# 1AC

## 1AC---Blockchain

### 1AC---Blockchain ADV

#### Contention 1 is BLOCKCHAIN.

#### Blockchain development is inevitable, but beyond the scope of antitrust---the narrow focus on the ‘firm’ is fundamentally inapplicable, that creates an anticompetitive environment that’ll centralize applications and limit uptake.

Dr. Thibault Schrepel 21, PhD in Antitrust Law from Université Paris-Saclay, LLM in International Law and Legal Studies from the Brooklyn Law School, Associate Professor of Law at VU Amsterdam University, Faculty Affiliate and Creator and Director of the Computational Antitrust Project at the Stanford University CodeX Center, Blockchain + Antitrust: The Decentralization Formula, p. 134-136

5 A WIN-WIN THEORY

The creation of a legal fiction around blockchain nuclei will benefit both antitrust and blockchain communities. By facilitating the enforcement of the rule of law, blockchain participants will indeed be able to enforce antitrust laws or be sanctioned when infringing them.

5.1 A Win for Antitrust

The theory of granularity helps create a legal fiction for public permissionless blockchains and private ones (whose governance is not vertical). Surely, other legal fictions will be proposed in the coming years. Regardless of its name, creating a legal fiction is a prerequisite for applying the rule of law to blockchain layer 1. The ability to do so is crucial.

First, the creation of a legal fiction ensures that blockchains do not escape antitrust enforcement for theoretical reasons. This is a prerequisite before discussing the technical barriers to enforce antitrust against illegal practices (see the following chapters). Second, assigning liability to the right entity ensures that whoever controls blockchains will have a strong(er) incentive to comply with legal requirements. The urge to play by the rules is always stronger when one knows that the rules could actually be enforced. As such, antitrust will not only protect actors that lie outside of blockchain ecosystems; it will also protect those inside the blockchain who cannot stop the anticompetitive practices. Antitrust will free blockchain layer 1 from these practices.

5.2 A Win for Blockchain

Creating a distinct legal fiction centered on blockchains’ nucleus will present an important step forward for related ecosystems. First, the creation of such fiction will attribute rights to blockchains’ nuclei. This will legitimize collaboration between blockchain participants in the nucleus that would otherwise have been prohibited. Indeed, I have explained that antitrust law defines a legal fiction (e.g., the firm) and then applies only to the effects that occur outside of it. Decisions that produce an effect outside of the blockchain nucleus will be submitted to antitrust law. In contrast, decisions taken by the nucleus whose effects are purely internal to that entity will be exempt from antitrust scrutiny.98

Second, creating a legal fiction will increase legal certainty pertaining to the application of antitrust law and regulation. Decades of research suggest that doing so will encourage investments,99 and will make entrepreneurs want to “embark” on the creation of innovative products and services.100 Blockchain communities say so themselves: regulatory issues and accompanying legal uncertainty are the most important reasons preventing greater investment and adoption of blockchain technology.101 The sooner a legal fiction is created, the better for the ecosystem. In its absence, one could imagine court decisions holding all blockchain participants liable for wrongdoings, even though most of them will not have the power to prevent these illegal practices.

Finally, the creation of a legal fiction will give the nucleus the right to institute legal actions and claim damages in cases of antitrust violation, whether caused by another nucleus or a non-blockchain entity. Going back to Christopher Stone’s writing, blockchain’s legal fictions will be able to institute legal actions in their name; courts will calculate injury to them, and relief will be run to their benefit. For example, one could imagine that a blockchain layer 1 (illegally) excluded from the market by another blockchain that engaged in predatory pricing could introduce a valid claim before the courts or antitrust agencies. In the following chapters, I will explain how this will play out when it comes to collusion and monopolization practices.

For all these reasons, creating an antitrust-related legal fiction will be invaluable for blockchain ecosystems and, ultimately, for decentralization. It will protect them from illegal practices that could hinder blockchain’s capacity to decentralize the economy. There is no doubt that centralized companies will multiply illegal behaviors toward blockchain ecosystems in the years to come, as we will see in the coming chapters. Being recognized as a legal entity will allow them to protect their interests and innovate toward decentralization.

6 CHAPTER SUMMARY AND BEYOND

In this chapter, 1 have used the theory of granularity to open the blockchain “black box.” First, I have discussed blockchain governance and shown how the influence of different participants neutralize their position. As no block- chain participant can control the blockchain by itself - and ensure its survival - I have explained that a group of participants may want to come together to achieve common goals. By doing so, they free themselves from other participants’ constraints and end up forming the blockchain nucleus.

The blockchain nucleus gives rise to an entity that should benefit from rights, but could also be held liable for illegal conducts. I have shown how this would work by analyzing relevant markets and market power, evaluating anticompetitive practices and assigning liability.

#### Anticompetitive exclusions and lack of legal certainty over the applicability of antitrust dry up investment and innovation, which artificially consolidates digital ecosystems.

Dr. Thibault Schrepel 21, PhD in Antitrust Law from Université Paris-Saclay, LLM in International Law and Legal Studies from the Brooklyn Law School, Associate Professor of Law at VU Amsterdam University, Faculty Affiliate and Creator and Director of the Computational Antitrust Project at the Stanford University CodeX Center, Blockchain + Antitrust: The Decentralization Formula, p. 74-77

2 THE SPECTER OF NEUTRALIZATION

I hope to have convinced readers that antitrust law and blockchain contribute to similar, if not identical, objectives (i.e., preserving agents’ ability to act freely in the market, which entails the decentralization of decision-making processes).42 For that reason, one might expect that both communities would work hand in hand to achieve decentralization. And yet, despite pursuing a common goal, blockchain and antitrust may end up canceling each other out. Here’s why.

2.1 One Goal, Two Methods

Blockchain seeks the decentralization of decision making by eliminating intermediaries, while antitrust aims to achieve it by eliminating anticompetitive practices. They converge toward the same objective. That said, one should not be candid about how easy it will be to make them cooperate. First, the Sherman Act is concerned with trusts43 - hence the name “anti-trust”. Since there is no trustee in the sense of a third-party fiduciary in blockchain’s first layers, the target of antitrust laws is absent.44 Blockchain may thus undermine the *raison d'etre* of antitrust law, which will trigger epidermal reactions.

Furthermore, blockchain and antitrust may at times attack each other. Blockchain may be used to implement anticompetitive practices and be enforcement resistant, while antitrust may reinforce the role of intermediaries in the economy (by protecting them from different forms of anticompetitive exclusions) and label various blockchain behaviors as anticompetitive - regardless of the overall usefulness of these blockchain features.

In fact, antitrust law and blockchain ecosystems seek decentralization at two different levels. Antitrust law prohibits certain categories of conduct, creating tensions with tech communities without focusing much on digital architectures. Blockchain, on the contrary, seeks to decentralize by providing its users with a specific digital architecture. It does not prohibit (anticompetitive) practices where code allows. This creates tensions between them, as I show in Part 2 of this book. Their cooperation will require the identification of ways to deal with these mutual provocations, as I will explain in Part 3.

As things stand, both of these communities exhibit what Veblen called “trained incapacity” - the difficulty to think beyond a set of constraints and assumptions. Policymakers tend to believe that the law should be the most important constraint organizing our lives. For that reason, legal rules are often applied without looking for ways to coordinate with other constraints, including digital architectures.45 In the meantime, blockchain communities tend to view legal enforcement as an adversary, and not as an ally. As John Perry Barlow stated in 1996: “I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.” After all, the law liberates, but it also implies illegality, lawsuits, liability assignment and sanctions. The antitrust and blockchain communities will gain from over- coming these biases.

2.2 The (Long) Road Ahead

If we want antitrust and blockchain to collaborate on a long-term basis, we need to talk about the problems that their cooperation will encounter along the way. The challenge before us is intricate.46 On the one hand, it is a matter of getting legal minds to recognize that technology can help achieve objectives that the law cannot achieve on its own. There are three reasons for this. First, blockchain provides a technical approach to the subject. It serves as a framework for decentralizing the economy by default, while antitrust mostly applies ex post by correcting past behaviors.47

Second, antitrust agencies’ detection rate remains low, meaning that illegal behavior often goes unpunished.48 And enforcement is costly, which makes it impossible to pursue all potentially illegal practices. This is particularly problematic in a world where illegal practices can be implemented through coding that quietly and immediately affects billions of users. Also, the rule of law is (unfortunately) inapplicable in some places. This is the case when the state bypasses legal constraints,49 and when jurisdictions are mutually unfriendly and do not enforce foreign laws.50 For example, enforcement of U.S. court judgments abroad can prove especially difficult in light of divergent rules on jurisdiction, requirements for special service of process, reciprocity and some foreign countries’ public policy concerns,51 including in Europe.52

Finally, antitrust law is complex and cannot be fully mastered by all companies - the compliance costs are high and many firms unwittingly infringe the law. Blockchains could therefore supplement antitrust by creating an architecture that leads to fewer anticompetitive practices.

On the other hand, blockchain communities would gain from working with (not against) antitrust law enforcers. That is because antitrust would eliminate practices that artificially centralize blockchain ecosystems and that blockchain architecture cannot stop or prevent. 1 will analyze them in Part 2. Doing so would also provide legal certainty, thus fostering investments and benefiting all the actors involved in commercial activities that rely on blockchain. For these reasons, one should think of antitrust and blockchain as allies - not enemies - as they both seek the same objective, while presenting complementary strengths and defects. Doing so would lead policymakers to promote and implement a new “law + technology” approach that recognizes that the benefits of cooperation outweigh those of one-off confrontations. A game theorist would represent that approach as illustrated in Figure 5.1.

#### Averting the consolidation of blockchain allows scalable transaction validation.

Dr. Thibault Schrepel 21, PhD in Antitrust Law from Université Paris-Saclay, LLM in International Law and Legal Studies from the Brooklyn Law School, Associate Professor of Law at VU Amsterdam University, Faculty Affiliate and Creator and Director of the Computational Antitrust Project at the Stanford University CodeX Center, Blockchain + Antitrust: The Decentralization Formula, p. 271-273

2 BLOCKCHAIN INTERNAL FACTORS

The evolution of blockchain also depends on internal balances in terms of design and governance. Overall, choices that will be made within each blockchain will prove important for their evolution. As I show, it all comes down to human interactions.

2.1 The Trifecta: Intra-blockchain Evolution

A blockchain trilemma has emerged in the literature over the last several years. It can be summed up as follows: ensuring blockchain’s decentralization, scal- ability and security entails tradeoffs, at least in the short term. Although this makes sense on a technical level, it does not capture the entirety of our subject. Let us take a closer look. I have discussed decentralization at length through- out this book. It is blockchain’s central feature, in terms of both architecture and philosophy. “Scalability” refers to the ability to validate large volumes of transactions rapidly. Last, blockchain’s security hinges upon its ability to maintain integrity: that only desirable transactions take place - for example, by preventing double spending.42

To a certain extent, we have seen together that the mechanisms that ensure decentralization at different blockchain layers may conflict with security.43 This is what Awemany’s story in Chapter 1 revealed. Decentralization implies the distribution of power, limiting the ability to act unilaterally in case of an emergency. At the same time, decentralization can also affect the scalability of blockchain: Proof of Work is decentralized by nature, but it prevents the rapid validation of large transaction numbers. Conversely, a private blockchain can restrict access to the ledger or certain functions, raising security and scalability issues.44

In the long run, however, these three objectives are mutually reinforcing. The more a blockchain is decentralized, the more it stands out from the centralized platforms and services that readers know only too well. By differentiating themselves, blockchains attract users by offering a different value proposition. In turn, this generates scalability. The same goes for security, as the more participants use a public blockchain, the harder it becomes to alter the registry or perform a 51 percent attack. The blockchain trilemma is thus useful for thinking about what needs to be done, but it cannot provide a coherent analytical framework in the long term. It will become less relevant with technical advances, to the point where some blockchains will maximize these three objectives. Those who manage to do so will prosper.

#### That is vital to secure critical infrastructure (CI) AND the integrity of the IoT.

Dr. Amit Kumar Tyagi et al. 22, PhD, Assistant Professor, Vellore Institute of Technology; Ishani Tibrewal, Senior Electrical Engineer, Technocrats Robotics. Vellore Institute of Technology; Manas Srivastava, Software Engineer, Optum. Vellore Institute of Technology, "Blockchain Technology for Securing Cyber-Infrastructure and Internet of Things Networks," in Intelligent Interactive Multimedia Systems for e-Healthcare Applications, 2022, pg. 337-343.

Today’s Internet of things is mostly used smart devices in many applications. Internet of things when integrates together, they create a network of smart devices called computing infrastructure. This computing infrastructure needs to be properly maintained and secure against many available beaches or critical attacks. Internet of things is an emerging collaborative research environment for today’s researchers, because it creates/provides many other benefits like building cyber physical system and autonomous cars. But, when these devices are being used on a large scale and generate a lot of data, and this data is stored at cloud (public, private and hybrid). This data needs to be protected against many serious attacks, and this task can be fulfilled by “Blockchain technology”. Blockchain technology concept in 2008– 2009 by anonymous user/group of users in cryptocurrency [1], and this concept has been introduced in many applications [2] like finance, manufacturing, medical care, agriculture and autonomous cars.

The Internet of things (IoT) will connect not only computers and mobile devices, but it will also interconnect smart buildings, homes and cities, as well as electrical grids, gas and water networks, automobiles, airplanes, etc. IoT will lead to the development of a wide range of advanced information services that need to be processed in real-time and require data centres with large storage and computing power. The integration of IoT with cloud and fog computing [3, 4] can bring not only the required computational power and storage capacity, but they enable IoT services to be pervasive, cost-effective and can be accessed from anywhere using any device (mobile or stationary). However, IoT infrastructures and services will introduce grand security challenges due to the significant increase in the attack surface, complexity, heterogeneity and number of resources. Some of the examples of IoT technology usage and major implications during cyber-attacks are:

1. Maritime shipping: There are multiple usage of IoT technology in Maritime shipping as the shipping companies have equipped their fleets with a variety of sensors to monitor critical vessel systems, weather and sea conditions, and cargo. The Marine industry can be impacted cyber-attack [5] on terminal computer system, navigation system and point of sale system. Possible consequences are business interruption, damage to data, theft of property through alternation of shipping contacts, bodily injury and property damage.
2. Aviation: There are several usage of IoT in both commercial and military aviation [6]. Connecting IoT to aviation will help to access real-time data for engine performance improvement, accurate weather forecast and pilot monitoring. The cyber risk in aviation may allow hackers to gain access to some sensitive data such as the location of troops or detailed mission plans for IoTconnected military planes. There could be remote terrorism acts where the hacker could gain access to an aircraft’s control system and weaponry, similar to drone hacks, and use it against the enemy.
3. Smart City: A Smart City [7] can be equipped with IoT platform has multiple usages such as smart parking, public safety and traffic balancing. Smart grid is one of the examples which are implemented in Smart City to realize great cost savings and efficient troubleshooting. If there is no effective cyber security maintained, Hacker can gain access to such public infrastructure from his computer to shut down an entire city’s electrical supply.
4. Critical infrastructure: Because of the networked nature of IoT, i.e. that each connected object uses data from other connected objects–there is also the risk that a malfunction could lead to catastrophic system failure. The critical infrastructure like dams, bridges embedded with censors to monitor structural integrity as well as environmental conditions are vulnerable to cyber threats. Malfunctioning of these sensors may bring risk of a catastrophe if those objects fail and could lead to massive property damage or even loss of life.

Amit and Shamila [8] discussed some more examples, where Internet of things devices can be enhanced/used in everyday examples.

On another side, such infrastructure requires secure cyber security mechanisms, i.e. no more breaches/attacks on public networks. This chapter has provided introduction of Industry 4.0/smart manufacturing using IoT [9] while mapping the relevant security and privacy challenges, threats, risks and attack scenarios. This chapter presents an IoT security framework for smart infrastructures such as smart homes (SH) and smart buildings (SB) [10]. Also, it presents a general threat model that can be used to develop a security protection methodology for IoT services against cyber-attacks (known or unknown) with provisioning several issues and challenges in respective IoT-based cyber-infrastructure. The vast diffusion of connected devices in the IoT has created enormous demand for robust security in response to the growing demand of millions or perhaps billions of connected devices and services worldwide. The number of threats is rising daily, and attacks have been on the increase in both number and complexity. Not only is the number of potential attackers along with the size of networks growing, but the tools available to potential attackers are also becoming more sophisticated, efficient and effective.

Cyber-infrastructure is a word commonly used but lacking a single, precise definition. One recognizes intuitively the analogy with infrastructure, and the use of cyber to refer to thinking or computing but what exactly is cyber-infrastructure as opposed to information technology infrastructure? [11] propose definition of cyberinfrastructure as: “cyber-infrastructure consists of computing systems, data storage systems, advanced instruments and data repositories, visualization environments, and people, all linked together by software and high-performance networks to improve research productivity and enable breakthroughs not otherwise possible”. In this chapter, we discuss the origin of the term cyber-infrastructure based on the history of the root word infrastructure, discuss several terms related to cyber-infrastructure and provide several examples of cyber-infrastructure. Cyber security is a necessary task in building and proposing an attack-free infrastructure (using by public users). Note that some elements of cyber security are application security, information security, network security, disaster recovery/business continuity planning, operational security, end-user education. Also, some benefits of using/requirement of cyber security to secure an infrastructure:

* Business protection against malware, ransomware, phishing and social engineering.
* Protection for data and networks.
* Prevention of unauthorized users.
* Improves recovery time after a breach.
* Protection for end-users.
* Improved confidence in the product for both developers and customers.

Internet of things (IoT) is an emerging concept describing a wide ecosystem where interconnected devices and services collect, exchange and process data in order to adapt dynamically to a context. IoT is tightly bound to cyber physical systems and in this respect is an enabler of smart infrastructures by enhancing their quality of service provisioning. Cyber physical systems and autonomous applications are IoT-based application development, major development/invention of the previous decade. Both the IoT critical infrastructures and cloud are subject to cyberattacks [12]. Cloud environments experience the same threats (at a high level) as traditional data centre environments; the threat picture is the same. That is, cloud computing runs software, software has vulnerabilities, and adversaries try to exploit those vulnerabilities. However, unlike information technology systems in a traditional data centre, in cloud computing, responsibility for mitigating the risks that result from these software vulnerabilities is shared between the cloud service provider (CSP) and the cloud consumer. A secure cyber-infrastructure is need of many organization/research communities (especially computer science) around the world. Hence now, the remaining part of this chapter is organized as (in further sections):

Sect. 2 discusses work related to Blockchain used to secure Internet of things (IoTs)-based cyber-infrastructure smart contact, i.e. evolution of smart contract with Blockchain technology’s growth.

Sect. 3 discusses motivation behind this work, i.e. intention behind choosing area related to Blockchain-enabled and IoT-based cyber-infrastructure.

Sect. 4 discusses necessity of secure cyber-infrastructure today and tomorrow, i.e. in current century.

Sect. 5 discusses tools or mechanisms available for securing a cyber-infrastructure and Internet of things-based infrastructure

Sect. 6 discusses many issues, problems and challenges in using Blockchain technology during securing respective (cyber) infrastructure.

Sect. 7 discusses opportunities for future researchers and computer science community.

Finally, this chapter is concluded in Sect. 8 with some future research directions (including some research gaps).

2 Related Work

Internet of things (IoT) as a technological term is around 16 years old, but the actual idea of connected devices had been around longer, at least since the 70 s and at that time it was referred to as “embedded Internet” or more as to say “pervasive computing”. The coining of the actual term “Internet of things” was done by Kevin Ashton during his work at P&G in the late 20 s. Kevin used to manage supply chain optimization and wanted to attract senior management’s attention to a new exciting technology called RFID, now as because the Internet was one among the burning trends during the late 20 s so it somehow made sense, he called his presentation “Internet of things” and thus giving a new identity to the technology. By the year 2010, the Internet of things (IoT) started gaining popularity because of the leakage of information of Google took people into guesses that it might be Google one of the new strategies to index not only the Internet but also the entities in the physical world. Followed by this, in the consecutive years the technology took off after which different countries, market research companies and many other organizations took over it very seriously and started researching into this particular emerging new phenomenon and now it is predicted that by the end of 2020, IoT would have gained a huge stake over the market. Currently, the technology has outgrown to such an extent that there has been mass-market awareness. From dominance motivation behind the present, a critical number of the establishments that help and oversee current lives, social requests and work practices will appear to be dull, level and still. The more settled the establishment, the more certified this feels: we consider boulevards until we can drive impact on them, and thereafter in a flash neglect (until induced by setbacks, advancement and vehicle over-burdens to re-examine). We drink from the city water supply until we cannot, and a short time later examine water. Once here, amazing establishments appear as everlasting, unsuspected, even regular features of contemporary life. This sort of naturalization and disregarding is critical to the ampleness and significant estimation of establishment and is to be certain maybe the most raised want. Be that as it may, it in like manner makes it attempting to audit what is being referred to with establishment (which winds up being an extensive sum) or to plot the methodology by which systems create and change. This is an insightful issue for capable understudies of history and social scientists; for would-be makers of a system, it is something more. Computerized establishment was developed with the arrangement to help customers with winning through our high IT aptitudes and to get new work open entryways in India and help in the country’s social improvement. CIS continues creating at a pace of 300% consistently. Advanced structure continues developing its assortment of organizations and advancement portfolio to get new markets and spaces. Advanced establishment encounters critical improvements with respect to structure, bunch size and overall reach.

Hence, this section discusses work related to Internet of things, cyberinfrastructure, also Blockchain role in IoT-based applications in detail. In next section, we will discuss motivation behind this work in brief.

3 Motivation

Internets of things (IoTs) are used in building cyber physical systems, i.e. largescale cyber-infrastructure. For that, we require proper rules and cyber security to prevent from any breaches/attacks. In general terms, cyber security is safeguarding the Internet-connected systems, including hardware and software data, from cyberattacks, whereas information security, which is devised to preserve the confidentiality, integrity and availability (CIA) of data, is a fragment of cyber security. There are many cyber threats like malware, ransomware, social engineering and phishing on existed infrastructure (build by integration of IoT/smart devices). Such infrastructure requires strong and secure mechanism/algorithms to provide reliable and efficient services to end-users. As we have discussed many popular attacks have been mitigated (in the past decade) like Stuxnet [13], this attack has downgraded many nuclear facilities in Iran in 2010. Further, [14, 15, 16] have discussed many examples of cyber-crime in their work. But, due to getting rapid growth in innovation, we need Blockchain type of solution to secure an infrastructure. Hence, Blockchain technology has been started using in many applications for protecting critical system/infrastructure. Providing efficient and reliable services to end-users and more security to the same users is our higher (main) priority. Blockchain [17] concept fulfilled this goal in this current era. So, we started to write some important work on Blockchain, which can play an essential role in IoT-based cloud infrastructure or IoT-based infrastructure in making a secure cyber-infrastructure. Hence, this section discusses motivation behind this work, and it provides answer to many questions, i.e. related to topic of interest and how this work will be useful to society or researchers/readers. Now, next section will discuss the necessity of cyber-infrastructure or IoT-based cyber-based physical systems in current century.

4 Necessity of Cyber-Infrastructure in Current Century

There exists a positive national framework for the general public for its smooth working and thus making it powerful. The significance of these is generally comprehended and has since quite a while ago perceived the requirement for interest in their creation and upkeep. Such frameworks will, in general, give widespread administrations, range national and universal limits and are inherently depended upon by people and associations. The need for the digital framework is difficult to disparage, and even generally minor disappointments can affect huge quantities of individuals. Disappointments can bring about genuine ramifications for the working of society, and this has additionally been perceived by assailants who have focused on these national frameworks as a method for disturbing enormous quantities of individuals generally effectively. While the profoundly interconnected nature of pc frameworks can experience challenges related to frameworks security, it can likewise be utilized as a method for upgrading it as well. A considerable lot of the techniques and advantages that identify with the utilization of processing for the basic foundation have as of late gone to the fore. Organized frameworks can give expanded vigour against both focused on assaults and incidental disappointment. These incorporate perception procedures to give mindfulness and displaying capacities; frameworks of frameworks security to all the more likely comprehend the security results of associations between numerous frameworks. Utilizing these methods in a bound together manner will give benefits as far as better seeing, ongoing mindfulness and the improvement of security strategies customized to assurance against disappointment and assault of basic framework frameworks. The genuine advantage to be picked up from combining the strategies digital foundation is to give procedures that length innovative limits. cyber-infrastructure that help our general public are produced using an accumulation of frameworks and systems worked over registering advancements and data frameworks. cyber-infrastructure are going under expanding dangers, the insurance of basic foundations requires a superior comprehension of how the control should be structured to cover all the parts of these frameworks.

Hence, this section discusses “why we require cyber-infrastructure in today’s era”? Now, next section will discuss several tools available for securing cyberinfrastructure/IoT-based infrastructure in detail.

5 Tools Available for Securing Cyber-Infrastructure and Internet of Things-Based Infrastructure

There is a great significance of tools that are being developed to secure cyberinfrastructure; Blockchain is one of them. Risks, vulnerabilities, threats, cyber-crimes and frauds are increasing exponentially with the world being digitalized. To get a shield from these potential threats, Blockchain is gaining tradition today but still, significant phases of the world are unaware of it. Critical infrastructure in many countries will soon become vulnerable to cyber terrorism. Ingenious uses for Blockchain technology are already becoming incorporated of fields other than cryptocurrencies [18] and can be exclusively useful to boost cyber security. Several security techniques and approaches have been developed using Blockchain that plays a major role in securing many IoT applications. A Blockchain system depends upon the participation of allocated nodes to build a loyal chain-connected network, in which every decision is made based on the consent. The required system is proposed to have specific major components such as Blockchain-based distributed data repository and verification platform, Internet of things (IoT)-based noticeable environment and cloud-based versatile assistance delivery system. The parts sum up together to develop an infrastructure and a dynamic functional operational environment for overall entities in generation, transmission and delivery. As IoT is an ordinary result of the sensing technology and wireless sensor network, IoT technology will in future enter into each segment of the energy system and connects with other components of the cyber-infrastructure (Blockchain and cloud).

Blockchain takes the involvement of very basic technologies into IoT to make it secure. First of all, it decentralizes the data storage which is its backbone and uses consensus mechanism, this structure ensures data is not traceable nor even tamper able thus as a result giving a no-point fault system so that it can be used in the upper-level application. The connection between the blocks of data is done with a smart contract which is based on contrasting application logic. The information in Blockchain is transferred on a trusted mechanism that verifies and authorizes the user based on agreements, intellectual property rights and so on. In summary, Blockchain along with IoT in phases of cloud coordinated can work together to form a guarded, effective, service-oriented environment, which can strongly support various applications in various domains. Blockchain has promising applications across the domain of network security. IoT can contribute to big data at any level of abstraction, data acquisition could be applied at any level but the main point of data security lies in hands of Blockchain. The complete infrastructure has complete reliability and dependency on its security parameters which should be fault-tolerant, which can be smoothly accomplished through Blockchain. The monitor, control and coordination of units of the cyber-infrastructure should be supported by a dynamic cyber physical system. In any of the proposed cyber-infrastructure model, the cyber-infrastructure is mainly the backboned level of abstraction and security achieved. Under reliable supervision of IoT through Blockchain could help us in attaining a better cyberinfrastructure for a better tomorrow.

#### BUT widespread adoption is reliant on further innovation AND continued decentralization.

Dr. Amit Kumar Tyagi et al. 22, PhD, Assistant Professor, Vellore Institute of Technology; Ishani Tibrewal, Senior Electrical Engineer, Technocrats Robotics. Vellore Institute of Technology; Manas Srivastava, Software Engineer, Optum. Vellore Institute of Technology, "Blockchain Technology for Securing Cyber-Infrastructure and Internet of Things Networks," in Intelligent Interactive Multimedia Systems for e-Healthcare Applications, 2022, pg. 346-349.

Blockchain technology (in near future) will attract attention from several research communities and can be used in the following areas like Internet-connected things, banking, retail and health care. Such applications are requiring Blockchain, due to the property of distributed digital data (encrypted form, using Hash Keys). Many applications or future uses of Blockchain have been included in Fig. 2. Such functionality in Blockchain is provided by distributed ledger. Using Blockchain technology (a decentralized technology), in respective application, we can secure/store data safely with efficient authentic mechanism at remote location (also in form of Cloud). Data stores at remote location are in inconvertible and immutable using Blockchain/distributed ledger in it.

Blockchain technology has its powerful use in business domain, insurance being one of the prime commercial commodities. The trend of Blockchain within insurance will help in transforming insurance into Insurtech (i.e. Insurance + Technology). One of the many examples where Blockchain can help is in Travel Insurance, i.e. delays and cancellation of flights, can be prevented by Travel Agencies using Blockchain. Blockchain, which was just a virtual ledger, is spreading like a wave across extensive number of industries. Also, businesses are expected to spend colossal amount of money on this powerful technology in this year. From Insurance to gaming to cannabis, almost all industries are looking to develop and apply Blockchain technology, there is hardly any domain not looking for Blockchain applications because this technology is more likely to transform the industries.

Since Blockchain technology does not hold any central supervision and acts on decentralized platform, it has made Blockchain having a prominent feature of being resistant to fraud.

Diagram

Description automatically generated

Companies are striving hard to implement Blockchain technology as it will provide veracity to the stored digital data information. Here are many other industries who are mobilizing the power of Blockchain technology:

* Speculative Funds: With a vast range of Numerai, systems have started adopting hedge fund model with a firm support included by First Round Capital and Union Square Ventures, it involves employment of a group of stockbrokers and quants and then regionalizing it. The distribution of data through Numerai is done when it sends its numerous quants to various distinct locations, encrypts the datasets and then is preceded by building protective models and the one among with best of them is awarded with Numerai token known as Numeraire [19]. Further, the strategy is to strategize and develop a meta-model to make trades.
* Medical Management: The medical reports associated with a person are one of the vital parameters of an individual’s security, preserving this data is sole responsibility of the organization whosoever beholds it. While sharing the data among different platforms, the data may get leaked which may lead to some unavoidable circumstances. So in order to prevent this data to falling into dangerous hands, Blockchain technology allows hospitals [20], other institutions/organizations and payers to split access to their networks without compromising or suspecting data security and integrity.
* Public Mobility: Due to increase in use of public transport of vehicles, it becomes difficult for government in cities to know the status of public transportation being used, so on implementing Blockchain technology will help the cities to know and understand that how the public mobility is being used by their residents and how can they develop some different options for transportation.
* Track of Credit History: On the basis of past records, lenders tend to reduce the risk that is posed by lines of credit or loans to small ventures which also makes credit bureau to have all powers in terms of loans. It also works as a trusted platform where business owners can build a trusted network.
* Charity: Using Blockchain technology in charity institution or organization will help donators to track where their donations are going and who is going to use it. Blockchain will provide transparency and security to all the financial records and will give a greater visibility to the donors.

As mentioned above, there are many other similar industries that have great potential future with implementation of Blockchain in them like loyalty programs, natural resource management, education, advertisement, public assistance, publishing, gaming, travelling and even more. Moreover this, some other opportunities with Blockchain in near future are summarized (also included in Fig. 3) here as:

* Improve social media functionalities
* Digital ownership revolution
* Keeping our ID (Identification) and personal information secure
* Keep your identity safe and location privacy safe.

Blockchain provides digital freedom by using smart contracts: It means that the system is not governed by any central authority so that any kind of manipulation cannot be done by them. Note that Blockchain is more popular in mortgage industry, i.e. with its transparent system, speed (when compared to the typical mortgage underwriting process) and immutability that will secure your home for as long as you own it. Hence, this section discusses several opportunities for future readers and research communities. Now, next section will wrap up this work (including some research gaps) in brief.

