However, regulators' ineffective actions might fail to achieve this outcome.

II. WHAT ARE THE OBJECTIVES OF THE PROPOSED POLICIES AND REGULATIONS?

Concerning the objectives of existing blockchain policies and regulations, either explicitly stated or implicitly interpreted in the laws, regulations, policy documents, government announcements, and officials' speeches—China and the United States have made efforts to maintain a fair and efficient market, while simultaneously encouraging technology innovation. Under these objectives, existing policies and regulations have successfully addressed some issues in the blockchain space. Nevertheless, some problems continue to exist, and some new problems have appeared, as analyzed in the previous section.

Therefore, the proposed policies and regulations should include the following high-level and primary objectives: facilitating a fair and efficient market and promoting technology innovation. These are critical and worthy pursuits to properly

[75] Jiang, *supra* note 18, 349–51.

[76] Interview by Dr. Jiaying Jiang with Coinbase Legal Counsel (2019).

[77] ACHIEVING REGULATORY EXCELLENCE 10 (Cary Coglianese ed., 2016).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

guide blockchain development and deployment in a balanced market environment. Meanwhile, some adjustments should be made on the lower-level and secondary objectives, considering the unsolved problems and new issues.

A. A Fair and Efficient Market

While China and the United States both seek to establish and maintain a fair and efficient blockchain market, these two countries have slightly different interpretations and focuses of fulfilling these objectives. Specifically, China seeks to reduce cryptocurrency and ICO-related crimes to prevent market turmoil, provide a safer environment for consumers and SMEs, and integrate blockchain into existing markets smoothly.[78] Overall, "market safety and stability" has been an explicit goal in China's policy guidance in the blockchain space.[79] The United States, on the other hand, concentrates on protecting consumers and investors and strengthening criminal enforcement.[80]

While both countries intend to strengthen criminal enforcement of blockchain practice, to reduce scams and crimes, and protect market participants (investors, consumers, and entrepreneurs), China policymakers have an ambitious plan to integrate blockchain into existing markets—financial markets, supply chain markets, entertainment industries, and the judicial sector. In contrast, the United States does not have a national strategy to apply or implement blockchain. Due to the nature and mission of regulatory agencies in the United States, each regulatory agency may lay emphasis on achieving specific goals. Some regulatory agencies may have overlapping goals and conflicting interpretations for regulating the blockchain industry. In China, both governments and private entities promote blockchain applications and implementations. In the United States, private entities are the major players in advocating for blockchain while regulators act as gatekeepers and constantly adopt a "wait and see" approach.[81]

In addition to these existing interpretations and focus on a fair and efficient market, the objectives of proposed policies and regulations should especially look into the unsolved problems and tackle new problems under the existing regulatory

---

[78] Jiang, *supra* note 18, at 339–44.

[79] *Id.* at 339.

[80] *Regulatory Impact Assessment*, *supra* note 46, at 18–20.

[81] David J. Kappos, D. Scott Bennett, Michael E. Mariani & Sasha Rosenthal-Larrea, *United States Blockchain*, THE LEGAL 500 COUNTRY COMPAR. GUIDES (Oct. 29, 2021), https://www.cravath.com/a/web/f1XPajgBFUABNhTE51sdJ7/3eQYhm/legal-500-blockchain-comparative-guide-us-chapter-b.pdf%20p5 [https://perma.cc/3LU4-Z9HR].

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

regimes. Understanding why problems cannot be solved or alleviated and why new problems arise can help refine or adjust the lower-level and secondary objectives.

For instance, both countries seek to address fraud and crimes, but blockchain-related crimes become even more diverse and difficult to track over time. What new technologies are needed to address these crimes? Regarding the unprotected investors and consumers, what new mechanisms should be adopted for better protection? In terms of entrepreneurs' limited innovation on blockchain projects and regulators' difficulties in catching up with interruptive impacts of blockchain, is there a new framework to connect entrepreneurs and regulators in the same space sharing information and fostering innovation without too much additional cost? These are and should be novel pursuits of the proposed policies and regulations in order to achieve a fair and efficient blockchain market.

B. Technology Innovation

Technology innovation is China's national strategy and long-term policy objective. Promulgation of any technology-related policy or regulation should take this objective into account. Blockchain policies and regulations are no exception. China seeks to build a blockchain ecosystem connecting everything in cyberspace to standardize the blockchain industry and to acquire leading innovation capacities for blockchain.[82]

In addition to these existing pursuits, the objective of proposed blockchain policies and regulations for China should also consider Chinese President Xi's most recent call for more research and investment into blockchain.[83] He emphasized that blockchain is important to independent innovation and urged acceleration in the development of blockchain and its industry innovation.[84] Specifically, he enumerated six objectives to enhance the future work in blockchain.[85] China needs

---

[82] Jiang, *supra* note 18, at 344–49.

[83] *Xi Jinping Zai Zhongyang Zhengzhi Ju Di Shiba Ci Jiti Xuexi Shi Qiangdiao Ba Qukuailian Zuowei Hexin Jishu Zizhu Chuangxin Zhongyao Tupokou Jiakuai Tuijin Qukuailian Jishu he Chanye Chuangxin Fazhan* (习近平在中央政治局第十八次集体学习时强调 把区块链作为核心技术自主创新重要突破口 加快推动区块链技术和产业创新发展) [*During the 18th Collective Study of the Political Bureau of the Central Committee, Xi Jinping Emphasized on the Use of Blockchain as an Important Breakthrough in Independent Innovation of Core Technology and Accelerating the Development of Blockchain Technology and Industrial Innovation*], PEOPLE.CN (Oct. 25, 2019), http://cpc.people.com.cn/n1/2019/1025/c64094-31421403.html [https://perma.cc/E46H-JL9P].

[84] *Id.*

[85] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

to (1) strengthen research and improve innovation capacity, striving to keep China at the forefront of blockchain theory and practice; (2) promote collaboration and accelerate technology breakthroughs, providing technology support for blockchain; (3) work on blockchain standardization, enhancing the right to rule-making internationally; (4) speed up industry development, further opening up the innovation chain, application chain and value chain; (5) build blockchain ecosystem, accelerating the deep integration of blockchain and other cutting-edge information technologies such as artificial intelligence, big data, and the Internet of Things; and (6) cultivate a group of leading figures and high-level innovation teams.[86]

Technology innovation is also a policy or regulatory objective in the United States. Most blockchain-related policies and regulations exist in financial markets. Thus, the goal of technology innovation should be interpreted narrowly with a focus on financial markets, where regulators have been pretentiously and precariously placing their attention. Outside of these financial markets, for instance, blockchain-related policy has focused on innovation in supply chain management, innovation in protecting digital intellectual property for music or art, and its advancement in keeping record of government documents. However, such innovations may be beyond regulators' radar.

In the financial markets, different regulators may have slightly different aims around promoting innovation. Securities regulators have concluded that many cryptocurrencies are securities by applying Howey Test. However, they still leave room for innovation and try to see if blockchain can enable new forms of capital formation. Commodities and futures regulators have concluded that some cryptocurrencies are commodities subject to the Commodity Exchange Act. However, they also leave room for innovation by publishing two reports on smart contracts and wait to see how smart contracts can impact financial markets. Law enforcement officials keep their focus on balancing whether blockchain could be an innovation in the payment industry or just provide a new channel for criminal activities. Regulators need to conduct a cost-and-benefit analysis whenever they face technology interruption. One the one hand, regulators want to encourage blockchain innovation that could solve long-lasting problems in the financial markets, but on the other hand, they don't want to fuel the already very risky financial markets.

[86] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

III. WHAT ARE THE POLICY AND REGULATORY OPTIONS?

Policy and regulatory options are the instruments to deliver mechanisms that are most likely to achieve intended objectives surrounding blockchain.[87] The state can regulate an industry directly, or the regulatory function can be delegated to bodies beyond the state.[88] Under different arrangements, a number of instruments—policy and regulatory options—could be deployed.

In the blockchain space, regulators selecting the best policy and regulatory options should particularly lay eyes on the problems they intend to solve and consider how effectively they could solve the problems and achieve the intended objectives. Therefore, this Article proposes three options: command-and-control regulation, self-regulation, and technology-enabled co-regulation. Theoretically, an additional option, no policy and regulatory change, should also be considered as a baseline scenario. However, I argue that this approach—following the existing policy and regulatory framework and failing to implement policy and regulatory change—would not effectively solve many of the problems facing blockchain; rather, it would create new issues articulated in the aforementioned section. Thus, the discussion below intentionally excludes this approach.

In the Section below, I explain what these three options are and how they work. Technology-enabled co-regulation is both my preferred option and my regulatory suggestion for the blockchain industry. It is important to note my preferred option is industry and context-specific, which specifically addresses problems caused by the blockchain implementation in the financial markets. The approach is not a permanent solution to all blockchain problems. Instead, it's a temporary solution to the early stage blockchain implementation when market participants are still experimenting with novel blockchain products, services, or business models and when regulators and policymakers are still exploring their impacts. Once the blockchain market matures and people have sophisticated knowledge about blockchain innovations and their impacts, the regulatory approach could shift to command-and-control regulation or self-regulation, based on further studies and assessments.

It is also very important to note that this section does not intend to lay out every policy and regulation in great detail but presents a high-level outline explaining principles, components, and operations.

---

[87] *CEPA Strategy Guidance Note*, *supra* note 14, at 29.

[88] ROBERT BALDWIN, MARTIN CAVE & MARTIN LODGE, UNDERSTANDING REGULATION: THEORY, STRATEGY, AND PRACTICE 105 (2d ed. 2013).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

A. Command-and-Control Regulation

Gunningham and Rees suggested that regulation can be perceived on a spectrum "ranging from a detailed government command and control regulation to 'pure' self-regulation, with different points in the continuum encapsulating various kinds of co-regulation."[89] Following their suggestion, Bartle and Vass presented a figure to illustrate the extent of state involvement varying from noninvolvement to full involvement.[90]

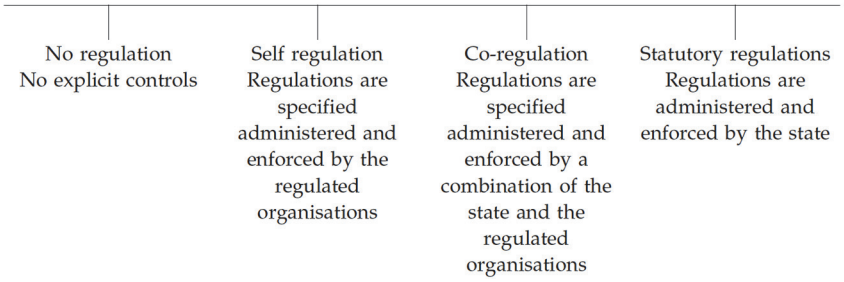


Figure 5.1 Regulatory spectrum[91]

According to this spectrum, the command-and-control regulation indicates that the state (regulators) administers and enforces rules. Just as Robert Baldwin et al. points out, "the essence of command and control . . . regulation is the exercise of influence by imposing standards backed by criminal sanctions."[92] Specifically, command and control can take place in the three traditional components of the separation of powers: legislation, enforcement, and adjudication.[93] Backed by the state authority, regulators take control in this regulatory relationship by issuing legislation, executive orders, and administrative rules. Regulators adjudicate if the

[89] Neil Gunningham & Joseph Rees, *Industry Self-Regulation: An Institutional Perspective*, 19 LAW & POL'Y 363, 366 (1997).

[90] IAN BARTLE & PETER VASS, SELF-REGULATION AND THE REGULATORY STATE: A SURVEY OF POLICY AND PRACTICE 19 (2005).

[91] *Id.*

[92] BALDWIN, CAVE & LODGE, *supra* note 88, at 106.

[93] National Telecommunications and Information Administration, *Chapter 1: Theory of Markets and Privacy*, U.S. DEP'T COM., https://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy [https://perma.cc/U7WU-2M2Q].

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

regulated groups violate these rules—initiating actions against these groups with binding effects of law.