8 Summary

Blockchain is the necessity of the future in building trust among peers and providing more privacy-preserving too many applications (like location-based services, etc.), also security to computing environments. This concept is enhancing everyday with its uses in many applications. Today’s Blockchain is the most trusted technology among all existing mechanisms (for protecting an infrastructure). Generally, Blockchain technology allows distribution of digital information in decentralized manner, but not duplicated. Blockchain also allows us to own digital assets, goods and data through its novel concept. Similarly, we face several cyber-crimes and attacks on many critical or cyber-infrastructure, [21] discussed several privacy issues), for that we suggested Blockchain to be used for the same infrastructure for providing sufficient level of security layers. This chapter has discussed several interesting components of Blockchain with Internet of things-based infrastructure and other cyberinfrastructure. We also discuss several benefits, disadvantages, issues and challenges (including opportunities) of Blockchain in securing an infrastructure, and this information will help future researchers/scientists or readers in continuing their research work in near future. In near future, some possible changes are possible with Blockchain are “Distributed Web (new Internet with Blockchain)”, “Decentralized Autonomous Blockchain” and “Blockchain-based Cloud”. For providing more efficient services, the world is watching and waiting for more innovations in technologies.

#### Attacks against CI are imminent, vicious, and incalculable.

Ted P. Delacourt 22, Supervisory Special Agent, Mission Critical Engagement Unit, Cyber Division, Federal Bureau of Investigation. MA, Science & Technology Intelligence, National Intelligence University. MBA, Finance & Economics, University of Chicago. BS, Accounting, Georgetown University, "Cyberattacks on Critical Infrastructure as The New WMD," HS Today, 02/01/2022, https://www.hstoday.us/featured/cyberattacks-on-critical-infrastructure-as-the-new-wmd/.

Should the acronym WMD, which stands for “Weapons of Mass Destruction,” be updated to “Weapons of Mass Disruption?” I think it is a timely question in this Digital Age as we connect and integrate billions of new digital devices into our lives and business processes and when a cyber-attack against one supply chain provider can lead to cascading effects on entire communities across the globe. Cyberattacks on Critical Infrastructure (CI) can cause mass economic and societal impacts. Fewer strategies than cyber-attacks can offer better plausible deniability and can cause greater anxiety and instability to our society than targeting the systems and networks that enable our day-to-day activities. Consider that 20 years ago terrorists killed 3,000 Americans and disrupted the entire U.S. and global economies with only four planes. Given the growth and ubiquity of technology today we must consider how the exponential growth of cyberattacks on CI might be similarly leveraged by adversaries and criminal actors as Weapons of Mass Disruption, the new WMD.[1]

Cyberattacks take many forms, often progressing through multiple phases as they escalate in severity. Malicious actors often initiate a network intrusion through phishing campaigns or the purchase of compromised user credentials on the dark web. What begins as the hijack of a single user profile expands in severity. Intruders move laterally across internal systems, conducting surveillance and gathering intelligence on network environments before escalating to data theft, service disruptions, and ransomware extortion.

The goals of these actors may be both strategic and economic in nature, and targets may be government and/or the private sector. Cyberattacks perpetrated on CI elements develop into the new WMD when the intended and unintended consequences cause widespread damage and societal impacts. A disruption of essential services, even if brief, can occupy significant civilian and military resources in a region or entire country.[2]

Russian military doctrine views the battle of the information space, to include cyber activities, as unending.[3] As such, the bar to initiate cyber-attacks appears low and the past two decades have witnessed numerous cyberattacks on CI around the world. The march toward a more interconnected and networked world increases the likelihood that cyberattacks against CI could be used as the new WMD. In this new threat environment, more than ever we need to increase and leverage government and private-sector partnerships to mitigate and neutralize these cyber threats.

Cyber Threat Technology

Cyber threats combine numerous attack vectors and strategies in a single attack. Common attacks include malware, denial-of-service attacks, phishing, structured query language (SQL) injection, and zero-day exploits. Some attacks specifically target critical nodes, software, or people, while others overwhelm internet websites with massive, automated amounts of data requests. Malware attacks install malicious code, transmit sensitive data, and corrupt, destroy or deny access to data by overwriting or encrypting files, often referred to as ransomware. Phishing attacks target users with false messages that request they open a file or access a link that secretly installs malware. SQL injection attacks insert malicious code into servers running SQL database software to reveal sensitive data not normally available. Vectors for SQL injections include inserting malicious code in search boxes of vulnerable web pages. These attack opportunities persist due to inconsistent patch implementation and failure by end users to employ cyber best practices, often called cyber hygiene, which increase the risk of cyber-attack on vulnerable systems. Zero-day exploits, alternatively, may be known vulnerabilities that lack immediate solutions. Even if a zero-day exploit is known, the threat continues until a patch is developed and the end user installs it. The combination of attack vectors with new and old malware options creates opportunities for both intelligence gathering and development of mass disruption strategies of CI operations by and against U.S. adversaries.[4]

Critical Infrastructure Sectors

Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience identified 16 sectors and identified specific federal agencies charged with their security. PPD-21 addressed the reality that advances in technology led to increases in each sector’s interconnectivity and reliance on online and networked resources to accomplish their fundamental missions. [5]

[Figure omitted]

CI elements do not stand alone, but rather are interconnected and interdependent. This interconnectivity makes them vulnerable to direct and indirect cyber threats. An attack on one may initiate a failure in another or cascade to the entire interconnected CI network. The mix of public, private, and non-governmental operations across each CI sector complicates remediation of identified vulnerabilities and information sharing on actual or potential attacks. The ubiquitous nature of these CI sectors and the distribution of their physical and networked assets across a wide geographical area, often spanning the entire country, make CI sectors attractive targets. State, non-state, and criminal actors continually seek victims of opportunity across all CI sectors for monetary and strategic gain.[7]

Past Attacks on Critical Infrastructure

The threat against CI elements is neither theoretical nor improbable. Cyberattacks have occurred independently and as part of multi-domain conflicts involving Russia, China, and others over the past two decades. Connell and Vogler described the Russian military view of cyber operations as part of the larger concept of information warfare, and not a distinct tactic. They assessed that in line with traditional Soviet military thinking, Russian decision-makers view the battle for the information space as unending. Such a doctrinal view of an information space in constant conflict stands in sharp contrast to the U.S. view. Furthermore, Russian decision-making informed by this view likely sets a low bar for the initiation of offensive cyber operations.[8]

In 2008, cyberattacks attributed to Russia disrupted Georgian government websites, financial institutions, private telecommunications companies, and other organizations in the opening stages of the military conflict between the two countries over breakaway regions. Given the limited nature of Georgian information technology at the time, the impact of the cyber operations was reduced. This application of cyberattack methodologies, however, stands as the first large-scale use of cyber operations in support of a military conflict. In this multi-domain example, a cyberattack designed to cause widespread disruption preceded a physical attack. [9]

In December 2015, the Ukrainian Energy Minister attributed the first known power outage caused by a cyberattack to Russian actors, when three power distribution companies were targeted. The timing and coordination among the attacks across central and regional facilities pointed to a high level of sophistication. The subsequent investigation revealed an initial intrusion occurring at least six months prior, allowing the actors to gather intelligence on company operations and likely remediation responses. This surveillance allowed the cyber actors to insert additional malware to wipe key recovery servers and computers to stymie restoration efforts. The attack left approximately 225,000 customers without power for six hours in the middle of a Ukrainian winter. The investigation also revealed the attack could have been larger, and the damage permanent, but the cyber actors chose to limit the scope. This points to the scalability of damage from the spectrum of cyberattack methodologies and their potential as a WMD.[10]

In the spring and summer of 2020, the People’s Liberation Army (PLA) of China and the Indian Army were involved in multiple skirmishes in the vicinity of the Actual Line of Control that defines their common border in the Himalayas. One such engagement resulted in the deaths of 20 Indian soldiers. Unwilling to back down, that August the Indian Army seized additional strategic locations. In an apparent tit-for-tat response, hostilities escalated and entered the cyber domain when a power outage struck the power utility in the Indian state of Maharashtra, which includes India’s financial capital Mumbai. The attack was attributed to a group known as RED ECHO, potentially a state-sponsored group affiliated with China’s PLA Strategic Support Forces. In response to the cyberattack, India mobilized additional troops to the disputed region and expanded the hostilities into the economic domain – India banned Chinese mobile apps, limited Chinese investments in India, and joined an informal grouping of the U.S., Japan, and Australia dedicated to limiting Chinese advancement in Indo-Pacific. In this multi-domain example, the cyberattack causing widespread disruption was a response to the physical attack, which was met with economic sanctions.[11] Such an attack against such a large power grid and financial capital could be characterized as a WMD attack.

In their 2021 study, Izycki and Vianna defined a cyberattack as an operation conducted with a kinetic intent or result. Using this definition, they identified seven significant cyber-attacks between 2010 and 2019. Their results are illustrated in the table below.[12]

[Figure omitted]

The attributions noted by Izycki and Vianna, if accurate, highlight how various actors employed cyber weapons across a wide range of political conflicts and actors. The authors concluded that the small number of campaigns highlighted the rarity of what they termed “kinetic attacks” against CI assets. Cyberattacks on CI sectors like those noted by Izycki and Vianna have the potential to cause massive disruptions and societal displacement if the underlying interconnected computer systems were destroyed or disabled for extended periods.[13]

Discussion of the Threat

Cyberattacks on interdependent CI sectors have the potential for secondary and tertiary effects in addition to the cascade of physical disruption that follows.[14] Beyond impairing physical assets, cyber-attacks on the foundational services of a society also function as psychological and strategic weapons. CI disruptions may undermine confidence in the state to provide security or basic services. Such attacks may serve as existential threats to unstable regimes. As strategic weapons, cyberattacks on CI causing mass disruptions have the potential to tie up significant military and economic resources at the same time the nation faces a military threat. Such attacks have the potential to fully occupy the time and attention of decision-makers as well as field commanders, causing them to miss or ignore other pending threats. This exemplifies the multi-domain use of cyberattacks.[15] Recently, plans purportedly developed by units within Iran’s Islamic Revolutionary Guard Corps (IRGC) leaked to a British reporter described various cyberattack strategies for cargo ships, building HVAC systems, and fuel pumps manufactured in the U.S. and sold worldwide. If authentic, such plans highlight in detail how CI sectors might be attacked via the cyber domain.[16]

Based on the attacks studied, the threshold for initiating a cyberattack appears low, and not all attacks produce an immediate or identifiable impact. Attacks may occur unnoticed, with bad actors lying dormant within systems for an extended time period. The nature of an attack may change over time, in that an intrusion may progress to an intelligence-gathering operation and data theft, before escalating into a denial-of-service or ransomware attack. The progression of an attack may change depending on the nature of the actor. The goal of non-state or criminal actors in conducting cyberattacks may be profit-driven or center on causing economic damage, while state actors may favor intelligence gathering and the creation of strategic options or outcomes. In the case of North Korea, the goals may be both financial and intelligence gathering, as they gather technical knowledge and the financial means to purchase necessary materials and equipment. The ubiquity of networked systems and the wide availability of cyber intrusion tools leave no country or critical infrastructure sector immune.[17]

Determining attribution for an attack is difficult. The use by cyber actors of Virtual Private Networks (VPNs), leased server infrastructure, and the cross-border nature of the internet complicate attribution efforts. Intelligence services can be reluctant to publicly disclose sensitive techniques and classified information in order to explain attribution conclusions. Additionally, public prosecution of these malicious actors may risk disclosure of investigative techniques, particularly in national security investigations. Complicating the matter further, cybercriminal organizations frequently operate from countries unwilling to arrest and extradite malicious actors to the United States. As a result, there appears to be limited consequences levied on adversaries for intrusion or intelligence-gathering activities. For example, in July 2021, in the same week the U.S. and NATO allies publicly identified the Chinese Ministry of State Security (MSS) as the perpetrator of the hack of the Microsoft Exchange email server uncovered three months prior, the U.S. Department of Justice filed motions to dismiss visa fraud charges against five Chinese scientists accused of concealing their ties to the PLA. This public shaming of cyber aggression by the MSS did not include economic sanctions against China, while a similar public disclosure in April 2021 about Russia included economic sanctions its cyber actions related to election interference.[18]

Conclusions and Judgments

Cyber intrusions utilize a volume attack scenario, leveraging automated software to continually probe end points and network connections for vulnerabilities. Hackers count on the incomplete implementation of software patches and poor cyber hygiene to provide illicit access. The assessment, based on this research, is cyberattacks on CI will continue to grow in number and frequency and continue to escalate in severity. As the world becomes more reliant on systems connected to the internet the attack surface expands. CI sectors are no exception, and their interconnectivity creates a risk of a failure cascade. Furthermore, cyberattacks are becoming automated and more anonymized. Consequently, if we have not yet met the threshold, we may soon, where cyberattacks against CI with large-scale impacts may be characterized as WMD.

#### Malware spreads between interlinked systems---causing use or lose pressures AND nuclear use.

James M. Acton 20, holds the Jessica T. Mathews Chair and is Co-Director of the Nuclear Policy Program at the Carnegie Endowment for International Peace, “Cyber Warfare & Inadvertent Escalation,” Daedalus, vol. 149, no. 2, MIT Press, 03/23/2020, pp. 133–149

The vulnerability of nuclear forces and C3I systems creates the risk of inadvertent escalation: that is, escalation resulting from military operations or threats that are not intended to be escalatory. So-called crisis instability, for example, could arise if a state were afraid of being disarmed more or less completely in a preemptive strike by an adversary, whether or not such fears were well founded.4 In the most extreme case, “use-’em-or-lose-’em” pressures could lead the state to employ nuclear weapons, conceivably in its own preemptive attempt to disarm its adversary, but more likely in a limited way to try to terrify the opponent into backing down. In less extreme scenarios, a state afraid of being disarmed might take steps–issuing nuclear threats, for example, or dispersing mobile nuclear forces– that raised the likelihood of nuclear use later.

This danger is likely to be exacerbated by any cyber vulnerabilities affecting nuclear forces and C3I systems. Most directly, the existence of such vulnerabilities could intensify existing fears of being disarmed–fears that are already acute in China and Russia (as well as in Pakistan and, most likely, North Korea).5 However, because of their unique characteristics and effects, cyber threats could create at least three qualitatively new mechanisms by which a nuclear-armed state might come to the incorrect conclusion that its nuclear deterrent was under threat. First, the purpose of cyber interference could be misinterpreted. In particular, espionage could be mistaken for an attack. Second, a cyberattack could have a more significant effect than intended. Malware implanted into information technology (IT) systems associated with non-nuclear weapons could accidentally spread into more sensitive nuclear-related systems, for instance. Third, the initiator of a cyber operation could be misidentified. An operation carried out by a third party, for example, could be misattributed by one state in a bilateral confrontation to its opponent. What makes these pathways so pernicious is that the catalyst for escalation could appear to its initiator to be a relatively benign action.

To make matters worse, such pathways could lead to inadvertent escalation even if the target of the cyber interference were not afraid of being completely disarmed. Today at least, this description fits the United States. If, in a conflict against Russia, say, the United States wrongly concluded that its strategic early-warning system was under cyberattack, it might reason that Moscow was seeking to undermine U.S. missile defenses, which use early-warning data, prior to launching a nuclear attack.6 Given that U.S. declaratory policy explicitly highlights the option of a nuclear response to non-nuclear attacks on nuclear C3I assets, such a “misinterpreted warning” might lead Washington to use nuclear weapons.7 But even if it did not, its response, which might include nuclear threats, could still be escalatory.

My focus here is narrowly limited to inadvertent cyber threats against, or interference with, one state’s nuclear forces or C3I systems by another nuclear-armed state (C3I systems encompass not only communication capabilities, but also the intelligence, surveillance, and reconnaissance capabilities, including early warning, that would be critical to decision-making). To be sure, cyber vulnerabilities probably create other escalation risks too, though, in my judgment, they are less serious.8 For example, while no state would likely try to detonate another’s nuclear weapons, a nihilistic terrorist group might (though it is unclear whether such a group could obtain the requisite cyber capabilities). Separately, vulnerabilities associated with conventional forces or their C3I systems could increase the likelihood of a conventional war’s escalating to a higher level of violence, thus making nuclear use more credible.9

Cyber interference with nuclear forces and C3I systems can involve two (not mutually exclusive) types of operations: espionage and attack. Cyber espionage involves collecting data from a target IT system without otherwise damaging it. A cyberattack involves undermining the operations of the target system, typically by compromising the integrity or availability of data. Cyber tools suitable for surveilling or attacking nuclear forces or C3I systems have innumerable differences from noncyber tools, which are themselves quite varied. Six of these differences are particularly salient to the risk of inadvertent nuclear escalation.

First, cyber espionage offers the potential to obtain information about an adversary’s military forces and operations that cannot plausibly be obtained in any other way. By accessing an adversary’s C3I systems directly, cyber tools may be capable of exfiltrating exceptionally sensitive information, such as the locations of mobile delivery systems. This is not to suggest that cyber surveillance is infallible. As a security measure, for example, a state could choose not to track the movements of its mobile delivery systems (or it could do so only approximately). Alternatively or additionally, it could try to use a cyber intrusion in its networks to feed misinformation to the adversary. In spite of these and other limitations, however, cyber espionage almost certainly offers unique advantages. For example, no practical constellation of high-resolution surveillance satellites in low Earth orbit could provide continuous coverage of a given location on Earth’s surface.10 Cyber surveillance, by contrast, may allow for continuous monitoring of an adversary’s military posture.

Second, cyber weapons offer an unparalleled capability to manipulate the data that go into decision-making. Other types of weapons, by destroying or disabling sensors or communication systems, can also deny data to decision-makers. However, their use generally alerts the target to the fact it is under attack. By contrast, if a well-designed cyber weapon is used, a loss of data may appear to be, say, the result of a malfunction, potentially allowing the attacker to conduct surprise follow-on attacks. Even more significant, cyber weapons can be used to feed false information to decision-makers. For example, the Stuxnet virus, which was reportedly developed by the United States and Israel, was designed not only to destroy centrifuges at Iran’s Natanz enrichment plant, but also to hinder plant operators from discovering the cause of these failures by producing falsely reassuring readings on monitoring equipment.11 In a similar vein, sophisticated cyber weapons offer a unique capability to shape an adversary’s perception of a battlefield by feeding misinformation into C3I systems.12 To be sure, information operations have always been a part of warfare. However, cyber weapons represent a sea change because their effects can be tailored with great precision in real time, and because they could be used to directly influence the perceptions of high-level decision-makers.

Third, cyber operations–whether conducted for espionage or offensive purposes–can present particularly significant risks of unanticipated collateral effects, that is, of affecting IT systems other than the intended target.13 Noncyber weapons can, of course, lead to collateral damage. Yet such effects are inherently constrained by geography. Moreover, the likelihood of physical collateral damage can be often quantified, at least to some extent (military planners may be able to estimate, for example, the probability of an incoming weapon missing its military target and hitting a nearby civilian facility).14 The risks of collateral effects in cyberspace are much more difficult to estimate. Minimizing such effects relies, in part, on detailed intelligence about the target network and on connections between it and other networks. Obtaining the requisite intelligence is potentially much more difficult than identifying what surrounds a target in physical space (as is verifying that the resulting picture is complete). To complicate matters further, sophisticated malware must generally be tailored to each target and, if revealed, will become ineffective once the adversary can clean its networks and fix whatever exploit was used to gain access. As a result, the effects of cyber weapons cannot usually be understood through testing, further increasing the likelihood of unanticipated collateral damage (simulations can be used but they are only as good as the available intelligence on the target).

Fourth, in peacetime, malware used to enable a cyberattack may often be inserted into an enemy’s networks–but not activated–in the hope that it will remain undetected and thus can be used in a potential future crisis or conflict. (In theory, not only can a vulnerability in an operational IT system be exploited in this way, but so too could security weaknesses in the supply chain for the system’s components.) Noncyber weapons, by contrast, are generally used as and when the decision to authorize a strike on a particular target is taken.15 One consequence of this difference is that, if a state discovers dormant malware in its networks, it can be faced with the challenge of attributing it–that is, identifying which entity is responsible for its implantation–before activation. The equivalent challenge rarely arises with the kinds of noncyber weapons typically used in interstate warfare (though it does arise in irregular warfare or counterterrorism with unexploded ordnance).

Fifth, and relatedly, cyberattacks are generally easier to conceal than other forms of attack. As a result, decision-makers may be more inclined to authorize them. In fact, if the goal is for a cyber weapon to have either a persistent effect or an effect when triggered at some future time, the malware used in the attack must remain hidden to be effective because exposure could enable the adversary to take countermeasures.

Sixth, and finally, distinguishing between offensive operations and espionage is significantly more challenging in cyberspace than in other domains.16 To be sure, the line dividing espionage and offensive operations in physical space is not always entirely clear. Aircraft–unmanned aerial vehicles (UAVs), in particular –are used for both surveillance and offensive operations. But the distinction is much murkier in cyberspace. One challenge is that identifying the purpose of a piece of malware–understanding whether it can be used for espionage, offensive purposes, or both–can be time-consuming. In a fast-moving conflict or crisis, this process might move slower than decision-making. Moreover, even if a state quickly and confidently established that a piece of malware could be used solely for espionage, it could not be confident that whatever vulnerability was used to introduce the malware would not also be exploited for offensive purposes–at least until it had identified and fixed the vulnerability.

States can threaten each other’s nuclear forces through a combination of offensive “counterforce” operations to target nuclear-weapon delivery systems preemptively, and air and missile defense operations to intercept whatever remained. The United States openly acknowledges it would seek to limit the damage it would suffer in a nuclear war.17 Russian doctrine is believed to embrace a similar concept.18 India may be moving in the same direction.19

The question of whether, in practice, a state could actually succeed in limiting the damage it would suffer in a nuclear war to an extent that decision-makers would consider meaningful is currently a subject of considerable debate.20 However, from the perspective of inadvertent escalation, what matters is not whether damage-limitation operations would actually prove effective, but whether a potential target believes they might. In this context, Chinese and Russian fears that the United States is seeking the capabilities–non-nuclear capabilities, in particular–to negate their nuclear deterrents could prove escalatory in a crisis or conflict by generating “crisis instability,” that is, pressures to use nuclear weapons before losing the capability to do so.21 And even though the United States is not concerned today about the possibility of being disarmed, Washington appears to be less sanguine about the future, given growing threats to its C3I assets, in particular.

Cyber capabilities could contribute to damage-limitation operations in two distinct ways. First, cyber espionage could prove useful in collecting intelligence that might increase the effectiveness of counterforce attacks and air and missile defenses, especially if complemented by effective analytic tools for synthesizing large amounts of data from multiple sources.22 If cyber espionage helped reveal the locations of mobile weapons, for example, it could enable preemptive attacks against them. And if it helped to reveal targeting data, it could assist defenses in intercepting missiles and aircraft after launch.

Second, cyber weapons could be used, alongside other capabilities, to conduct counterforce strikes. A hypothetical cyber “kill switch” that could permanently shut down an adversary’s nuclear C3I systems would certainly be attractive to any state with a damage-limitation doctrine. In practice, this kind of perfect capability seems fanciful, not least because a state could find analog or even nonelectronic ways to use its own nuclear forces given enough time (in fact, some states may even prepare such means in advance). At best, therefore, a cyberattack could be a “pause button” that delayed an adversary’s ability to use its nuclear weapons. Real cyber weapons are likely to be still less effective, however. All nuclear-armed states likely operate multiple C3I systems with some degree of redundancy between them. Cyber operations would probably not prove equally effective against these different systems, potentially delaying the target from using some elements of its nuclear forces for longer periods of time than others.

Even given these limitations, however, cyberattacks could still assist with damage limitation. They could buy more time for counterforce operations to attrite an opponent’s nuclear forces and reduce the coherence of any retaliatory attacks, somewhat simplifying the task of air and missile defenses. Moreover, the potential for cyberattacks to shape an adversary’s perceptions could prove valuable. For example, an attacker might try to “blind” its adversary’s early-warning system just before launching counterforce strikes on its nuclear forces.

Just how effective cyber-enabled damage-limitation operations might prove in an actual conflict is far from clear, not least because of the difficulty of testing cyber weapons. That said, any state that has made the enormous investments necessary to develop damage-limitation capabilities is likely to spend relatively modest additional sums on developing complementary cyber tools, and it might reach a different conclusion about their potential efficacy. Even more important, from the perspective of inadvertent escalation, its potential adversaries might do so too.

China, in particular, appears to be concerned about cyber-enabled damage limitation. Summarizing the thinking of their peers on this subject, two Chinese scholars, Tong Zhao and Li Bin, have concluded that “Chinese analysts have demonstrated an acute awareness of the potential vulnerabilities of the country’s nuclear C3I system, particularly against cyber infiltrations.”23 Russian views have been less aired. In fact, a dichotomy has emerged in what little public discussion there has been. For example, three respected experts, including a former general officer in Russia’s Strategic Rocket Forces, have recently played down the threat, arguing that “because the command-and-control systems of strategic nuclear forces are isolated and highly protected, they are, in all probability, not vulnerable to cyber attacks.”24 At about the same time, however, another influential Russian scholar argued that, among the emerging non-nuclear technologies that could threaten nuclear forces, “probably the most dangerous development is cyber weapons, which could be used for non-nuclear disarming and decapitating attack by completely paralysing the entire command-and-control system.”25 News reports that Russia has created cyber defense units for its nuclear forces suggest that the Russian military may be less than sanguine about the cyber threat.26

Fears about cyber-enabled damage limitation may be particularly pernicious because of the potential difficulty of detecting a cyberattack. A sophisticated cyberattack on nuclear forces or C3I systems could conceivably occur without being detected. In the extreme case, a state might only find out that it had been attacked when it attempted to launch nuclear weapons and discovered that its ability to do so had been impeded in some way. If a state believed that it would be unlikely to detect an ongoing cyberattack, then it could rationally conclude that it might be under attack even in the absence of attack indicators. The simple belief that an opponent had highly sophisticated cyber capabilities could, therefore, precipitate a false positive–the incorrect assessment that an attack was underway–by itself. By contrast, if a state’s nuclear forces were under assault from kinetic strikes, the target would likely be aware. To be sure, it is still not entirely impossible that a state could wrongly come to believe it was under kinetic attack. Early-warning systems, for example, have produced false warnings of incoming ballistic missile strikes.27 But mistakes of this kind could be identified once the incoming weapons ceased to exist (though the window of time before they disappeared could be particularly dangerous).

To make matters worse, a state that was concerned about its nuclear forces and C3I systems coming under cyberattack might be inclined, especially in a crisis or conflict, to interpret ambiguous indicators in the worst possible light. For example, if one of its nuclear C3I systems malfunctioned because of, say, bad design or aging components, it might wrongly attribute the failure to a cyberattack (in fact, the temptation among operators to do so might be particularly strong if they would otherwise be held responsible for an internal failure). Regardless of precisely how it arose, however, a false positive that occurred in a crisis or conflict could generate significant escalation pressures.

Concerns about the potential for cyber operations to enhance the effectiveness of damage limitation can have effects beyond generating crisis instability at a time of heightened tensions or during a conflict. In peacetime, such concerns may induce nuclear-armed states to take steps to try to ensure that nuclear weapons could be employed when duly ordered in a crisis or conflict, even at the expense of exacerbating the danger of inadvertent or unauthorized use. Concerned states, for example, could remove permissive action links–electronic “locks” designed to prevent the unauthorized use of nuclear weapons–because of the perceived danger that they could be hacked and thus subverted to prevent authorized use.28

Alternatively or additionally, states could make plans to predelegate the authority to use nuclear weapons down the chain of command to guard against the possibility of the communication links serving national leaders being severed. The dangers of predelegation depend, in part, on the degree of flexibility afforded to commanders in determining whether and how to use nuclear weapons. Nevertheless, certain risks are inherent in any model. A localized communications failure might be mistaken for an attack, for example, leading to inadvertent use.29 Predelegation also increases the risk of unauthorized use because a field commander could order the use of nuclear weapons in a scenario in which he or she was not permitted to do so. This danger becomes greater as more people are granted launch authority. In this respect, cyber threats could promote a particularly dangerous form of predelegation by inducing a state to entrust launch authority to the relatively large number of lower-level officers who are capable of issuing a launch order without electronic communications.

Surveillance operations in cyberspace, even if conducted exclusively for defensive purposes, pose unique risks of escalation. Cyber surveillance of an adversary’s nuclear forces can serve purposes besides damage limitation. In any dyad involving two nuclear-armed states, each has a strong incentive to monitor the status of the other’s nuclear forces at all times–and particularly during a crisis or conflict–including for the exclusively defensive purpose of spotting any preparations for nuclear use. Several intelligence collection techniques, including overhead imagery and signals intelligence, are likely used for this purpose. Given the potentially unique advantages of surveillance in cyberspace, however, states may see good reason to adopt it alongside these other approaches, especially if they judge that the likelihood of cyber espionage being detected is small.

Depending on the sophistication of the malware used and the target’s defenses, the true likelihood of being detected may or may not be small, but the consequences of being caught could be significant. In fact, if the target detected ongoing cyber espionage of networks associated with its nuclear forces or C3I systems, inadvertent escalation could result from either of two concerns that are distinct from those that might plausibly be generated by other forms of surveillance.

First, even if the target of cyber interference were convinced that the operation was being conducted exclusively for the purpose of espionage, it might worry that the data being collected could be used against it in damage-limitation operations. Intelligence collection in physical space could also enable damage limitation, but it differs from cyber surveillance in one critical respect. In a crisis or conflict, a state would generally have no way of knowing whether or not countermeasures against physical surveillance (such as camouflage or concealment) had proved effective–unless its nuclear forces were successfully attacked. By contrast, if it detected an ongoing effort to collect intelligence through its C3I networks, it would know definitively that at least some of its cyber defenses had failed. This realization might lead the state to fear that attacks on its nuclear forces were imminent.

Second, because of the difficulty of rapidly distinguishing cyber espionage from a cyberattack, espionage against nuclear forces or C3I systems would risk being misinterpreted as an attack. In theory, the use of armed UAVs for surveillance of an adversary’s nuclear forces could generate a similar risk. However, a state motivated by purely defensive considerations would have strong and obvious reasons not to use armed UAVs in this way.

The risks resulting from cyber espionage being mistaken as an attack would depend on who had initiated the operation and who was the target. China or Russia might assess that U.S. cyber surveillance was actually an offensive effort intended to undermine–or, more likely, give Washington the option of undermining– Beijing’s or Moscow’s ability to launch nuclear weapons, thus potentially generating crisis instability. By contrast, because Washington is apparently more confident in the survivability of its nuclear deterrent, cyber espionage directed against U.S. nuclear forces or C3I systems would be less likely to have the same result. Nonetheless, such operations would likely be of real concern to Washington and could, for example, be misinterpreted as a prelude to nuclear use by China or Russia.

Even if the two states involved in a crisis or conflict did not engage in any kind of deliberate cyber interference with one another’s nuclear forces or C3I systems, one of them might wrongly conclude that the other had. Such a misperception, which could be the result of collateral effects or third-party action, could also induce escalation through crisis instability or misinterpreted warning.

A state that eschewed cyber operations of any kind against an opponent’s nuclear forces or C3I systems might still launch such operations against adversary military networks involved exclusively in non-nuclear operations. If, because of design flaws, imperfect intelligence, or mistakes in execution, the malware used in such attacks spread and infected networks that were involved in nuclear operations, the target might conclude that its nuclear forces or C3I systems were under deliberate cyberattack or cyber surveillance.

There could be collateral effects even if a state’s networks for nuclear operations were entirely isolated; air-gapping (physically isolating one particular network from others) is, after all, not a cyber security panacea.30 Moreover, achieving perfect isolation could prove difficult in practice.31 To give but one reason, every nuclear-armed state, apart from the United Kingdom, has dual-use delivery systems, which can be used to deliver nuclear or non-nuclear weapons. Such delivery systems represent a potential point of contact between the C3I systems supporting nuclear operations and those supporting non-nuclear operations.

In practice, some nuclear-armed states–perhaps many or even all of them– have not tried to isolate their nuclear C3I systems. The United States, for example, has a number of dual-use C3I assets for communications and early warning that support both nuclear and non-nuclear operations.32 Other nuclear-armed states, including China and Russia, may as well, but are less transparent.33 Because the networks supporting dual-use C3I assets are likely to be connected directly to others involved in non-nuclear operations, there may be a particularly high risk of their being subject to collateral effects.