Command-and-control regulation is commonly seen in environmental law.[94] Regulators set specific limits for pollution emissions and/or mandate that specific pollution-control technologies be used.[95] When the United States started passing comprehensive environmental laws in the late 1960s and early 1970s, a typical law specified how much pollution could be emitted out of a smokestack or a drainpipe and imposed penalties if that limit was exceed.[96] Other laws required the installation of certain equipment—for example, on automobile tailpipes or on smokestacks—to reduce pollution.[97]

Similarly, in the blockchain space, regulation could also consider the command-and-control approach where regulators dominate the regulatory process. The regulatory process generally consists of three stages: creating regulations; monitoring for compliance; and enforcing regulations—although the nature of regulations and the institutions used to create them may vary. To begin, regulators should create blockchain-related regulations. They can take the form of legislation, executive orders, or administrative rules. An existing department or office should administer and enforce regulations, or a new department or office could be created. This department or office can set up rules that entail some kind of licensing process to screen entry to an activity. Additionally, it may set out to control not merely the quality of a service or the manner of production but also the allocation of resources, products, or commodities and the prices charged to consumers or the profits made by enterprises.[98] Compliance monitoring can take many forms: having the blockchain entities file periodic reports, receiving complaints from the general public, or directly communicating with the blockchain company in question. Those responsible for enforcement against violators should adhere to the rules equally.

For instance, to reduce blockchain-related scams or fraud in the financial market, the government could create an office under an existing regulatory agency. This office would be set up specifically for monitoring blockchain practices and thus would be delegated powers to promulgate new rules; these rules would specify which

---

[94] OpenStax, *12.2 Command-and-Control Regulation—Principles of Economics*, BC OPEN TEXTBOOKS, https://opentextbc.ca/principlesofeconomics/chapter/12-2-command-and-control-regulation/ [https://perma.cc/XYN7-BPUR].

[95] *Id.*

[96] *Id.*

[97] *Id.*

[98] BALDWIN, CAVE & LODGE, *supra* note 88, at 107.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

blockchain business models are permitted and which are not (e.g. applications with high risk in causing scams or fraud, such as the use of cryptocurrencies for fundraising, would be prohibited), who are eligible investors to participate in cryptocurrency trading, and what amounts are permitted. Alternatively, the office could demand that blockchain service providers use specific technologies to track and identify any suspicious use of cryptocurrencies. The office could require blockchain entities to file periodic reports to disclose their state of compliance on the matters concerned. The general public could also file complaints to the office with respect to violations of certain rules. Rule violators would be denied the right to participate in the market or they would face other penalties.

B. Self-Regulation

Regulation can be carried out by the state or by a variety of other organizations—notably by self-regulatory institutions, such as professional bodies, trade associations; public interest groups, business partners, consumers; or corporations.[99] Self-regulation is a shift away from state regulation. There is no single definition of self-regulation. Larry Irving, former U.S. Assistant Secretary of Commerce, observed:

> At one end of the spectrum, the term is used quite narrowly, to refer only to those instances where the government has formally delegated the power to regulate, as in the delegation of securities industry oversight to the stock exchanges. At the other end of the spectrum, the term is used when the private sector perceives the need to regulate itself for whatever reason—to respond to consumer demand, to carry out its ethical beliefs, to enhance industry reputations, or to level the market playing field—and does so.[100]

Additionally, Graham suggested that "[s]elf regulation can be seen as the delegation of public policy tasks to private actors in an institutional form with one of the main objectives being the regulation of markets (industry) by the participants (players) within."[101] It is "a regulatory process whereby an industry-level organization (such as a trade association or a professional society), as opposed to a

[99] *Id.* at 137.

[100] Larry Irving, *Privacy Report—Introduction*, U.S. DEP'T COM., https://www.ntia.doc.gov/page/privacy-report-introduction [https://perma.cc/L3X5-682L].

[101] COSMO GRAHAM, ADMINISTRATIVE LAW AND GOVERNMENT ACTION: THE COURTS AND ALTERNATE MECHANISMS OF REVIEW 241 (Genevra Richardson & Hazel Genn eds., 1994).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

governmental- or firm-level, organization sets and enforces rules and standards relating to the conduct of firms in the industry."[102]

Diverse industries—such as health care, higher education, fashion, advertising, mining, marine fishing, professional sports, and nuclear power—have used self-regulatory processes to govern industry practices.[103] Specifically, self-regulation can address a variety of issues ranging from establishing industry standards, to developing and applying codes of professional ethics, to ensuring consumer confidence.[104]

Similarly, in the blockchain industry, self-regulation is a regulatory option that shifts rule-making power from public authority to the industry. It aims to have voluntary agreements among industry participants, who create, monitor, and enforce rules. The industry can have the same separation-of-powers structure as government regulation: legislation, enforcement, and adjudication. Self-regulation should be a response to both the absence of government regulation and the threat of excessive government regulation.

Self-regulation could take the form of self-regulatory organizations ("SROs"). SROs are the non-governmental organizations formed by the private sector to set standards, monitor for compliance, and enforce their rules.[105] SROs could establish rules that govern a specific industry rather than rules that apply across all industries.[106] For example, the National Advertising Review Council has created four specialized self-regulatory systems: the National Advertising Division, the Children's Advertising Review Unit, the National Advertising Review Board, and the Electronic Retailing Self-Regulation Program.[107] Each of these SROs develop rules tailored to meet a specific need, such as designing child-appropriate advertising and ensuring truth-in-advertising for direct-response marketing (e.g., infomercials).[108]

---

[102] Anil K. Gupta & Lawrence J. Lad, *Industry Self-Regulation: An Economic, Organizational, and Political Analysis*, 8 ACAD. MGMT. REV. 416, 417 (1983).

[103] *See, e.g.*, Gunningham & Rees, *supra* note 89.

[104] Daniel Castro, *Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising*, INFO. TECH. & INNOVATION FOUND. 1, 1 (Dec. 2011), https://itif.org/files/2011-self-regulation-online-behavioral-advertising.pdf [https://perma.cc/CB52-TXDR].

[105] *Id.* at 3.

[106] *Id.* at 4.

[107] *Id.*

[108] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

In the blockchain industry, self-regulation could also take the form of SROs, which should be industry- and content-specific. Because blockchain is involved in various industries, its applications or implementations in one industry are very different from those in other industries. It would be impractical to have one SRO and one set of rules that apply to all industries. For instance, in the legal space, blockchain's application in recording evidence is different from how it is used in finance, such as for cross-border payment. Rules for recording evidence should be different from those governing cross-border payments. SROs in the legal space would need legal experts to design rules for recording evidence while SROs in finance would look for experts with a financial background. In addition, SROs should also be content-specific because even in the same industry, blockchain's uses are different. Take the legal industry as an example. Rules governing evidence recording in court proceedings, which emphasize the authenticity of the evidence, should be different from rules governing blockchain's recording function at notary offices, which focuses on facilitating the notarization process, such as proof of ownership, proof of existence, and document ownership transfer.

Self-regulation in the blockchain industry taking the form of SROs consists of three steps: rule creation, monitoring for compliance, and rule enforcement. First, when crafting rules, SROs should consult sufficient stakeholders in the industry. Take finance as an example. In establishing rules to govern the blockchain-backed cryptocurrency market, an independent SRO specific for the cryptocurrency market should be established. The cryptocurrency SRO should consult cryptocurrency trading platforms, cryptocurrency listers, wallet providers, cryptocurrency traders (consumers), project investors, engineers behind the scenes, and even regulators. Regulators could make recommendations or deliver opinions on specific matters. Knowing the concerns and expectations of representative stakeholders serves as the foundation for making rules applicable and acceptable for all of them.

Next, SROs should commit to undertaking the monitoring of rule compliance. SROs should not only have systematic discovery process for any violations, but they should also create incentives and channels for industry participants to detect and disclose violations of rules. In the blockchain space, the discovery process could, in part, rely on technologies. For instance, artificial intelligence, machine learning, or data analytics could be used to analyze or identify suspicious transactions on blockchain. The mechanisms for incentivizing industry participants to detect and disclose violations of rules could also take account of the distinctive nature of blockchain by rewarding coins. For instance, if a user of a cryptocurrency platform discovers any wrongdoing of that platform, the user could disclose it to the SRO, and according to the rule, the user could be rewarded a certain amount of coins tradable on the platform. SROs should also provide more channels to receive complaints from the industry, not just from their members.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

Last but not least, rule enforcement is a critical component of self-regulation. SROs could enforce rules in several ways by investigating the complaints filed with them, conducting compliance reviews to determine whether covered entities are in compliance, and performing education and outreach to foster compliance with the requirements of the rules. Once a violation is identified, SROs could impose fines, corrective actions, or restraining orders. SROs could assess penalties on entities or individuals for any economic benefits they may have obtained due to noncompliance. The enforcement process could be kept confidential to avoid malice claims against competitors. However, if the violating firm or individual is not willing to resolve a violation, then the issue could be made public as a form of punishment. In the end, SROs could consider handing some cases to regulatory agencies or courts if the enforcement is not considered satisfactory.

C. Technology-Enabled Co-Regulation

Much of the current debate has been characterized by a choice between two mutually exclusive policy options: 'strict' command and control on one hand, and 'pure' self-regulation on the other.[109] In fact, as posited by Baldwin and Cave, "[t]here is not (…) a clear contrast or choice between self-regulation and a regulation by a state agency."[110] Self-regulation is an important alternative to public regulation, but it is rarely completely decoupled from public authority.[111] Therefore, co-regulation is a more feasible and common practice in an industry where regulations are specified and enforced by a combination of state and industry organizations. These organizations can be authorized by the state or agreed by industry participants, or both.[112]

Co-regulation is the regulatory approach I propose for regulating the blockchain industry. It should be supplemented and augmented by technology. This new approach represents a collaborative and technology-enabled paradigm.

Compared to the command-and-control approach, where regulators play a dominant role in the regulatory process, technology-enabled co-regulation calls for more industry participation. Compared to self-regulation, where the industry may have too much discretion, technology-enabled co-regulation reserves the right of

[109] BALDWIN, CAVE & LODGE, *supra* note 88, at 106.

[110] *Id.*

[111] *Id.*

[112] BARTLE & VASS, *supra* note 90, at 27.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

regulators' exercise of state power. Technology-enabled co-regulation acknowledges the fact that both regulators and the industry participants have critical roles to play in the regulatory process. In this regard, I agree with Bartle and Vass's position that the effectiveness and efficiency of regulation depends to a large extent on the interplay between the mixture of controls on the continuum between the state on the one hand and the industry or stakeholders on the other.[113] This position can also be seen in the examples provided by Ayers and Braithwaite.[114]

In addition to the discussion of *who* should play what role in carrying out the regulation, technology-enabled co-regulation also embraces the idea of *how* to regulate—what mechanisms to use to solve blockchain-specific problems and achieve its policy and regulatory objectives. In many cases, even if a clear division and cooperation between regulators and the regulated exists, without a functional mechanism embedded in the regulatory process, it will still be difficult for the blockchain regulation to achieve its intended effects. Therefore, this Article proposes a technology-enabled mechanism to address the novel and unprecedented regulatory issues in the blockchain space.

Technology-enabled co-regulation has two distinctive elements: a collaborative environment and a technology-enabled mechanism. In the section below, I will explain what these two elements are and how they work, as well as provide a high-level overview of this collaborative and technology-enabled paradigm.

1. Collaborative Environment

The first element of the technology-enabled co-regulation approach focuses on collaboration. Co-regulation aims at creating a collaborative environment—the environment among market participants, and between regulators and the regulated groups. Different from self-regulation, where collaboration happens mainly horizontally among regulated groups or market participants, co-regulation also encourages vertical collaboration between regulators and the regulated groups. Different from the command-and-control exercise with one-way order, co-regulation encourages two-way communications.

The design of the co-regulation model in the blockchain industry should allow the industry to enjoy considerable flexibility in shaping their own guidelines and allow consumer privacy groups or other industry participants to have a seat at the

[113] *Id.*

[114] IAN AYRES & JOHN BRAITHWAITE, RESPONSIVE REGULATION: TRANSCENDING THE DEREGULATION DEBATE 4 (1992).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

table. Regulators should set default requirements and retain general oversight authority to approve and enforce these guidelines.[115] Regulators and self-regulatory institutions "can negotiate the proper regulatory goals, collaborate on drafting standards and work cooperatively to enforce the standards against specific firms that violate them."[116] Stakeholders should also have a seat at the bargaining table, identify regulatory goals, and participate in standard-setting and rule enforcement.[117]

Exploring the co-regulation model in the blockchain industry does not vary significantly from that of other industries. As noted, the key idea of co-regulation is regulators with the regulated and stakeholders in rulemaking, monitoring for compliance, and rule enforcement. Thus, it is a collaborative process. But a unique aspect of dealing with the blockchain industry is that the collaborative process should start at a very early stage because of the novel implementation of blockchain technology in finance and limited knowledge of its impacts on the financial system.

Therefore, the section below emphasizes the early-stage collaboration among all participants in the regulatory process. I suggest that both China and the United States adopt regulatory sandboxes (vertical collaboration) and industry sandboxes (horizontal collaboration) for blockchain-related innovations.

a. Regulatory Sandboxes

The term "sandbox" originated from computer science.[118] A sandbox is a security mechanism for separating running programs, usually in an effort to mitigate system failures or software vulnerabilities from spreading.[119] Running a program in a sandbox can prevent it from doing any damage to the system: "[a] regulatory sandbox is a 'safe space' in which businesses can test innovative products, services, business models, and delivery mechanisms without immediately incurring all the

[115] Darren Sinclair, *Self-Regulation Versus Command and Control? Beyond False Dichotomies*, 19 LAW & POL'Y 529, 532 (1997); *see also* Ira S. Rubinstein, *The Future of Self-Regulation is Co-Regulation*, CAMBRIDGE HANDBOOK CONSUMER PRIV. 1, 2 (2016).

[116] Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 SEATTLE U. L. REV. 438, 460–64 (2011); *see also* Rubinstein, *supra* note 115, at 4.

[117] Rubinstein, *supra* note 115, at 1, 4.

[118] ENCYCLOPEDIA OF CRYPTOGRAPHY AND SECURITY 1076 (Hank C.A. Van Tilborg & Sushil Jajodia eds., 2d ed. 2011).

[119] Ian Goldberg, David Wagner, Randi Thomas & Eric Brewer, *A Secure Environment for Untrusted Helper Applications (Confining the Wily Hacker)*, *in* SAN JOSE, PROCEEDINGS OF THE SIXTH USENIX UNIX SECURITY SYMPOSIUM 2 (1996).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

normal regulatory consequences of engaging in the activity in question."[120] In a regulatory sandbox, regulators provide regulatory relief for startups to test innovative ideas in a limited or unlimited pool of consumers.[121] The idea of a regulatory sandbox was first proposed by the United Kingdom's Financial Conduct Authority ("FCA") in 2015[122] and was implemented in 2016.[123]

To become an eligible firm in the regulatory sandbox, the FCA set up five criteria necessary for entry: (1) scope of the firm: is the planned new solution designed for or supporting the financial services industry? (2) genuine innovation: is the new solution novel or significantly different to existing offerings? (3) consumer benefit: does the innovation offer a good prospect of identifiable benefit to consumers? (this criterion should continue to be met throughout the period of sandbox testing) (4) need for sandbox: what is the objective of testing? does the business have a genuine need for testing within the sandbox framework? (5) background research: has the business invested appropriate resources in developing the new solution, understanding the applicable regulations, and mitigating the risks?[124]

The regulatory sandbox offers three major relief options for eligible firms: (1) a tailored authorization process for new firms in the testing phase; (2) individual guidance for firms testing ideas that do not easily fit into the existing regulatory framework; and (3) waivers or no enforcement action letters in some circumstances.[125]

As of December 2019, mainland China did not have a regulatory sandbox in place. On December 5, 2019, Beijing's Municipal Bureau of Local Financial Supervision announced that Beijing would be the first to pilot an inclusive and prudent regulatory sandbox in China, under the guidance of the People's Bank of

[120] *Regulatory Sandbox*, FIN. CONDUCT AUTH. 2 (Nov. 2015), https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf [https://perma.cc/785D-936L].

[121] *Id.*

[122] *Id.*

[123] Press Release, Fin. Conduct Auth., Financial Conduct Authority's Regulatory Sandbox Opens to Applications (Sept. 5, 2016), https://www.fca.org.uk/news/press-releases/financial-conduct-authority%E2%80%99s-regulatory-sandbox-opens-applications [https://perma.cc/LBA6-T2YS].

[124] *Regulatory Sandbox*, *supra* note 120, at 7.

[125] *Id.* at 8–10.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

China ("PBOC").[126] Beijing aims to (1) operate the regulatory sandbox with "flexible management methods" such as information disclosure, product display and joint supervision; (2) guide licensed financial institutions to foster Fintech and improve the quality and efficiency of financial services under the premise of proper compliance and consumer protection; and (3) further create a safe, inclusive, and open environment for Fintech development.[127] No further details have been disclosed as to the design and operation of this regulatory sandbox implementation.

In the United States, the Consumer Financial Protection Bureau ("CFPB") was the first federal regulatory agency to have taken action by implementing a regulatory sandbox. In 2016, Republican Congressman Patrick McHenry introduced a bill to create a regulatory sandbox in the United States.[128] Later, the U.S. Treasury also called for the adoption of a regulatory sandbox to bolster the global competitiveness of the U.S. Fintech industry in July 2018.[129] In September 2018, the CFPB proposed a "disclosure sandbox" to test new ways to inform consumers.[130] After a year of collecting public comments, the CFPB finally issued three new policies to promote innovation and facilitate compliance in September 2019: the No-Action Letter Policy, Trial Disclosure Program Policy, and Compliance Assistance Sandbox

[126] *Beijing Shuaixian Shidian Jinrong Keji "Jianguan Shahe"* (北京率先试点金融科技"监管沙盒") [*Beijing Takes the Lead in Piloting FinTech "Regulatory Sandbox"*], GOV.CN (Dec. 5, 2019), http://www.gov.cn/xinwen/2019-12/05/content_5458821.htm [https://perma.cc/3R9L-J63M].

[127] *Id.*

[128] Financial Services Innovation Act of 2016, H.R. 6118, 114th Cong. (2016); *see also* Rachel Witkowski, *U.S. House Bill Aims to Set Up 'Sandbox' for Fintech Innovation*, WALL ST. J. (Sept. 22, 2016), https://www.wsj.com/articles/u-s-house-bill-aims-to-set-up-sandbox-for-fintech-innovation-1474539893m [https://perma.cc/3232-BFXS].

[129] STEVEN T. MNUCHIN & CRAIG S. PHILLIPS, U.S. DEP'T TREASURY, A FINANCIAL SYSTEM THAT CREATES ECONOMIC OPPORTUNITIES: NONBANK FINANCIALS, FINTECH, AND INNOVATION 222 (2018).

[130] *CFPB Office for Innovation Proposes "Disclosure Sandbox" for Companies to Test New Way to Inform Consumers*, CONSUMER FIN. PROT. BUREAU (Sept. 13, 2018), https://www.consumerfinance.gov/about-us/blog/cfpb-office-innovation-proposes-disclosure-sandbox-companies-test-new-ways-inform-consumers/ [https://perma.cc/P9XB-TWT2].

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

("CAS") Policy.[131] Thus far, the CFPB is the only regulatory agency at the federal level that has implemented a regulatory sandbox.[132] The results have yet to be seen.

b. Industry Sandboxes

The FCA also proposed industry-led sandboxes called Virtual Sandbox and Sandbox Umbrella.[133] A virtual sandbox is "an environment that enables firms to test their products and services in a virtual space without entering the real market" (for example, by testing with publicly available data sets, or with data provided by other firms through the virtual sandbox).[134] A sandbox umbrella means private-sector stakeholders acting together should consider setting up a not-for-profit sandbox umbrella company.[135] A company could seek authorization from the FCA and then allow innovative businesses to act as 'appointed representatives' for the duration.[136] Innovate Finance, an independent association representing the UK's Fintech community, further categorizes and defines Virtual Sandbox and Sandbox Umbrella as Industry Sandbox—"a shared off-market development environment where developers of Fintech solutions can access data, technologies and services from different providers in order to validate innovative ideas or address common industry challenges."[137] The term "is in effect loosely defined to include various industry-led initiatives such as API and data marketplaces, software development platforms and platforms for shared resources."[138]

Tsang suggests that Industry Sandbox can be very broadly referred to as a semi-open, membership-based platform where sandbox participants can share data, exchange resources, develop technologies, and explore solutions in a controlled

---

[131] *CFPB Issues Policies to Facilitate Compliance and Promote Innovation*, CONSUMER FIN. PROT. BUREAU (Sept. 10, 2019), https://www.consumerfinance.gov/about-us/newsroom/bureau-issues-policies-facilitate-compliance-promote-innovation/ [https://perma.cc/G78T-359X].

[132] Although Arizona has implemented a regulatory sandbox, this project only focuses on regulatory agencies at the federal level.

[133] INNOVATE FINANCE, A DEVELOPMENT IN OPEN INNOVATION: INDUSTRY SANDBOX CONSULTATION REPORT 8 (2017), https://issuu.com/innovatefinance/docs/industry_sandbox_consultation_repor [hereinafter INNOVATE FINANCE].

[134] *Id.*

[135] *Id.*

[136] *Id.*

[137] *Id.* at 4.

[138] Cheng-Yun Tsang, *From Industry Sandbox to Supervisory Control Box: Rethinking the Role of Regulators in the Era of FinTech*, 2019 J. LAW, TECH & POL'Y 355, 382.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

environment.[139] Different from a regulatory sandbox where regulators play a major role in design rules, selecting participants, and conducting assessments, an industry sandbox is led by the industry.[140] Industry participants could range widely, including Fintech startups, financial institutions, technology vendors, and professional services firms.[141] Regulators would be observers or other participants with no dominating role, or they would act in an auxiliary manner in an industry sandbox.[142]

To implement an industry sandbox, Innovate Finance outlines options for the design, governance, funding, and regulatory and academic engagement in a sandbox through studying best practices from industry and proprietary sandboxes globally, as well as other collaborative environments within and outside the financial services.[143] A noteworthy suggestion from Innovate Finance is that industry sandboxes could have the following components: application assessment mechanism, data sets, permissions for data access, reference architectures, product certification, showcase space, advisory space, analytics and audit tools, and participants' forum.[144]

In practice, an industry sandbox could take place in many forms. In China, the Andrew International Sandbox Institute claimed that it released the world's first blockchain-based industry sandbox, "Taishan Sandbox," in Qingdao on December 29, 2017.[145] With the support of its blockchain-based assessment tool, Taishan Sandbox provides a platform to evaluate blockchain projects by examining underlying technologies, whitepapers, code developers, communities, and activities. Taishan Sandbox 1.0 was released at the end of 2017 with the establishment of its cloud service. Taishan Sandbox 2.0 was released in June 2018 with the capability to test APIs, operations, and the quality of blockchains. With the support of its blockchain-based assessment tool, Taishan Sandbox conducted an assessment of 200 public blockchain projects with open-source data on GitHub such as Ethereum, Bitcoin, and Cardano. This assessment also signaled the formation of a public

[139] *Id.* at 383.

[140] *Id.* at 387; *see also* INNOVATE FINANCE, *supra* note 133, at 4.

[141] INNOVATIVE FINANCE, *supra* note 133, at 26.

[142] Tsang, *supra* note 138, at 389.

[143] INNOVATIVE FINANCE, *supra* note 133, at 25.

[144] *Id.* at 28.

[145] Information related to Taishan Sandbox was obtained through interviews with scientists and engineers at Tain De Xin Lian, the company owning Andrew International Sandbox Institute which released Taishan Sandbox.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

blockchain database for future assessment services. Taishan Sandbox is now a paid service that individuals, entities, or governments could purchase to examine the quality of a blockchain project.