#### It triggers nuclear retaliation.

Dr. Scott D. Sagan 21, Caroline S.G. Munro Professor of Political Science, the Mimi and Peter Haas University Fellow in Undergraduate Education, and Senior Fellow at the Center for International Security and Cooperation and the Freeman Spogli Institute at Stanford University, PhD in Political Science from Harvard University, and Allen S. Weiner, JD from Stanford University, Senior Lecturer in Law, Director of the Stanford Program in International and Comparative Law, and Director of the Stanford Center on International Conflict and Negotiation, “The U.S. Says It Can Answer Cyberattacks With Nuclear Weapons. That’s Lunacy.”, The Washington Post, 7/9/2021, https://www.washingtonpost.com/outlook/2021/07/09/cyberattack-ransomware-nuclear-war/

Over the July 4 weekend, the Russian-based cybercriminal organization REvil claimed credit for hacking into as many as 1,500 companies in what has been called the largest ransomware attack to date. In May, another cybercriminal group, DarkSide, also apparently located mainly in Russia, shut down most of the operations of Colonial Pipeline, which supplies nearly half the diesel, gasoline and other fuels used on the East Coast — setting off a round of panic buying that ended only when the company handed over a ransom. These incidents were bad enough. But imagine a much worse cyberattack, one that not only disabled pipelines but turned off the power at hundreds of U.S. hospitals, wreaked havoc on air-traffic-control systems and shut down the electrical grid in major cities in the dead of winter. The grisly cost might be counted not just in lost dollars but in the deaths of many thousands of people.

Under current U.S. nuclear doctrine, developed during the Trump administration, the president would be given the military option to launch nuclear weapons at Russia, China or North Korea if that country was determined to be behind such an attack.

That’s because in 2018, the Trump administration expanded the role of nuclear weapons by declaring for the first time that the United States would consider nuclear retaliation in the case of “significant non-nuclear strategic attacks,” including “attacks on the U.S., allied, or partner civilian population or infrastructure.” The same principle could also be used to justify a nuclear response to a devastating biological weapons strike.

But our analysis suggests that using nuclear weapons in response to biological or cyberattacks would be illegal under international law in virtually all circumstances. Threatening an illegal nuclear response weakens deterrence because the threat lacks inherent credibility. Perversely, this policy could also wind up committing a president to a nuclear attack if deterrence fails. While the American public would indeed be likely to want vengeance after a destructive enemy assault, the law of armed conflict requires that some military options be taken off the table. Nuclear retaliation for “significant non-nuclear strategic attacks” is one of them.

The Biden administration is now conducting its own review of the U.S. nuclear posture. The 2018 Trump change is an urgent candidate for reevaluation, but people have generally ignored it up to now. As officials work on this process, they have the chance to take full account of what could be called the “nuclear law revolution” — a growing recognition that international-law restrictions on warfare, and especially those that protect civilians, apply even to nuclear war.

Most Americans are aware of the strategic revolution that nuclear weapons themselves kicked off: The massive destruction they created made deterrence the highest national security priority. Soon after the bombing of Hiroshima in 1945, for example, Bernard Brodie, a preeminent early Cold War strategist, wrote: “Thus far the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them.”

Inherent in the idea of deterrence for decades was the notion that the United States would rain “assured destruction” on the cities of any nation that attacked us or our allies with nuclear weapons. During the height of the Cold War, for instance, U.S. nuclear war plans were designed to destroy “at least 70% of the urban industrial bases of the USSR and Communist China” and expected to kill “30% of the people,” according to declassified top-secret documents from the Nixon administration written in 1969 and 1971.

But such plans were manifestly not reconcilable with the central principles of the international law of armed conflict. This helps explain why the U.S. government asserted at the time of its negotiation that the 1977 Protocol I to the 1949 Geneva Conventions did not apply to nuclear weapons. That later treaty codified the obligation of all state parties to follow in war the principles of distinction (drawing a line between military targets and civilians), proportionality (making sure the unintended or “collateral” civilian harm resulting from a legitimate attack does not exceed the military advantage of that attack) and precaution (doing everything feasible to avoid or at least minimize collateral civilian deaths). U.S. nuclear war plans in the 1970s didn’t follow any of these rules.

In 2013, however, the Obama administration’s official nuclear weapons employment guidance announced that henceforth, “all plans must also be consistent with the fundamental principles of the Law of Armed Conflict.” From then on, even nuclear war plans would apply the principles of distinction, proportionality and precaution.

The Obama guidance document was categorical: “The United States will not intentionally target civilian populations or civilian objects.” According to Gen. C. Robert Kehler, the head of U.S. Strategic Command from 2011 to 2013, implementing this guidance led the command to develop nuclear delivery “tactics and techniques to minimize collateral effects,” and to “expand non-nuclear strike alternatives and add significant flexibility to our contingency plans.” The Trump administration’s 2018 Nuclear Posture Review reaffirmed the U.S. commitment to “adhere to the law of armed conflict” in any “initiation and conduct of nuclear operations” — but its interpretation of the law (allowing nuclear weapons to be used in response to a massively destructive biological or cyberattack) was flawed.

The unambiguous embrace of the application of international law to nuclear weapons means that if a future president ordered a Hiroshima-like attack, striking a city to kill as many enemy civilians as possible, it would be an illegal order that senior generals would be required to disobey. This would be true even if the order came in response to a nuclear attack on an American city; nations are not permitted to flout the rules of war protecting civilians simply because their enemies do. (A theory called “belligerent reprisal” holds that states may strike back at civilian populations in a proportionate way if the intent is to get the enemy to stop its own illegal warfare. We and other scholars have argued that this practice is not compatible with current understandings of international law.)

Yet it is not only pundits and the public that have failed to notice this legal revolution. Some writings by nuclear strategists, even those seeking to limit the dangers of nuclear war, have ignored the shift. In 2018, for instance, the late Princeton research scholar Bruce Blair proposed a policy of what he and others have called “minimal deterrence”: His version involved cutting the U.S. arsenal to fewer than 700 warheads, from some 2,000 today, and aiming them to guarantee “the annihilation of scores of [Russian] cities housing banking and oil infrastructure as well as key manufacturing and leadership facilities.” But a policy targeting civilian infrastructure would clearly violate international-law rules that Washington recognizes apply to nuclear targeting.

This is not to say that the laws of war preclude all use of nuclear weapons (a conclusion that some legal scholars have embraced). The principle of proportionality permits some U.S. nuclear attacks against military targets — for example, when the harm such a strike would prevent to U.S. and allied populations would exceed the foreign collateral damage it caused. (Any associated civilian deaths would have to be truly incidental and unavoidable. Deliberately causing purported “collateral” civilian damage to force an enemy to stand down would be illegal.) Those planning a nuclear counterattack would also be obliged to use the lowest-yield weapons necessary to destroy or neutralize the legitimate military targets they place in their sights.

If the laws of war strictly constrain nuclear retaliation for a nuclear attack on the United States, they all but certainly bar such a strike in response to a cyber- or biological attack — even one causing many civilian casualties. In almost any imaginable scenario, the use of nuclear weapons would violate the principle of precaution, the requirement to minimize harm to civilians if feasible. That’s because the formidable U.S. military has the capacity to halt, or to induce the adversary to halt, ongoing cyberattacks through conventional or cyber-responses that would cause less harm to foreign civilians than would a retaliatory nuclear strike.

There are a few possible, but largely hypothetical, exceptions to this rule. One would be if the individuals or organization responsible for the cyber- or biological attack were in an underground bunker that couldn’t be destroyed any other way. Another hypothetical option, a nuclear demonstration strike against an isolated military target, might be legal, but it would be strategically stupid, as it would actually demonstrate lack of resolve. A stronger response would directly target — through conventional means — the perpetrators and their ability to launch further attacks on us or our allies.

Using nuclear threats to deter cyberattacks is also inherently less credible than threatening retaliation with conventional weapons or in kind (that is, with cyber-retaliation). The states that we worry most will launch cyberattacks — Russia, China and North Korea — also have nuclear weapons, and their leaders might reasonably calculate that any U.S. president would be reluctant to use nuclear weapons against a nation that can retaliate in kind. An adversary might also believe that the U.S. military would refuse to use nuclear weapons in response to non-nuclear attacks precisely because of questions around legality. Such suspicions undermine the deterrent force of nuclear weapons; in contrast, if the United States were to commit to only conventional or cyber-retaliation to “significant non-nuclear strategic attacks,” adversaries would have fewer doubts that we would follow through.

Not only might a U.S. nuclear threat against a cyber- or biological attack be perceived as a bluff, it could be doubly dangerous if it subjected the president to what has been called the “commitment trap.” If Washington threatens a nuclear response to deter a cyberattack, but adversaries go ahead anyway because the threat is deemed not credible, then there would be increased pressure on the president to order a nuclear strike to rebut domestic political claims of weakness and shore up international perceptions about the credibility of future threats. But succumbing to such political pressure or the urge for vengeance would create an unacceptable risk of further nuclear escalation.

#### CI collapse metastasizes---extinction.

Benjamin Monarch 20, University of Kentucky College of Law, J.D. May 2015, LLM in Energy, Natural Resources, and Environmental Law and Policy from the University of Denver Sturm College of Law, Deputy District Attorney at Colorado Judicial Branch, and Term Member at the Council on Foreign Relations, “Black Start: The Risk of Grid Failure from a Cyber Attack and the Policies Needed to Prepare for It,” Journal of Energy & Natural Resources Law, vol. 38, no. 2, Routledge, 04/02/2020, pp. 131–160

In the industrial world, when a switch is flipped, we take for granted that it will produce light, boot a computer, illuminate a stadium or activate a power plant. We know, of course, that power losses can and do occur. Many of us have lit candles during a thunderstorm or brought out extra blankets when a blizzard takes down transmission lines. As of this writing, the most populated state in the United States, California, is experiencing rolling blackouts.1 Yet even in prolonged power outages, we expect that electricity will be restored and, consequently, life will return to normal. Perhaps we need ask, however, what if power cannot be restored in a timely manner? Concern is growing that in the not-too-distant future our electricity supply could be irreparably compromised by a cyber attack. The issue when considering a systemic grid failure of this nature is twofold: how did we reach a point where something so critical to routine life now presents an existential threat, and what can we do to mitigate the risk of a catastrophic grid attack?

This article posits that the emergence of cyber attacks on industrial control systems, as a means of war or criminal menace, have reached a level of sophistication capable of crippling those systems. This article argues that a new grid security policy paradigm is required to thwart catastrophic grid failure – a paradigm that recognises the inextricable link between commercial power generation and national security. In section 5, seven policy recommendations are outlined that may, in part, mitigate a future where grid attacks pose existential risk to nations and their citizenry. Those recommendations are: first, develop a comprehensive insurance programme to minimise the financial risk of grid disruption; second, train more cybersecurity professionals with particular expertise in industrial control systems; third, institute a federally mandated information-sharing programme that is centralised under United States Cyber Command; fourth, subsidise and/or incentivise cybersecurity protections for small to mid-size utilities; fifth, provide university grants for grid security research; sixth, integrate new technologies with an eye towards securing the grid; and, lastly, formulate clear rules of engagement for a military response to grid disruption.

The purpose of this article is to provide the reader with an introduction to this complex topic. It is the aim of the author to give orientation to this issue and its many branches in the hope that better understanding will animate further curiosity and, ultimately, positive action on the part of the reader. Although many skilled and earnest people work tirelessly to prevent a grid failure scenario, it is essential that more be added to their ranks each day. Advisors, engineers, regulators, private counsel to power generators, and many others who play roles in electric power production are crucial to this subject. So, while this article provides entrée to the topic of grid security, its long-term objective is to spur action by the entire energy-related community. In the end, no one is immune to consequences of grid failure and, therefore, everyone is responsible, in part, for promoting grid integrity.2 In this regard, lawyers who represent various actors in the energy sector are going to be faced with questions and potential legal risks of a magnitude that they have never experienced before.

1.2. Turning the power back on in a powerless world

‘Black start’, not to be confused with the term ‘blackout’, is the name given to the process of restoring an electric grid to operation without relying on the external electric power transmission network to recover from a total or partial shutdown.3 At first glance, this description is unremarkable, but it implies a disturbing catch-22 – how might one restore power if the entire external transmission network is compromised?

If an electric disruption occurs at a household level, some homes may be equipped with a modest gasoline generator to temporarily restore power. If a hospital loses power, it will almost invariably be resupplied by automatic, industrial-scale generators. These micro considerations hardly give anyone pause; they are hiccups on a stormy night or a snowy day. In other words, their ‘black start’ is a quick and effective process for restoring power. But what happens, at a macro level, when an electric grid supplying power to large portions of the United States goes black, or worse, what happens if all of the United States’ electric grids go down simultaneously?4 In that scenario, how might enough non-grid power be harnessed and transmitted to turn the United States’ lights back on? Moreover, how might such a catastrophe occur in the first place? Perhaps the more ominous question is not how, but whether or not we can survive such circumstances if they persist in the long term.

The United States electric grid (‘the grid’) is the ‘largest interconnected machine’ in the world.5 It consists of more than 7000 power plants, 55,000 substations, 160,000 miles of high-voltage transmission lines and millions of low-voltage distribution lines.6 The scale and complexity of the grid in the context of the modern digital world are beyond comprehension because within it are innumerable industrial control systems; incalculable connections to digital networks; millions, if not billions, of analogue or digital sensors; many thousands of human actors; and trillions of lines of programming code.7 Further complexifying the grid is that it is comprised of generations of technologies, stitched together in ways that are not inherently secure in a world of cyber threats.8 The vastness of the grid makes security of it challenging. Likewise, the vastness of the grid makes the opportunities for intrusion seemingly infinite.

By any measure, grid failure will unleash a parade of horrors. Stores would close, food scarcity would follow, communication would cease, garbage would pile up, planes would be grounded, clean water would become a luxury, service stations would yield no fuel, hospitals would eventually go dark, financial transactions would stop, and this is only the tip of the iceberg – in a prolonged grid failure social chaos would reign, once-eradicated diseases would re-emerge and, increasingly, hope of returning to a normal life would fade.9 The notion of complete grid failure, once relegated to science fiction comics or James Bond movies, is now not only possible but also one of the most pressing national security threats today.10

#### IoT enables effective climate mitigation.

Huawen Tian et al. 22, Law, Shandong University of Science and Technology; Liwen Jiang, Economics & Management, Shandong University of Science and Technology; Jie Zhang, Management, Shandong University of Technology, "Construction of Wireless Sensor Model for Carbon Neutralization and Environmental Protection From The Perspective Of Energy Internet Of Things Transformation," Journal of Sensors, 01/17/2022, Hindawi.

Climate change has a profound impact on the earth’s environment, which is a great challenge facing mankind [1]. In order to cope with global climate change and realize the progress of human civilization and the sustainable development of the earth’s ecosystem, the 21st United Nations Climate Change Conference adopted the Paris climate agreement, which proposed to achieve the goal of “net zero emission” of CO2 around 2050, that is, carbon neutralization [2]. Broadly speaking, carbon neutralization refers to the dynamic balance between carbon source systems such as human fossil energy utilization, land use, and natural volcanic eruption carbon emission and carbon sink systems such as earth’s carbon cycle system, marine carbon dissolution, and biosphere carbon absorption. In a narrow sense, carbon neutralization refers to the CO2 emission of an organization, group, or individual in a period of time, which is offset by forest carbon sink, artificial transformation, geological storage, and other technologies to achieve “net zero emission” [3]. Carbon neutralization is an important way to effectively control the rapid rise of global temperature, promote the green transformation of energy utilization, and promote green, low-carbon, and other technological progress [4]. It is a new driving force for world economic development and growth [5]. Realizing carbon neutralization will improve the earth’s ecological environment on which human beings depend and reduce environmental problems caused by human activities [6]. In 2019, the World Health Organization announced that air pollution and climate change ranked first among the top ten health threats in the world [7]. It is estimated that from 2030 to 2050, climate change will cause about 250000 new deaths from malnutrition, malaria, diarrhea, and excessive temperature in the world every year, and 7 million people will die prematurely from diseases such as cancer, stroke, heart disease, and lung disease every year [8]. Carbon neutralization will promote the transformation of human energy system to green, low-carbon, and carbon-free, realize the substitution of carbon-free new energy for high-carbon fossil energy, and drive the growth of jobs and GDP in the field of new energy industry [9]. It is estimated that by 2050, the average annual investment in the field of global energy low-carbon transformation will exceed US $3.2 trillion, the cumulative investment will exceed US $95 trillion, and more than 100 million jobs will be provided [10]. Carbon neutralization is the common goal and pursuit of all mankind. The global cooperation mechanism with consultation as the main body is the premise and guarantees to achieve carbon neutralization [11]. In the process of actively promoting carbon neutralization all over the world, it is necessary to carry out carbon neutralization research guided by scientific issues [12].

The automatic identification center established by MIT proposed a radio frequency identification system-item loading sensing equipment [13]. Through the application of RF technology, it is connected with other objects to realize the interconnection of objects and form an intelligent control system [14]. Internet of things is another widely concerned network in the network field after the Internet. It is based on standards and has the ability of self-configuration and management [15]. The Internet of things supports the direct information interaction between people and things, and wireless sensor networks only support the information exchange between things, in order to provide users with the environmental information they need [16]. Therefore, wireless sensor network is the technical basis of the Internet of things and a branch network of the Internet of things. From the historical background of the emergence of wireless sensor network technology, wireless sensor network has experienced wireless data network, wireless ad hoc network, and wireless sensor network [17]. The traditional environmental detection method is to manually obtain various material samples in the environment, such as air, water, and soil, and test the collected samples on the instruments in the laboratory [18]. Such a sample acquisition method can only collect limited data, and the data is not reliable. In order to meet people’s demand for various resource monitoring in the future and maintain the sustainable development of economy and environment, we need to obtain a large amount of environmental information timely and accurately [19]. Because of its own characteristics, wireless sensor networks are different from traditional fixed networks. They have the characteristics of limited resources, self-organization, dynamic network, wide scale, and high density [20]. The characteristics of wireless sensor network, such as single deployment, low cost, network self-configuration, and no manual maintenance, make it suitable for the field of environmental monitoring. Multiple nodes carrying various sensors are distributed in the required monitoring environment, and the nodes cooperate to complete the remote monitoring task [21]. Although the research time of wireless sensor network is very short, a large number of sensor network research and application make its technology develop rapidly. With the continuous exploration of wireless sensor networks all over the world, the application of wireless sensor networks has widely existed in all fields of production and life [22]. It is the research focus and application technical basis of wireless networks in the future. Wireless sensor networks (WSNs), which combine sensor technology, microelectronics technology, and wireless technology, are a powerful network. It has been widely used in road traffic, military safety, environmental monitoring, intelligent life, and other aspects. Today’s society is affected by the technology and application of WSN [23]. Wireless sensor networks play an important role in monitoring, such as the concentration of carbon dioxide in the air, air humidity, and light intensity. The monitoring of these indicators can well reflect the results of carbon neutralization and provide an important basis for the early realization of carbon neutralization. This paper analyzes the development background and research status of energy Internet of things technology at home and abroad and determines the overall design scheme of environmental monitoring Internet of things system. Then, the wireless sensor network model is applied to the detection of air quality in the environment to detect the content of CO2 in the air more accurately, which is of great significance to achieve the goal of carbon neutralization as soon as possible.

2. Related Work

The Internet of things takes data networking as the essential core, while the energy Internet of things has a large number of users and devices, and the data collected by its measurement and perception is very valuable. On the one hand, the use of massive data enables the energy industry to fully understand its own characteristics and provide new technical support means for low-carbon green development, energy efficiency improvement, energy conservation and consumption reduction, economic operation, and system planning of the energy industry; on the other hand, data analysis and processing based on deep learning, artificial intelligence and other technologies can improve the production efficiency of the energy system, provide better consumer services for users, and provide more efficient decision support for system operators. The Internet of things and wireless sensor networks have been widely favored all over the world. In 1991, the concept of “pervasive computing” proposed by the United States involved perceptual technology, and then, MIT first proposed the “Internet of things” [24]. IBM announced the “smart earth” plan to the outside world in November 2008. Immediately, the plan received strong support from the government and jointly developed smart grid and smart medicine [25]. Carbon neutralization means that enterprises, groups, or individuals calculate the total amount of greenhouse gas emissions directly or indirectly generated within a certain period of time to offset their own carbon dioxide emissions through afforestation, energy conservation, and emission reduction, so as to achieve “zero emission” of carbon dioxide. As a new form of environmental protection, carbon neutralization has been adopted by more and more large-scale events and conferences. Some other developed countries have also set development goals and taken a number of feasible measures to promote their rapid development. In the field of agricultural environmental monitoring, data transmission technology and environmental data acquisition technology have been developed [26]. In terms of data transmission, there are two measures to ensure the correctness of data transmission: the optimal network protocol and the appropriate network deployment [27]. The correctness of agricultural environmental data transmission first needs the optimal network protocol. The agricultural environment monitoring based on wireless sensor network needs to deploy the network according to the characteristics of the monitoring area. When wireless sensor networks need a single network in a small-scale agricultural monitoring environment, the physical layer and data link layer of the network protocol are the same [28]. However, when wireless sensor networks need composite networks in complex environments, different network layer and application layer specifications are formulated due to specific network protocols. It can be seen from the literature that the fusion between networks requires standards to agree on the communication between different networks [29]. According to different monitoring environments, the research focus of routing algorithm is also different. It can be seen from the literature that the protocols related to wireless sensor networks are appropriately tailored to meet the characteristics of agricultural monitoring environment. Second, select the appropriate topology to deploy the network nodes to make the network reach the optimal state, so as to transmit data reliably [30]. Wireless sensor networks deployed in various regions as the experimental field of project research have promoted the rapid development of Internet of things related technologies. Gong and Jiang [31] proposed a smart city Internet of things system for monitoring indoor temperature, humidity, and CO2. It uses PIC24F16KA102 chip as the main control and NRF24L01 RF module with 2.4 GHz bandwidth as the transmitting and receiving node to collect temperature, humidity, CO2, and other sensing data, transmit it to PC through USB, and transmit the data to mobile phone app through the Internet, so as to obtain, save, and process environmental data. Liu et al. [32] proposed a low-power Internet of things system for long-term monitoring of outdoor environment. It is composed of sensor node, gateway node, application server, and back-end alarm equipment. The sensor node collects temperature data through the main control and sends the sensor data to the gateway equipment through CC1150 RF module; the gateway device collects RF data through the 433 module and drives the GPRS module to transmit the data to the application server through the main control module; the application server stores and provides data support for the back-end alarm device; the back-end alarm device runs data query and alarm functions. Vijayalakshmi et al. proposed a real-time environment monitoring Internet of things system using solar energy self-power supply [33]. It is composed of solar panel, power management module, main control module, XBee RF module, and sensor module. Solar panels generate electric energy during the day, provide electric energy for system operation, and charge 50 f capacitors; The main control module collects the information of temperature, humidity, CO, CO2, and LDO sensors and transmits the data through XBee module. The power consumption of the whole system is about 4.907 mW. At the same time, the 50 F capacitor can be charged to 4.6 V by the solar module during the day; when the operating voltage of the system is between 3.6 V and 4.6 V, the 50 F capacitor can provide the power of the whole system for 12 hours at night [34]. Muthukumaran et al. [35] put forward a cloud service monitoring system for diabetes patients. In the system, the sensor node layer is composed of two parts. One part collects indoor environmental information, such as temperature, humidity, time, location, and air quality, and the other part collects patient information, such as heart rate and body temperature; the gateway is responsible for local data storage, data packaging, data push, and other functions; the cloud service layer is responsible for cloud data storage, data query, and other functions; the equipment terminal can view the information of patients and rooms in real time. The sensor node layer communicates through a 2.4 GHz radio frequency module; the sensor node and gateway transmit data through WiFi module.

3. Research Methods and Key Technologies

3.1. Transformation of Energy Internet of Things

This paper will explore the path description and research methods of energy Internet of things transformation and discuss how to use power system, Internet of things, and social factors to strongly support energy transformation. In 2015, the proportion of nonfossil energy power generation was 30%. The schematic diagram of energy transfer path is shown in Figure 1, showing the change curve of the proportion of renewable energy in primary energy. Under the goal that the proportion of nonfossil energy power generation will reach 80% in 2050, there can be different paths to achieve this goal, and different paths will have different effects on the national economy. How to plan the energy transfer path can take into account the constraints of coordinated economic development and carbon emission, which is worthy of in-depth research.

[Figure omitted]

In many paths, the transformation task can be allocated to each year by linear method; we can also increase the amount of renewable energy as soon as possible, so as to obtain carbon emission benefits as soon as possible and save resources. However, due to immature technology and other reasons, the investment will increase. Or use the opposite method to accumulate experience at the beginning and accelerate the pace of transformation when the technology is mature. Therefore, among many paths, how to find a feasible method to compare different paths and select the optimal path has become an urgent problem to be solved. The proportion of nonfossil energy power generation is used as the characteristic quantity of energy transformation, as shown in Figure 1. The time series trajectories of different transformation curves are marked with typical power functions. The power of the transformation curve is represented by , the linear transformation curve is a special case where the power is equal to 1, and represents the power of the transformation curve. represents the initial proportion of new energy, represents the target proportion, and represent the starting year and target year, respectively. In year , the proportion of new energy can be expressed as

[Equation omitted]

3.2. Key Technologies of Energy Internet of Things

The network nodes in the energy Internet of things can ensure the comprehensive monitoring of the external environment and improve the overall quality of data transmission. In environmental monitoring, we need to improve the security and stability of data transmission. Combined with the actual characteristics of the Internet of things, we can optimize the design of link layer data transmission and enhance the security of data. We can also establish the reliability analysis method of data transmission of the Internet of things system and take corresponding management measures to ensure the overall effect of data transmission of the Internet of things. The Internet of things system mainly includes three parts: application layer, perception layer, and network layer. The sensing layer is composed of various sensor devices, including reader, terminal camera, and GPS. It can sense the external environment and collect a variety of signals and physical information. The network layer refers to the IOT network communication system, including information processing center and intelligent control center, which can process information quickly and timely.

A large number of microsensor nodes are arranged in the monitoring area to realize the self-organizing network system by means of wireless communication. Various microsensors can be integrated to realize the real-time reception and transmission of information. Wireless communication transmits various data information, and the information obtained by the sensor can also realize the development of integration, miniaturization, and networking, as shown in Figure 2. Wireless sensor network integrates embedded computing, sensor technology, wireless communication technology, and modern network technology, which can enhance the perception ability of the whole device. It is an important prospect in the field of Internet of things.

[Figure omitted]

3.3. Construction of Wireless Sensing Model under Energy Internet of Things Technology

Under the condition of Internet of things technology, it is necessary to analyze the application characteristics of ecological environment, meet the overall needs of system architecture, and improve the overall quality of service monitoring. Wireless sensor nodes with self-organizing function are connected in the form of wireless transmission, which can conduct three-dimensional and comprehensive monitoring of the ground, underground, and air environment, forming a 3D Internet of things environment monitoring system, as shown in Figure 3. The detection system uses Ethernet to monitor different indicators in the environment, such as temperature and humidity. Then, it is transmitted to the remote client through the network.

[Figure omitted]

The core node design of the Internet of things needs to be composed of control and information processing unit, storage unit, and communication unit, and the distributed power supply is used to provide support. Build a monitoring system suitable for the ecological environment of different villages and towns, analyze it combined with the Internet of things node technology and ecological environment sensing data, and develop a sensor module to meet the monitoring of multi environmental parameters such as gas, water, and soil. In order to improve the security and reliability of data and information transmission in the Internet of things, it is necessary to effectively control the nodes of the whole data transmission, design specific methods such as error recovery, congestion control, and flow control, establish sensor models, comprehensively optimize the deployment and coverage of regional sensor nodes, and take corresponding management measures to ensure the quality of information transmission.

The whole IOT monitoring system can realize two working modes to adapt to different application environments.

The situation in the working mode of the area coverage monitoring system is as follows. As shown in Figure 4, the regional monitoring system includes LAN nodes, main control module, and data cloud platform. It can carry out real-time environmental monitoring for large areas, upload data to the data platform in real time, and synchronously monitor the information of each node (impact, temperature, humidity, light and general ad data, etc.).

[Figure omitted]

The working mode of the fixed-point direct connection monitoring system is as follows. Based on the regional coverage monitoring system, the fixed-point direct connection monitoring system removes the monitoring ability of multinode environment and retains the passive wireless impact sensor node network. Its environmental data collection mainly comes from the data collection of the main control module (impact, temperature, humidity, light, dust, general AD data, etc.). At this time, the monitoring range of fixed-point direct monitoring becomes smaller, but the data acquisition frequency increases, which is mainly applicable to scenes with high data requirements. Its design architecture is shown in Figure 5.

[Figure omitted]

4. System Test and Analysis

This chapter mainly tests the environment monitoring Internet of things system, including passive wireless impact sensing module, area coverage monitoring system, and fixed-point direct connection monitoring system, tests and detects the overall function of the system, and verifies the function of the whole system.

4.1. Node Circuit Test

For the node circuit, it is necessary to test the energy storage capacitance and the operation of the control circuit. The energy storage capacitor is a 10 uF tantalum capacitor. After receiving the DC voltage converted by the impulse signal, its voltage test is shown in Figure 6. As can be seen from the figure, the maximum output voltage can reach about 7.2 V, and the voltage shows an exponential attenuation trend with time, which can realize the storage of electric energy and meet the power supply of ultralow power RF module. Since the back-end control circuit will turn on when it is above 3.2 V, the output voltage is the energy storage capacitor voltage, and the voltage of 7.2 V will burn the ultralow power RF module chip, a voltage stabilizing diode must be added at the output voltage to protect the RF chip.

[Figure omitted]

Add the control circuit after the energy storage capacitor and test its output voltage, as shown in Figure 7. When the energy storage voltage of the energy storage capacitor increases from 0 V to 3.2 V, the voltage of the control circuit is 0 V; when the voltage of the energy storage capacitor is greater than 3.2 V, the voltage of the control circuit changes with the voltage of the energy storage capacitor; after that, the voltage of the control circuit will always follow the voltage of the energy storage capacitor to drop to about 1.6 V, and then turn off the output. The control time of the whole control circuit is about 40 ms, that is, the normal working time of ultralow power RF circuit; the voltage output is 1.6 V to 3.2 V, closely following the voltage change of the energy storage capacitor. The design function of the control circuit is verified.

[Figure omitted]

4.2. Overall Function Test

In the overall function test, the fixed-point direct monitoring Internet of things system will be tested in the field. Through the real-time monitoring of the surrounding environment, the data of dust, temperature, humidity, and illumination of the surrounding environment will be collected in real time to verify the working condition and stability of the whole system. The monitoring time is one hour, and the change curve of each environmental information is obtained, as shown in Figure 8. The system works stably, and all sensing data curves are displayed and saved in real time. At the same time, it can be seen from the data that the system can stably monitor all kinds of data information in the outfield environment.

[Figure omitted]

According to the above tests, the basic functions of the whole Internet of things system have been realized, including the alarm function of passive wireless impact sensing, the cloud real-time monitoring function of environmental data, and the real-time sending function of cloud instructions. The real-time monitoring of indoor and outdoor environment has been realized under two working modes, and the task objectives set in the early stage of the whole system have been realized. The test results show that the environmental monitoring Internet of things system can realize the real-time acquisition and data transmission of passive wireless impact sensing signals, use 10 uF tantalum capacitor to store energy and complete about 20 m RF data transmission with about 42 uJ energy supply; the completed area coverage monitoring system uses five ZigBee sensor nodes and master control nodes to collect a variety of sensor data (temperature, humidity, and light) and interact with the data instructions of ONENET cloud platform, with stable operation and reliable performance; the completed fixed-point direct connection monitoring system can collect a variety of sensing data and interact with the data instructions of Alibaba cloud platform, with strong reliability and stable operation. The system achieves the expected design and functional objectives.

5. Conclusion

Internet of things technology can automatically analyze the concentration, emission, and emission speed of toxic and harmful substances in the natural environment. It can also transmit data information to the environmental monitoring and management department in real time, formulate scientific and reasonable pollution management strategies, and ensure the rapid and timely treatment of pollution problems. Wireless sensor networks are widely used in environmental monitoring. Atmospheric monitoring is mainly online monitoring or mobile monitoring. Online monitoring can realize synchronous monitoring and monitoring prediction. Comprehensively analyze the future atmospheric environment conditions, and install fixed monitoring equipment at the discharge of pollution sources to form a distributed network to comprehensively control specific pollutants. Various wireless sensor network devices can be used to collect the data of sulfur dioxide and inhalable particles of nitrogen oxides in the atmospheric environment in an all-round way and use the network to transmit the real-time data to the monitoring center to automatically analyze the environmental quality and clarify the overall effect of environmental data processing. Aiming at the environment under the background of carbon neutralization, this paper carries out the research on the technology of environmental monitoring Internet of things system, focuses on the key technologies such as multisensor terminal, local area network communication, wide area network communication, and data cloud platform, and develops a complete set of Internet of things system, which realizes the monitoring of dust, light, temperature, and real-time monitoring of humidity and other environmental parameters, and on this basis, support the scalability of the system to meet the needs of different environmental conditions. We have added relevant contents as follows: today’s world is experiencing great changes that have not been seen in a century. The ecological environment is related to human survival and sustainable development, which requires the unity and cooperation of all countries to jointly meet the challenges. Carbon neutralization is a consensus reached by mankind in response to global climate change. Countries all over the world actively commit to achieving the goal of carbon neutralization. Carbon substitution, carbon emission reduction, carbon sequestration, and carbon cycle are the four main ways to realize carbon neutralization, and carbon substitution is the backbone of carbon neutralization.

#### Absent that, extinction.

Simon Beard et al. 21, Centre for the Study of Existential Risk, University of Cambridge; Lauren Holt, Centre for the Study of Existential Risk, University of Cambridge; Asaf Tzachor, Centre for the Study of Existential Risk, University of Cambridge. Cambridge Global Food Security Interdisciplinary Research Centre, University of Cambridge; Luke Kemp, Australia National University; Shahar Avin, Centre for the Study of Existential Risk, University of Cambridge; Phil Torres, Institute of Philosophy, Leibniz University Hannover; Haydn Belfield, Leverhulme Centre for the Future of Intelligence, University of Cambridge, "Assessing Climate Change’s Contribution to Global Catastrophic Risk," Futures, Vol. 127, March 2021, ScienceDirect.

While most of the impacts of climate change so far have fallen within the range of what was experienced during the Holocene, the rate of change is faster than in the Holocene and we are now beginning to see climate change push beyond these boundaries. In the latest edition of the planetary boundaries’ framework, climate change is placed in the zone of increasing risk, implying that while this boundary has been breached, there remains some potential for normal functioning and recovery (Steffen et al. 2015). It thus lies between what the authors identify as the ‘safe zone’ and other ‘high risk’ transgressions, such as disruption to the biochemical flows of nitrogen and phosphorus and loss of biosphere integrity.

As part of their discussion of BRIHN Baum and Handoh (2014) note that climate change is the planetary boundary for which the risk to humanity has received most meaningful consideration and they suggest that this attention is deserved. Yet little research attention has been paid to climate change’s extreme or catastrophic effects. Kareiva and Carranza (2018) argue that, despite currently falling outside of the area of high risk, climate change has the clear potential to push humanity across a threshold of irreversible loss by “changing major ocean circulation patterns, causing massive sea-level rise, and increasing the frequency and severity of extreme events… that displace people, and ruin economies.” Even if humanity was resilient to each of these individual impacts, a global catastrophe could occur if these impacts were to occur rapidly and simultaneously.

One scenario that has received comparatively more attention is that of the global climate crossing a tipping point that would trigger environmental feedback loops (such as declining albedo from melting ice or the release of methane from clathrates) and cascading effects (such a shifting rainfall patterns that trigger desertification and soil erosion). After this point, anthropogenic activity may cease to be the main driver of climate change, making it accelerate and become harder to stop (King et al. 2015).

Other scenarios can be discerned from the numerous historical cases in which the modest, usually regional, climatic changes experienced during the Holocene have been implicated in the collapse of previous societies, including the Anasazi, the Tiwanaku, the Akkadians, the Western Roman Empire, the lowland Maya, and dozens of others (Diamond 2005, Fagan 2008). These provide a precedent for how a changing climate can trigger or contribute to societal breakdown. At present, our understanding of this phenomena is limited, and the IPCC has labelled its findings as “low confidence” due to a lack of understanding of cause and effect and restrictions in historical data (Klein et al. 2014). Further study and cooperation between archaeologists, historians, climate scientists and global catastrophic risk scholars could overcome some of these limitations by identifying how the impacts of climate change translate into social transformation and collapse, and hence what the impacts of more rapid and extreme climatic changes might be. There is also the potential for larger studies into how global climate variations have coincided with collapse and violence at the regional level (Zhang 2005; 2006). However, these need to be interpreted and generalized with care given the differences between pre-industrial and modern societies.

Societies also have a long history of adapting to, and recovering from, climate change induced collapses (McAnay and Yoffee 2009). However, there are two reasons to be sceptical that such resilience can be easily extrapolated into the future. First, the relatively stable context of the Holocene, with well-functioning, resilient ecosystems, has greatly assisted recovery, while anthropogenic climate change is more rapid, pervasive, global, and severe. Large-scale states did not emerge until the onset of the Holocene (Richerson et al, 2001), and societies have since remained in a surprisingly narrow climatic niche of roughly 15 mean annual average temperature (Xu et al, 2020). A return to agrarian or hunter-gatherer lifestyles could thus have more devastating and long-lasting effects in a world of rapid climate change and ecological disruption (Gowder 2020).[12] Second, modern human societies may have developed hidden fragilities that amplify the shocks posed by climate change (Mannheim 2020) and the complex, tightly-coupled and interdependent nature of our socio-economic systems makes it more likely that the failure of a few key states or industries due to climate change could cascade into a global collapse (Kemp 2019b).

A third set of plausible scenarios stem from climate change’s broader environmental impacts. Apart from being a planetary boundary of its own, Steffen et al. (2015) point out that climate change is intimately connected with other planetary boundaries (see Table 1). Climate change is thus identified by the authors as one of two ‘core' boundaries with the potential “to drive the Earth system into a new state should they be substantially and persistently transgressed.” This transformative potential was elaborated on in subsequent work exploring how the world could be pushed towards a ‘Hothouse Earth’ state, even with anthropogenic temperature rises as low as 2°C (Steffen et al. 2018).

[Figure omitted]

The connection between climate change and biosphere integrity (the survival of complex adaptive ecosystems supporting diverse forms of life) is particularly strong. The IPCC is highly confident that climate change is adversely impacting terrestrial ecosystems, contributing to desertification and land degradation in many areas and changing the range, abundance and seasonality of many plant and animal species (Arneth et al. 2019). Similarly, the Intergovernmental Science-Policy Platform on Biodiversity and Ecosystem Services (IPBES) has reported that climate change is restricting the range of nearly half the world’s threatened mammal species and a quarter of threatened birds, with marine, coastal, and arctic ecosystems worst affected (Diaz et al. 2019). According to one estimate, climate change could cause 15-37% of all species to become ‘committed to extinction’ by mid-century (Thomas et al. 2004).

Disruption to biosphere integrity can have profound economic and social repercussions, ranging from loss of ecosystem services and natural resources to the destruction of traditional knowledge and livelihoods. For instance, desertification, which threatens a quarter of Earth’s land area and a fifth of the population, is already estimated to cost developing nations 4-8% of their GDP (United Nations 2011). Many other rapid regime shifts involving loss of biosphere integrity have been observed, including shifts in arid vegetation, freshwater eutrophication, and the collapse of fish populations (Amano et al. 2020). There is a theoretical possibility of still more profound regime shifts at the global level (Rocha et al. 2018). However, the contribution of loss of biosphere integrity to GCR is yet to be assessed. Kareiva and Carranza (2018) argue that it is unlikely to threaten human civilization, due both to a lack of plausible mechanisms for this threat and the fact that “local and regional biodiversity is often staying the same because species from elsewhere replace local losses.” However, in their classification of GCRs, Avin et al. (2018) suggest the potential for ecological collapse to threaten the safety boundaries of multiple critical systems with diverse spread mechanisms at a range of scales, from the biogeochemical and anatomical to the ecological and sociotechnological. Note that both these studies were conducted for largely conceptual purposes and should not be taken as rigorous analyses of this risk, this topic warrants further investigation.

3.2 Classifying Climate Change’s Contributions to Global Catastrophic Risk

Climate change's contribution to GCR goes well beyond its impact on the earth system. Taking Avin et al.’s list of critical systems, we note that previous studies have mostly focused on the effects of climate change on physical and biogeochemical systems (e.g. global temperature and sea-level rise) or the lower-level critical systems that are most directly related to human health and survival (e.g. Heath Stress). However, these represent a very limited assessment of risk as it only accounts for climate change as a direct hazard/threat and our "ontological" vulnerabilities to it. A more comprehensive risk assessment must consider the higher-order critical systems threatened by climate change passively (through a lack of alternatives) and actively (through intentional design).

The probability of a global catastrophe is higher when socio-technological and environmental systems are tightly coupled, creating a potential for reinforcing feedback loops. If environmental change produces social changes that perpetuate further environmental change, then this could actively work against our efforts at adaptation. When this change has the potential to produce significant harm, via human vulnerabilities and exposure, we describe such loops as ‘global systems death spirals.’ These spirals could produce self-perpetuating catastrophes, whereby the energy and resources required to reverse or adapt to collapse are beyond the means of dwindling human societies. Feedback loops like this could thus create tipping points beyond which returning to anything like present conditions would become extremely difficult. Global systems would shift to very different states in which the prospects for humanity would likely be bleaker.

In the rest of this section, we explore just one potential spiral, between an ecological system (the biosphere) and two sociotechnological systems (the human food and global political systems). We explore each system and its interactions. Figure 2 illustrates our model of this spiral.

[Figure omitted]

The human food system

Climate change’s impact on biosphere integrity (discussed in the previous section) could harm the human food system due to loss of ecosystem services, disruption of the cycles of water, nitrogen and phosphates, and changes in the dynamics of plant and animal health (Bélanger and Pilling 2019). Crossing this planetary boundary is already having severe implications for global food security, including loss of soil fertility and insect-mediated pollination (Diaz et al. 2019).

Systems for the production and allocation of food are already enduring significant stress. The sources of stress include climate change, soil erosion, water scarcity, and phosphorus depletion. The natural resource base, arable land and freshwater upon which food production rely are being degraded. While global food productivity and production has increased dramatically over the past century to meet rising demand from an expanding global population and rising standard of living, these constraints and risks are increasing the vulnerability of our global food supply to rapid and global disruptions that could constitute global catastrophes (Baum et al. 2015).

Climate change will further reduce food security in at least three interconnected ways. First, it will affect growing conditions, including direct threats to agricultural yields from heat, humidity, and precipitation in many regions; although initially improving conditions in some (Lott, Christidis and Stott 2013). Second, it will increase the range of agricultural pests and diseases (Harvell 2002). Third, it will increase the occurrence of extreme weather events that impair the integrity of food production and distribution networks, from production to harvest, post-harvest, transport, storage, and distribution, thereby increasing our vulnerability and exposure to supply shocks (Bailey et al. 2015). The IPCC estimates, with medium confidence, that at around 2°C of global warming the risk from permafrost degradation and food supply instabilities will be ‘very high’, while at around 3°C of global warming the risk from vegetation loss, wildfire damage, and dryland water scarcity will also be very high (Arneth et al. 2019). Very few studies have considered the impacts of 4°C of global warming or more; however, the IPCC highlighted one study finding that any potential agricultural gains from climate change will be lost by this point and there could be a decrease of 19% in maize yields and 68% in bean yields in Africa, an 8% reduction in yields in South Asia, and a substantial negative impact on fisheries by 2050 (Porter et al. 2014). Furthermore, multiple extreme weather events could disrupt food distribution networks (Baily and Wellesley 2017).

While there are opportunities to adapt, disruption to the entire global food system cannot be resolved via food aid alone. Indeed, there is the potential for isolationist or heavy-handed responses that would do more harm than good. Given the high degree of interconnectivity and feedback within the global food system, our initial research suggests that any one of these climate change effects could trigger scenarios that would critically undermine the global food system’s ability to meet the minimum nutrition for well-being; making food security for all an unachievable goal, let alone rise to the challenge of continuing to grow (Tzachor 2019a; 2020); this would constitute what Kuhlemann (2019) terms a ‘threshold of significance.’

The global political system

Disrupting the global food system can create and exacerbate conflict and state failure (Brinkman and Hendrix 2011). However, once again, this needs to be seen against the backdrop of a global political system under stress, with climate change as a significant contributing factor. Climate change influences political systems in many ways, from being a locus of activism and a stimulus for reform to driving rising inequality and population displacement (Arneth et al. 2019, Diffenbaugh and Burke 2019). This is not a new phenomenon, changes in the climate are believed to have contributed to conflict between people and states throughout human history, driven by resource scarcity, population displacement, and inequality (Lee 2009, Mach et al. 2019). As part of a comprehensive risk assessment of climate change, David King and colleagues (2015) conducted an extensive literature review on climate change and conflict and used this to inform a series of international wargaming exercises. These found that climate change is expected to increase international conflict while highlighting the role that population displacement, state failure, and water and food insecurity would play in this (see also Natalini, Jones and Bravo 2015, Mach et al. 2019).

Quantitative studies of the impact of climate change on violence and conflict have provided more mixed results. A survey of empirical studies by Detges (2017) found that there may be multiple differing trends: extreme weather events appear to have more significant effects on violence than do long-term climate trends, while levels of small-scale conflict and interpersonal violence appear to be more affected than large-scale conflicts and international war. Empirical studies also highlight how climate change’s impact on conflict is predominantly as a risk multiplier and intensifier. Thus, climate change may contribute more by increasing our vulnerability to other conflict-inducing factors, such as loss of livelihood, forced migration, environmental change, and food insecurity, than by acting as a direct cause of conflict (Schubert et al. 2008, Hsiang et al. 2013, Abel et al. 2019).[13]

Of particular relevance to GCR is the effect of climate change on the risk of nuclear war (Parthemore, Femia and Werrell 2018). However, to our knowledge, this has never been rigorously assessed, although the potential is certainly there. One recent model of the risk of nuclear war highlighted how varied, and common, incidents with the potential to trigger a nuclear exchange are (Baum, de Neufville and Barrett 2018). It outlined 14 different causal pathways to an exchange, including the escalation of conventional wars and international crises, human error, and the emergence of new non-state actors. For all but two of these, they identify historical examples of potentially precipitating incidents, with 60 incidents in total (i.e. a little less than one a year). This suggests that the absence of nuclear war was less due to a lack of potential causes, than the global political system’s ability to defuse them. Thus, the real significance of climate change may be its capacity to undermine this system: the combination of social, political, and environmental disruption, a lingering sense of global injustice, and rising food, water, and energy insecurity could increase the probability that crises escalate or that false alarms are mistaken for genuine emergencies. This topic needs further research.

3.3 The emergence of a global systems death spiral

Yet, we should not conclude that a nuclear exchange is the only, or even most likely, scenario in which political instability might produce a global catastrophe. Conflict and political instability, even of moderate severity, are themselves two of the most significant drivers of biodiversity loss due to breakdowns in monitoring, governance, and (public and private) property rights (Baynham-Herd et al. 2018). This closes a potentially reinforcing feedback loop between loss of biosphere integrity, food insecurity and political breakdown.

The mechanisms by which these cascading failures might spread include many of the natural, anthropogenic, and replicator effects identified by Avin et al. (2018), making them harder to contain. At the natural level, climate change involves changes to the global atmospheric and biogeochemical systems and poses other naturally spreading harms, like global ecological collapse. At the anthropogenic level, the global interconnectedness of sociotechnological systems means that while small shocks are easier to recover from, larger shocks can be harder to contain and control. Finally, biological and informational replication can also spread the negative impacts of climate change, from vector-borne diseases and invasive species to climate fatalism and dangerous geoengineering technologies.

Given these numerous spread mechanisms, critical system failures could precipitate global catastrophes. Furthermore, the spiral we have explored is unlikely to be the only set of interlinked systemic disruptions that climate change could initiate (other death spirals could involve bio-insecurity and disease), nor are these the only causal connections between these three systems. Until we understand the nature of such death spirals better, we must act cautiously. We now turn to consider what this would mean.

#### Federal antitrust signals a balanced, light-touch approach that reinvigorates U.S. global leadership on blockchain.

Matt Sandgren 21, Former Staff Director of the Senate Republican High-Tech Task Force, Former Senior Counsel on the Senate Judiciary Committee, Final Chief of Staff to Senator Orrin G. Hatch, Executive Director of the Orrin G. Hatch Foundation, “How New Regulations from Washington Could Lead to a Blockchain Brain Drain”, The Hill, 10/27/2021, https://thehill.com/blogs/congress-blog/technology/578834-how-new-regulations-from-washington-could-lead-to-a-blockchain

The internet is what it is today—with its ability to connect people across countries, time zones, and cultures—thanks to the friendly regulatory climate it was born into. Sadly, the regulatory climate of 2021 is far less welcoming to disruptive technologies. This is bad news for the future of U.S. innovation and the emerging blockchain industry.

Whether Washington takes a heavy-handed or a light-touch approach to crypto regulation over the next few months could make a multitrillion-dollar difference over the next few years. To understand how much we stand to lose as a result of bad blockchain policy, it’s first important to understand just how much we have gained as a result of good internet policy in the ’90s.

It’s easy to forget that the success of today’s internet behemoths was anything but certain in the early years of the tech boom. During the Dotcom Bubble of the late '90s, for example, many companies were dismissed as scams (and some of them were). But even the most promising companies were still seen as speculative bets, and their stock prices were subject to extreme volatility.

It’s also easy to forget that the very concept of the internet was foreign to most people in its early years. By today’s standards, it was slow, overly complex, and difficult to use by anyone without a strong technical background. Many dismissed the internet as a fad, including Nobel Prize-winning economist Paul Krugman, who made this prediction in 1998: “By 2005 or so, it will become clear that the internet’s impact on the economy has been no greater than the fax machine’s.”

Noted.

“A scam,” “a fad,” “a bubble,” “overly complex,” “too volatile.” Does any of this sound familiar? History doesn’t rhyme so much as it plagiarizes. And it’s impossible to ignore that the crypto skeptics of today use the same vocabulary as the internet naysayers of yesteryear.

Now imagine if U.S. policymakers had heeded the words of the internet’s critics in the mid-to-late ’90s. Imagine if they had cracked down on e-commerce, digital publishing, and fledgling social media platforms to preserve the old way of doing things. Imagine if they had shaped regulations to stem the free flow of physical goods, ideas, and information made possible by the internet.

The American people would have missed out on trillions of dollars in economic opportunity—and the bounties of the digital age would have gone to countries with more tech-friendly policies.

This is the risk we face today.

We find ourselves at the dawn of a new age of American innovation. Like the internet before it, crypto has the potential to redefine everything we know about how business, politics, media, finance, and even relationships work. But if legislators give in to crypto’s critics by taking a draconian approach to regulation, the U.S. will fail to reap the economic rewards of this world-changing technology—and entrepreneurs will flee to friendlier shores.

Even now, the stage is being set for a blockchain brain drain. Take the Senate-passed infrastructure bill, which includes a provision that would define crypto miners, validators, and even software developers as “brokers,” requiring them to report information to the IRS about anonymous blockchain participants that they would have no way of obtaining. In effect, this provision would kill the nascent DeFi (decentralized finance) industry and make it almost impossible for everyday Americans to invest in new cryptocurrencies. In other words, this latest move sends a hostile message to blockchain advocates: “We don’t want you here.”

At best, the Senate proposal belies a gross misunderstanding of how cryptocurrencies work; at worst, it exposes regulatory capture and the willingness of legislators to give in to special interests.

Sadly, the threat of bad regulation doesn’t end there. SEC Chair Gary Gensler has expressed his belief that many digital assets are not commodities but securities and should be regulated as such. Following this same logic, he’s signaled his intent to crack down on the use of stable coins—cryptocurrencies pegged to the value of the U.S. dollar. Americans are using stable coins to earn 4 to 8 percent APY on their savings through various lending programs. But the SEC wants to put a stop to these lending programs, ostensibly “to protect investors.” (What’s unclear is which government agency will protect investors from the unlimited money printing that is devaluing their dollar savings at a rate of 5.3 percent per year.)

Washington has gotten off on the wrong foot when it comes to crypto. But it’s not too late to correct course.

Regulation of crypto is not necessarily a bad thing. In fact, it’s a key step on the path to mainstream adoption. It’s critical, however, that policymakers shape regulation in a way that minimizes the risks of this new technology without eliminating its benefits. Congress found a way to do this with the internet in the ’90s. Section 230—while far from perfect and in need of reform today—paved the way for a flexible regulatory environment that allowed for many online companies to thrive. In the famous words of Jeff Kosseff, Section 230 contains “the 26 words that created the internet” (and, it’s worth adding, “trillions of dollars in economic wealth”).

Indeed, regulatory clarity is key to extracting maximum value from the emerging crypto economy, whether that value comes from DeFi protocols, decentralized forms of social media, tokenized assets, NFTs, or some other application of blockchain technology that we can’t even imagine today.

As policymakers seek to find the right balance on regulation, they should remember that the U.S. didn’t become the tech capital of the world by choking innovators with red tape. The U.S. became what it is today by taking a prudential approach to regulation—one that enabled the entrepreneurial spirit.

This is the same entrepreneurial spirit that inspired the private sector technological advances that made the Apollo moon landing possible. It’s the same spirit that brought about smartphones millions of times more powerful than the Apollo 11 guidance computers. And it’s the same spirit that has motivated a group of visionaries to push the boundaries of the digital frontier through blockchain technology.

Will Washington’s leaders stifle that spirit to the detriment of our economy and our reputation as a global leader in innovation? Or will they nourish that spirit to usher in the next chapter of the digital revolution?

Let’s hope they choose the latter.

#### That allows international standard-setting that leverages it for public benefits internationally.

Lou Kerner 18, Head Crypto Analyst at Quantum Economics, Partner at Blockchain Coinvestors Acquition Corp, MBA from the Stanford University Graduate School of Business, BA in Economics from UCLA, “A Call For U.S. Leadership in Crypto”, Medium, 7/6/2018, https://loukerner.medium.com/a-call-for-u-s-leadership-in-crypto-4b74d6deb4ad

Despite the striking fact that most of the programmers the U.S. has ever known are alive and working today, despite the fact that the U.S.’s technical capabilities are growing exponentially, despite that, the vast stretches of the unknown and the unanswered and the unfinished still far outstrip our collective comprehension.

No man can fully grasp how far and how fast we have come, but condense, if you will, the 50,000 years of man’s recorded history in a time span of but a half-century. Stated in these terms, we know little about the first 40 years, except at the end of them man had learned to use the skins of animals to cover them. Then 10 years ago, under this standard, man emerged from his caves to construct other kinds of shelter. Five years ago man learned to write and use a cart with wheels. The printing press came this year, and two months ago, the steam engine provided a new source of power. Last month electric lights and telephones and automobiles and airplanes became available. Only last week did we develop penicillin and television. Two days ago the internet browser was introduced. And earlier today, Satoshi wrote his white paper.

This is a breathtaking pace, and such a pace cannot help but create new ills as it dispels old, new ignorance, new problems. Now, when refer to “Crypto”, I mean the four technologies (blockchain, cryptocurrency, smart contracts, and zero knowledge proof), which collectively enable decentralization, all fueled by community. Surely these technologies promise disruption and high reward.

So it is not surprising that when it comes to Crypto our government would have us stay where we are a little longer to rest, to wait. But this city of New York, and this country of the United States was not built by those who waited and rested and wished to look behind them. Technological breakthroughs are driven by those who move forward — and we will continue to do so.

If this capsule history of our progress teaches us anything, it is that man, in his quest for knowledge and progress, is determined and cannot be deterred. The development of Crypto will go ahead, whether the U.S. regulators joins in or not. And I believe Crypto is one of the great adventures of all time, and no nation which expects to lead the world in technology can expect to lead while staying behind in the development of Crypto.

Our forefathers made certain that the U.S. rode the first waves of the industrial revolutions, the first waves of modern invention, and the first wave of the internet. This generation does not intend to founder in the backwash of the coming age of Crypto. We mean to be a part of it — we mean to lead it. For the eyes of the world will increasingly look at Bitcoin and blockchain and beyond. And those of us in Crypto are working to see it governed by a banner of freedom. We have vowed that we shall not see Crypto filled with scammers, but with scalable protocols that make the world a better place.

Yet the promise of Crypto can best be fulfilled if we in this Nation are there, and leading the way. In short, our leadership in technology, our hopes for a better future, our obligations to ourselves as well as others, all require us to make this effort, to solve these mysteries, to solve them for the good of all men, and to become the world’s leading Crypto nation.

We set sail on this new sea because there is new knowledge to be gained, and new rights to be won, and they must be won and used for the progress of all people. For Crypto, like all of technology, has no conscience of its own. Whether it will become a force for good or ill depends on [hu]man[s], and only if the United States occupies a position of pre-eminence can we help decide how this new technology evolves. I do not say that we should or will go unregulated against the misuse of Crypto any more than we go unprotected against the hostile use of cyber warfare. But I do say that Crypto can be developed and mastered without repeating the mistakes of past regulatory overreach.

Crypto’s development deserves the best of all [hu]mankind and its opportunity for community. But why, some say, Crypto? Why choose this as our next computing platform? And they may well ask why climb the highest mountain? Why, 75 years ago, fly the Atlantic?

We choose to to develop Crypto, and do the other things, not because they are easy, but because they are hard, because the goal of decentralization will serve to organize and measure the best of our energies and skills, because that challenge is one that we are willing to accept, one we are unwilling to postpone, and one which we intend to win.

It is for these reasons that I’m concerned by the inaction of our government to provide greater regulatory clarity. In the last months, we’ve seen progress in scaling like the Lightning Network. We’ve seen securities infrastructure like Templum and OpenFinance and Polymath being built.

To be sure, from a regulatory standpoint, we are behind. But we should not stay behind. This year, we should make up and move ahead. The growth of our science and education will be enriched by new knowledge of Crypto, by new decentralized governance mechanisms, by new token economics.

The Crypto community itself, while still in its infancy, has already created a great number of new companies, and tens of thousands of new jobs. Crypto is generating new demands in investment and skilled personnel, and New York and the U.S. can share greatly in this growth.

To be sure, all this comes with uncertainty of the role of government and fiat in the future. I recognize that the belief in Crypto’s potential is in some measure an act of faith , for we do not now know what benefits await us.

But I believe that we can develop a decentralized currency that can be used as a means of exchange. I believe we can leverage blockchain technology to provide identity for the 23 million children on this planet without identity papers. I believe we can use these technologies for voting purposes, and ensuring our elected officials follow through on their promises.

However, if we’re going to do all those things, and countless other positive things for mankind, then we must pass accommodating regulations. I‘m encouraged that New York and the United States are playing a big part in the development of Crypto,. With more regulatory clarity, we can solidify our leading position in Crypto, the greatest adventure on which [hu]man[ity] has ever embarked.

#### Globally collaborative blockchains prevent nuclear war from miscalc, accidents, and arms racing AND builds global co-op, stopping existential threats.

Dr. Lyndon Burford 21, PhD in Politics and International Relations from the University of Auckland, Visiting Research Associate at the Centre for Science and Security Studies at King’s College London, Member of the New Technologies for Peace Working Group, a Part of the Vatican’s COVID-19 Commission, “Could Blockchain Technology Help Advance Nuclear Disarmament?”, Medium International Affairs Blog, 2/19/2021, https://medium.com/international-affairs-blog/could-blockchain-technology-help-advance-nuclear-disarmament-6efaab35e277

New and maturing technologies are often seen as possible drivers of conflict, not least in the context of rising nuclear risks. In 2019, for example, the UK House of Lords Select Committee on International Relations concluded, “The risk of the use of nuclear weapons has increased, in the context of rising inter-state competition, a more multipolar world, and the development of new capabilities and technologies.” In a recent policy report published by the Centre for Science and Security Studies at King’s College London, I explored the flipside of that coin. The trust machine: blockchain in nuclear disarmament and arms control verification looks at how blockchain technology could help to reduce nuclear risks, by strengthening systems to verify the dismantlement of nuclear warheads.

The ‘trust machine’

Blockchain is best known as the technology that underpins the cryptocurrency Bitcoin, but it already has a wide range of alternative uses in areas such as medicine, transport, manufacturing, finance and governance. During the COVID-19 crisis, blockchain was used to produce a cheap, reliable solution for contact tracing. In Syria, blockchain is being used to create a permanent record of potential war crimes, increasing the security and integrity of the data and strengthening its admissibility as evidence in future war crimes prosecutions.

Contests of legitimacy and value: the Treaty on the Prohibition of Nuclear Weapons and the logic of…

Blockchain is a de-centralized, digital record-keeping technology. It combines cryptography and social/economic incentives to build a shared, permanent, and virtually un-hackable record of events, without needing to trust a third party authority to manage the data. Unlike Bitcoin, which is a ‘public’ network that allows anyone to interact with it, a private blockchain creates a ‘permissioned’ network of participants who collectively store and manage data in a way that allows them to maintain extremely high confidence in the integrity of the data. The result is a shared, digital record of events — a blockchain — that is practically immutable, establishing a single, collective, and irrefutable ‘truth’ about the nature and sequence of events within the network. In a post-truth world, blockchain thus offers an invaluable technical foundation for cooperation among parties that have a limited basis to trust each other, leading to its nickname, ‘the trust machine’.

Blockchain as a disarmament mechanism

At present, extremely low levels of international trust hamper efforts to advance nuclear disarmament. The ongoing development of new nuclear weapons, warheads and increasingly capable ballistic missile defences are undermining the theories and practices of deterrence, and point to the resurgence of a spiral of mistrust that characterized the Cold War nuclear arms race. Developing robust, multilateral verification tools and processes could help to mitigate the trust deficit. It would enable countries to pursue their shared interests in nuclear disarmament — reduced costs, less chance of escalation and nuclear use, greater scope to cooperate on global threats like climate change and pandemics — by increasing confidence that other countries are fulfilling their disarmament commitments in good faith. One way to strengthen verification would be to use a private blockchain to manage and store the data that a disarmament process creates.

In a verified disarmament process, parties need to track and record things like the status and movements of individual inspectors and weapon parts, and the status and material holdings of different facilities. These activities create large amounts of data that need to be stored in a secure, permanent and transparent manner that also allows for its easy retrieval by permissioned actors. The core attributes of blockchain correspond closely to these requirements. The technology would allow parties to maintain very high confidence in the immutability of verification data, creating a strong technical foundation for future cooperation from a shared, trusted baseline.

International collaborations like the 25-country International Partnership for Nuclear Disarmament Verification and the Quad Nuclear Verification Partnership (made up of Norway, Sweden, the United Kingdom and the United States) are already exploring how nuclear-armed and non-nuclear-armed states can cooperate in verifying the dismantlement of nuclear warheads without revealing sensitive information. Blockchain could complement their approach, enabling countries to create a permanent, immutable record of verification data.

Nuclear weapons threaten the survival of humanity and divert tens of billions of dollars each year away from efforts to address other collective security challenges like mitigating and adapting to climate change and responding to pandemics like COVID-19. As such, we all share an interest in disarmament processes that can reduce the likelihood of deliberate or accidental nuclear explosions and free up urgently needed resources for other global security priorities. We owe it to ourselves and to future generations to consider all options that could help to advance nuclear disarmament. In addressing the regular obstacle of distrust between the nuclear powers, blockchain is one technological option that we should be exploring.