Unlike China, an industry sandbox particularly for blockchain innovations in the United States has not yet been created. The Fintech industry has started to explore industry sandboxes, but there are very few success stories. However, a startup called FinTech Sandbox is an early pioneer of the industry sandbox, particularly with respect to industry sandboxes designed for blockchain innovations.[146] Specifically, Fintech Sandbox is a Boston-based nonprofit that enables financial technology entrepreneurs to build robotic products by providing access to critical data, development tools and a curated network of customers, entirely for free.[147] FinTech Sandbox works with thirty-seven industry-leading providers, three infrastructure partners, fifteen accelerators, and four value-add partners to offer participations a broad selection of data and other necessary support.[148] The application for FinTech Sandbox is open to all startups and is relatively clear. First, applicants conduct a self-assessment with nine questions and submit their application. Then, FinTech Sandbox conducts two rounds of interviews.[149] As its website shows, FinTech Sandbox provides services to 214 startups.[150] Not much information has been disclosed with respect to the progress.

c. High-Level Design of Sandboxes for the Blockchain Industry

FCA's regulatory sandbox regime and Innovate Finance's industry sandbox suggestions could be good resources for both China's and the United States' sandbox implementations. However, the design and operation of a sandbox can vary depending on the objectives, underlying legal and political frameworks, and supporting technical infrastructure. With respect to blockchain innovations, the effectiveness of any type of sandbox implementation will also vary enormously. This is partially due to its jurisdictional context, which varies widely, and partially to blockchain's involvement in various industries, a highly variable matter as well—factors which make generalization very difficult.

---

[146] Homepage, FINTECH SANDBOX, https://fintechsandbox.org/ [https://perma.cc/PQJ6-8MMZ].

[147] *Id.*

[148] *Partners*, FINTECH SANDBOX, https://fintechsandbox.org/partners [https://perma.cc/2WJL-ZN89].

[149] *How to Apply*, FINTECH SANDBOX, https://fintechsandbox.org/how-to-apply [https://perma.cc/M7DY-5K8C].

[150] *Startups*, FINTECH SANDBOX, https://fintechsandbox.org/startups [https://perma.cc/PB57-8HPV].

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

Therefore, I propose a broad framework for the design of regulatory and industry sandboxes. China and the United States can adjust their approaches to meet the needs of blockchain implementations in their respective jurisdictions. The design of a regulatory sandbox for blockchain innovations should take into account the following principles:

- Objectives: policy and regulatory objectives (market stability and safety and technology innovation) should be clearly articulated in the administrative rules or the legislation creating the regulatory sandbox to ensure its legitimacy.
- Objects: operating a sandbox should consider the urgency and efficiency of the need of voluntary participants from a variety of industries. In China, the regulatory sandbox should open to blockchain innovations in the financial space before introducing the entire blockchain ecosystem. In the United States each agency's regulatory sandbox should open to the blockchain ecosystem under its authority.
- Administrators: in China, financial regulatory departments at both central and municipal levels could administer a regulatory sandbox. In the United States, each regulatory agency should implement its own regulatory sandbox under its respective authority. The key is to hire or consult blockchain experts in addition to tasking regulators to design, operate, and moderate the sandbox.
- Criteria for entry: FCA's five criteria should be sufficient for considering potential sandbox participants.
- Relief options: options should be considered on a case-by-case basis. At the early stage, administrators should focus on individual guidance. After the number of firms testing the sandbox has reached a critical mass, administrators could tailor the authorization process for future firms with similar backgrounds. Authorization requirements should be proportionate to testing activities. Waivers or no enforcement letters could also be options, depending on what sector blockchain becomes involved in. The sectors that have less systematic risks would be more appropriate.
- Trial duration: 6–12 months.
- Follow up: administrators should follow up with firms that are still testing or have completed a trial. Administrators should continue to issue

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

interpretive guidance, advisory opinions, and legal opinions for improvement of rule implementation.[151]

- Disclosure: firms should disclose relevant information to administrators when applying for entry, and administrators should disclose operation progress to guide future firms that intend to enter the sandbox.
- Collaboration among regulators: regulatory authority is not segregated but sometimes overlaps. Thus, respective authorities need to collaborate. For instance, when the CFPB carries out the CAS Policy, other regulatory agencies may need to issue interpretive guidance or legal opinions to assist companies when a particular practice or activity also falls under its supervision.

By studying Taishan Sandbox and FinTech Sandbox, the industry sandbox implementation for blockchain innovations should consider the following principles:

- Administrators: any public or private entities, NGOs, and industry associations with sufficient technology support that could conduct tests and assessments for blockchain applications.
- Objects: in general, industry sandboxes should be open to the entire blockchain ecosystem on a voluntary basis. Industry sandboxes could also vary in industry (i.e. an industry sandbox for blockchain applications in finance or health) or functions (i.e. an industry sandbox for blockchain applications for payment systems or supply chain management).
- Criteria for entry: because blockchain applications are involved in various industries, criteria for entry should operate on a case-by-case basis. Criteria should be consistent, predictable, and non-discriminatory towards similar applicants from the same administrator. Criteria for entry to a commercial industry sandbox should be broadly or loosely defined, because it is a paid service. Administrators could streamline criteria for entry.
- Governance: administrators should set up a governance structure different from a regulatory sandbox, where regulators play a major role in setting up and operating the sandbox. An industry sandbox should have a

[151] Inspiration comes from the public comments to the CFPB regarding the CAS Policy; *see* Bureau of Consumer Fin. Protection, Policy on the Compliance Assistance Sandbox, Docket No. CFPB-2018-0042, 5 (Sept. 10, 2019); MARK WALPORT, U.K. GOV'T OFF. FOR SCI., FIN TECH FUTURES: THE UK AS A WORLD LEADER IN FINANCIAL TECHNOLOGIES 68 (2015), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/413095/gs-15-3-fintech-futures.pdf [https://perma.cc/9CZC-U3PE].

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

governance body, a daily operation team, dispute resolution procedures, and mechanisms to deal with complex relationships with all participants in the industry sandbox.

- Business model: a regulatory sandbox could be free of charge and could act as a forum for voluntary collaboration among participants. It could also be a commercial industry sandbox, providing testing services for a fee.
- Certification: administrators could issue certificates to certify that the tested application has certain properties or has the ability to perform certain functions.
- Participant forum: because the industry sandbox is a collaboration among industry participants, the administrator should provide forums for discussions and feedback.
- Relationship with regulators: regulators here should mainly be observers without exercising the power of regulatory intervention. However, different from Innovate Finance's "off market" proposal in which sandbox participants would test applications in an off-market setting, I suggest testing in a semi-real-life scenario. Administrators could invite regulators to provide support, such as a limited amount of real customer data, for the operation of industry sandboxes. Thus, sandbox participants would know whether their proposed products or services are viable and can sustain themselves in a live market. At the same time, industry sandboxes could also help regulators test technologies for regulatory sandboxes.
- Information/data protection: administrators should have mechanisms to protect applicants' information or data not intended for public disclosure.

2. Technology-Enabled Mechanisms

The second element of technology-enabled co-regulation emphasizes the role of technology in solving problems. I suggest using technology to regulate technology. The first "technology" refers to means or tools, such as cloud computing, artificial intelligence (machine learning and natural language processing), and big data analysis. The second "technology" refers to ends—in this case, blockchain applications or its implementations in various industries. In other words, I propose the use of technology-enabled tools to solve problems created by blockchain applications and implementations. The technology-based tools here refer to RegTech and SupTech.

To illustrate, on the spectrum below, the far left represents regulatory and supervisory processes without any technological support. For instance, banks

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

recorded all needed information in papers in the early days. Regulators reviewed paper records or conducted on-site inspections. Later, with the advent of computers and the internet, most records became digitalized and stored in the cloud. Regulators reviewed documents on the screen and conducted on-site inspections as needed. On the other end of the spectrum, with RegTech and SupTech, regulators and the regulated can automate supervisory and regulatory processes to a greater extent. Regulators can monitor the regulated activities in real-time and use various technologies to analyze those activities. If any suspicious activities are detected, regulators can develop an immediate technological response, such as pausing a transaction or moving funds between accounts.

The scope of RegTech and SupTech solutions is concentrated in the context of finance because of the nature of these technologies, which are designed to advance regulatory and supervisory processes. In addition, solutions concentrated in the context of finance are particularly critical for blockchain implementations in finance as blockchain has the most significant impacts on and potential in this space. Addressing problems in finance can pave the way for blockchain implementations and bring about positive impacts.

Although RegTech and Suptech, if appropriately implemented, can more effectively and efficiently address problems posed by blockchain and its applications, they are not perfect. Some problems remain, such as governance issues. Other issues, such as surveillance and censorship, could arise depending on the extent to which the regulators want to participate in the supervisory process. Maximizing the benefits of RegTech and SupTech requires rigorous and careful design and deployment of emerging technologies.

a. Regulatory Technology

The idea of RegTech was generated from the concept of financial technology, Fintech. Defined by the UK's Government Office for Science, Fintech integrates finance and technology in ways that will disrupt traditional financial models and business and provide an array of new services to businesses and consumers.[152] Fintech is the use of technologies to provide financial products and services. Fintech has the potential to be applied to regulation and compliance to make financial

[152] WALPORT, *supra* note 151.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

regulation and reporting more transparent, efficient, and effective—creating new mechanisms for RegTech.[153]

The FCA defines RegTech as a subset of Fintech that uses innovative and integrated technology to facilitate the delivery of regulatory requirements more effectively and efficiently than existing capacities.[154] However, the RegTech market keeps developing, so there is not yet an agreed-upon definition of RegTech and its typology.[155] Ernst & Young ("EY") defines RegTech as "the use of new technologies to address the increasingly dense data landscape required to meet regulatory compliance challenges."[156] Christophe Chazot, HSBC Group Head of Innovation, describes RegTech as "technological solutions to regulatory processes."[157] The Institute of International Finance ("IIF") defines RegTech as "the use of technologies to solve regulatory and compliance requirements more effectively and efficiently."[158] This section follows the Institute of International Finance's ("IIF") broad definition of Fintech.

Technologies used in RegTech are the same as those used in Fintech but with a specific focus on regulatory and compliance requirements. The IIF summarizes some of the most relevant technologies covering API, AI, machine learning, Internet of Things, big data analysis, distributed ledger technology, smart contracts, cloud computing, cryptography, and biometrics.[159] With these technologies, the following areas of RegTech solutions can be identified: compliance, identity management and

---

[153] *Id.*

[154] *Id.*

[155] *Fintech, Regtech and Suptech: What They Mean for Financial Supervision*, TORONTO CENTRE 8 (Aug. 2017), https://res.torontocentre.org/guidedocs/FinTech%20RegTech%20and%20SupTech%20-%20What%20They%20Mean%20for%20Financial%20Supervision%20FINAL.pdf [https://perma.cc/ENY4-H3A3] [hereinafter *Fintech, Regtech and Suptech*].

[156] Anita Bafna et al., *Regulatory Technology (RefTech)*, ERNST & YOUNG LLP, 2 (2019), https://assets.ey.com/content/dam/ey-sites/ey-com/en_us/topics/financial-services/ey-regulatory-technology-regtech.pdf?download.

[157] *RegTech: Exploring Solutions for Regulatory Challenges*, INST. INT'L FIN. 2 (Oct. 2015), https://www.iif.com/Portals/0/Files/content/Innovation/10_01_2015_regtech_exploring_solutions.pdf [https://perma.cc/M3JS-KR5V].

[158] *Regtech in Financial Services: Technology Solutions for Compliance and Reporting*, INST. INT'L FIN. 3 (Mar. 2016), https://www.iif.com/Portals/0/Files/private/iif-regtech_in_financial_services_-_solutions_for_compliance_and_reporting.pdf?Ver=2019-01-04-142943-690 [https://perma.cc/JX2E-EQ4R].

[159] *Fintech, Regtech and Suptech*, *supra* note 155, at 4–5.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

control, risk management, regulatory reporting, transaction monitoring, and trading in financial markets.[160]

Take RegTech's solution in compliance as an example. RegTech can help identify and keep track of changes in regulatory requirements at local or global levels and automate real-time monitoring of compliance levels and compliance risk, based on the analysis of operational and other data.[161] This form of automated compliance may be called "dynamic compliance"—that is, regulatory requirements are embedded into information technology protocols to ensure continuous compliance and confirm whether the data reported to supervisors is accurate and relevant.[162]

In addition, based on the EY Horizon Scanner (a global database of over 16,000 Fintech firms), 1,300+ companies identified themselves as RegTech.[163] Below are examples of various RegTech solutions across the companies' regulatory compliance capabilities.[164]

[160] *Id.* at 9–10.