#### It ensures a credible verification system.

Michal Onderco & Madeline Zutt 21, Associate Professor, International Relations, Erasmus University Rotterdam; Research Associate, Erasmus University Rotterdam, "Emerging Technology and Nuclear Security: What Does the Wisdom of The Crowd Tell Us?" Contemporary Security Policy, Vol. 42, Issue 3, pg. 299-302, 2021, T&F.

Our third finding focuses on whether emerging technologies could enhance or impede nuclear disarmament efforts. Some work has already exposed how new technologies have the potential to strengthen nuclear disarmament and verification measures. A prototype “SLAFKA” was recently jointly developed by a nuclear regulator in Finland (STUK), the University of New South Wales in Australia, and the Stimson Center in the United States which tests whether a distributed ledger technology (DLT) can effectively safeguard nuclear material (Stimson Center, 2020). A DLT platform is “a system of electronic records that enables independent entities to establish consensus around a “ledger”—without relying on a central coordinator to provide the authoritative version of the records” (Rauchs et al., 2018, p. 23). Blockchain is the most well-known type of distributed ledger. Importantly, blockchain is structured in such a way that all who participate in the shared ledger must agree upon a set of records or data, and this data cannot be changed or tampered with by one actor alone (Rockwood et al., 2018). When it comes to accounting for nuclear materials, blockchain could be used by member states to confidentially and securely provide data to the IAEA (Vestergaard, 2018). By using a shared ledger system, the transmission of data by a member state would be visible to other member states, while maintaining the anonymity of participants (Rockwood et al., 2018).

In a recent report, Burford (2020) notes that the characteristic features of blockchain, namely its immutability and security as a data management tool, are uniquely suited to “help to build technical capacity among [non-nuclear weapons states] and habits of cooperation among NPT parties, while protecting proliferation-sensitive data” (p. 21). Finally, others have noted that advances in image-recognition software combined with the increased sophistication in and availability of satellite imagery could open up space for more actors to get involved in verification activities (Kaspersen & King, 2019). This would make verification more robust by allowing a greater number of states to participate in what has traditionally been the domain of states that are more technologically superior.

The security, transparency, and confidence-building features of these emerging technologies could thus enhance verification by strengthening the safeguards system as well as increasing trust and cooperation among states normally suspicious of one another. These features could prove useful in helping to close both institutional and compliance gaps within the non-proliferation regime. That said, as with any other global governance regime, a compliance gap is very difficult to fully bridge. On this point, Sagan notes that even with advances in verification technology “there will remain the problem of what to do if an erstwhile nuclear nation is caught secretly preparing to rearm” (see Sagan in Sagan & Waltz, 2010, p. 90). While the inclusion of new technologies in verification and safeguards will not wipe away the challenges associated with verification, emerging technologies can play a role in strengthening verification and safeguarding measures.

Since we were interested in whether the experts and policymakers considered the positive applications of new technologies on disarmament efforts, our final question in the survey asked experts to express their views on nuclear disarmament.

Table 3 illustrates that the majority of our experts across regions agreed that complete nuclear disarmament would happen when leaders are confident that technology will allow for its verification, underlining the pivotal role verification plays in disarmament. This was echoed by some of the policymakers whom we spoke to who said that AI and remote sensing could help make verification measures more robust (Interviewee I & F). On the other hand, Table 3 also highlights that European and American experts are more skeptical (than experts in other regions) of the fact that nuclear disarmament will occur when leaders believe new technologies make nuclear weapons unnecessary.

#### Policy must be certain and originate at the federal level to signal U.S. commitment to accommodative blockchain policy.

Michele Benedetto Neitz 21, Professor of Law at the Golden Gate University School of Law, Member of the California Blockchain Working Group, Affiliated Scholar at LexLab at the U.C. Hastings College of the Law, “How to Regulate Blockchain's Real-Life Applications: Lessons from the California Blockchain Working Group”, Jurimetrics Journal, 61 Jurimetrics J. 185, Winter 2021, Lexis

A. Why Create Laws Related to Blockchain Technology?

1. Protecting the Public from Harm

Blockchain technology is a complicated field, and innovation in this space is developing rapidly. This innovation will occur regardless of a legislature's reluctance or willingness to draft laws to regulate this industry. As state and federal legislators are struggling to define a regulatory scheme, members of the public who are excited about the possibilities of investing in something new like digital assets may suffer from harm.

This has, of course, already happened in various ways. In a recent high-profile example, members of the public were invited to invest in initial coin offerings (ICOs), buying tokens as a way to invest in start-up companies. 25 One study reported that approximately 78 percent of the ICOs offered in 2017 were actually scams. 26 In the United States, 33 percent of ICO investors believe that ICO operators "deceived them or withheld information from them." 27 The ICO market significantly cooled as federal prosecutors and the SEC began aggressively taking action against leaders of fraudulent ICOs, demonstrating how regulatory enforcement can indeed protect investors from harm. 28

[\*190] However, cryptocurrency scams are persisting beyond the ICO craze. The FTC recently warned the public that scammers are continually finding new ways to "trick people." 29 Members of the public are clearly at risk of a multitude of foreseeable--and unforeseeable--problems as applications of this technology develop, including fraudulent investments, breaches of privacy on blockchain platforms, digital identity theft, and insufficient data protection. Given these threats to the public, it is not appropriate for regulators to dawdle as blockchain applications continue to rapidly advance.

2. Attracting Innovation

While they work to protect the public, legislators and regulators can also use laws to signal their commitment to attracting blockchain-related companies to their locations. Some jurisdictions, including countries like Estonia and Switzerland 30 and U.S. states like Wyoming, 31 have already implemented regulatory schemes designed to win the interjurisdictional competition for blockchain business. 32

The resulting tension between protecting the public while promoting innovation lies at the heart of regulating digital assets and other applications of blockchain technology, as discussed in more detail in Section III.A. Despite the need for blockchain-related regulation, numerous challenges exist for lawmakers seeking to draft laws in this area--starting with the fact that the word "blockchain" does not have a commonly understood definition.

B. The Legislative Definition Problem

What is the legal definition of blockchain? This simple question has proved to be exceedingly difficult to answer. States considering blockchain legislation have focused on different characteristics of this new technology, meaning that "[d]efinitions in legislation introduced in 2018 in California, Florida, Nebraska and Tennessee differ[ed] from those of industry groups and from each other." 33 In some cases, the definitions were in conflict. 34 These inconsistent definitions [\*191] are problematic, as they "actually introduce legal uncertainty where it did not previously exist, and invite unnecessary and expensive litigation." 35

A clear definition of blockchain is necessary for legislative purposes as well, as it is required to help a jurisdiction create clear policies. 36 Moreover, a state's definition should enable policymakers and the public to focus on "the most unique value that the technology can deliver. It should be accessible to and understandable by the public, and yet technically specific enough to ensure that the [jurisdiction] can reap maximum benefit." 37 With such a high bar, legislators have understandably struggled to construct a working definition for this new technology.

The California Blockchain Working Group, after much discussion and debate, created a new definition of blockchain in 2020 for state legislative purposes:

"Blockchain" is a domain of technology used to build decentralized systems that increase the verifiability of data shared among a group of participants that may not necessarily have a pre-existing trust relationship.

Any such system must include one or more "distributed ledgers," specialized datastores that provide a mathematically verifiable ordering of transactions recorded in the datastore. It may also include "smart contracts" that allow participants to automate pre-agreed business processes. These smart contracts are implemented by embedding software in transactions recorded in the datastore. 38

The New York Senate took a simpler approach, defining blockchain as "a mathematically secured, chronological, and decentralized consensus ledger or database, whether maintained via internet interaction, peer-to-peer network, or otherwise used to authenticate, record, share and synchronize transactions in their respective electronic ledgers or databases." 39

Both of these definitions are technically correct, and they both reflect the policy decisions of their respective states. For example, California deliberately used the more flexible term "datastore," instead of "record" or "log," to reflect the verifiability of data shared amongst participants, the many use cases of this type of ledger, and the fact that many datastores could exist at once. 40

[\*192] One could argue that the lack of a uniform statutory definition is partly responsible for the patchwork nature of state blockchain regulation. After all, without a similar definition, it is nearly impossible to set policy goals and pass parallel legislation in multiple jurisdictions. However, the problem of inconsistent definitions is just the tip of the iceberg of interjurisdictional competition. 41 This competition is unlikely to subside even if the federal government or the Uniform Law Commission enacted a well-accepted, standardized definition of blockchain technology.

C. The Fast Pace of Blockchain Technology Development

Law always moves slower than technology. 42 This is partly because lawmakers and agencies can "struggle to capture emerging technologies in dusty regulatory frameworks." 43 For example, securities laws drafted in the 1930s could not have anticipated the sale of digital assets. 44 Even more recently drafted laws and regulations relating to the Internet do not fit blockchain technology. 45 Lawmakers must decide whether to fit this revolutionary technology within existing legal frameworks or start all over with new legislative schemes.

The constantly evolving nature of blockchain technology presents another challenge. This "industry is in its early stages of maturation," making it difficult to determine the initial policy choices that would lead to effective regulation. 46 There are also technical concerns still lurking within blockchain technology, such as locating the "weak points" that might be "gamed by bad actors," which could give rise to unanticipated legal problems. 47

Finally, even at this early stage, lawmakers must consider which aspects of the technology are important enough to regulate. Some of these are obvious, such as cryptocurrency and other forms of digital assets that involve sales to members of the public. But even within this category, it is "still too early to tell exactly which of the drivers of digital asset excitement is dominant," putting [\*193] "regulatory bodies in a tough position." 48 In this way, the wide variety of blockchain projects and the speed at which they are developing creates an additional barrier to effective regulation.

As an example, imagine a developer creates a brand-new digital asset and offers it to the public. How should regulators approach the regulation of this asset? Should regulators first consider the substance of the project, its connection to a decentralized ledger, its effect on consumers' privacy and security, or its potential to evade anti-money laundering and "[k]now [y]our [c]ustomer" laws 49 (or all of the above)? An effective regulatory scheme would need to include rules that are flexible enough to manage future technical developments as well as today's technologies. Otherwise, laws may need to be reconsidered and amended whenever a new technical application emerges.

D. Blockchain Technology's High Learning Curve for Lawmakers

Blockchain technology can be complicated and intimidating, and few lawmakers have training in computer science. A 2016 survey found only that only four of the 535 members of Congress had formal computer science degrees. 50 While the technical aspects of blockchain can be difficult to explain, most legislators can learn enough to understand the fundamentals. 51

New York's State Senate offers a case in point. The Senate's technical advisor reported that in 2019, "staffers and senators asked basic questions about blockchain and distributed ledger technology, prompting [the technical advisor] to develop an explainer presentation." 52 One year later, in 2020, many of the senators "appear more comfortable with the technology, which helps them see the value of [potential] legislation." 53

Legislators need not dive into minor technical details of blockchain to be able to regulate it. It is more important for legislators to focus on the function of blockchain and its practical applications, asking not "what is blockchain?" but [\*194] "what can blockchain do?" 54 Policymakers should focus on the use cases of blockchain, rather than its underlying technology. 55

Professor Angela Walch offered prescriptive recommendations for regulators learning about blockchain, advising them to cultivate their expertise (including self-education), consult with other regulators, follow the activity of standards organizations and academia, and "[w]atch and [l]earn" as the technology stabilizes. 56 Professor Walch also counsels lawmakers to "[a]dopt a [c]ritical [m]indset" in this educational process, to ensure they are not unduly influenced by hype or unreliable sources. 57

Legislators could also learn more about blockchain through the use of legislative working groups or task forces. For example, California's Blockchain Working Group drafted a report in accessible language, enabling state legislators to learn more about the technology and its potential applications for California in one comprehensive document. 58 The federal government has tried to follow this path. In 2019, a bipartisan group of senators proposed a bill directing the Secretary of Commerce to establish a federal Blockchain Working Group in 2019. 59 However, the bill, entitled the "Blockchain Promotion Act," is still currently in committee. 60

As a law professor who taught the first Blockchain and the Law class in San Francisco, I can anecdotally report that blockchain and cryptocurrencies are not easy concepts for nontechnical learners to grasp. However, over the course of one semester, my law students (most of whom did not have any technical training beforehand) were able to draft final reports and presentations not just describing the technology, but also analyzing the use cases deploying the technology. With a bit of time and effort, state and federal lawmakers can understand the potential for blockchain to transform their jurisdictions.

II. FIVE FACTORS FOR LEGISLATIVE CONSIDERATION

In light of the difficult nature of regulating blockchain, this Part offers five factors lawmakers should consider as they work to draft blockchain and crypto regulation.

[\*195] A. Policy Decision: Innovation vs. Protecting the Public Interest

In an ideal world, governments would be able to promote both innovation and the public interest. In reality, however, legislators usually need to debate and choose whether they will prioritize innovative technological development or consumer/public protection. This is especially true in the context of blockchain, since the public perception of blockchain varies widely. Many members of the public first heard of blockchain through Bitcoin, the digital currency. But early illegal use cases of blockchain technology also made headlines, including the infamous Silk Road darknet marketplace 61 and repeated cases of fraudulent theft through Initial Coin Offerings. 62 While the technology is neutral, blockchain can be used in malicious ways that harm the public. 63 Even well-meaning technology can implicate privacy and data protection concerns. 64

It is therefore "essential for both the industry and society that consumers and the capital market are protected from abuse." 65 No state or federal jurisdiction should enable blockchain technology to develop without guardrails to protect the public. The question is where those guardrails should lie. If states wait too long to regulate, the public may be harmed, and the costs of imposing requirements on industries that have already been established will be too great. However, if states develop restrictive regulations too early or the laws "become onerous," 66 businesses will relocate to more friendly jurisdictions. States in this position risk killing off innovation or pushing it to other states. 67 [FOOTNOTE] Blockchain businesses will move for regulatory reasons. See Daniel Kuhn, The Cryptocurrency Act of 2020 Is 'Dead on Arrival,' Washington Tells Sponsors, COINDESK (Mar. 11, 2020, 1:19 P.M.), https://www.coindesk.com/the-cryptocurrency-act-of-2020-is-dead-on-arrival-washington-dc-tells-sponsors [https://perma.cc/AP8X-KULR] ("Many projects are simply choosing to move elsewhere" because of regulatory uncertainty.). [END FOOTNOTE]

Part of the reason blockchain technology's applications are so challenging to regulate is that it "is difficult, if not impossible, for regulators to construct a framework that achieves clear rules, market integrity, and financial innovation." 68 This complex question explains the spirit of experimentation among states discussed in Part V, with some choosing restrictive regulatory structures, some choosing permissive approaches, and others choosing the middle. Regardless [\*196] of a jurisdiction's ultimate direction, legislators drafting blockchain legislation must evaluate how to protect the public while encouraging creative technological development.

B. Ethical Considerations

California was the first (and so far, the only) state to consider ethical considerations in the early stages of regulation. This author published the first law review article analyzing ethics in the blockchain industry in December 2019, 69 and also served as the primary drafter of the Ethical Considerations section in California's Blockchain Working Group report. 70

Depending on the type of blockchain at issue, numerous ethical issues may come up for regulators. For example, the increasing centralization of permissionless blockchains and the rise of permissioned blockchains may raise concerns about personal ethics, such as bias and conflicts of interest. As trends suggest that governance of blockchain systems is moving toward centralization, 71 individuals may have power to influence decisions made on that blockchain. If so, there is a potential for that individual's bias and conflicts of interest to come into play. 72

Although ethical discussions around blockchain appear slower to develop than the technology itself, several paradigms have been put forth advocating ethical considerations in this industry. 73 For example, the World Economic Forum recently asked participants and policymakers to sign on to its "Presidio Principles," an agreement to consider transparency and accessibility, agency and interoperability, privacy and security, and accountability and governance. 74 MIT's Digital Currency Initiative included the topic of blockchain ethics at its 2019 "Cryptoeconomics Systems Summit." 75

[\*197] In addition, the Beeck Center for Social Impact + Innovation at Georgetown University published the "Blockchain Ethical Design Framework," with a focus on six "root issues": "governance, identity, access, verification and authentication, ownership of data, and security." 76 This structure more specifically applies to developers, and is not a code of conduct or a legislative model, but it reiterates the idea that "we all share the responsibility to . . . demand intentional ethical approaches in the design and application of data and technology for social good." 77

California's Blockchain Working Group considered ethical issues related to social impact, including fairness, equity, accessibility, trust and transparency, and sustainability. 78 The Group proposed an ethical framework for the adoption of blockchain technology that is directed toward lawmakers as well as industry players. 79 This framework encompasses three main principles:

i. Address key ethical design goals

a) Seek societal benefit: Maximize good and minimize bad. b) Equity: Does this benefit all Californians, or only a few? c) Efficiency and effectiveness: How can we achieve ethical design and use cases without slowing innovation?

ii. Consider ethical uses of blockchain technology

a) Fairness: Is this technology designed and deployed in a fair, nondiscriminatory manner? b) Accessibility: Design to include the most vulnerable user. c) Responsibility: Anticipate and design for all possible uses. d) Sustainability: Create technology to advance sustainability, public health, and corporate social responsibility.

iii. Minimize unintended consequences

a) Are there unintended biases or conflicts in the design or use of this technology? 80 [\*198] b) Are any populations being unintentionally harmed by the way this technology is developing? c) Does this technology promote violations of local, national, or international law? 81

This useful framework offers guidance to regulators seeking to make sure they do not inadvertently violate ethical considerations, especially with hastily drafted legislation. Two examples illustrate the usefulness of this approach. First, it could be relatively easy to create a certification process for blockchain developers who provide services to the State of California. But will that certification process limit approval to developers with degrees from elite institutions? This type of action would raise equity concerns, as the blockchain industry should be working more toward diversity in gender, cultural backgrounds, and perspectives of industry participants. Second, could companies who advance environmentally sustainable blockchain development receive tax credits from the state? Although different jurisdictions may embrace different ethical principles, legislators should discuss these issues as they contemplate ways to regulate this new technology.

C. Transparency

Since "the rule of law requires transparency," 82 jurisdictions in the United States are governed by transparency laws. The federal government's administrative agencies must abide by the Administrative Procedure Act, which (among other things) orders federal agencies to act "transparently and fairly." 83 California's Bagley-Keene Act requires state boards or commissions (including working groups) to "publicly notice their meetings, prepare agendas, accept public testimony and conduct their meetings in public unless specifically authorized to meet in closed session." 84

Legislators are likely already aware of the government transparency laws in their jurisdiction, but there are other reasons transparency is especially important in the context of blockchain regulation. First, all stakeholders should be given the opportunity to weigh in on laws governing this nascent industry. 85 The industry players on the front line have valuable perspectives to share with legislators, and input from various stakeholders will create more efficient regulation. Moreover, the technology is moving quickly, and there may be applications of blockchain in development that legislators do not even know about yet. As the Cryptocurrency Act of 2020 revealed, 86 drafting laws without the collaboration of diverse stakeholders is ineffective.

[\*199] Second, although blockchain technology may eventually touch all areas of business, members of the public may be unaware of blockchain technology's potential. Legislative debates could double as community education opportunities, allowing people who would not ordinarily be interested in blockchain to attend Working Group meetings, task force briefings, and other public discussions of this new technology. Such meetings could be advertised to nontechnical professions and community organizations, and should be held in easily accessible public places and online. Legislators themselves could reach out to their nontechnical constituents and offer ways to connect them to educators and leaders in the blockchain industry. Such transparency could create a culture of innovation in a particular jurisdiction, while increasing public credibility for whatever regulations eventually develop.

D. Interjurisdictional Competition

States have been competing with each other since the beginning of the republic, and the competition has not decreased as our economy has become more complex. 87 In corporate law, interjurisdictional competitions are a common affair. The state that "wins" the race, creating the environment to attract the most businesses to that state, can secure both tax revenue and additional jobs for state residents. Delaware indisputably won the fight for corporate charters among states, with over 1.5 million legal entities, including 67 percent of all Fortune 500 corporations, incorporated there. 88 The reasons for Delaware's success include specialized legislation that is updated each year to adapt to technical and other changes, as well as a corporate-specific chancery court that can move cases quickly along. 89

When Limited Liability Companies (LLCs) were created in Wyoming in 1977, another interjurisdictional race was on. 90 Despite concerns that interstate LLCs would have problems without uniform LLC statutes among the states, "most states enacted LLC statutes before efforts to develop standardize statutes came to fruition." 91 As a result, only twelve states ultimately adopted uniform acts, and there is less uniformity for LLC statutes than for other business forms. 92

The same is happening now with statutes related to blockchain technology. States who can win the race to attract blockchain businesses to incorporate and domicile in their state can earn more than just increased tax revenues from start-up companies. Such a state could also create a reputation for being friendly to [\*200] technological innovation, a reputation that would have impacts beyond blockchain technology. For this reason, some states (including Wyoming, the first state to draft LLC statutes in 1977) jumped out first to enact permissive blockchain-and crypto-friendly regulations. 93

Before enacting regulations, however, state legislatures should ensure they are clear on the policies underlying those regulations. For example, as discussed in Section II.A above, states should consciously strike a balance between protecting the public and encouraging innovation. Without establishing prioritized policies in advance, a state may win the interjurisdictional competition in the short term but create unintended consequences, such as unnecessary litigation or public harm, in the long term.

E. Uniformity

As a member of the California Blockchain Working Group, this author asked industry leaders in late 2019 what they preferred to see in blockchain regulation. Each of them clearly and unequivocally stated that uniformity of regulation across the United States would be good for business. It would be much easier for blockchain businesses to plan and expand their operations if states were aligned on regulatory issues, particularly in the area of digital assets.

The Uniform Law Commission (ULC) has made several attempts to create a standardized approach to digital asset regulation. 94 In 2017, the ULC proposed the Uniform Regulation of Virtual-Currency Businesses Act to provide "a statutory framework for the regulation of companies engaging in 'virtual-currency business activity.'" 95 An accompanying "Supplemental Act" in 2018 provided rules related to commercial law and the Uniform Commercial Code. 96

These model acts had a short and controversial lifespan. No state enacted the model legislation, and only a handful of states introduced it. 97 Wyoming actively resisted the ULC's request to withdraw Wyoming's pending blockchain [\*201] legislation in favor of adopting the ULC's approach. 98 Wyoming's legislators noted that the ULC's model acts had not yet been enacted by any jurisdictions, and explained why they considered Wyoming's regulatory approach to be the superior one. 99 One month later, the ULC recognized the need to convene a committee to study how the Uniform Commercial Code could be amended in order to "deal with emerging technologies." 100 The ULC urged "states to refrain from enacting legislation pending the result of the committee's work," 101 an act suggesting that the ULC recognized flaws in its proposed acts. 102 Given the ongoing interjurisdictional race described in Section II.D, it seems absurd to ask states to wait on enacting blockchain legislation.

As of December 2020, only one state (Louisiana) had passed a virtual currency licensing statute based on the ULC's uniform act. 103 It is clear that, much like the race for corporate and LLC charters, the uniformity train has left this station. In the absence of federal legislation or effective model acts, states have already invested time and energy into drafting new laws. States like Wyoming, which has "actively decided to lead the charge in ensuring solvent, blockchain based" companies, 104 will not willingly give up their leading positions in this area.

III. THE CURRENT UNEASY MIX OF FEDERAL AND STATE BLOCKCHAIN REGULATION

Federal and state regulators are struggling to keep up with the fast pace of blockchain technology development. This Part will demonstrate how this struggle is creating a wide variety of regulatory approaches.

[\*202] A. Patchwork Agency Regulation

The federal government's attempt to regulate blockchain technology, particularly cryptocurrencies, is (to put it bluntly) a mess. Federal authorities interpret laws relating to blockchain and cryptocurrencies differently. 105 This confusing, piecemeal approach is epitomized by the struggle to determine how to even classify digital currency for regulatory purposes. The Internal Revenue Service (IRS) views cryptocurrency as property, the Securities and Exchange Commission (SEC) classifies such currencies as securities, and the Commodity Futures Trading Commission (CFTC) considers cryptocurrency to be a commodity. 106 There is clearly a need for a unified methodology, even just within blockchain's narrow use case of cryptocurrencies, but this confusion is not a surprising result when "neither Congress nor the SEC has formally elucidated which digital assets are securities and which are not." 107

Different agencies are sending different messages, creating "regulatory whiplash." 108 Some, like the CFTC, are inclined toward experimentation to support blockchain and cryptocurrency development, while others are more cautious. 109 All of the agencies seeking to regulate blockchain technology and its applications would benefit from consideration of the five factors listed in Part III. Below is a short explanation of three distinctive agency approaches.

[\*203] 1. SEC Safe Harbor Provision--A Work in Progress

The SEC missed its chance to establish a clear regulatory framework early in the life span of blockchain technology, instead adopting an approach characterized by delay and a series of reversals on important decisions. 110 The SEC's delay "simultaneously encouraged unscrupulous actors to take advantage of ambiguous regulations" and issue fraudulent tokens to Americans, while "driving away conscientious developers and entrepreneurs" to places with more developed laws. 111 The SEC's attempt to clarify its position in a limited area with the April 2019 issuance of a "Framework for 'Investment Analysis' of Digital Assets" has been called "too little too late." 112

In the meantime, SEC Commissioner Hester Peirce has earned the nickname "Crypto Mom." 113 In early 2020, she offered her take on the legislative problems related to blockchain technology, saying "[i]t is important to write rules that well-intentioned people can follow. When we see people struggling to find a way both to comply with the law and accomplish their laudable objectives, we need to ask ourselves whether the law should change to enable them to pursue their efforts in confidence that they are doing so legally." 114 Peirce clearly views law and regulation as a way to promote, not thwart, the development of blockchain and its use cases.

In February 2020, Peirce proposed a safe harbor provision for firms in the cryptocurrency space selling tokens to the public. 115 Peirce described her proposal as recognizing "the need to achieve the investor protection objectives of the securities laws, as well as the need to provide the regulatory flexibility that allows innovation to flourish." 116 The safe harbor proposal includes disclosure requirements for issuers and good faith obligations to ensure that token issuers are not fly-by-night companies. It also sets forth rules related to the purpose of token issuances and efforts to create liquidity for token users. 117

[\*204] The idea underlying the proposal is to "give new projects some breathing room where they can do their work without fear of being fined, arrested or having their offices raided." 118 This also filters "out the bogus projects that have no intention of building a workable, decentralized product." 119 Peirce appears to be seeking a way to protect consumers from unscrupulous token issuers while allowing companies to move forward with technical developments.

Many members of the blockchain industry welcomed the safe harbor proposal. The General Counsel for a cryptocurrency exchange declared, "Today we both congratulate and thank SEC Commissioner Hester Peirce . . . . This is a great day for the blockchain industry and the United States." 120 But the proposed safe harbor is just that: a proposal. It is not yet law, and may never become law. 121 Even so, the willingness of Commissioner Peirce to think outside of the box with this proposal has reinforced her reputation (and her nickname) within the blockchain community.

2. The Federal Reserve's Digital Dollar

The Federal Reserve revealed in February 2020 that it was working toward a potential central bank digital currency (CBDC). 122 A CBDC, colloquially [\*205] known as a "digital dollar," is not a token based on a decentralized blockchain. 123 It would instead be a "debt notation on a centralized ledger maintained by the Federal Reserve," which would use a centralized database to track consumer or business balances. 124 Individuals could "access funds through digital dollar wallets, which would also be managed by the Fed." 125

Although the digital dollar is different from a crypto asset on a blockchain, the policy issues at hand are quite similar. The Federal Reserve recognizes that these policies include financial stability and legal considerations, such as privacy concerns and protections for data and digital identity safety. However, the Federal Reserve clearly wishes to be on the cutting edge of the digital dollar debate, with one of its members noting that "it is essential that we remain on the frontier of research and policy development regarding CBDC." 126

At the time, there was pressure on the Federal Reserve to begin researching a digital dollar. China is creating a digital yuan, 127 and some argue that the United States is already "falling behind" other countries in developing a CBDC. 128 In addition, the surprise release of Facebook's Libra in 2019 (now rebranded as "Diem") apparently inspired the Federal Reserve to accelerate its research on the potential of a CBDC. 129 The arrival of the COVID-19 pandemic expedited the discussion, as millions of people around the world moved toward cashless payments. 130

The discussion of a digital dollar jumped quickly during the pandemic from the Federal Reserve to Congress. Drafts of congressional emergency pandemic relief legislation in March 2020 included a digital dollar concept to speed up the delivery of stimulus payments. 131 A Congressional Task Force on Financial [\*206] Technology held hearings on the issue in June 2020. 132 Indeed, "the question might be not if digital currencies will find their way into the financial system, but when--and how." 133 As federal lawmakers move toward the creation and regulation of a CBDC, they should be pondering how to encourage innovation while protecting consumers. In addition, anyone involved with the CBDC should consider transparency issues involving the input of multiple stakeholders, as well as ethical considerations such as concerns for unbanked populations.

3. Treasury Department Regulations to Increase Cryptocurrency Transparency

Unlike SEC Commissioner Hester Peirce and the Federal Reserve, U.S. Treasury Secretary Steven Mnuchin has taken a more cautious (and arguably negative) approach to cryptocurrency. 134 In February 2020, Secretary Mnuchin told the Senate Finance Committee that the Treasury Department would be enacting "stricter regulations around digital currencies to help expose 'secret' accounts and other nefarious activities." 135 Although Mnuchin acknowledged that "[w]e want to make sure that blockchain technology moves forward," he also noted that "[w]e want to make sure cryptocurrencies aren't used for the equivalent of old Swiss secret number bank accounts." 136

The goal of Treasury regulations will be to "ensure law enforcement can see where the money is flowing, and that it's not used for money laundering." 137 A March 2020 press release from the Treasury Department announced that the Department had held a meeting of "industry thought leaders and compliance [\*207] experts" on the issue of cryptocurrency regulation. 138 The press release also explained that as these regulations develop, Treasury will remain focused on preventing illegal conduct by "money launderers, terrorist financiers, and other bad actors." 139 The repeated use of such negative terms indicates the Department's adverse stance toward cryptocurrencies, as well as an example of lawmakers and regulators "still cling[ing] to an outdated trope where cryptocurrencies are used to underwrite criminal activity." 140

What can we make of this patchwork approach to regulation among U.S. federal agencies? Some may argue that it is better for the federal government to allow the blockchain industry and cryptocurrency markets to evolve before finalizing a regulatory structure. There can also be benefits to regulatory divergence, such as enhanced innovation as agencies compete to become the preferred regulator in a particular field. However, the absence of "intelligent rules and regulations that provide a clear and predictable framework for investors, issuers, and their lawyers" is complicating that evolution. 141 How can lawyers advise clients--such as start-up companies desiring to operate in the cryptocurrency sphere or offer tokens to investors--if it is unclear how such assets would be regulated? Policymakers are not sufficiently considering important factors, including transparency and uniformity, under this current approach.

Perhaps the problem is a lack of unity among federal agencies, who appear to be tripping over themselves to get in on the digital asset regulatory action. Federal policymakers may be concerned that they are not yet educated enough to make cohesive decisions about overarching regulatory frameworks, or they are waiting for Congress to step up. In any case, this confusion at the federal level is wreaking havoc on the blockchain industry in the United States. Innovative companies must risk inadvertently violating regulations (and having to pay the ensuing fines) just to push the industry forward. 142 Alternatively, companies are choosing to leave the U.S for other jurisdictions with better regulatory [\*208] clarity. 143 Piecemeal regulation among federal agencies is "not a substitute for transparent legislation or judicial rulings to guide market participants." 144

### 1AC---FTC ADV

#### Contention 2 is FTC.

#### FTC credibility is tanked by both unwillingness to launch bold antitrust AND a track record of losing in court, but Khan’s appointment is a window to revamp its policy.