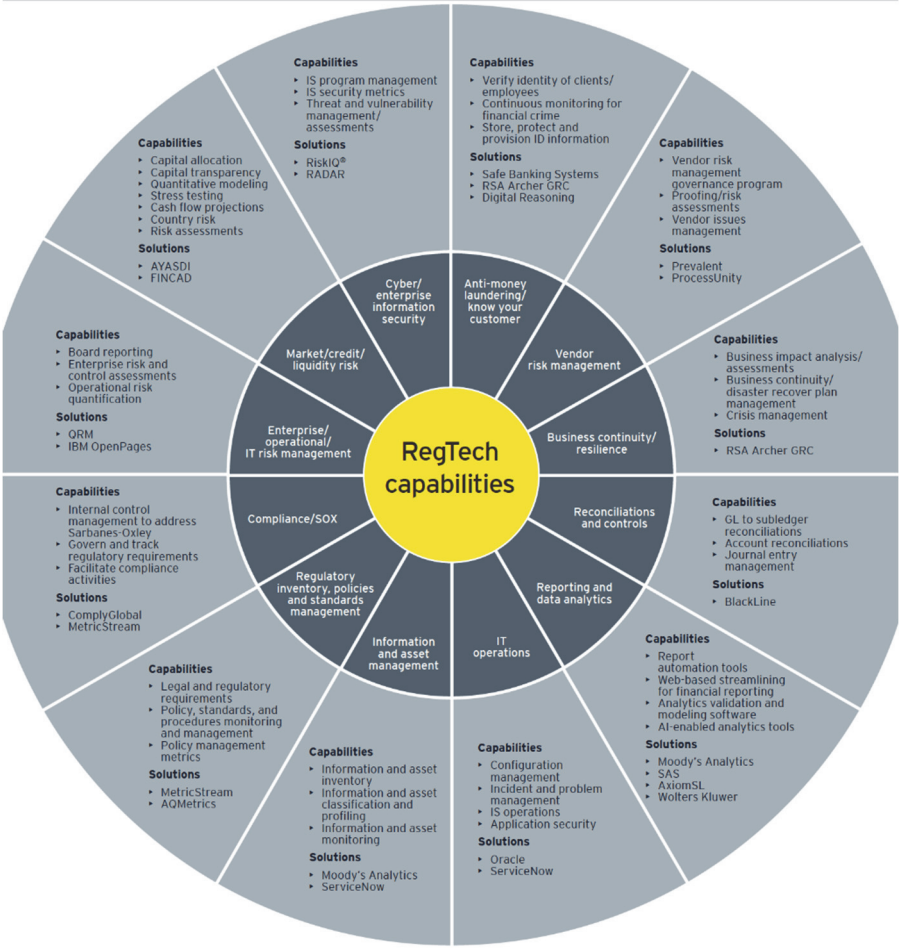
[161] *Id.* at 9.

[162] *Id.*

[163] Bafna et al., *supra* note 156, at 9.

[164] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu



Source: EY regulatory technology (RegTech) brief 2019[165]

b. Supervisory Technology

SupTech was first mentioned by the UK's Government Office for Science when it was contemplated within the context of RegTech.[166] Later discussions and literature gradually distinguished the use of the two terms, with SupTech starting to

[165] *Id.*

[166] Tsang, *supra* note 138, at 394.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

tackle challenges faced by supervisory agencies.[167] The differences between RegTech and SupTech have been addressed by a scholar in a recent piece:

> RegTech assists regulated institutions in complying with laws and regulations, whereas SupTech enables financial regulators to more effectively and efficiently carry out supervisory missions and oversight. RegTech emphasizes on the ability of the regulated institutions to understand the regulatory position and interact with regulators during the compliance process, whereas SupTech focuses on the need to improve the efficiency and quality of the supervisory process and regulatory rulemaking.[168]

SupTech could offer new supervisory approaches and transform the regulatory process. It has the potential to shift away from "current supervisory approaches based on past data, lengthy onsite inspection and often delayed supervisory action towards a pro-active, forward-looking supervision that relies on better data collection and sophisticated data analytics, and greater storage and mobility capacity such as by using cloud computing."[169]

Take data collection as an example. The prevalent approach by many supervisory agencies is to collect business data periodically via standard report templates.[170] There are several problems with this approach including, limited flexibility for the supervisor to manipulate data, the costly data aggregation process, involving manual procedures, the high costs of reporting granular data or greater volumes of data when using templates, and potential inconsistency of indicators across different templates.[171]

SupTech provides several new approaches: (1) data-input approach where reporting institutions could automatically package business data in a standard and highly granular format; (2) data-pull approach where raw business data are sourced directly from the institutions' operational system by automated processes triggered and controlled by the supervisory agency; (3) real-time access so that the supervisor pulls or sees operational data at will instead of pre-determined reporting periods;

---

[167] *Fintech, Regtech & Suptech*, *supra* note 155, at 8.

[168] Tsang, *supra* note 138, at 394.

[169] *Fintech, Regtech and Suptech*, *supra* note 155, at 10.

[170] *Id.*

[171] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

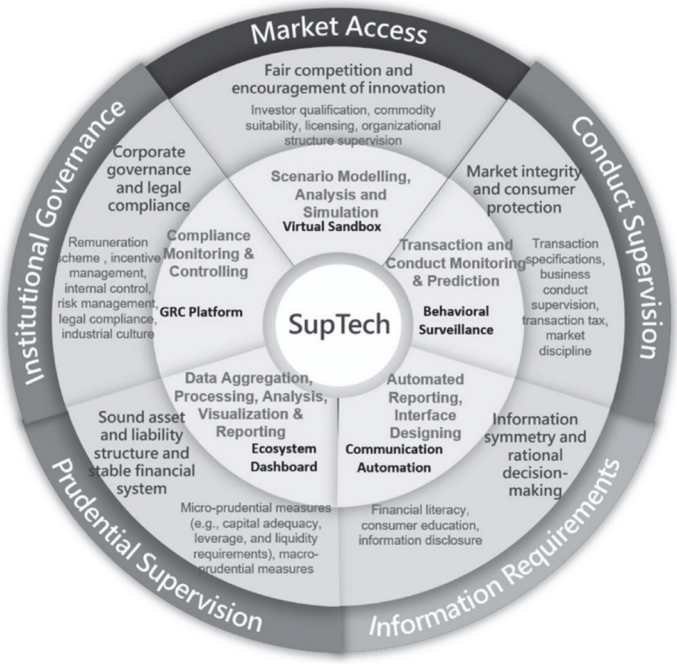
(4) reporting utilities where SupTech could create reporting utilities interpreting reporting rules in a format that is readable by computers; (5) gathering intelligence from unstructured data so that supervisors could be relieved from time-consuming tasks such as reading numerous .pdf files, searching the Internet, etc.; and (6) regulatory submissions and data quality management which could benefit supervisors in jurisdictions where these tasks involve manual procedures.[172]

Tsang proposed a SupTech roadmap for possible future development. He estimates SupTech will play an important role in five dimensions: namely, market access, information requirements, prudential supervision, and institutional governance.[173]

[172] *Id.* at 11.

[173] Cheng-Yun Tsang, *A Tentative Analytical Framework and Developing Roadmap for SupTech*, 37 MGM'T REV. 105, 114 (2018).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu



Source: Cheng-Yun Tsang, *A Tentative Analytical Framework and Developing Roadmap for SupTech.*[174]

c. High-Level Design of RegTech and SupTech for Blockchain Regulation

Blockchain's implementations in the financial sector primarily exist in the use of cryptocurrencies, payments, and managing transactions related to trade and commerce.[175] As addressed in the first section, scams and fraudulent activities using blockchain are overwhelmingly present in the financial market. A root cause is information asymmetry, but many factors worsen the situation. For instance, the existing financial system is ineffective in identifying bad actors and suspicious transactions with blockchain. Regulatory fragmentation—owing to the borderless nature of blockchain—results in ineffective and inefficient law enforcement. The

[174] *Id.*

[175] Dean Hobbs, Rich de Moll & David Griswold, *Crunch Time IV: Blockchain for Finance*, DELOITTE 22 (2018), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance-transformation/us-ft-crunch-time-blockchain-finance.pdf [https://perma.cc/244E-NGD7].

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

demanding regulatory and supervisory requirements also result in inefficient compliance, reporting, and supervision.[176]

All these issues could benefit from RegTech and SupTech solutions. First, a new design of blockchain infrastructure can be used for real-time monitoring and enforcement (if needed) of the transactions in the blockchain. This could create a new supervisory approach. Tsai proposed a new design of blockchain for trade finance: Trade Blockchain ("TBC") and Account Blockchain ("ABC").[177] TBC stores information at the transactional level, while ABC stores account information.[178] Splitting traditional blockchain into these two blockchains allows one to optimize the system with respect to monitoring and enforcement.[179] Compared to the early blockchain design where a blockchain is both a trade blockchain and account blockchain at the same time, this new design of blockchain is more efficient in trade finance applications.

In this new design, a regulatory agency can participate in the TBC as a node with voting rights. This node cannot only inspect transaction data in the TBC on a real-time basis, but also can halt suspicious transactions immediately. Compared to the traditional supervisory model where the regulated entity needs to submit data periodically via standard report templates, or regulators conduct lengthy off-site or on-site inspection, this new blockchain infrastructure allows regulators to participate in the operational system directly, getting access to the data in a timely manner to meet the supervisory purpose. Additionally, in the traditional supervisory model, regulators can only take action after transactions are completed and reported to them. With this new model, regulators can take enforcement actions during the transaction.

Second, the regulated groups and regulators can also benefit from the use of technologies such as machine learning, robotics, and artificial intelligence to organize, analyze, and interpret data. Many of blockchain's uses in finance—cryptocurrency trading, payments, and transactions related to trade and commerce transactions—involve large sets of data. To address the problems of blockchain's uses in finance it is necessary to tackle problems in the data. Tackling problems in data involves the process of organizing, analyzing, or interpreting data. EY

---

[176] Douglas W. Arner et al., *Fintech and Regtech: Enabling Innovation While Preserving Financial Stability*, 18 GEO. J. INT'L AFF. 47, 57 (2017).

[177] Wei-Tek Tsai et al., *A System View of Financial Blockchains*, *in* 2016 IEEE SYMPOSIUM ON SERVICE-ORIENTED SYSTEM ENGINEERING (SOSE) 450, 455–57 (2016).

[178] *Id.* at 455–56.

[179] *Id.* at 456.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

introduced a new, next-generation data architecture which can help with organizing data:

> Next-generation data architecture is a data-lake-based architecture with unified sourcing and consumption, and flexible and iterative data models. It differs from traditional data warehouses that contain numerous hops, rigid data models and manual processes. Through the implementation of data lakes, firms have the capability to consolidate data into a single source across multiple source systems. Data lakes consisting of a data ingestion layer, conformed layer and analytical layer allow data to be cleansed, mapped, transformed and reconciled at different levels. Source data can be profiled as it is ingested to test data quality and fit for purpose. Data can be harmonized across disparate systems and provide a data aggregation layer for downstream systems to consume. In addition, data lakes provide the ability to quickly ingest more data and scale horizontally.[180]

In this design, the key is to have the regulated firms use a single platform to consolidate upstream source systems and quickly ingest data in a controlled environment. In addition, many other technologies are helpful for organizing, analyzing, and interpreting data, just as introduced by the IFF:

> Data mining algorithms based on machine learning can organize large sets of data, even if this data is unstructured and of a low quality, such as sets of emails, pdfs and spoken word. It can also improve the interpretation of low-quality data outputs from payments system. Machine learning can create self-improving and more accurate methods for data analysis, modeling and forecasting as needed for stress testing. In the future, artificial intelligence could even be applied in software automatically interpreting new regulations.[181]

Third, technologies such as application programming interfaces ("APIs"), cloud computing, and smart contracts can automate regulatory reporting, compliance, and the supervisory processes. APIs that allow for interoperability ensure that different software programs can communicate with each other.[182] Cloud computing could allow for automated reporting of data to regulators. For instance, if a new regulation requires cryptocurrency trading platforms to report the identity

[180] Bafna et al., *supra* note 156, at 6.

[181] *Regtech in Financial Services: Technology Solutions for Compliance and Reporting*, *supra* note 158, at 3.

[182] Kevin Wentzel, *How is Interoperability Changing Software Development*, KOPIS (Mar. 28, 2019), https://kopisusa.com/interoperability-software-development/ [https://perma.cc/9GG2-AST5].

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

information of every newly joined member to regulators, this cryptocurrency platform can store members' identity information in the cloud shared with the regulators. The moment it uploads the identity information to the cloud, it fulfills the reporting requirement automatically.

Smart contracts can automate compliance, reporting, or supervisory processes by executing codes. The idea is to translate rules legible by humans (in the form of words) into machine-readable languages (in the form of code) and design a triggering condition to run codes.[183] The moment the codes run, rules are executed accordingly. Thus, this specific regulatory or supervisory requirement is met.

For example, OpenLaw allows employers to simultaneously withhold federal wage withholdings from the salaries that they pay their employees.[184] Every minute employees are paid, a portion of their salary is withheld, and timely withholding payments are tracked on the blockchain. The withholding amounts and matching employer tax obligations are immediately remitted to the IRS in real time through smart contracts—making the collection of revenue instantaneous.[185] To do this, tax provisions must be first translated into codes, and then a design must be created to trigger a condition to execute the codes. In this case, the triggering condition is "every minute employees are paid."[186] Smart contracts then "withhold amounts matching employer tax obligations and immediately remit the amounts to the IRS."[187] The moment smart contracts complete the execution, this employer's compliance with tax law is also completed.

IV. WHAT ARE THE POSSIBLE IMPACTS OF THESE OPTIONS?

The purpose of estimating the impacts of these policy options is to understand whether the options could generate their intended effects—namely, solving problems and achieving policy and regulatory objectives. Thus, the impacts should consider all stakeholders through the inquiry of who is impacted by a specific regulatory

[183] Cai Weide (蔡维德) & Jiang Jiaying (姜嘉莹), *Qukuailian Zhongguo Meng Zhi San: Zidong Zhixing Jiang Dianfu Faxue Yanjiu, Falü Zhidu he Falü Shijian* (区块链中国梦之三：自动执行将颠覆法学研究、法律制度和法律实践) [*The Third Chinese Dream of Blockchain: Automatic Execution will Subvert Legal Research, Legal System and Legal Practice*], JINSE CAIJING (Nov. 9, 2018).

[184] OpenLaw, *Code as Law: Using Ethereum Smart Contracts to Ensure Compliance with Federal Tax Law*, Medium, CONSENSYS MEDIA (May 30, 2018), https://media.consensys.net/code-as-law-using-ethereum-smart-contracts-to-ensure-compliance-with-federal-tax-law-3fc67cb7b956 [https://perma.cc/8KVS-3QUA].

[185] *Id.*

[186] *Id.*

[187] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

option in what way, as well as the impacts on regulators, such as whether the policy increases or simplifies their administrative burdens. In addition, the potential risks and uncertainties of policy options cannot be ignored.

A. Impacts of Command-and-Control Regulation

In the field of environmental law, command-and-control approach has had positive impacts. For example, in the United States:

> Command-and-control policy has been highly successful in protecting and cleaning up the US environment. In 1970, the Environmental Protection Agency (EPA) was created to oversee all environmental laws. In the same year, the Clean Air Act was enacted to address air pollution. Just two years later, in 1972, Congress passed and the president signed the far-reaching Clean Water Act. These command-and-control environmental laws, and their amendments and updates, have been largely responsible for America's cleaner air and water in recent decades.[188]

Similarly, in the blockchain space, China's all-out ban, announced on September 4, 2017, falls under the command-and-control approach, because regulators demanded that all cryptocurrency trading platforms halt their trading businesses, delist all cryptocurrencies, and return investments. All ICO projects also had to stop immediately. Cryptocurrency trading platforms and ICO project issuers had no choice but to follow the demand. This command-and-control approach did directly reduce blockchain- and cryptocurrency-related fraud and crimes due to the ban of any related activities. However, it was not the best approach to reduce such crime because not only did service providers, investors, and consumers suffer a great loss, but also fraud and crime persisted in other channels.

Similarly, if we posit a command-and-control regulation to address specific problems brought by blockchain implementations, it could probably solve the problems and achieve specific goals quickly and directly because the strength of command-and-control rules are that the force of law can be used to impose fixed standards with immediacy and to prohibit activities not conforming to such standards.[189] Regulators could also easily monitor and enforce command-and-control regulation, which would provide a safer and more stable market. Enforcement backed by state authority could also effectively deter misconduct. Command-and-control rules can give industry participants a clear signal with respect to regulators'

[188] OpenStax, *supra* note 94.

[189] BALDWIN, CAVE & LODGE, *supra* note 88, at 107.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

attitudes on certain matters, which provide certainty for better decision making. In addition, as a gatekeeper of an industry, regulators could be fair in interest allocation among industry participants.

However, the command-and-control regulation does have flaws. This section highlights three of the most salient problems. First, the command-and-control regulation is likely to be less cost-effective. Command-and-control policies have the propensity to set up rules in great detail. The costs for rulemaking could not only become a burden for the regulatory agencies, but also the regulated groups. The regulatory agencies may have limited expertise because blockchain's involvements in various industries are quite novel, so they must seek the help of outside experts, which increase time and financial costs. The regulated groups' burden of compliance would impede them (especially blockchain startups with limited sources) from allocating funding to value-added activities (i.e., less innovative products or services). In the end, the additional compliance costs could be internalized and carried by consumers purchasing their blockchain products and services.

Second, the command-and-control regulation is inflexible. The process of creating and amending rules takes a long time and is complicated owing to regulatory agencies' overlapping realms of authority, as well as the novelty of the technology itself. It could be not as adaptable to the rapid changes taking place in the blockchain industry. For instance, when rules were established to regulate ICOs, the market soon invented Initial Exchange Offerings ("IEOs"), and later Security Token Offerings ("STOs") appeared. Rules made through the command-and-control paradigm can never catch up with the rapid changes of the market, which results in ineffective regulation. In addition, a command-and-control regulation usually requires the same standards for many regulated groups. This means that a command-and-control regulation draws no distinctions between firms that would find it easy and inexpensive to meet the standard and firms that might find it difficult and costly to meet the standard. It might also ignore the fact that some firms might not need to apply the same standard as other firms in order to achieve the same goal.

Consider a situation wherein Blockchain Company A provides cryptocurrency trading services and Blockchain Company B provides government record-keeping services. Both are blockchain service providers, but they have different technological standards to meet the requirement of reducing scams or fraud. Blockchain Company A might have to adopt machine learning and automated data analytics for real-time inspection of each of its transactions, which is more difficult and expensive, while Blockchain Company B would only need to use data verification tools to guarantee the accuracy of the data stored, which is less expensive and easier. If constrained by the same technology requirements, it would be ineffective and efficient for both companies to meet the same goal.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

Third, a command-and-control regulation may lead to capture. In command-and-control regulation, the relationships between regulators and the regulated might tend to become too close, leading to capture—the pursuit of some of the regulated enterprises' interests, rather than those of the public at large.[190] This is particularly the case in the blockchain space. Without up-to-date knowledge of blockchain and first-hand information about this industry's operation, regulators must rely to some extent on the cooperation of the regulated firms when drawing up and enforcing rules. This gives the regulated firms leverage over regulatory procedures and objectives, a leverage that, over time, produces capture.[191]

B. Impacts of Self-Regulation

The impacts of self-regulation are twofold. On the one hand, self-regulation benefits the blockchain industry by creating flexible regulatory environment, providing industry expertise for effective rulemaking, and reducing information asymmetry in the blockchain industry. As a result, technology innovation and market stability and safety are enhanced. On the other hand, the effectiveness of rule monitoring and enforcement could be controversial. Self-regulation also presents governance and free-rider problems. These problems may affect the effective protection towards investors and consumers.

First, self-regulation would benefit the blockchain industry by creating a flexible regulatory environment, which could foster technology innovation. Regulation in the blockchain space has special considerations. Regulation not only needs to support the open and decentralized network architecture of blockchain applications and implementations; it also needs to form a flexible response to the dynamic and ongoing evolution of blockchain innovation in various sectors. Self-regulation allows industry experts to review current activities, identify best practices, and develop these into industry guidelines. The guidelines continue to evolve over time in response to feedback from industry leaders. This more flexible regulatory environment may allow firms to operate more efficiently and minimize compliance costs. Flexible regulations tend to maximize economic efficiency by providing firms multiple pathways for innovation. SROs may be more likely to use less stringent "moving target" regulations that change over time in response to the market and social norms. This allows for both incremental and radical innovation. The flexibility of self-regulation also means that SROs may be more experimental than regulatory agencies and more willing to test rules since they can more easily retract them.

---

[190] *Id.*; *see also* CHRISTOPHER HOOD, EXPLAINING ECONOMIC POLICY REVERSALS 21 (1994).

[191] BALDWIN, CAVE & LODGE, *supra* note 88, at 107.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

Second, self-regulation provides industry expertise for rulemaking. When industry participants come together to develop rules, those involved are likely to have a higher degree of technical and industry expertise than outside regulators. This is particularly true in the blockchain industry. Many blockchain applications and implementations are quite novel. Participants involved in designing and operating them would have better first-hand knowledge with respect to the problems and underlying causes than those who are not involved in the process. Developing rules from the bottom up would be more down-to-earth and can directly address the root causes and target problems effectively. Rules made by market participants and designed for them to follow are more likely to place the blockchain market in order.

Third, self-regulation can help reduce information asymmetry in the blockchain market, which could effectively reduce blockchain-related scams and crimes, because SROs act as independent third-party organizations to evaluate compliance with standards. SROs could disclose firms' information and status via periodical reports or prompt online updates. Consumers and investors can get more information about a firm's compliance status, history of rule violations, response to punishment, and so on. With such information, consumers can make better informed decisions.

However, self-regulation does not come without limitations.

The first limitation is that the enforceability of rules is questionable. Some claim that SROs may lack enforceable power because they are not backed by the state authority. SROs may not impose meaningful sanctions on industry players.[192] Self-regulatory standards are, according to critics, usually weak, enforcement is ineffective, and punishment is often secret and mild.[193] Therefore, the unenforceability of rules further results in inefficient compensation and deterrence.

However, this limitation is arguable. Some argue that SROs can be self-policing organizations, particularly when the institutions are designed to eliminate conflicts of interest.[194] If conflicts between different interest groups are well-addressed, rules under this situation are more acceptable and can more easily be carried out by industry participants. In addition, most rules are either made by joint efforts of industry representatives or agreed upon by members of SROs once they join the

[192] Monroe Price & Stefaan Verhulst, *The Concept of Self-Regulation and the Internet*, *in* PROTECTING OUR CHILDREN ON THE INTERNET: TOWARDS A NEW CULTURE OF RESPONSIBILITY 133, 148 (Jens Waltermann & Marcel Machill eds., 2000).

[193] *Id.*

[194] Castro, *supra* note 104, at 6.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

SROs. Once a certain mass of industry participants has been reached, industry representatives or members of SROs face increased peer pressure and public expectation. They face reputation and opportunity risks once they offend rules made or agreed upon by them. Therefore, the chance for noncompliance is low.