Kiran Stacey 21, Washington Correspondent for The Financial Times, Graduated from Oxford University, Postgraduate Diploma from City University, London, Former South Asia Correspondent, “Washington vs Big Tech: Lina Khan’s Battle to Transform US Antitrust”, Financial Times, 8/10/2021, Lexis

Since taking over at the FTC, Khan has quickly begun to remodel it. Some of these changes look like technical internal reforms, while others are major policy statements. Almost all have been fiercely opposed by Republicans and the business community.

In the past few weeks, Khan has begun holding commission meetings in public - something Democrats say makes the commission more open to scrutiny, but which the two Republican commissioners say makes it harder for them to negotiate compromises.

She has banned staff from making public appearances such as conference panel sessions, saying the commission has too much work to do. She has passed a rule which allows FTC staff greater leeway to pursue investigations in certain priority areas, giving them the power to issue their own subpoenas for documents and testimony.

Khan is also promising to help rewrite the US merger guidelines, a complex set of documents laying out what kinds of evidence regulators look for when deciding whether a merger is illegal.

And, in a pair of crucial decisions, she and her fellow Democratic commissioners voted to rescind two key FTC policy statements.

The first was written in 1995 during Bill Clinton's first term as president, and deemed that companies that had previously proposed unlawful mergers no longer had to notify the FTC before completing future transactions in the same market.

By undoing that policy, Khan said she hoped to stop companies simply trying again and again to complete a merger even after it had been rejected by regulators. The second statement was written in 2015 during the Obama administration and set down limits on when the FTC would prosecute a company for socalled "unfair methods of competition".

"These changes are going to make dealmakers think about things differently," says one senior Democrat working for the commission. "They are not filing an application, we are investigating as to whether there is a violation of the law. That is a fundamentally different way of thinking about things."

Meanwhile, the White House has given the FTC the even bigger task of helping rewrite the rules that underpin the American economy. Under the terms of a sweeping order signed by Biden last month, the commission has been asked to devise rules which would ban companies from stopping employees moving to rivals, and prevent pharmaceutical companies from paying generic rivals not to enter a certain market for a period of time.

The moves have delighted progressives, who say Khan's willingness to push through reform quickly shows she is serious about putting the commission back at the heart of Washington rulemaking and enforcement.

"The commission has been lazy," says Matt Stoller, director of research at the American Economic Liberties Project and a former colleague of Khan at the Open Markets Institute. "It has been a place where you send political cronies who don't have to do any work if they don't want to.

"This is such a different form of politics from the normal bullshit."

Republican concerns But if the reforms have pleased Khan's supporters, they have worried conservatives who say the commission lacks both the legal authority and the institutional capacity to do what is being asked of it.

For example, Khan says she wants to renew the commission's appetite for bringing cases against companies for "unfair methods of competition" - a vague category of corporate behaviour which allows the FTC to act even when there is no merger in question or when a company is not large enough to be a monopoly. She and fellow progressives argue that by not pursuing such cases the FTC has taken away one of its most powerful weapons.

Such behaviour is often very hard to prove, however. When the FTC charged Abbott Labs in 1994 with trying to rig a bid to supply the Puerto Rico government with infant formula, for example, it alleged the company's choice not to bid in one of the rounds provided evidence of collusion with rivals. Abbott Labs' lawyers, however, successfully used game theory to explain why a "no bid" could in fact have made rational economic sense.

More controversial is the idea that the commission is going to start writing wide-ranging new rules of its own, as envisioned in Biden's competition order. This would test the limits of the FTC's powers in both court and on Capitol Hill, critics say, and could end in Congress clipping its wings as it did in 1980 when the FTC was forced to subject its rules to Congressional review.

Sean Heather, senior vice-president for antitrust at the US Chamber of Commerce, says: "The FTC is writing its own rules and acting as prosecutor, judge and jury. This is deeply concerning for a regulatory agency with broad powers."

Christine Wilson says: "I believe competition rulemaking is institutional suicide."

If Khan wanted an indication of how courts might view her approach, she got one within weeks of taking over the commission. In June, a federal judge dismissed the commission's complaint against Facebook, its most high-profile in years.

The commission had argued the social media company had engaged in anti-competitive conduct for years, including by buying up potential rivals such as WhatsApp and Instagram. In June, however, a federal judge ruled the commission had failed to prove that Facebook had monopoly power.

Khan's critics worry that if the commission loses a series of high-profile court cases it will fatally undermine its authority. "If you lose enough cases your credibility evaporates," says William Kovacic, a former Republican chair of the commission. "You can lose it all - not right away, but you can lose it all."

For Khan's supporters, however, this criticism borders on the absurd. "Don't you think the FTC is already seen as weak?" says Rohit Chopra, a Democratic commissioner.

Progressives argue the FTC has for years only enforced competition rules against large companies in a fraction of the cases it should have. "Do you think there are only 10 anti-competitive mergers a year?" says Chopra. "I'm not sure it can get any worse."

"The FTC can put together legal teams that can match the best in the bar, punch for punch, in a major case," says Kovacic. "But the number of those teams is a couple, it is not 10."

For years the commission's budget and staffing levels have been chipped away. It now has roughly 50 per cent of the staff it had in 1980 and is currently trying to review a record number of mergers. In the first nine months of this fiscal year, the FTC received 2,573 notifications ahead of a large merger - already 50 per cent more than were received in the whole of last year.

Last week, the commission published a statement warning that it would not be able to review all mergers within 30 days of a notification being made, as required by law. Instead, the FTC said, if it had not had time to review a merger before it took place, it would reserve the right to take action even after it had been completed.

The commission is also facing an uphill battle to retain staff. Some people say they feel demoralised by the pace of change and irritated they have not yet met their new chair - something Khan's allies say is an unfortunate result of the pandemic. "There are only so many times you can hear that your institution has failed for years before you start to doubt your place in it," says one staff member.

#### Specifically, blockchain is key.

Dr. David Morris 21, PhD in Media Studies from the University of Iowa, Former Academic Sociologist of Technology, CoinDesk’s Chief Insights Columnist, “Biden’s New FTC Chair Could Be a Big Web 3.0 Ally”, The Crypto Daily News, 6/16/2021, https://thecryptodailynews.com/2021/06/bidens-new-ftc-chair-could-be-a-big-web-3-0-ally/

Yesterday, the Biden administration named Lina Khan, a 32-year-old Columbia Law professor, as the brand new head of the Federal Trade Commission. Khan, who would be the youngest FTC head ever, is called a fierce critic of massive tech monopolies like Amazon. While there’s typically a knee-jerk resistance to regulation and regulators amongst blockchain advocates, Khan’s considerations make her a potential ally on huge points like privateness. Her antimonopoly work might additionally create substantial market alternatives for brand new sorts of tech companies – together with these constructing decentralized techniques and “Web 3.0.”

Enforcing U.S. antitrust regulation is a main a part of the FTC’s mandate, and Khan might be greatest identified for serving to redefine simply what a “monopoly” is. She has been essential, together with throughout seven years on the Open Markets Institute, in growing and selling the concept a firm could be a monopoly even when its practices drive prices down – even, the truth is, if its product is free to customers. That principle largely hinges on how the companies collect and use knowledge: Khan has been among the many loudest critics of the way in which Amazon makes use of knowledge gathered by its storefront, akin to by leveraging sales data to compete with third-party sellers who’re, a minimum of buyers, its prospects.

#### Failing to control blockchain violations will outstrip federal enforcement capacity, making traditional antitrust completely ineffective.

Drew Stanko 21, JD Candidate at St. John's University School of Law, BS in Economics from Villanova University, “Recent Developments and the Need for Nuance”, Journal of Civil Rights & Economic Development, 4/8/2021, https://www.jcred.org/shortreads/efforts-to-modernize-antitrust

I. IS NEW SCHOOL OFFICIALLY HERE?

In January 2007, the Economic Analysis Group at the Department of Justice Antitrust Division published a Discussion Paper entitled "Does Antitrust Need to be Modernized?" The paper reviewed whether "globalization and rapid technological change" necessitated changing federal antitrust laws. This Discussion Paper has proven prescient; it identified as a "key issue" the growing need for improving antitrust enforcement of alleged exclusionary conduct related to intellectual property.

Bipartisan support for antitrust reform has grown immensely since January 2007 due to heightened market concentration and Mergers & Acquisitions (M&A) rates in an increasingly complex digital economy. Senator Amy Klobuchar introduced antitrust reform legislation in February that would provide substantial funding increases to the FTC and the DOJ Antitrust Division, and the Biden Administration appears to be supporting efforts to modernize antitrust enforcement.

Recently, President Biden indicated intent to name two prominent "New School" antitrust attorneys and scholars, Lina Khan and Tim Wu, to positions in his administration. Kahn, who rose to prominence as a student at Yale Law School for "Amazon's Antitrust Paradox" and has since held positions at the Open Markets Institute and the FTC, will reportedly be nominated to serve as the Commissioner of the Federal Trade Commission. Wu is famous for coining the term "net neutrality" and authoring "The Curse of Bigness: Antitrust in the New Gilded Age," and he will serve on the National Economic Council as a special assistant to the president for technology and competition policy. Kahn and Wu have helped establish and develop the "New School" of antitrust jurisprudence, and both have taught related courses at Columbia Law School. Generally, the New School aims to prioritize "innovation, entrepreneurship, privacy, freedom of the press, and economic and civil liberties" rather than strictly focusing on "consumer welfare."

II. SENATOR KLOBUCHAR'S COMPETITION AND ANTITRUST LAW REFORM ACT:

Senator Amy Klobuchar, who spoke passionately about her concerns related to antitrust enforcement throughout her Presidential campaign, introduced antitrust reform legislation in February.

Sen. Klobuchar's proposal, the Competition and Antitrust Law Reform Act, aims to "give federal enforcers the resources they need [to] . . . strengthen prohibitions on anticompetitive conduct and mergers, and make additional reforms to improve enforcement." In order to accomplish these goals, the proposal would provide increased funding for the DOJ Antitrust Division and the FTC and would create a new FTC "Market Analysis" Bureau. While these structural and administrative reforms may receive bipartisan support, Sen. Klobuchar's proposal would also substantially alter the legal standards used to evaluate antitrust challenges under the Sherman and Clayton Acts, a change likely to be met with pushback by conservative economists and lawmakers. Sen. Klobuchar's proposal aims to accomplish important goals, but some argue the Sherman and Clayton Act amendments included in the legislation would "add friction to M&A Activity, stalling capital markets, reducing innovation and investment, and frustrating economic growth."

1. CLAYTON ACT REFORMS

Senator Klobuchar's proposal would modify the Clayton Act to "restore its original intent by amending it to include reference to 'exclusionary conduct.'" The legislation would define exclusionary conduct as "any conduct that would materially disadvantage . . . actual or potential competitors, or foreclose the ability of or incentive to compete." Currently, antitrust challenges require the plaintiff provide prima facie evidence that alleged anticompetitive effects of proposed mergers would result, and "proponents of the merger are then permitted to rebut by providing evidence that the merger will not have the feared anticompetitive effects."

The amendments would shift the presumption that "exclusionary conduct" presents a violative "appreciable risk" where such conduct is taken by a firm with a market share greater than 50% or otherwise wields significant market power. In turn, the burden would be on firms to prove the procompetitive market effects of the challenged conduct or merger rather than on the challenging entity to establish the anticompetitive impacts of the conduct that would result.

While it is important that antitrust reform efforts prioritize enforcement of anticompetitive exclusionary conduct, the legislation arguably defines the term overbroadly. Accordingly, the proposal may result in disincentivizing innovation that would ultimately benefit consumers and the overall economy. By presuming the illegality of any conduct taken by large firms that disincentivizes market entry or competition, the proposal risks unintentionally penalizing firms for achieving beneficial economies of scale or otherwise innovating to provide higher quality products more cheaply than competitors. Arguably, threatening firms with costly antitrust litigation whenever they undertake innovative conduct that negatively impacts competitors risks disrupting market incentives and stalling economic growth.

2. SHERMAN ACT REFORMS

Similarly, the Sherman Act would be modified to allow civil penalties of either 15% or 30% of a firm's US revenues for anticompetitive exclusionary conduct. Sen. Klobuchar has indicated that civil penalties are necessary because the existing remedies—injunctions, equitable monetary relief, and private damages—have not sufficiently deterred anticompetitive conduct. This may be true, but civil penalties of this size likewise risk stifling and disincentivizing innovation.

3. FUNDING ENFORCEMENT AGENCIES, FINANCING NEW "MARKET ANALYSIS BUREAU"

While the Sherman and Clayton Act reforms are unlikely to garner significant support from conservative lawmakers, the funding increases and creation of the FTC Market Analysis Bureau are more likely to win bipartisan support.

Increasing the funding available to the FTC and the DOJ would enable the agencies to hire more attorneys and would finance the creation of the Market Analysis Bureau. The MA Bureau would supplement the FTC's existing Competition, Consumer Protection, and Economics Bureaus. It would be tasked with conducting market, industry, and retrospective merger analyses aimed at helping the FTC develop a better understanding of the competitive conditions and underlying economic dynamics affecting complex markets. The creation of the MA Bureau is likely to gain support because it would demonstrate a commitment to ensuring continued reliance on empirical analyses rather than judicial or political discretion. Accordingly, these reforms would likely bolster enforcement efforts without necessarily adopting the "Big is Bad" approach that has historically divided lawyers and economists.

III. MODERNIZING ANTITRUST ECONOMICS

The Market Analysis Bureau would theoretically improve enforcement agencies' understanding of the economics underlying complex markets. This would provide enforcers with the tools needed to prosecute anticompetitive conduct that may have otherwise skirted enforcement due to the difficulty of establishing the negative economic effects of the conduct in question.

The complexity of the digital economy and increasing market concentration has made it more difficult for prosecutors to prove these anticompetitive results, but advances in machine learning and computational antitrust may assist in identifying and consistently enforcing antitrust violations.

While computational antitrust is certainly in its nascent stages of development, the early returns from Stanford's new Computational Antitrust Project are promising. The project's seminal article, authored by Project Director Thibault Schrepel, defines computational antitrust as a "new domain of legal informatics which seeks to develop computational methods for the automation of antitrust procedures and improvement of antitrust analysis." There are more than fifty global antitrust enforcement agencies participating in the project, including both the US FTC and the DOJ Antitrust Division.

Schrepel situates computational antitrust within "Antitrust 3.0," which he explains "is emerging but remains incomplete." At the core of Antitrust 3.0 is the goal of developing consistent enforcement frameworks designed to combat anticompetitive conduct in digital markets.

IV. OUTLOOK

In "The End of Antitrust History Revisted," Kahn "reviews" Wu's The Curse of Bigness and explains that the "task facing reformers is to translate their critiques into a positive vision, including legal rules and analytical frameworks." These analytical frameworks will be critical to ensuring that antitrust law promotes free market economics, rather than subjects firms to inconsistent judicial interpretation and prosecutorial discretion.

The majority of federal antitrust law applicable today was authored prior to 1915, and the unique challenges associated with prosecuting exclusionary conduct in digital markets have presented concerns for nearly twenty years. While bipartisan support for antitrust reform and emerging scholarship both provide legitimate reason to be optimistic about efforts to modernize federal antitrust law, it is important that reforms are nuanced enough to confront the complex problems they are enacted to address.

Accordingly, while Senator Klobuchar's proposal is certainly "well-intentioned," the budgetary reforms and creation of the Market Analysis Bureau should be separated from and passed without the proposed Sherman and Clayton Act amendments included in the legislation. The newly-appointed experts in the Biden Administration should be afforded the requisite resources to capitalize on the promise of New School antitrust jurisprudence and the development of Antitrust 3.0. By providing these resources, those leading antitrust modernization efforts will be equipped with the tools needed to create nuanced legal frameworks that reflect modern critiques and ensure consistent enforcement practices.

#### It creates a legitimacy crisis that threatens the foundational credibility of the FTC.

Dr. Thibault Schrepel 19, PhD in Antitrust Law from Université Paris-Saclay, LLM in International Law and Legal Studies from the Brooklyn Law School, Associate Professor of Law at VU Amsterdam University, Faculty Affiliate and Creator and Director of the Computational Antitrust Project at the Stanford University CodeX Center, “Collusion by Blockchain and Smart Contracts”, Harvard Journal of Law and Technology, 33 Harv. J. Law & Tec 117, Fall 2019, Lexis

V. CONCLUSION

Blockchain is a new and yet little-explored territory. It is, amongst other things, the Amazon 228 of tomorrow's collusive agreements: full of different life forms and new possibilities, the technology will give rise to unidentified creatures and dangerous species that we do not really know how to approach.

I have first shown that blockchain will be used to enhance the functioning of collusive agreements as we know them and that new forms of collusion linked to the technology conditions of access and use will appear as well. Second, blockchain will increase the stability of collusive agreements, providing them with a good life. Depending on whether the blockchain is public or private, a double paradox could emerge. One paradox is related to the visibility of all practices to colluders while ensuring their opacity to non-colluders. The other is associated with the fact that collusive agreements will be more robust during their lifetime by eliminating a large proportion of deviant behaviors, but will die in more brutal ways.

For these reasons, one can expect an increase in the number of collusive agreements along with an increase in their profitability, but not necessarily in their duration. The number of leniency applications may also drop because blockchain will reinforce trust during the lifetime of collusive agreements. This is largely due to the potential use of smart contracts because once again, "[o]ne of the greatest checks on crime is not the cruelty of punishments, but their inevitability," 229 which is precisely what smart contracts provide by automating punishments.

[\*164] The time has now come to detect collusion by blockchain and smart contracts, however difficult that may be. I have shown that some blockchains are more likely to induce collusive agreements than others. Antitrust and competition authorities may start with focusing their efforts on these blockchains and creating safe harbors for the others, for instance, by ensuring that no sanction will be imposed under antitrust and competition law for a specified number of years. Antitrust and competition authorities may also, when sending questionnaires to undertakings, ask whether they use blockchain, and if so, what type of blockchain, using which consensus, and for what purpose.

But perhaps it is even more urgent to adapt existing legal toolboxes before they become entirely ineffective, which implies considering a "law is code" approach and, generally speaking, transforming part of antitrust and competition law to become allies to blockchain core developers rather than mere threats. 230 It is said that "it is tempting, if the only tool you have is a hammer, to treat everything as if it were a nail." 231 As true as this statement is, all we have in existing laws is one size of pliers. With the wrong tools, the most sophisticated technology requiring great precision will not be as adjusted as it could be. Antitrust and competition agencies are currently not equipped to fight collusive agreements by blockchain. This may cause a legitimacy crisis for antitrust and competition law that may become ineffective sooner than expected. Indeed, it is more than likely that the use of current regulatory tools will be prevented by the technical characteristics of blockchain. Agencies further need to start analyzing code and software programming. Without doing so, most illegal activities on blockchain will remain safe. The same is true for all practices outside of blockchain which use the Internet. To date, antitrust and competition agencies refuse to analyze the programming of platforms and software. This creates a legal loophole and encourages companies to commit anti-competitive strategies precisely here. 232

Without fundamental research on this subject, palliatives will continue to be present, risking the survival of blockchain 233-- or antitrust [\*165] and competition law. 234 Some propose the creation of an identity management system so that the real identities of blockchain users can be revealed. 235 Others have suggested "adding a regulatory node in the blockchain" to spy on it 236 or imposing fines to the core developers when blockchain is used for illegal activities. 237 Going even further, it has been said that public blockchains "governed by international institutions from the legal tradition" such as the United Nations should be created. 238 But in fact, these solutions are either ineffective or would jeopardize the utility of the technology as its applications rely on the key characteristics that I have exposed in our introduction and that would be challenged by these various initiatives. Let us recall first and foremost that blockchain is a fundamental technology that may create good for the world. 239 The creation of safe harbors 240 and regulatory sandboxes 241 will enable competition agencies to respond quickly to the challenges posed by blockchain, but in the end, only a re-conceptualization of the law will provide a satisfactory answer. 242 Without it, antitrust and competition law will face a second legitimacy crisis arising from the absence of decentralized regulatory mechanisms. After all, how can decentralized transactions be properly regulated by pyramidal rules and institutions?

#### Failure of FTC legitimacy crushes the effectiveness of the agency.

William E. Kovacic 15, Global Competition Professor of Law and Policy at the George Washington University Law School and Non-Executive Director of the United Kingdom Competition and Markets Authority, “Creating A Respected Brand: How Regulatory Agencies Signal Quality”, George Mason Law Review, 22 Geo. Mason L. Rev. 237, Lexis

Introduction

One determinant of a government agency's effectiveness is its reputation, or "brand." Much like a commercial enterprise, an agency develops a brand that signals quality to various observers. A good reputation can help the agency recruit skilled personnel, gain deference from courts, build credibility with business managers, and build popular support that can yield larger budgets and enhancements to its powers. An agency with a strong brand stands a greater chance of being effective than one with a weak brand.

This Essay considers how branding can affect the performance of the Federal Trade Commission ("FTC") and other agencies responsible for economic regulation. It analyzes how investments in building a good brand enable the regulatory agency to signal quality to various observers - insiders such as agency staff and outsiders such as businesses, consumer groups, courts, and legislators. Part I of this Essay defines the concept of a brand for public agencies. Part II then discusses why an agency's brand can be important to its effectiveness and identifies what types of agency activities either enhance or degrade an agency's brand.

The examination of agency branding has several purposes. One aim is to improve our understanding of how public agencies build a reputation, and to study the role of reputation in determining effectiveness. A closely related goal is to give public officials a better understanding of how they should approach the task of deciding what their agencies must do to prosper.

A further aim is to underscore the impact of institutional design and managerial incentives on agency performance and to illuminate how design choices and incentive schemes influence the development of a well-respected, coherent agency brand. Various design choices - for example, whether to give the competition agency a single function or a multi-purpose substantive mandate, whether to govern the agency by a single executive or [\*238] by a board, whether to integrate the tasks of prosecution and adjudication in a single body or to unbundle them among distinct entities - affect the capacity of the agency to enhance the quality of its brand. Incentives that give incumbent leaders reason to make investments in long-term agency capacity and quality have the same effects.

I. Brands and Public Institutions

Public institutions, such as competition or consumer protection agencies, build reputations or "brands" that the agency's own employees and external observers associate with the agency. 1 Brands perform two functions for the public agency. The first function is informational. 2 A good brand conveys a good sense of what an agency does. It communicates, at least in a general way, the scope of the agency's responsibilities and the aims that motivate the agency in the exercise of its powers.

A brand also signals institutional quality. For an agency such as the FTC, the foundations for a good brand are sound substantive programs (e.g., cases, regulations, reports), sound procedures (e.g., meaningful disclosure of information, rigorous testing of evidence, regular assessment of outcomes), strong capabilities (e.g., deep expertise in economics and law), and a healthy culture (e.g., thoughtfulness, integrity, courage, and a commitment to continuous improvement). 3 For several reasons, explained below, a strong brand is a valuable asset for a regulatory agency.

#### Its credibility’s key to global cooperation to contain spyware.

Ari Schwartz 12, Deputy Director of the Center for Democracy and Technology, “Federal Trade Commission Reauthorization”, Hearing Before the Subcommittee on Interstate Commerce, Trade, and Tourism of the Committee on Commerce, Science, and Transportation United States Senate One Hundred Tenth Congress First Session, Government Printing Office, https://www.govinfo.gov/content/pkg/CHRG-110shrg75970/html/CHRG-110shrg75970.htm

Mr. Schwartz. Thank you very much, Chairman Dorgan. Thank you for holding this public hearing today and inviting CDT to participate.

As more consumers' services move online, consumer protection agencies are facing new challenges. The Federal Trade Commission has played a leadership role to meet these challenges, including overcoming such difficulties as locating the perpetrators of online schemes, keeping up with the rapid pace of technological evolution, and following the increasing financial motivation of Internet fraudsters.

In particular, the FTC has been the lead law enforcement agency in the world in the fight against spyware. Spyware has become one of the most serious threats to the Internet's future. Consumer Reports magazine estimates that consumers will lose $1.7 billion this year to spyware attacks alone. The magazine estimates that almost 1 million consumers simply gave up fixing their spyware-riddled computers and had to throw them away.

The good news is that consumer losses are down dramatically from 2006, when they peaked at $2.6 billion. The main reasons for this decrease in the spyware threat are, first, the improvement in anti-spyware technology; second, the public pressure on companies advertising with nuisance or harmful adware; and, finally, the enforcement of consumer protection law, led by the work of the FTC and some State attorneys general.

The FTC recognized the profound threat posed by the rising tide of spyware early, and actively moved to limit its spread. The Commission has been the leading enforcer against spyware, pursuing 11 cases to fruition in the past two and a half years, including three based, at least in part, on the petitions brought my organization, the Center for Democracy and Technology. CDT has learned, through our own research, that, as consumer fraud increases, the FTC's ability to work internationally becomes more important. Congress passed the SAFE WEB Act late last year to provide the FTC powers to promote international cooperation. The FTC's ability to use this new law, and staff resources that it will need, will be very important to monitor.

#### Spyware norms are solidifying but require strong U.S. leadership---success stops human rights crackdowns.

Marietje Schaake 21, International Policy Director at Stanford University’s Cyber Policy Center, Senior Advisor for Tech & Geopolitics at Eurasia Group, President of the Cyberpeace Institute, “We Need a New Global Standard to Curb Intrusive Spyware”, Financial Times, 11/10/2021, Lexis

After more than a decade, democratic governments are finally waking up to the hazards of commercial spyware. Recent media coverage has exposed how authoritarian regimes are using NSO Group’s Pegasus software to spy on journalists and politicians. The EU has now tightened its rules on the export of surveillance technology, and the US Department of Commerce last week determined that Israel-based NSO Group and three other hacking companies were “engaging in activities that are contrary to the national security or foreign policy interests of the United States”. However, these modest steps do not go far enough: what’s needed is a global standard to reign in technologies that violate the rights to privacy, free assembly as well as free expression.

From ~~crippling~~ [devastating] ransomware to questionable neural algorithms which use AI to identify suspicious non-verbal activity, to face and emotion-detecting technologies, there is a proliferation of software applications which conflict with liberal democratic values.

Traditionally, export controls are imposed on products that threaten national security, such as those that could boost the manufacture of nuclear weapons. The EU has recently extended its export regime to include spyware technologies, and added human rights violations as a criterion for potential harm. But since the NSO Group is based outside the EU, it lies outside Brussels’ jurisdiction. Without a wider international agreement, options for curbing these companies are limited.

The absence of global restrictions brings further credibility risks: how can liberal democracies lobby against human rights abuses by authoritarian regimes, when they are in effect permitting the development and marketing of digital weapons?

While restricting exports may help prevent the flow of intrusive technologies from democracies to dictatorships, imports and domestic uses remain unaddressed. The Pegasus Project revealed how, in the heart of the EU, Hungarian prime minister Viktor Orban has deployed commercial surveillance systems to target the few remaining independent media outlets within his own country.

Even some democratic states, such as the Netherlands, are guilty of procuring hacking and surveillance systems, but do not disclose which ones. Undoubtedly, they will claim these are only ever used to track down the most serious criminal and terror suspects. Yet this lends credibility and capital to an exceedingly harmful industry. If democracies are serious about curbing surveillance, they should exercise greater transparency and lead by example.

More than ad hoc measures or restrictions applied to individual companies, the US should partner with the EU and other willing countries to set a new international standard for the use of, and trade in, spyware. This would be a tangible outcome for President Biden’s upcoming Summit for Democracy, a US-led virtual meeting in early December aimed at preventing authoritarianism, fighting corruption, and promoting human rights.

Beyond spyware, a variety of other technologies deserve greater scrutiny and regulation. Illegitimate mass surveillance systems, facial recognition software and tools used for illegal cyber operations are traded across borders to facilitate repression, conflict, and instability. Poor cyber security is now a source of systematic risk which threatens national resilience. Greater co-ordination is necessary to ensure that technologies which are currently legal do not provide the means for widespread rights violations.

Moreover, an international agreement between democratic states against malicious uses of technology will help set multilateral norms. UN human rights experts this week raised the alarm once more about how tech companies serve as modern-day “mercenaries”. “Private actors provide a wide range of military and security services in cyber space, including data collection, intelligence and surveillance,” they warned.

In the future, a licensing requirement should be the default for tech companies that contravene the human rights standard of democratic states. This would ensure better controls of end use and exports. Regulation would also allow for mapping of how software is being deployed, and enable greater transparency. Equally, companies should strengthen their own risk-management. The very credibility of democracies is at stake when tech companies can undermine global security unhindered.

#### Those trigger nuclear conflict.

Gregory Treverton 17, Chair of the National Intelligence Council, Office of the Director of National Intelligence, National Intelligence Council Unclassified Strategic Assessment Of Global Trends, Authored by ODNI Personnel Including the Chairman of the NIC, “The Near Future: Tensions Are Rising”, 2017, <https://www.dni.gov/index.php/global-trends/near-future>

These global trends, challenging governance and changing the nature of power, will drive major consequences over the next five years. They will raise tensions across all regions and types of governments, both within and between countries. These near-term conditions will contribute to the expanding threat from terrorism and leave the future of international order in the balance.

Within countries, tensions are rising because citizens are raising basic questions about what they can expect from their governments in a constantly changing world. Publics are pushing governments to provide peace and prosperity more broadly and reliably at home when what happens abroad is increasingly shaping those conditions.

In turn, these dynamics are increasing tensions between countries—heightening the risk of interstate conflict during the next five years. A hobbled Europe, uncertainty about America’s role in the world, and weakened norms for conflict-prevention and human rights create openings for China and Russia. The combination will also embolden regional and nonstate aggressors—breathing new life into regional rivalries, such as between Riyadh and Tehran, Islamabad and New Delhi, and on the Korean Peninsula. Governance shortfalls also will drive threat perceptions and insecurity in countries such as Pakistan and North Korea.

* Economic interdependence among major powers remains a check on aggressive behavior but might be insufficient in itself to prevent a future conflict. Major and middle powers alike will search for ways to reduce the types of interdependence that leaves them vulnerable to economic coercion and financial sanctions, potentially providing them more freedom of action to aggressively pursue their interests.

Meanwhile, the threat from terrorism is likely to expand as the ability of states, groups, and individuals to impose harm diversifies. The net effect of rising tensions within and between countries—and the growing threat from terrorism—will be greater global disorder and considerable questions about the rules, institutions, and distribution of power in the international system.

Europe. Europe’s sharpening tensions and doubts about its future cohesion stem from institutions mismatched to its economic and security challenges. EU institutions set monetary policy for Eurozone states, but state capitals retain fiscal and security responsibilities—leaving poorer members saddled with debt and diminished growth prospects and each state determining its own approach to security. Public frustration with immigration, slow growth, and unemployment will fuel nativism and a preference for national solutions to continental problems.

* Outlook: Europe is likely to face additional shocks—banks remain unevenly capitalized and regulated, migration within and into Europe will continue, and Brexit will encourage regional and separatist movements in other European countries. Europe’s aging population will undermine economic output, shift consumption toward services—like health care—and away from goods and investment. A shortage of younger workers will reduce tax revenues, fueling debates over immigration to bolster the workforce. The EU’s future will hinge on its ability to reform its institutions, create jobs and growth, restore trust in elites, and address public concerns that immigration will radically alter national cultures.

United States. The next five years will test US resilience. As in Europe, tough economic times have brought out societal and class divisions. Stagnant wages and rising income inequality are fueling doubts about global economic integration and the “American Dream” of upward mobility. The share of American men age 25- 54 not seeking work is at the highest level since the Great Depression. Median incomes rose by 5 percent in 2015, however, and there are signs of renewal in some communities where real estate is affordable, returns on foreign and domestic investment are high, leveraging of immigrant talent is the norm, and expectations of federal assistance are low, according to contemporary observers.

* Outlook: Despite signs of economic improvement, challenges will be significant, with public trust in leaders and institutions sagging, politics highly polarized, and government revenue constrained by modest growth and rising entitlement outlays. Moreover, advances in robotics and artificial intelligence are likely to further disrupt labor markets. Meanwhile, uncertainty is high around the world regarding Washington’s global leadership role. The United States has rebounded from troubled times before, however, such as when the period of angst in the 1970s was followed by a stronger economic recovery and global role in the world. Innovation at the state and local level, flexible financial markets, tolerance for risk-taking, and a demographic profile more balanced than most large countries offer upside potential. Finally, America is distinct because it was founded on an inclusive ideal—the pursuit of life, liberty, and happiness for all, however imperfectly realized—rather than a race or ethnicity. This legacy remains a critical advantage for managing divisions.

Central and South America. Although state weakness and drug trafficking have and will continue to beset Central America, South America has been more stable than most regions of the world and has had many democratic advances—including recovery from populist waves from the right and the left. However, government efforts to provide greater economic and social stability are running up against budget and debt constraints. Weakened international demand for commodities has slowed growth. The expectations associated with new entrants to the middle class will strain public coffers, fuel political discontent, and possibly jeopardize the region’s significant progress against poverty and inequality Activist civil society organizations are likely to fuel social tensions by increasing awareness of elite corruption, inadequate infrastructure, and mismanagement. Some incumbents facing possible rejection by their publics are seeking to protect their power, which could lead to a period of intense political competition and democratic backsliding in some countries. Violence is particularly rampant in northern Central America, as gangs and organized criminal groups have undermined basic governance by regimes that lack capacity to provide many basic public goods and services.

* Outlook: Central and South America are likely to see more frequent changes in governments that are mismanaging the economy and beleaguered by widespread corruption. Leftist administrations already have lost power in places like Argentina, Guatemala, and Peru and are on the defensive in Venezuela, although new leaders will not have much time to show they can improve conditions. The success or failure of Mexico’s high-profile reforms might affect the willingness of other countries in the region to take similar political risks. The OECD accession process may be an opportunity—and incentive— for some countries to improve economic policies in a region with fairly balanced age demographics, significant energy resources, and well-established economic links to Asia, Europe, and the United States.

An Inward West? Among the industrial democracies of North America, Europe, Japan, South Korea, and Australia, leaders will search for ways to restore a sense of middle class wellbeing while some attempt to temper populist and nativist impulses. The result could be a more inwardly focused West than we have experienced in decades, which will seek to avoid costly foreign adventures while experimenting with domestic schemes to address fiscal limits, demographic problems, and wealth concentrations. This inward view will be far more pronounced in the European Union, which is absorbed by questions of EU governance and domestic challenges, than elsewhere.

* The European Union’s internal divisions, demographic woes, and moribund economic performance threaten its own status as a global player. For the coming five years at least, the need to restructure European relations in light of the UK’s decision to leave the EU will undermine the region’s international clout and could weaken transatlantic cooperation, while anti-immigration sentiments among the region’s populations will undermine domestic political support for Europe’s political leaders.
* Questions about the United States’ role in the world center on what the country can afford and what its public will support in backing allies, managing conflict, and overcoming its own divisions. Foreign publics and governments will be watching Washington for signs of compromise and cooperation, focusing especially on global trade, tax reform, workforce preparedness for advanced technologies, race relations, and its openness to experimentation at the state and local levels. Lack of domestic progress would signal a shift toward retrenchment, a weaker middle class, and potentially further global drift into disorder and regional spheres of influence. Yet, America’s capital, both human and security, is immense. Much of the world’s best talent seeks to live and work in the United States, and domestic and global hope for a competent and constructive foreign policy remain high.

China. China faces a daunting test—with its political stability in the balance. After three decades of historic economic growth and social change, Beijing, amid slower growth and the aftereffects of a debt binge, is transitioning from an investment-driven, export-based economy to one fueled by domestic consumption. Satisfying the demands of its new middle classes for clean air, affordable houses, improved services, and continued opportunities will be essential for the government to maintain legitimacy and political order. President Xi’s consolidation of power could threaten an established system of stable succession, while Chinese nationalism—a force Beijing occasionally encourages for support when facing foreign friction—may prove hard to control.

* Outlook: Beijing probably has ample resources to prop up growth while efforts to spur private consumption take hold. Nonetheless, the more it “doubles down” on state owned enterprises (SOEs) in the economy, the more it will be at greater risk of financial shocks that cast doubt on its ability to manage the economy. Automation and competition from lowcost producers elsewhere in Asia and even Africa will put pressure on wages for unskilled workers. The country’s rapidly shrinking working-age population will act as a strong headwind to growth.

Russia. Russia’s aspires to restore its great power status through nationalism, military modernization, nuclear saber rattling, and foreign engagements abroad. Yet, at home, it faces increasing constraints as its stagnant economy heads into a third consecutive year of recession. Moscow prizes stability and order, offering Russians security at the expense of personal freedoms and pluralism. Moscow’s ability to retain a role on the global stage—even through disruption—has also become a source of regime power and popularity at home. Russian nationalism features strongly in this story, with A Chinese man rides a bike among luxurious cars. China’s dramatic economic growth has highlighted greater gaps between rich and poor.

President Putin praising Russian culture as the last bulwark of conservative Christian values against the decadence of Europe and the tide of multiculturalism. Putin is personally popular, but approval ratings of 35 percent for the ruling party reflect public impatience with deteriorating quality of life conditions and abuse of power.

* Outlook: If the Kremlin’s tactics falter, Russia will become vulnerable to domestic instability driven by dissatisfied elites— even as a decline in status suggests more aggressive international action. Russia’s demographic picture has improved somewhat since the 1990s but remains bleak. Life expectancy among males is the lowest of the industrial world, and its population will continue to decline. The longer Moscow delays diversifying its economy, the more the government will stoke nationalism and sacrifice personal freedoms and pluralism to maintain control.

An Increasingly Assertive China and Russia. Beijing and Moscow will seek to lock in temporary competitive advantages and to right what they charge are historical wrongs before economic and demographic headwinds further slow their material progress and the West regains its footing. Both China and Russia maintain worldviews in which they are rightfully dominant in their regions and able to shape regional politics and economics to suit their security and material interests. Both have moved aggressively in recent years to exert greater influence in their regions, to contest the US geopolitically, and to force Washington to accept exclusionary regional spheres of influence—a situation that the United States has historically opposed. For example, China views the continuing presence of the US Navy in the Western Pacific, the centrality of US alliances in the region, and US protection of Taiwan as outdated and representative of the continuation of China’s “100 years of humiliation.”

* Recent Sino-Russian cooperation has been tactical, however, and is likely to return to competition if Beijing jeopardizes Russian interests in Central Asia and as Beijing enjoys more options for cheap energy supply beyond Russia. Moreover, it is not clear whether there is a mutually acceptable border between what China and Russia consider their natural spheres of influence. Meanwhile, India’s growing economic power and profile in the region will further complicate these calculations, as New Delhi navigates relations with Beijing, Moscow, and Washington to protect its own expanding interests. A Chinese development firm—with links to the Chinese Government and People’s Liberation Army— today announced that it recently purchased the uninhabited Cobia Island from the Government of Fiji for $850 million. Western security analysts assess that China plans to use the island to build a permanent military base in the South Pacific, 3,150 miles southwest of Hawaii.

Russian assertiveness will harden anti-Russian views in the Baltics and other parts of Europe, escalating the risk of conflict. Russia will seek, and sometimes feign, international cooperation, while openly challenging norms and rules it perceives as counter to its interests and providing support for leaders of fellow “managed democracies” that encourage resistance to American policies and preferences. Moscow has little stake in the rules of the global economy and can be counted on to take actions that weaken US and European institutional advantages. Moscow will test NATO and European resolve, seeking to undermine Western credibility; it will try to exploit splits between Europe’s north and south and east and west, and to drive a wedge between the United States and the EU.

* Similarly, Moscow will become more active in the Middle East and those parts of the world in which it believes it can check US influence. Finally, Russia will remain committed to nuclear weapons as a deterrent and as a counter to stronger conventional military forces, as well as its ticket to superpower status. Russian military doctrine purportedly includes the limited use of nuclear weapons in a situation where Russia’s vital interests are at stake to “deescalate” a conflict by demonstrating that continued conventional conflict risks escalating the crisis to a large scale nuclear exchange.

In Northeast Asia, growing tensions around the Korean Peninsula are likely, with the possibility of serious confrontation in the coming years. Kim Jong Un is consolidating his grip on power through a combination of patronage and terror and is doubling down on his nuclear and missile programs, developing long-range missiles that may soon threaten the continental United States. Beijing, Seoul, Tokyo, and Washington have a common incentive to manage security risks in Northeast Asia, but a history of warfare and occupation along with current mutual distrust makes cooperation difficult. Continued North Korean provocations, including additional nuclear and missile tests, might worsen stability in the region and prompt neighboring countries to take actions, sometimes unilaterally, to protect their security interests.

Competing Views on Instability

China and Russia portray global disorder as resulting from a Western plot to push what they see as self-serving American concepts and values of freedom to every corner of the planet. Western governments see instability as an underlying condition worsened by the end of the Cold War and incomplete political and economic development. Concerns over weak and fragile states rose more than a generation ago because of beliefs about the externalities they produce— whether disease, refugees, or terrorists in some instances. The growing interconnectedness of the planet, however, makes isolation from the global periphery an illusion, and the rise of human rights norms makes state violence against a governed population an unacceptable option.

#### Containing spyware prevents the complete erosion of Indian democracy

Mauktik Kulkarni 21, Trained in Engineering at the University of Pune, Biophysics at the University of Illinois at Urbana-Champaign, and Neuroscience at Johns Hopkins University, Author at The Fair Observer, Writer for National Public Radio, All India Radio, BBC Marathi, National Geographic, LiveMint, Times of India, and The Hindu, “Why Americans Should be Alarmed by the Pegasus Spyware Controversy in India”, Scroll, 8/2/2021, https://scroll.in/article/1001373/why-americans-should-be-alarmed-by-the-pegasus-spyware-controversy-in-india

Under a collaboration called the Pegasus Project, 17 media organisations from around the world have recently released startling information about the way several governments have allegedly used spyware made by Israeli firm NSO to snoop on perceived adversaries.

Pegasus spyware, classified as a weapon to be used against criminals and terrorists, was allegedly used in India to spy on opposition politicians, bureaucrats and journalists, among others. While the Indian government has denied the charges, all the evidence points to the executive branch running amok.

The unravelling of Indian democracy offers important lessons for the United States, especially with recent revelations regarding former President Donald Trump’s final days in office and the reluctance of his Republican Party in the legislature to hold him accountable.

The destruction of Indian democratic institutions under Narendra Modi since he came to power in 2014 is well documented. If these new allegations are left unaddressed, which is the most likely outcome, their chilling effect on society will ensure India’s swift decline into a sham democracy like Russia.

If true, the implications of such surveillance are not limited to political, bureaucratic, journalistic, or judicial opponents of the current government. They will affect the economic climate, open-minded academic inquiry, and spirited debates among students and civil society, which are all essential for a thriving democracy.

#### Backsliding obliterates containment of disease, pollution, and nukes---extinction.

Akshai Vikram 21, Doctoral Candidate in Security Studies at the University of Central Florida, Roger L. Hale Fellow at the Ploughshares Fund, M.A from Johns Hopkins University SAIS and B.A. from Johns Hopkins Baltimore, “Indian Democracy Is on The Ropes. The US Must Act”, Defense One, 6/12/2021, https://www.defenseone.com/ideas/2021/06/indian-democracy-ropes-us-must-act/174679/

Even as the U.K. hosted President Biden on a visit to “rally the world’s democracies,” Britain’s reopening is under threat from a new strain of the COVID-19 virus. This new variant, which originated in India, is directly related to Narendra Modi government’s disappointing and less-than-democratic handling of the pandemic. The new coronavirus strain is just one example of the threat that awaits U.S. interests if India, the world’s largest democracy, should complete its slide into authoritarianism. Thankfully, the U.S. still has a number of options to combat, if not prevent, democratic backsliding in India.

Democratic or not, India’s relevance is assured. Its size alone guarantees this. India’s largest state, Uttar Pradesh, boasts a population of over 200 million people, larger than any individual country in Africa, Europe, or Latin America. This hard fact has led Republicans and Democrats to agree on India’s importance, with both sides emphasizing its potential role as a regional counterweight to China. The Trump administration’s National Defense Strategy stressed the benefits of a “free and open Indo-Pacific region” and promised to “strengthen our alliances and partnerships in the Indo-Pacific…to preserve the free and open international system.” The Biden administration made similar pronouncements in its Interim National Security Guidance, saying it will “reinvigorate and modernize our alliances and partnerships,” partially to “hold countries like China to account.” The Biden administration specifically promised to “deepen our partnership with India” as part of this effort.

This strategic logic presumes the United States will be dealing with a democratic India that prefers a “free and open international system,” rather than an authoritarian India that domestically more closely resembles “countries like China” than it does a full-functioning democracy.

But the pace of Indian democratic backsliding has noticeably quickened. It was an ominous warning when Narendra Modi, who was banned from the United States for turning a blind eye to a virtual pogrom against Muslims while chief minister of Gujarat, was elected Prime Minister in 2014. After seven years in power, Modi and his Hindu nationalist Bharatiya Janata Party, or BJP, have further eroded Indian democracy, leading the nonprofit Freedom House to rank India as “partly free” for the first time in 30 years.

Modi’s authoritarian actions have ranged from the pseudo-scientific and laughable to the egomaniacal and lethal. Most notoriously, the BJP sought in 2019 to openly discriminate against Muslim immigrants. The law passed, and when it drew mass protests across the country, the BJP met them with authoritarian force. Later in the year, India stifled the Internet in Kashmir.

India’s democratic backsliding has also hurt its lackluster COVID-19 response. Modi’s BJP has propagated a number of inane myths about the disease, especially quack cures. Party leaders from Modi on down have set bad examples, appearing at large rallies, without masks, and turning the Hindu Kumbh-Mela festival into a superspreader event because “the faith in God will overcome the fear of Covid-19.”

The Modi government has also moved to stifle dissent, especially investigative journalism on its pandemic response. In April, the chief minister of Uttar Pradesh threatened to seize the property of people propagating “rumors” of oxygen shortages. And just last month, when information on the Indian variant was desperately needed, a top Indian virologist on a government panel to investigate the variant suspiciously resigned, after he had been quoted in the New York Times criticizing the government. All this suggests that continued democracy in India is no sure thing.

A fully authoritarian India could take a number of forms, with disparate effects on its relationship with the United States. Shared concerns about China could lead the U.S.-India relationship to mirror the path of American relations with Vietnam, where the two countries have managed to work constructively despite their tempestuous past and Vietnam’s one-party rule.

Perhaps more likely, India under Modi could present a challenge not dissimilar to that of the Philippines under Duterte, a country too strategically important for the U.S. to ignore in its efforts to counter Chinese influence in the region, but one whose authoritarian streak routinely impedes greater cooperation.

Most detrimentally for the United States, India could even one day seek to follow the path of Russia, prioritizing allegiance to right-wing authoritarian ethno-nationalism rather than its historical and geographic disputes with China. This worst case scenario is not as far-fetched as it once might have seemed: in the last few months alone, Russia and India have taken eerily similar steps to stifle Twitter in response to domestic critics.

No matter how authoritarian the government in New Delhi becomes, the United States will need to engage with it constructively on certain issues, especially transnational threats like climate change and nuclear weapons. Fortunately, the Biden administration has already demonstrated its capability to do just that by cooperating constructively with Russia on nuclear arms control and with both China and Russia on climate change, while at the same time confronting both countries on other issues as necessary.

However, there is no scenario where further democratic backsliding in India would make life easier for the United States. At the very least, an increasingly authoritarian Indian would jeopardize the push for cooperation among ‘like-minded’ democracies, especially when it comes to countering China.

International partnerships, like the recent project of coordinated vaccine production from the emerging ‘Quad’ countries—India, Australia, the U.S., and Japan—could conceivably continue even if India moves further from the democratic camp. Even so, they would surely be less resilient if based solely on common interests rather than common values. Efforts by the European Union to increase ties to India would also likely be undermined.

#### The plan solves:

#### 1. UPDATING.

#### Prohibiting violations at the infrastructure level establishes a collaborative relationship between blockchain and antitrust that infuses technological principles into legal enforcement.

Dr. Thibault Schrepel 21, PhD in Antitrust Law from Université Paris-Saclay, LLM in International Law and Legal Studies from the Brooklyn Law School, Associate Professor of Law at VU Amsterdam University, Faculty Affiliate and Creator and Director of the Computational Antitrust Project at the Stanford University CodeX Center, Blockchain + Antitrust: The Decentralization Formula, p. 247-249

1.2 Enforcement

1.2.1 Not this...

Enforcement is the second pillar of a collaborative approach between law and tech, antitrust and blockchain. I realize that this may seem counterintuitive; enforcement is, by definition, confrontational. In reality, distinct types of enforcement can lead to varying degrees of confrontation: some harm the entire blockchain, while others target the sole perpetrators of illegal practices. One should avoid the former, as it would reduce blockchain’s usefulness and thus deprive policymakers and regulators of an important ally. It is in the interests of both communities to encourage the latter.

I concluded the first part of this book by underlining that making law and tech work toward the same objective implied bearing with some assaults by each on the other. This means that blockchain communities should not only tolerate antitrust sanctions, but also facilitate them, because they ultimately lead to further decentralization. It also means that antitrust agencies and courts should direct their enforcement activities in a specific way. Overall, they should seek to preserve blockchain. This will be challenging, as agencies generally conduct their enforcement activities one case after the other, without such a long-term objective. That being said, agencies could still achieve the overall goal of enabling blockchain technology to flourish while ensuring case-by-case enforcement.

For that, agencies should avoid enforcement activities against practices that directly arise from the intrinsic characteristics of a blockchain. For example, public permissionless blockchains distribute information throughout the marketplace, including the number of transactions implemented by specific users, the fees being paid and so on. This transparency could lead to antitrust concerns, especially when it comes to tacit collusion.14 Nevertheless, because this essential feature makes markets more fluid and mitigates information asymmetry,15 enforcement activities should not be directed at it.

The same goes for the opacity that blockchains create. As we have seen together, the identity of a blockchain’s participants and the content of their transactions are protected by encryption. Yet one should not consider this a relevant element in European competition law for presuming the intention to collude (moral component), for systematically making cartelization on block- chain a restriction “by object” rather than “by effect,” or for easing the burden of proof on antitrust agencies. Doing so would deter legal uses of blockchain.

More generally, it is important to underline that all blockchain participants agree to the same set of rules. That should not be seen as an illegal agreement between them, even though it affects their economic behavior. Agreeing to the same rules is, in fact, necessary for blockchain’s survival, as it creates consistency in the blockchain ledger in the absence of central coordination. It solves the Byzantine Generals Problem, according to which a central power is always needed to coordinate actions and maximize outcomes. That applies to forks, which should only rarely be seen as illegal (as I discussed in Chapter 8), because they create checks and balances within each blockchain. Let me reiterate that without consensus regarding the rules and their modification, the whole system would collapse, as the ledger integrity could not be maintained. All practices engaged by the blockchain nucleus to ensure survival, such as their forks and modifications of the core client, should thus be presumptively legal as far as antitrust enforcement is concerned.

1.2.2 ...but that!

I recommend that antitrust agencies focus their enforcement activities on practices that affect the “real space”, and on practices that defeat blockchain’s purpose.

As I discussed in Chapters 9 and 11, the first type of practice covers the use of blockchains to support firms’ efforts to collude or monopolize markets. These practices have a strong and direct impact on consumers. Detecting this type of behavior will require proactive actions by antitrust agencies. If they engage in such actions, enforcement in the field will increase consumer welfare.

The second category concerns practices that centralize blockchain ecosystems artificially. More specifically, agencies should target practices that centralize the infrastructure level of a blockchain. As I have explained, that level has a critical influence on the decentralization of other levels. Prohibiting artificial forms of centralization at that layer will free most of the ecosystem from coercive forms of power. In doing so, it will make blockchain a more potent ally to antitrust law. Furthermore, this type of enforcement will prove increasingly important over time. If blockchain adoption continues to increase, it could very well become a key infrastructure for the world economy. At that point in time, the artificial centralization of blockchain will become antitrust agencies’ top enforcement priority.

Overall, directing enforcement activities toward these two types of practices would free blockchain, and its economic ramifications, from the most restrictive practices without diminishing its usefulness or creating resentment within blockchain communities. Antitrust would thus become the ally of blockchain ecosystems and would start being perceived as such.

#### 2. LEADERSHIP.

#### Going bold builds FTC’s brand and secures a foothold for future experimentation.

Philip J. Weiser 17, Hatfield Professor of Law and Dean Emeritus at the University of Colorado Law School, Former Senior Advisor for Technology and Innovation to the National Economic Council Director in the White House, “Entrepreneurial Administration”, Boston University Law Review, 97 B.U.L. Rev. 2011, December 2017, Lexis

Introduction

A core failing of today's administrative state and modern administrative law scholarship is the lack of imagination as to how agencies should operate. On the conventional telling, public agencies follow specific grants of regulatory authority, use the traditional tools of notice-and-comment rulemaking and adjudication, and are checked by judicial review. In reality, however, effective administration depends on entrepreneurial leadership that can spearhead policy experimentation and trial-and-error problem-solving, including the development of regulatory programs that use non-traditional tools.

Entrepreneurial administration takes place both at public agencies and private entities, each of which can address regulatory challenges and earn regulatory authority as a result. Consider, for example, that Energy Star, a successful program that has encouraged the manufacture and sale of energy efficient appliances, is developed and overseen by the Environmental Protection Agency ("EPA"). 1 After the EPA established the program, Congress codified it and, eventually, other countries followed suit. 2 By contrast, the successful and complementary program encouraging the construction of energy efficient buildings, the well-respected Leadership in Energy and Environmental Design ("LEED") standard, was developed and is overseen by a private organization. 3 After it was developed, a number of governmental authorities endorsed it and [\*2013] have encouraged LEED-certified construction projects with both carrots 4 and sticks. 5 Significantly, although neither the Energy Star program nor the LEED standard were originally anticipated by any regulatory statute, both have had tremendous impacts.

The Energy Star and LEED case studies exemplify the sort of innovative regulatory strategies taking root in the modern administrative state. 6 Despite the importance of entrepreneurial administration in practice, scholars have failed to examine the role of entrepreneurial leadership in spurring policy innovation and earning regulatory authority for an agency (or private entity). 7 This oversight is most unfortunate in the case of technologically developing fields where experimental regulatory strategies - as opposed to traditional notice-and-comment rulemaking or adjudication - are often essential. 8 In short, administrative law needs an account of agency action that explains why entrepreneurial leadership matters in government and how agencies should operate. 9

[\*2014] This Article: explains that the conventional view of agency behavior - following the specific direction of Congress or the President and using notice-and-comment rulemaking or adjudication processes - does not capture how public agencies and private entities develop innovative regulatory strategies and earn regulatory authority as a result. In particular, this Article: explains how governmental agencies like the EPA and private entities like the United States Green Building Council ("USGBC") (which oversees the LEED standard) depend on entrepreneurial leadership to develop experimental regulatory strategies. It also explains how, in the wake of such experiments, legislative bodies have the opportunity to evaluate regulatory innovations in practice before deciding whether to embrace, revise, reject, or merely tolerate them. To be sure, such experimental strategies are not always preferable to traditional administrative rulemaking and adjudication, but considering experimental strategies and evaluating whether they would be more effective than traditional regulatory approaches is.

Legal scholarship on experimental regulation is well-developed in the context of states serving as laboratories of democracy. 10 Scholars have not, however, discussed the significant role that federal agencies and private bodies can play in experimenting with regulatory strategies in advance of congressional action. 11 Scholars have also failed to examine the role of entrepreneurial leadership in developing successful experiments. This Article: does just that, highlighting the importance of entrepreneurial leadership in government, discussing a number of [\*2015] emerging regulatory experiments, and suggesting how Congress should evaluate such experiments.

This Article: proceeds in four parts. Part I examines the traditional model of regulation and the emerging alternative models of agency action through co-regulation, developing best practices through convening, and encouraging private regulation. In so doing, it underscores that entrepreneurial leadership and a culture of experimentation and trial-and-error learning is essential to developing the best solution. Part II discusses the relevant criteria for evaluating such experiments and examines potential objections to the earned regulatory authority model. Part III discusses four case studies of experimental regulatory strategies: (1) the USGBC's development of the LEED standard; (2) the Federal Trade Commission's ("FTC") oversight of information privacy and data security practices; (3) the National Institute of Standards and Technology's ("NIST") development of a strategy for cybersecurity readiness; and (4) the Department of Health and Human Services' ("HHS") oversight of electronic health records. In all of these cases, the private body or federal agency acted to oversee an emerging technology or issue (often in advance of explicit congressional direction and guidance), allowing Congress to observe the strategy in action and evaluate it after the fact. Part IV examines the concept of policy entrepreneurship, explaining both the barriers and opportunities it faces in the modern administrative state.

I. The Traditional Model and Emerging Realities

The traditional model of regulation relies on notice-and-comment rulemaking and agency adjudication. 12 Under this model, the output - the starting point for traditional administrative law analysis - is generally a form of positive law developed and enforced by a government agency through traditional tools (rulemaking or adjudication). 13 As Professors Charles Sabel and William Simon have observed, this model, "pejoratively called command and control, is identified with rule-bound bureaucracy and deference to ineffable expertise." 14

The traditional model can be depicted neatly as a hierarchy. 15 Congress sets a specific policy direction and empowers an administrative agency to implement that policy. The agency, in turn, uses either its rulemaking or adjudication authority to implement that direction. Finally, owing to the agency's expertise and congressional authorization, courts review the agency's action with deference.

[\*2016] Driven by technological changes and globalization, regulatory agencies increasingly are looking to alternative regulatory strategies, many of which fit under the "New Governance" label. 16 In some cases, innovative regulators experiment with new approaches to address emerging issues and fill gaps in the existing regulatory regime. In other cases, an agency might experiment with a co-regulatory strategy (where the agency integrates its authority with private sector efforts); exercise its authority in creative ways, such as developing best practices through convenings; or rely on private regulation. In that last category, as is the case with Energy Star, the government agency (or private entity, for that matter) can certify compliance with best practices, thereby sharing valuable information with the public and shaping norms of behavior. 17 In each of the above examples, the regulatory agency acts not within a hierarchy, but within a network. 18

[\*2017] The traditional, hierarchical model follows a familiar, step-wise approach to regulation. 19 The first step is establishing a standard of conduct. 20 The second step is implementing that standard of conduct, generally through a monitoring regime. 21 The final step is enforcement, in which parties are sanctioned for any failures to comply with the rules. 22 This model of regulatory action still holds strong in some areas, but it is no longer - and should not be - the exclusive strategy for addressing emerging policy issues.

In the emerging, networked environment, regulatory agencies find themselves with a range of options and tools for developing standards of conduct, monitoring behavior in the marketplace, and enforcing or encouraging compliance. The conversation around such emerging solutions has taken a number of forms, sometimes under the headings of "responsive regulation," "experimentalism," or "New Governance." However framed, there is a pressing need for more adaptable approaches that can operate effectively in technologically changing environments or in fields where the circumstances differ across geographic (or other) contexts. 23 To address emerging challenges, regulatory agencies will increasingly be called upon to experiment with non-traditional regulatory strategies, requiring legislatures to monitor and evaluate the effectiveness of innovative regulatory initiatives after the fact.

A. The Limits of the Traditional Regulatory Approach

The traditional model of regulation is coming under strain in the face of increasing globalization and technological change. 24 Consider, for example, the traditional model of drug and medical device approval used by the Food and Drug Administration ("FDA"). The legacy model of regulation envisioned the FDA reviewing a drug and making an up-or-down decision on whether to approve the marketing of the drug. 25 By putting all of the pressure on the front [\*2018] end (ex ante), the legacy model creates two sets of challenges: (1) the pre-approval process takes a long time, costs a lot of money, and, in some cases, unnecessarily delays access to potentially beneficial drugs; and (2) the lack of a post-approval review process allows drugs to "be marketed despite evidence that they were doing unanticipated harm." 26 Unfortunately, the second type of error - a lack of responsiveness to on-the-ground realities - reinforces the first type of error, creating more pressure on the FDA to withhold approval until it satisfies itself that the relevant drug or device will not cause harm. 27

Congress is well aware of the limits of traditional ex ante regulation. In the food and drug arena, it has worked to update the FDA's model of regulation. In the Food and Drug Administration Amendments of 2007, for example, Congress gave the FDA increased flexibility to approve drugs and require ongoing research as to how the drugs work, called for an improved Adverse Event Report System at the agency, and mandated a framework for monitoring drug efficacy in practice. 28 More recently, the FDA established fast-tracks for approving drugs and medical devices that promise life-saving breakthroughs. 29 As the FDA explained with respect to the medical device review process, "reducing premarket data requirements while increasing postmarket requirements for devices subject to a [Pre-Market Approval], when appropriate, can assist the FDA in making medical devices available to patients sooner than if following the traditional premarket review pathway." 30

[\*2019] This Article: , while sympathetic to the need to reform existing regulatory structures, does not focus on this issue. 31 Rather, it explains how considerable flexibility for a range of alternative options exists within current structures and is already being used by agencies and private entities to great effect. As such, this Article: describes the underappreciated model of earned regulatory authority, calls for a more self-conscious use of this model, and explains how agencies can spearhead and implement this model successfully through entrepreneurial leadership and a culture of trial-and-error problem solving. 32

The role of a more imaginative approach to regulation relates back to the "responsive regulation" movement led by Ayres and Braithwaite. On their account, regulatory strategies can be conceptualized as an "enforcement pyramid," with "persuasion" on the bottom and "license revocation" at the top (as the regulatory equivalent of the death penalty for a regulated firm). 33 In all cases, a responsive regulation approach emphasizes dialogue and engagement around the impact of regulatory efforts in practice. 34 In so doing, it underscores that regulators need not always use their traditional tools (notice-and-comment rulemaking and adjudication). Rather than reflexively adopting traditional approaches, regulatory agencies can (1) embrace and oversee self-regulation (enforced self-regulation or co-regulation), (2) convene stakeholders to develop best practices, or (3) persuade parties to develop private regulatory initiatives. The next three Sections discuss each strategy in turn.

[\*2020]

B. The Promise of Co-Regulation

Even when using its traditional authority, an agency can operate more nimbly and effectively by integrating its efforts with private bodies who have expertise in the field. Where that integration involves the explicit embrace, oversight, and enforcement of actions by private bodies, the model of regulation is aptly described as "co-regulation." 35 For a successful use of co-regulation, consider the FCC's use of frequency coordinators to assign rights to use the wireless spectrum. As I have explained previously:

One notable self-regulatory program that the FCC has overseen is the use of frequency coordinators, which manage voluntary cooperation in the use of point-to-point microwave links and private land mobile radio systems. In that context, the coordinator evaluates requests for new licenses and certifies that such new licenses will not cause undue interference to established users. Consequently, while the FCC is the authority that grants or denies licenses as a formal matter, it routinely relies on and defers to the judgment of the frequency coordinator. This deference to the frequency coordinator facilitates cooperation around the use of the relevant licenses. 36

The importance of this co-regulation model is that the FCC's delegation of authority enables practical problem-solving on the ground by the frequency coordinator. As Dale Hatfield, a former Chief Engineer at the FCC, explained, this system works because it encourages the local engineers to "sit down together, solve these problems, and say let's figure out how to do it," limiting the need for the FCC to use its backstop authority. 37

The FTC's partnership with the Better Business Bureau's National Advertising Division ("NAD") operates in a functionally similar fashion to the FCC's use of frequency coordinators. 38 Notably, the NAD has developed an [\*2021] effective model of dispute resolution around misleading advertising issues, deciding an array of issues and referring cases, where necessary and appropriate, to the FTC. 39 Because the NAD has developed such a trusted program, FTC leaders have praised its work and relied on it to carry the laboring oar in this area, 40 leaving the FTC's residual authority as a backstop. In particular, the NAD refers cases to the FTC where a party refuses to participate in its process or comply with a decision. 41

Learning from the NAD model, the European Union is working with the European Advertising Standards Alliance to develop a similar approach to overseeing false advertising claims. 42 In this case, however, the governmental authority is actively involved in developing and supporting this body rather than integrating its work after the body developed on its own. 43 In short, government can either embrace existing bodies as part of a co-regulation strategy or stimulate and steer the development of new ones.