The second limitation is that self-regulation inevitably presents governance issues, as the interests of members are necessarily divergent. Rather than operating in the public interest, critics may assume that SROs operate purely to protect the interests of individual firms or the industry as a whole.[195] This statement is particularly true when the interests of a particular firm or industry and the public do not align.[196] In numerous studies, reference has also been made to the tendency of self-regulatory bodies to act anti-competitively on access requirements and prices, so that members' interests, rather than those of the public, are served.[197]

In the blockchain industry, the most lucrative business model is running cryptocurrency trading platforms. If an SRO makes rules specifically for regulating cryptocurrency trading practices, governance issues can easily occur. Owners of cryptocurrency trading platforms have strong incentive to become members of SROs with rule-making power, while consumers, i.e., cryptocurrency traders—especially individual traders—have less incentive to do the same. It is very likely that these owners or their agencies can become members of SROs, because rulemaking needs expertise with firsthand knowledge in the matter concerned. If owners have a say in rulemaking, it would be hard to argue that they are impartial and do not act in their own interests (i.e., making rules favorable for themselves). It is also hard to argue that the public interest is served.

The third limitation is an economic limitation that SROs face the free-rider problem.[198] To be effective, an SRO may set rules for an industry, including firms

---

[195] *Id.* at 9; *see also* Anthony Ogus, *Rethinking Self-Regulation*, 15 OXFORD J. LEGAL STUD. 97, 98–99 (1995).

[196] *Id.*

[197] BALDWIN, CAVE & LODGE, *supra* note 88, at 142; *see also* RICHARD L. ABEL, THE LEGAL PROFESSION IN ENGLAND AND WALES 250–58 (1988); *see* Ogus, *supra* note 195, at 99 (indicating that the OFT has noted that the large majority of trade associations have neither the power nor the will to exercise effective control over those who breach codes of practice); *see* OFF. OF FAIR TRADING, RAISING STANDARDS OF CONSUMER CARE: PROGRESSING BEYOND CODES OF PRACTICE 16–17 (1998) ("Trade associations, set up for the benefit of members, frequently are neither comfortable nor effective in the role of sectoral regulator.").

[198] Castro, *supra* note 104, at 8; *see also* Thomas A. Hemphill, *Self-Regulating Industry Behavior: Antitrust Limitations and Trade Association Codes of Conduct*, 11 J. BUS. ETHICS 915, 916 (1992).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

that do not participate in the SRO.[199] These "outsider" firms obtain all of the benefits of the regulatory regime without paying any of the costs.[200] If an SRO specifies entry requirements for certain blockchain products or services, and members of this SRO comply with rules at certain costs, those entities providing the same products stay outside the SRO would be taking advantage of the system by not paying certain costs and lowering prices for the products or services, while attracting more clients. Thus, this system could be unfair to dues-paying businesses.

C. Impacts of Technology-Enabled Co-Regulation

The impacts of technology-enabled co-regulation are analyzed from two perspectives: the implementation of a collaborative environment with the use of a regulatory sandbox and industry sandbox, and the implementation of technology-enabled schemes with the support of RegTech and SupTech.

1. Impacts of a Collaborative Environment Supported by Sandboxes

The most significant merit of implementing sandboxes is that sandboxes can create a space that allows new ideas to be piloted and new technologies to be tested in virtual or semi-virtual environments. Therefore, sandboxes pose no threat to consumers and investors.

With regulatory sandboxes, through dialogues, regulators could learn from private sectors and understand the real problems. Firms would find it easier and less expensive to comply with reduced requirements and the process could be quicker and simpler than regular processes. Lower costs and efficiency in processes would encourage innovation. Under the situation of no enforcement letters or individual guidance, firms will also find certainty and clarity with the understanding that regulators will not take enforcement actions against their testing activities.

Industry sandboxes can reduce risks customers otherwise would face and costs entrepreneurs would otherwise bear. If implemented in an off-market scenario, consumers would face no detrimental risk. If the testing occurs in a semi-real-life scenario, the risks are, at least, controllable. Firms can obtain customers' consent collectively to test products and services and while simultaneously, address consumers' concerns. The cost is relatively inexpensive for firms to test their ideas because costs are shared by all sandbox members instead of one firm.

---

[199] Castro, *supra* note 104, at 8.

[200] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

Regulatory and industry sandboxes can foster innovation because regulators and industry participants pull resources and efforts to test novel ideas. Joint efforts are always better than one startup testing an idea with limited resources and talents. Running sandboxes also signals to the market that regulators value innovation.

However, some negative impacts of implementing regulatory and industry sandboxes in the blockchain space are hard to evade. Sandboxes represent a closer regulator–industry collaboration and thus can subject regulators to a greater regulatory capture and further undermine supervisory effectiveness.[201] Regulatory capture is unavoidable because it "depend[s] on constant interaction between the industry and regulators" and "we would want some degree of coordination between government and banks for the implementation of monetary policy and the maintenance of financial stability."[202]

Regulatory capture can be even more severe when sandboxes are used. In the first place, the novel nature of blockchain and its innovative implementations create difficulties for regulators to make proper rules for the industry. Such difficulties further result in regulators' greater reliance on the industry in rulemaking. This gives the industry (or sometimes participants of sandboxes) a degree of leverage over blockchain-related rulemaking. Interest groups in the sandboxes may take advantage of such rule-making power to protect certain interest groups or the industry as a whole. Thus, private distortion of public purposes could occur. Regulators then may fail to protect the general public—investors or consumers—as intended.

The regulatory sandbox regime is not cost-free: the regulated groups can create extra work and costs for regulators. If regulators adopt restricted authorization, firms still need to apply for authorization before being able to test new solutions. If regulators issue no enforcement letters or individual guidance, regulators will need to undertake extra work. The work will be resource-intensive and complex for regulators if a great number of firms require no enforcement letters or individual guidance. Some of the novel issues may arise outside regulators' capability to provide guidance.

Another concern is that the industry sandbox may not achieve its intended effects. The first reason is that an industry sandbox is difficult to set up. Neither a consistent definition of industry sandbox nor a standard model exists. Criteria for setting up an industry sandbox have yet to be developed by the industry. Second,

---

[201] Tsang, *supra* note 138, at 393.

[202] *Id.*; *see also* Lawrence G. Baxter, *Understanding Regulatory Capture: An Academic Perspective from the United States*, *in* MAKING GOOD FINANCIAL REGULATION: TOWARDS A POLICY RESPONSE TO REGULATORY CAPTURE 31, 34 (Stefano Cagliari ed., 2012).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

setting up an industry sandbox could be resource-intensive and thus hard to accomplish because interests are not always aligned. Such action requires effort from participants with various backgrounds and expertise, which is not always guaranteed and it needs to balance the interests of various participating groups. Setting up an industry sandbox may also require legislative change, which could take significant time and resources.

2. Impacts of a Technology-Enabled Scheme Supported by RegTech and SupTech

The most effective and direct impact of implementing RegTech and SupTech is that they will increase operational efficiency and reduce costs and human errors as a result of increased automation, which performs work in a more accurate and efficient manner. Essentially, the use of RegTech or SupTech in compliance, reporting, or the supervisory process is the use of technologies to replace some work usually done by humans. Technology can do such work more quickly and accurately. It is growing at an exponential rate, whereas human brains are not used to thinking in exponential parameters;[203] they are used to thinking linearly.[204] Therefore, technology can process specific and narrow tasks with a faster speed than humans. Much regulatory, reporting, or supervisory work is repetitive and structured in a way that can be simplified—and improved—by technology.[205] Technology can process tasks objectively and mechanically, which reduces the chance of introducing human errors.

Biometrics and blockchain are great applications for RegTech and SupTech solutions. The use of biometrics and blockchain for identification can enable timely, cost-effective, and reliable identity checks for regulators. Biometrics is already allowing for large efficiency and security improvements by automating client identification, which is required by Know Your Customer ("KYC") regulation.[206] KYC processes previously required paper-based documents like national identity cards, passports, and driving licenses, which are vulnerable to fraud and easy to forge. Implementing a biometric verification process along with paper-based documentation will ensure users' true identities and accelerate the verification

[203] Andrew Sullivan, Technology and the Law—New Opportunities for Lawyers and Their Clients 2 (2015) (unpublished manuscript), https://papers.ssrn.com/abstract=2648538 [https://perma.cc/HL7P-5M2F].

[204] *Id.*

[205] Brian Simpson, *Algorithms or Advocacy: Does the Legal Profession Have a Future in a Digital World?*, 25 INFO. & COMM. TECH. L. 50, 58 (2016).

[206] *Regtech in Financial Services: Technology Solutions for Compliance and Reporting*, *supra* note 158, at 4.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

process by reducing unnecessary and repetitive work, issues which are directly responsible for operational delays.

In addition, if paired with biometrics, blockchain can efficiently address two major threats—identity theft and data breaches—that compromise a user's capability to establish her identity. Identity theft and data breaches can be prevented through hashes which mark the original data with another value. This value can only be decoded by looking up the value from a hash table, which may be an array, database, or other data structure. The use of hashes can thus greatly reduce the chance of personal information being hacked and stolen and prevent illegal use of others' personal information. If every cryptocurrency holder can establish her identity, then whatever transactions she made will be on the record. This will help track illegal conduct and attribute liabilities. In reverse, it will prevent users from conducting illegal activities at the beginning.

The new design of blockchain architecture is a great SupTech solution that allows regulators to monitor and pursue enforcement actions in a timely manner. Real-time monitoring and prompt actions cannot only increase supervisory efficiency and lower costs, but also protect consumers from involving themselves in illegal transactions. Consumers' risks are reduced accordingly because of regulators' ability to take enforcement actions during a transaction and not after the transaction. Additionally, this new design is critical for law enforcement agencies. If they can participate as a node in every transaction in the TBC, the overall illegal transactions with blockchain will be reduced not only because of the real time monitor and enforcement, but also the effects of deterrence.

A better ability to organize, analyze, and interpret data can bring many positive impacts to both regulators and regulated groups to better manage blockchain's uses in finance. It helps regulators carry out their regulatory and supervisory responsibility more accurately and efficiently. Regulators can utilize automated data analytics or machine learning to automatically analyze transaction data and stop suspicious transactions immediately or take supervisory actions in a preemptive manner based on predictive behavioral analysis.

As a result of accurate data analytics, the regulated group can spot issues prior to reporting and improve their ability in risk management. Financial industries heavily rely on third-party service providers to provide risk management services, leading to increasing risk in outsourcing operations.[207] If the regulated entities have a better ability in risk management, not only will they reduce the risk in outsourcing risk, but they will also reduce the costs. With better organization of data—which

[207] Bafna et al., *supra* note 156, at 9.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

used to be large sets, unstructured, and of a low quality—they can efficiently meet the granular requirements needed for regulatory reporting. With data forecasting and enhanced analytics, the regulated groups can prevent future risks in transactions, further protecting consumers or anyone involved in the transactions. This is particularly useful in cryptocurrency trading. Cryptocurrency trading markets do not have the same regulatory oversight as the securities market does. Thus, participants in cryptocurrency trading do not have the same protection as securities traders do. If cryptocurrency trading platforms can use machine learning, data analytics, and artificial intelligence to identify or forecast illegal activities, not only can trading platforms avoid suffering any loss, but their customers can also be protected.

However, this technology-enabled scheme is unavoidably associated with some negative concerns. Such concerns are echoed by technology-related privacy and security issues, as well as technologies' failure in generating intended effects. For example, most RegTech and SupTech solutions require information to be digitalized and shared among multiple parties, which may introduce privacy and security concerns. The privacy and security of such digitalized information (data) not only requires a sound management plan but also IT support. These two requirements are not always guaranteed. A sound management plan sometimes is difficult to fulfill because of deficiencies in standards for managing and transferring data, protecting data privacy, and utilizing certain security mechanisms. IT support is not always up to date. It is sometimes fragmented because IT infrastructures in different systems may not be consistent and compatible with others.

The new design of blockchain infrastructure can partially address the privacy concern. The design of TBC will ensure that only those who need to see data can see data, and data will be available for a limited time only. This design is consistent with the Windhover Principles,[208] whereby individuals can keep their privacy while regulators can perform legitimate auditing and enforcement.[209] Privacy, in some cases, is more difficult to address because it is incompatible with the intention of certain use cases. For instance, the intention of APIs or cloud applications is to have multiple parties share data in the cloud to reduce information asymmetry and allow for automated reporting. Privacy and such intention are somehow incompatible.

Another concern is that automation may fail to produce its intended effects. In the case of using smart contracts to ensure compliance, some may ask: how to pick up the correct interpretation of a rule to translate into codes when many

[208] FROM BITCOIN TO BURNING MAN AND BEYOND: THE QUEST FOR IDENTITY AND AUTONOMY IN A DIGITAL SOCIETY (John H. Clippinger & David Bollier eds., 2014).

[209] Tsai et al., *supra* note 177, at 455.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

interpretations may exist? Assuming one could exhaust all interpretations, how would a machine choose which interpretation to execute? Under these situations, smart contracts seem unintelligent and inflexible.

It is true that not all regulatory or supervisory processes are automatable. With smart contracts, the idea is not to translate all rules into codes but only rules that are clear and translatable. Those translatable rules can be divided into multiple single tasks in codes, performed by machine efficiently and objectively. Rule execution (i.e., rule enforcement), in many cases, needs human judgment and subjective assessment, which should not be simply delegated to machine. For instance, in the previous case, human judgment may still play a dominant role in deciding what part of income is taxable, if one is eligible for tax returns, or if a local taxing authority should require a special report from individuals or entities. However, smart contracts can do much better job in calculating multi-jurisdictional taxes or transferring a certain amount to the IRS. Thus, to maximize the value of automation is to have each part do what each is good at.

V. HOW DO THE OPTIONS COMPARE?

The purpose of option comparison is to provide justification for the preferred option—technology-enabled co-regulation. Within the debate (positive and negative impacts) of three options (see the chart below), a way to conduct comparison is to assess how technology-enabled co-regulation can complement and address the limitations, or negative impacts, of the command-and-control regulation, as well as self-regulation. If technology-enabled co-regulation and the other two options can all produce the same positive impacts, the assessment should focus on how technology-enabled co-regulation can efficiently achieve the intended goal without sacrificing some benefits or generating certain costs.

This Part describes why technology-enabled co-regulation may be better than other policy options based on the following factors: cost, flexibility, enforceability, regulators' up-to-date knowledge, and regulatory capture.

Policy options	Positive impacts	Negative impacts
Command and control regulation	- achieving specific goals shortly and directly in some cases; - relative ease of monitoring and enforcement; - deterrence of misconduct because of clear punishment; - a clear signal on certain matters, giving	- high costs; - inflexibility in rule-making or changing rules; - regulatory capture

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

Policy options		Positive impacts	Negative impacts
		certainty to the industry; - being fair in interest allocation	
Self-regulation		- a flexible regulatory environment; - industry expertise for rule-making; - effective in reducing information asymmetry	- questionable enforceability; - governance issues; - free-rider problem
Technology-enabled co-regulation	Regulatory Sandbox and Industry Sandbox	- a safe space for innovation; - higher chance for regulators to keep updated regarding relevant knowledge; - support from a variety of expertise and resources	- regulatory capture; - not cost-free: the regulated groups and additional pressure and costs for regulators under the regulatory sandbox regime
	RegTech and SupTech	- increased operational efficiency and reduced costs and human errors, as a result of increased automation; - biometrics and blockchain enabling timely, cost-effective, and reliable identity checks for regulators; - improved security owing to biometrics and blockchain addressing identity threat and data breaches; - real-time monitoring and enforcement; - improved risk management	- privacy and security concerns; - effectiveness concern

First, every option has costs. A command-and-control regulation is expensive, and self-regulation is not cheap. Technology-enabled co-regulation, on the other hand, is cost-effective largely due to automation.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

Among these three options, the command-and-control regulation is the most expensive option. The costs lie in rulemaking, implementation, and compliance. Formulating laws or regulations in a formal setting, no matter whether they take the form of legislation or administrative orders, takes a long time and incurs significant costs. Implementing and complying with laws or regulations also entails significant costs, and efficiency losses associated with regulation can be high. Moreover, government regulation can be a blunt instrument and may impose unintended costs (on the customers of other, competitive industries) without any tangible benefits.[210]

Compared to a command-and-control approach, the "voluntary" nature of self-regulation implies, sometimes misleadingly, that the costs associated with compliance are lower and fall on those markets at which regulation is targeted. However, this is not accurate in some cases. For instance, Viviane Reding, Vice President of the European Commission, has stated that the complex and fragmented nature of the data-protection policies (a type of self-regulation) in the twenty-seven member states costs businesses 2.3 billion euros annually.[211] Not only do businesses face higher costs, which are then passed on to consumers, but consumers may also miss out on certain online services. For example, strict privacy regulations have led Google to cease development of its Street View map feature in Germany.

Technology-enabled co-regulation outweighs the costs of self-regulation because, to some extent, technologies greatly reduce costs by automating regulatory controls, procedures, and compliance requirements. Of course, it is not cost-free for regulatory agencies or the industry to set up sandboxes, nor RegTech or SupTech solutions. In a regulatory sandbox, if implemented in the form of restricted authorization, firms still need to apply for authorization before being able to test new solutions, which also comes with costs; if in the form of no enforcement letters or individual guidance, regulators would also need to bear the cost to do extra work. However, the greater automation empowered by RegTech and SupTech in reporting, compliance, and supervision greatly reduces intensive labor costs. If smart contracts can be widely used, the costs for rule enforcement would also see a greater cost-effective future.

The reduced costs may not directly achieve policy and regulatory objectives—achieving a fair and efficient market and fostering technology innovation—but indirectly, the answer is positive. With reduced costs in reporting and compliance,

---

[210] Price & Verhulst, *supra* note 192, at 145.

[211] Viviane Reding, Vice-President of the European Commission & EU Justice Commissioner, Building Trust in the Digital Single Market: Reforming the EU's Data Protection Rules (Nov. 28, 2011), https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_11_814 [https://perma.cc/G4YZ-MJF9].

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

the regulated can place money in more value-added work, which promotes innovation. With reduced costs in supervision, regulators could allocate more funding and resources to addressing other issues and providing more guidance to the market.

Second, technology-enabled co-regulation outdoes command and control policy in providing flexibility in rulemaking, monitoring for compliance, and rule enforcement. In the command-and-control option, rulemaking takes place in a formal setting which is very unadaptable to the rapidly changing blockchain market. On the other hand, technology-enabled co-regulation, either in the form of regulatory sandboxes or industry sandboxes, is more flexible to make changes in a shorter time and format. Such an informal setting can have rules to keep up with the rapidly changing market, as well as the flexibility to articulate different rules for different entities taking account of various situations. Such flexibility avoids applying the same rule to different entities, whereby some may find it easy and cheap to comply with, while some find it difficult and expensive to do so.

Third, technology-enabled co-regulation is better than self-regulation because enforceability is less controversial. Different from self-regulation where SROs create, monitor, and enforce rules—and thus may raise enforceability concerns as SROs are not backed by state authority—in technology-enabled co-regulation, regulators play a critical role in administering regulatory sandboxes. Thus, the same critique that the rulemaking institution may not be able to enforce rules does not exist, as regulators undertake the major responsibility of rule creation, monitoring for compliance, and rule enforcement. With respect to industry sandboxes, regulators can be a regular sandbox participant to oversee rule enforcement. If regulators act as pure observers, enforceability could become an issue. However, industry sandboxes do not prohibit regulators' involvement once an industry sandbox is ineffective under some circumstances. With RegTech and SupTech, enforceability is less an issue because technologies provide more channels for regulators to enforce rules more effectively and efficiently.

Fourth, among all three policy options, regulators' up-to-date knowledge in the blockchain industry can be greatly fulfilled with technology-enabled co-regulation. Regulators' knowledge is also a signal in determining the effectiveness and efficiency of blockchain regulations. In a self-regulation environment, regulators' participation is very limited. With a command-and-control approach, although regulators have a relative ease of monitoring for compliance and enforcement, their knowledge is still limited because the one-way order lacks feedback from the markets. Only in technology-enabled co-regulation can regulators obtain the most up-to-date knowledge and real-time information about the regulated entities.

Specifically, regulatory and industry sandboxes allow regulators to more closely observe the industry's use of new technologies, practices, and standards in a

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

controlled environment and further develop the proper regulatory response to challenges arising from it.[212] With SupTech and RegTech, collecting granular data that is not constrained by pre-formatted templates gives regulators more flexibility to build customized indicators and ensure the calculation is correct and harmonized across reporting entities, allowing them to create any desired report in any format at any time, and to conduct a much wider range of analysis. Granular data could give richer and more timely regulatory insights, particularly if advanced data analytical tools are used.

Fifth, with RegTech and SupTech, technology-enabled co-regulation provides a better solution for regulatory capture. As analyzed in the previous section, the command-and-control approach and technology-enabled co-regulation (the use of sandboxes) both present a regulatory capture issue. Self-regulation can also lead to the use of self-regulating power to protect certain interest groups or the industry as a whole instead of the public interest.

However, technology-enabled co-regulation is the superior option because it partially provides a solution. Baxter prosed five strategies to address capture: "adequate regulatory capacity; meaningful transparency; meaningful access by stakeholders, external checks; and internal checks [within the industry itself]."[213] After a close examination of these five strategies, Tsang found that "the key lies in whether the regulator has sufficient data and capacity and whether the industry has meaningful access to the formation of regulations and a self-constraint culture."[214] Thus, he argued that "access to meaningful and prompt data plays the most important role as data empowers regulators' supervisory capacity and informs their regulatory making, which will sufficiently enhance transparency and accountability."[215] Technology-enabled co-regulation empowered by RegTech and SupTech, to some extent, enables regulators with genuine and timely data which will enhance transparency and accountability.

A new design of the data-lake-based architecture with unified sourcing and consumption, and flexible and iterative data models, also provides a great channel for meaningful transparency. The use of technologies such as machine learning, robotics, and artificial intelligence to organize, analyze, and interpret data, and other automation technologies such as APIs and cloud computing, also empower external checks by the regulators and internal checks within the industry. Therefore, the

[212] Tsang, *supra* note 138, at 389.

[213] Baxter, *supra* note 202, at 35.

[214] Tsang, *supra* note 138, at 393–94.

[215] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu

design of RegTech and SupTech in the technology-enabled co-regulation regime can partially address the capture issue by empowering regulators to have real insights into blockchain industry members' intentions and behaviors and further to take actions to enhance its supervisory capacity.

VI. CONCLUSION

After singling out the most salient problems that have emerged from existing policies and regulations and identifying the common policy and regulatory objectives shared by the two countries, this Article proposes three policy and regulatory options: command-and-control regulation, self-regulation, and technology-enabled co-regulation. Each option can have positive impacts that effectively tackle some problems and achieve some policy and regulatory objectives. However, none of these options are perfect, as they all come with certain costs and negative impacts.

Technology-enabled co-regulation is the preferred option. With the support of sandboxes, this approach can create a space that allows new ideas to be piloted and new technologies to be tested in virtual and semi-virtual environments with very limited threat to consumers, investors, and the market. With the implementation of RegTech and SupTech, Technology-enabled co-regulation can increase operational efficiency, reduce costs and human errors due to increased automation, help regulators carry out their regulatory and supervisory responsibility more accurately and efficiently, and enable the regulated group to improve their ability in risk management.

Technology-enabled co-regulation is not perfect. It can subject regulators to a greater regulatory capture, and it is not cost-free. The impacts of the industry sandbox regime could be hard to estimate owing to the difficulties of setting up industry sandboxes and balancing the interests of various interest groups. The implementation of RegTech and SupTech is unavoidably associated with some negative concerns echoed by technology-related privacy and security issues, as well as technologies' failure in generating intended effects. However, technology-enabled co-regulation is the preferred option because it outperforms the other two options in cost, flexibility, enforceability, regulators' up-to-date knowledge, and regulatory capture. It helps to solve problems more effectively and achieve policy and regulatory objectives more efficiently.

Overall, this collaborative and technology-enabled paradigm supports blockchain implementation that reaches the potential of blockchain technology. In a broader sense, it presents a new regulatory approach that provides a framework for further interaction between law and emerging technologies, which will become a trend in the twenty-first century. In the meantime, seeing how policies and regulations can guide and affect the blockchain industry as well as making proper adjustments to advance this industry is and will continue to be a learning process.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2022.876
http://lawreview.law.pitt.edu