C. The Role of Best Practices and Agency Convened Efforts

For many regulatory agencies, the opportunity to act as a "convenor," to develop best practices, and to create "soft law" or norms is an important part of their mission. As former FTC Chair Bill Kovacic explained with regard to the FTC, "Congress gave the FTC capacity to serve as a convenor - to engage in a diverse array of activities that facilitate norms development," including "what we now call "soft law' measures (e.g., self-regulatory standards, proposed guidelines)." 44 In particular, Congress specifically authorized the FTC to collect information and develop reports on topics not immediately related to cases or regulatory matters before the Commission. 45 In Kovacic's view, the FTC has used its convening authority effectively, "improving understanding, building consensus, and supplying focal points for norms development" through thoughtful reports that distill key issues. 46

[\*2022] For a range of agencies, the role of developing and championing best practices is on the rise, 47 reflecting a number of trends. First, many agencies find themselves without sufficient authority to promulgate binding rules as new technologies emerge. Second, even where an agency may have formal authority, it might be reluctant to use it in the face of an emerging technology where it needs to act more quickly than formal notice-and-comment rulemaking allows. Third, the agency may lack sufficient confidence that a prescriptive rule is warranted and thus leaves open a range of options, merely narrowing the field of possibilities and pointing entities in the right direction. 48

To develop best practices effectively, an agency must invest significant resources in the enterprise. Stated generally, this effort involves "horizontal modeling rather than hierarchical direction" and is "a method of regulation in which central administrators provide advice and disseminate information, instead of mandating a one-size-fits-all regulatory scheme." 49 In an increasing number of cases, best practices focus not only on U.S. firms, but also those across the world, requiring that the regulatory agency coordinate its international counterparts. 50 Moreover, to develop emerging best practices, it is important that agency staff take the time to learn the details of "the regulated entities first-hand, develop a strong sense of emerging processes, and … [share] knowledge of these processes with staff at other locations." 51

Where an agency (or a private entity) identifies and disseminates a best practice, it acts as a "norm entrepreneur." 52 As discussed in Part III, the FTC has performed this role in the online privacy and data security contexts, articulating and recommending a set of best practices. 53 One virtue of this role - like soft law more generally - is that it may well make the adoption of more formal regulation less necessary. 54 To the extent that the articulation of the relevant [\*2023] norm itself does not overcome the collective action problem and catalyze compliance with a norm, a certification regime (like Energy Star) for those who are compliant (along with naming and shaming) might do so.

One path for catalyzing compliance, which can be labeled as "jawboning" or "threats," involves the use of apparent legal authority - say, opening up an investigation - to achieve a desired result. In a provocative article, Professor Tim Wu defends the use of "threats," calling for norm entrepreneurship by agency leaders and the development of limiting principles for the practice. 55 In criticizing Wu's argument, some commentators have characterized it as condoning lawless conduct. 56 In that spirit, I previously criticized the FCC's use of its merger review authority to secure outcomes in other contexts that were not specifically related to the merger. 57 I also called the FCC's use of "arm twisting" controversial when done without full transparency and a willingness to take formal action. 58 Finally, I noted that the tactic is "dangerous" if the agency is not willing and able to follow through with formal regulation if the called-for behavior does not take place, as the meaningless nature of the threat will become plain and the agency will lose credibility. 59

Any agency that develops best practices should be aware of the potential risks of such an effort. For starters, if an agency's identified best practices are allowed to become stale, some private actors might stick with them and fail to improve their practice. Second, given that there is no judicial oversight of best practices development, 60 it is important that agencies pre-commit to a level of procedural regularity and fairness in how they develop them. Third, without either carrots or sticks related to best practices, an agency may find it difficult to generate attention or catalyze compliance. 61

[\*2024]

D. Private Regulation

As exemplified by the LEED building standard, a private regulatory initiative can drive behavior toward a social goal. Given the need to respond to emerging issues more adaptably than traditional regulatory processes allow, public agencies may be tempted to rely on private bodies. 62 In the internet environment, for example, a range of issues are managed by multi-stakeholder organizations, which use "dialogue to develop voluntary norms and best practices." 63 Similarly, in the environmental field, a range of "private activity generates pressure on environmental behavior without resulting in a statute, regulation, agency enforcement action, or court decision for review by scholars and policymakers." 64

The role of private, multi-stakeholder efforts in internet governance is the U.S. government's official policy. 65 Since the development of the internet's basic technical standards in the 1980s and 1990s by groups like the Internet Engineering Task Force ("IETF") and the World Wide Web Consortium ("W3C"), "these entities have largely established the norms and standards for the global internet, but they are little known to the general public." 66 The U.S. government recently fully embraced this model, recognizing the need for internet policy and governance issues to be developed in an adaptable and global fashion. 67 This embrace includes supporting the Internet Corporation for Assigned Names and Numbers ("ICANN") as an independent, international body to oversee the internet's numbering system. 68

In the internet context, two private regulatory efforts bear notice, as both exist in tandem with legal and regulatory oversight. First, the Copyright Alert System (overseen by the Center for Copyright Information) was a cooperative effort between broadband providers and content providers focused on addressing [\*2025] piracy in peer-to-peer networks. 69 This initiative, which existed for four years, 70 provided some measure of guidance to the broadband industry on what sort of "repeat infringer" policy was reasonable. 71 In light of recent court decisions holding a broadband provider liable for failing to develop an appropriate repeat infringer policy, the guidance from this organization could be considered best practice and protect a provider from liability, 72 although its cessation of operations may limit its impact. Second, the Broadband Internet Technical Advisory Group ("BITAG") is a multi-stakeholder organization that seeks to define best practices and broadband network management ahead of any FCC action under its network neutrality regime. 73 In its most recent regulatory decision on network neutrality, the FCC highlighted its openness to "obtaining objective advice from industry standard-setting bodies or similar organizations," specifically citing BITAG as an example. 74

Both the Center for Copyright Information and BITAG relied on a mix of industry representatives and public interest advocates and operated in an open, transparent, and consensus-based manner. 75 Like frequency coordinators and the [\*2026] NAD, the bodies confronted the challenge of earning their legitimacy and claim to regulatory authority. If such efforts succeeded, the FCC and copyright courts would regard their guidance as meaningful, just as the FTC and courts do with respect to the actions of the NAD. 76

In the environmental realm, the Marine Stewardship Council ("MSC") is an instructive case study on how a multi-stakeholder private regulatory initiative can have a major impact. The MSC, founded by the World Wildlife Fund and Unilever, was launched to address the concern about fisheries operating in a sustainable fashion. 77 As one commentator explained, "the MSC administers standards for sustainable fisheries, updates the standards periodically with input from a stakeholder advisory group, evaluates fisheries, and allows those fisheries that meet certain criteria to label their fish as MSC-certified." 78 The MSC standard focuses on three core concerns: (1) maintaining sustainable fish stocks; (2) minimizing any adverse environmental impact; and (3) managing the fishery effectively, including compliance with relevant legal requirements. 79 Under the MSC-administered regime, independent private auditors must assess compliance with the relevant standards and compliant products can be labeled as such. 80 Indeed, the MSC regime allows any organization with concerns related to certification to make a formal objection during the certification process. 81

[\*2027] The MSC provides a powerful example of how private regulation can work even when not reinforced by public regulation. 82 By 2012, sixty percent of the fish caught in U.S. fisheries for human consumption were MSC-certified and major corporations, such as Wal-Mart and McDonald's, had committed to selling only MSC-certified, wild-caught fish. 83 Moreover, the MSC's private regime drove compliance with the nonbinding Code of Conduct, developed by the United Nations Food and Agriculture Organization, by making it part of its requirements. 84 After surveying this regime and formal regulatory efforts to address the issue, one commentator concluded that the MSC model was more successful than traditional regulatory efforts in this area and that "private regulation is best situated to address the complex problem of fisheries depletion." 85

In short, private regulatory efforts, such as those led by multi-stakeholder organizations, can influence private behavior whether they operate in tandem with public regulatory oversight or in a vacuum created by a lack of regulatory oversight. Whether they operate in the backdrop of public oversight or as a standalone effort, private bodies need to establish their legitimacy to influence behavior on the ground. To do so, they must have sufficient independence from those they oversee, enabling both regulators and consumers to trust their judgments (including determinations of compliance). 86

[\*2028]

E. Hacking the Bureaucracy

In most situations, Congress and agencies think along traditional lines and agency leaders continue on the established path of agency regulation, under-utilizing the alternative models discussed above. 87 There are a number of reasons for this dynamic, including the power of "path dependency and bureaucratic entrenchment." 88 Even more powerfully, the incentives for policymakers are often to avoid Type 1 errors - those visible errors of commission - that arise when trying a new strategy that might fail. By contrast, the hidden Type 2 errors - ones of omission - are permissible and a regular feature of bureaucratic inertia. 89

On one account, the challenge of leading a bureaucracy is captured by the reality that governmental employees, who enjoy civil service protection, can tell their politically-selected leaders, "I was here long before you arrived and will be here long after you are gone." In practice, such explicit defiance is the exception. Regardless of whether bureaucratic inertia is willful or based on an entrenched tradition governmental agencies are built to continue the same course. Consequently, any course corrections require energetic leadership. 90 And governmental employees are generally conditioned "to be quiet, take orders, and do their jobs in a repetitive way." 91 On the positive side, governmental employees tend to have a service orientation and are mission driven, meaning [\*2029] that effective engagement around the mission and purpose of the agenda can catalyze innovation and collaboration. 92

Bureaucratic inertia and autopilot administration not only prevent innovative programs from being developed, but also can lead existing programs to be administered badly. Take, for example, the development of the healthcare.gov website. After Congress passed the Affordable Care Act, a health care economist, David Cutler, encouraged the White House to treat the administration of the law more like "launching a start-up than passing a law." 93 In particular, Cutler made clear that the default strategy - using the existing personnel at the Center for Medicare and Medicaid Services ("CMS") - for administering the law was a recipe for failure. 94 In an assessment ignored by the White House, he explained that CMS "is demoralized, the best people have left, IT services are antiquated, and there are fewer employees than in 1981, despite a much larger burden." 95

Cutler's call for an entrepreneurial approach to implementing the Affordable Care Act was rejected by President Obama. 96 Perhaps fearing the need to manage political warfare with House Republicans or responding to the HHS' interest in protecting its turf, President Obama agreed to, in Cutler's words, pile "new responsibilities onto a broken system." 97 As this episode underscores, even when the current system is flawed, the pressure to use it is powerful. As a result, the healthcare.gov website cost $ 800 million to develop, whereas Twitter, which serves a similar number of users and is of comparable complexity, cost only $ 60 million. 98

The redeeming part of the healthcare.gov story is that it demonstrates that treating a government project like a startup can work. After the failed rollout of healthcare.gov (which only enabled six people to sign up for insurance on its first day), President Obama essentially embraced Cutler's recommendation, [\*2030] authorizing Todd Park, Mikey Dickerson, and a team of entrepreneurs to operate in a new structure that was called "tech surge." 99 This project, like a good startup, approached the challenge of building an effective website from first principles. Rather than ask how the government had done IT projects before, the team innovated (for government) in a number of important ways, including using Amazon Web Services to support the site. 100 In developing the new website, it broke from the traditional bureaucratic process of "waterfall" development (where every step is prescribed and locked-in) and used "agile" development (where the process is iterative and evolves along the way). 101 Finally, the team built a login system for $ 4 million (with annual maintenance costs of $ 1 million) to replace the initial version that did not work well and cost $ 250 million to build (with $ 70 million annual maintenance costs). 102

In an important legacy of this effort, Park and Dickerson continued to work in government after fixing healthcare.gov, developing the new U.S. Digital Service ("USDS"). 103 The goal of the USDS is to lure a range of talented technology professionals to the federal government, including data scientists, product managers, and product designers. 104 The USDS, in turn, provides guidance to government agencies on questions like how they can use Amazon Web Services. 105 In short, the USDS supports entrepreneurial leadership in government; and as Park said, it develops "people who can hack the technology, as well as people who can hack the bureaucracy." 106

The healthcare.gov story now has two parts. The first is the cautionary tale about government's traditional inertial default setting - that is, to do things as they were done before. The second underscores that entrepreneurial leadership [\*2031] in government is both possible and important, and can lead to transformative results. 107

The positive legacy of the healthcare.gov story is that entrepreneurial leaders in government can free their agencies from "the mental grip of conventional structures on the capacity to consider alternatives." 108 In so doing, such leaders can facilitate the development of alternative regulatory strategies. Similarly, governmental agencies face the challenge of overcoming the institutional bias that "experts may myopically focus on issues within their area of expertise and thereby fail to recognize that a decision would benefit from accessing other bodies of knowledge or ways of thinking." 109 In short, an important role of entrepreneurial leadership in government is to examine issues through the lens of first principles. 110

The concept of policy entrepreneurship recognizes that an entrepreneurial mindset and skillset can be applied to governance to foster innovative results. Professor Adam Sheingate, for example, defines the concept as the "skillful manipulation of politics [that] somehow results in the creation of a new policy or a new bureaucratic agency, creates a new institution, or transforms an existing one." 111 This type of leadership can also be seen in the development of, for example, the MSC program, the FTC's oversight of online privacy, and the Energy Star program. In a world where the best solutions may well require new models of regulation, it is critical that agency leaders experiment with new solutions. 112

[\*2032] A significant hurdle for entrepreneurial leadership in government - and a foundation of the inertial default setting - is the lack of acceptance of failure as an outcome. In practice, this means that governmental agencies often reflexively turn to traditional regulatory models and do not consider untested alternatives (often out of fear of failure). 113 This instinct mirrors the old private sector saw that "nobody got fired for buying IBM." 114 Citing the fear of failure and risk aversion, former Massachusetts Governor Deval Patrick explained, "there may be no industry less susceptible to innovation than government." 115 There are, however, exceptions, including the Defense Advanced Research Projects Agency ("DARPA"), which makes a conscious effort to promote a "risk-taking and failure-tolerant culture." 116

In the entrepreneurship environment, failure is a normal state, providing data, an opportunity to iterate, and a spur to refine a product offering. 117 Consequently, entrepreneurs celebrate the need to "fail fast" on new experiments by trying them on a small scale and determining as quickly as possible whether they can work. 118 As two advocates of innovation in government put it, "[a] [\*2033] culture of innovation means continuously exploring and adopting new processes in an ecosystem where risk is incentivized, not precluded." 119 Similarly, entrepreneurial leadership in government authorizes calculated risk-taking and, more importantly, provides cover for trial-and-error learning when the trials do not produce the envisioned results. 120 Unfortunately, leaders who support experimentation and are willing to accept the inevitable failures, are the exception, not the rule. 121

The basic entrepreneurial methodology of experiment-measure-iterate is captured in Eric Ries's classic book, The Lean Startup. 122 A core thesis of the book, widely accepted in the entrepreneurial community (and ignored by most legal scholars), 123 is that companies should develop and market a "minimum viable product," solicit feedback from actual customers, and improve it based on that data. 124 At Facebook, this philosophy was adopted and embodied in its mantra, "done is better than perfect." Citing that mantra, one commentator explained that "had Facebook waited so much as a year to perfect its model, the company might very well be where MySpace is today." 125

The Ries philosophy is famously captured in a feedback loop representing the cycle of innovation. 126 The core idea is to embrace experimentation, gather data [\*2034] (whether it signals success or failure), and iterate. 127 The lean startup model, represented by the following diagram, focuses on taking ideas from prototype to feedback to improvement: 128

This lean startup model echoes the style of software development championed by open source software, which calls for releasing code that can be viewed and improved by a community of users and developers. In what Eric Raymond dubbed "Linus's Law," in honor of the founder and coordinator of Linux, the open source maxim is "given enough eyeballs, all bugs are shallow." 129 This approach has spread far beyond open source, enabling "business webs where focused companies partner others to innovate and create value." 130 Although this [\*2035] approach and a commitment to prototyping and testing solutions is novel in government, it is starting to take root, with promising results. 131

With respect to the fear of failure, government operates quite differently than the entrepreneurial world. In government, the perceived costs of failure are sufficiently high that many governmental leaders decline to introduce a new initiative for fear it will fail or refuse to admit that an existing program is failing, even though that admission is a necessary predicate for improvement. To be sure, there are cases like the initial healthcare.gov rollout where the failure is readily apparent and must be fixed. In other cases, however, governmental leaders stand by programs where the data backing up its effectiveness is either uncertain or doubtful.

For an instructive case of governmental leaders refusing to acknowledge the limitations of a program, consider the case of the EPA's Performance Track program. When created, the program was supposed to highlight those companies with stellar environmental records. 132 In practice, however, it ultimately became, as EPA Administrator Lisa Jackson put it, "just one of those window-dressing programs that has little value." 133 Similarly, the EPA Inspector General criticized the program as ineffective, noting that it did not provide "a new model for achieving" its stated goals and very few companies met their stated goals. 134 Nonetheless, the Bush Administration did not make any real changes to the program before the Obama Administration cancelled it. 135

The Performance Track program story, like the failure to acknowledge the failings of the healthcare.gov website earlier, underscores that the hesitancy to acknowledge failure is a major challenge in governmental administration. If governmental leaders refuse to acknowledge failures, they undermine the ability to learn - and iterate - from mistakes and instead allow failed programs to [\*2036] continue during a period of denial. 136 Or, as Lawrence Summers put it while reflecting on the healthcare.gov debacle, it is crucial to resist the "overwhelming temptation for everyone involved [in a project] to circle the wagons and promise rapid repair so as to hold critics at bay." 137

Another challenging dynamic for governmental leaders to address is the impact of unconscious bias. It is normal for those involved in a project to believe that it is working, following what Nobel Laureate Daniel Kahneman calls "confirmation bias." 138 As one commentator put it, a challenge for those evaluating regulatory experiments is that those "deeply involved in the implementation of a particular regulation are likely to see the benefits of such a project far more clearly than the costs." 139 As commentators have explained, there are a number of strategies for overcoming this bias, including using red team-blue team exercises, appointing a Devil's Advocate, and creating a process for deliberate decisionmaking. 140 Of course, as happened in the Performance Track situation, new leadership is able to bring a fresh perspective. Ideally, however, existing leaders can step back and ask, "if a new leader came in and took a fresh look, what would she do?" 141

[\*2037] The role of entrepreneurial leadership in encouraging candid reflection and criticism is essential. As former FTC Chair Bill Kovacic and David Hyman explain, agencies develop an institutional culture and a reputation (or a brand, as they put it). 142 In some cases, that brand can be one of reliability and commitment to data-driven decisionmaking. An important role of an entrepreneurial leader is to develop and maintain that commitment. In the case of Underwriters Laboratory ("UL"), for example, its early leadership did just that, building up "UL's reputation for reliability by creating organizational structures, administrative routines, and oversight systems designed to prevent mistakes and misconduct." 143 To get past the natural status quo bias, an entrepreneurial leader should welcome diverse ideas, criticism, different options, and experimentation. 144 In Part II, to explain how policy entrepreneurship can earn regulatory authority, I discuss how experimental initiatives need to establish their effectiveness, legitimacy, and accountability to be embraced as lasting regulatory regimes.

#### AND improves resource efficiency and investigation accuracy.

Almudena Arcelus 21, Principal at Analysis Group, Mihran Yenikomshian, Vice President at Analysis Group, and Noemi Nocera, Associate at Analysis Group, “Mitigating Antitrust Concerns When Competitors Share Data Using Blockchain Technology”, Harvard Journal of Law and Digital Technology, Harv. J.L. & Tech. Dig. (2021), Spring 2021, Lexis

C. Transparency for regulators

Implementing transparency in the network design can improve regulators' ability to investigate claims of antitrust violations. First, blockchain networks could be designed to provide antitrust investigators with a clear audit trail of the life cycle of an asset as it moves through a firm's supply chain, providing critical information to investigators as they assess when and how a firm's products transformed from raw materials to a finished good. Second, networks can be designed to provide investigators with more accurate, reliable, and comprehensive transaction data across an entire firm, rather than the piecemeal and inconsistent data that regulators often receive. Last, we could imagine the development of a blockchain, potentially accessible only by select parties or regulators, that contains industry-wide transaction data, which could provide an unmatched tool for investigators. Furthermore, the standardized data format in a blockchain may lead to faster resolution of potential antitrust investigations.

Whether or not these particular strategies would be effective in a real-world setting will depend on the industry or business context, the design of the blockchain network at issue, and the effectiveness of governance and regulatory oversight.

V. CONCLUSION

Because of its potential to change the way many governments' and firms' services currently operate, blockchain technology has attracted extensive press coverage. Although antitrust concerns exist in relation to blockchain adoption and data sharing between competitors (including access to information, collusion, abuse of dominance, and enforcement), blockchain serves mainly as a data management tool. How it affects competition will depend on network design and regulatory oversight, among other things. When examining antitrust concerns, industry observers as well as regulators should assess blockchain technology according to its specific implementation and its role in the wider framework within which it is used.

### 1AC---Plan

#### Plan: The United States federal government should increase its prohibitions on private sector anticompetitive practices by nucleus blockchain participants.

### 1AC---Solvency

#### Contention 3 is SOLVENCY.

#### Prohibiting anticompetitive practices by the blockchain nucleus creates a principled basis to apply antitrust to distributed ledgers without overbroadening liability for all users.

Dr. Thibault Schrepel 21, PhD in Antitrust Law from Université Paris-Saclay, LLM in International Law and Legal Studies from the Brooklyn Law School, Associate Professor of Law at VU Amsterdam University, Faculty Affiliate and Creator and Director of the Computational Antitrust Project at the Stanford University CodeX Center, Blockchain + Antitrust: The Decentralization Formula, p. 110

2 BLOCKCHAIN’S LEGAL FICTION

In this section, I introduce the theory of granularity and outline how it enables the application of antitrust law to blockchains. Transactional by nature, that theory aims to explain public permissionless blockchains beyond the simple cost reduction framework. It seeks to translate accurately the governing reality of such blockchains, creating for the purpose a new legal fiction that encapsulates blockchain without forcing it into inadequate boxes.

2.1 Dynamics of Blockchain Governance

The theory of granularity, to which one may want to provide a semantic explanation, frames blockchain governance as a new transactional institution. By doing so, it fills the gap created by the impossibility of applying the theory of the firm to public permissionless blockchains.

2.1.1 Semantic explanation

In “The Nature of the Firm”, Ronald Coase distinguished between organizations and organisms.3 While firms are organizations, blockchains are clusters of organisms that, by nature, are spontaneous. Their functioning must be analyzed and understood this way so that antitrust and competition law can be properly applied when necessary.

The present chapter introduces the theory of granularity for the purpose. Generally, the notion of granularity defines the size of the smallest element in a system - that is, an organism. Thus, this theory aims to analyze the role played by each component of a blockchain. Unlike the firm, where vertical control is exercised over its components, blockchains are made up of horizontal governance mechanisms. This reinforces the importance of each organism, as one cannot merely assume that they will follow one coordinated direction.4 One must then study blockchain’s smallest organisms, the role they play and their dynamism.5 It is only by analyzing the granularity level that blockchain governance can be properly understood.6

2.1.2 Understanding blockchain governance

Blockchain is a space in which different forms of power are being exercised. However, unlike the firm, in which one exercises a power of command and control, I have explained that no single actor can entirely control a public permissionless blockchain.7 As a result, multiple interests can compete within the same blockchain; they may even be opposed. Blockchain “contribute[s] to the realization of a number of individual objectives which no one knows in their totality”8 For that reason, one must study the different types of power that are generally found within public permissionless blockchains to understand which interests may eventually prevail over others. In doing so, we should keep in mind that “people who think the purpose of blockchains is to completely expunge soft mushy human intuitions and feelings in favor of completely algorithmic governance (emphasis on ‘completely’) are absolutely crazy.”9

I study blockchain power games by analyzing what I have described as the fifth blockchain level in Chapter 4: the governance layer. That level sits on top of more technical ones, and it appears to be central in defining the activities at the levels above. Furthermore, different constraints come into play in blockchain governance - namely, economic, political, logical, sociological, architectural and legal ones. Understanding how these constraints interact is a challenge; but it is essential in order to get a grip on who holds control over blockchain layer 1 and how that power is exercised over other participants.

A distinction between all three categories of public permissionless blockchain participants is helpful in this regard - namely, between founders or core developers (I will often present them together for the sake of simplicity), users and miners. I show that although each blockchain has its specificities, the above-mentioned groups will use the same mechanisms to express their preferences,10 and will encounter the same limits if they act on their own. Eventually, their powers may suffer from four constraints that Lawrence Lessig described with his “pathetic dot theory”: law, markets, social norms and architecture.11

As for private blockchains, I have explained that they mimic that structure to different degrees, depending on their original design. The closer they are to public permissionless blockchains, the less the theory of the firm will be transposable to them. The following developments then become relevant for public permissionless as well as private blockchains.

2.1.2.1 The power of founders and core developers'2

Blockchain founders and core developers are those who implement the original rules of a blockchain.13 They design the code software and determine which consensus protocol will be used.14

Although core developers work on the fourth level of blockchain - its infra- structure - they interact with other blockchain participants at the fifth level. Indeed, one may stress that the blockchain architecture limits their power, as they lose any form of direct control over other participants once they put the blockchain online.15 For most blockchains (but not all!),16 founders and core developers cannot unilaterally impose any changes17 or control who may propose protocol updates.18 For instance, any Bitcoin Improvement Proposals must be voted upon, according to miners’ computing power, before they get implemented.19 Indeed,“[t]he nature of Bitcoin is such that once version 0.1 was released, the core design was set in stone for the rest of its lifetime,”20 unless the majority agrees to change it.

The more participants are included in those voting procedures, the more decentralized that blockchain layer is.21 The opposite is also true. For instance, Decred22 and Tezos23 are cryptocurrencies with more centralized governance systems. One of Tezos’ principal characteristics is the ability to amend its consensus when necessary.24 The presence of off-chain and side-chain governance mechanisms, usually controlled by developers, should also be closely studied.25

It remains that core developers do not control who can use the blockchain at the platform layer26 or who can build applications on top of it.27 That is because blockchain founders and core developers cannot impose changes on the blockchain code, interface, application, data or benefice.28 Their main role is thus close to that of “advisors,”29 but their influence is limited by blockchain participants’ desire to maximize their own benefit, which may lead them, should they disagree with core developers, to refuse the implementation of new rules, to move to a rival ecosystem or to fork the blockchain.30 Social norms further limit them because they may fear not being influential enough to prevent hard forks.

Hard forks result in backward-incompatible software updates. When they do not obtain a sufficiently broad consensus among miners,31 hard forks cause the chain to split in two, permanently. Indeed, miners who do not follow the new block validation requirements will be unable to add their blocks to the latest version of the blockchain, as the core client will automatically reject them as non-compliant. Instead, a new chain of blocks will form, creating a split: two chains following different rules. These forks limit the core developers’ willingness to act against the interests of other participants.32 And core developers may also fear soft forks, although to a lesser degree. Soft forks happen when new rules are implemented, but when the blocks following the original rules are not rejected from the chain. These modifications are backward-compatible, accommodating miners who implement the change and those who do not. Nevertheless, one should underline that these limits on core developers’ power are linked to the decentralized nature of blockchain governance, which is not a necessary feature, but needs to be enacted.33 New blockchains may appear in which greater power is given to the founders and core developers.34

However, such blockchains will suffer from two inherent limits. First, the extent to which a (re)centralized blockchain could thrive remains to be seen.35 Such blockchains could deplete trust by confining power in the hands of a few, thus disincentivizing users from joining them. Second, a (re)centralized block- chain could function less efficiently than a truly decentralized one, because all its participants would no longer be in a position to improve it. This lack of efficiency, even if it only concerned certain types of transactions, could hinder these blockchains - which probably explains why, to this day, they have not prospered.

2.1.2.2 The power of users36

On permissionless public blockchains, users propose new transactions. Anyone can become a user.37 Users exercise substantial power over the blockchain, since their decision to use it (or not) is central to the blockchain’s economic and social value.38 Their influence extends from influencing transaction fees39 to providing additional value by developing and using applications running on top of the platform layer.40 They can also force hard forks on the blockchain.41 However, their power is limited by the fact they cannot (easily) exercise coordinated control, as their actions are highly decentralized and spontaneous.42 This creates an architectural limit and makes their behavior primarily dependent on prices.43

2.1.2.3 The power of miners44

On permissionless public blockchains, miners validate transactions assembled into blocks. Any participant can become a miner.45 Miners follow the rules encoded in the fourth blockchain level (e.g., the Bitcoin Core client).46 They can comply with a different set of rules, but they will then waste computing power by producing an orphaned block, thus losing potential rewards. Following the main client’s rules is miners’ dominant strategy.47 If they coordinate their behavior, miners can influence a blockchain by realizing a 51 percent attack,48 thus forcing a soft fork.49 The risk is higher when miners are grouped into mining pools.50 In such a scenario, the blockchain protocol is changed to loosen the rule-set enforced by full nodes.51 Such a change occurs when enough hashing power, or energy expended to mine a cryptocurrency, is devoted to it.52 The power of miners to start soft forks is nonetheless limited by both the blockchain’s architecture53 and social norms - they must convince blockchain participants operating as nodes to run the new version of the software.54 Miners also suffer from market constraints, as initiating a soft fork may decrease the value of the tokens they own.55 The price mechanism also guides their actions, creating a strong market-related constraint. Finally, even if a fork were created, the new community would have the strenuous task of convincing other users to join it.56 For example, Bitcoin had been forked over 100 times at the time of writing. Over 30 of them are considered failures, while another 29 projects are no longer capable of transacting. Among the remaining forks Just a few are considered valuable.57

2.1.3 The blockchain power game

This overall balance of power, common to all public permissionless block- chains, is the general analytical framework (as illustrated in Figure 7.1) within which to analyze whether one of these groups, on a case-by-case basis, has sufficient influence to qualify as control under antitrust or competition law.

On top of all that, core developers, users and miners may also store a copy of the blockchain ledger. When doing so, their computers are labeled as light nodes if they store only a subset of the blockchain ledger and full nodes if they store a copy of the entire blockchain.58

Although these nodes are passive and cannot be designated as actors in the blockchain, they ensure its integrity. This role carries power. First, blockchain participants who are nodes may alter their copy of the blockchain.59 Second, they may also (threaten to) validate blocks in which there is double spending.60 Their job is indeed to prevent users from spending the same token twice by allowing miners to verify the proposed transaction against a list of previous unspent transaction outputs. They protect blockchains value. However, their power is mainly limited by the fact that they cannot either control or influence transactions.61

This is the blockchain power game. It is well balanced, and technical solutions (called “layer 2” solutions) are constantly provided to maintain that balance. But these solutions are insufficient to maintain balance when different groups of blockchain participants come together to escape these constraints to the detriment of the broader ecosystem. When this occurs, they are exercising control over the blockchain.

2.2 The Blockchain Nucleus

Thus far, the theory of granularity has allowed me to determine the different forms of power enjoyed by blockchain participants. I must now detail how to identify a legal fiction controlling the blockchain.62 To this end, I explain what a blockchain nucleus is and then analyze its influence over other blockchain participants. 1 then describe how to define such a nucleus.

2.2.1 Usefulness and challenges

2.2.1.1 The nucleus

None of the three types of blockchain participants - core developers, users and miners - can impose their power on other groups to the point of taking complete control over the blockchain. Blockchains are indeed decentralized. They prevent the exercise of vertical power, and this differentiates them from firms in which a group, or sometimes even an individual, can control the other participants and “force them to collaborate,” so to speak.

That being said, even with horizontal and decentralized governance, a group of participants may achieve a form of control over the blockchain by collaborating, by circumventing (some of) the constraints imposed on them,63 and by changing them in the long run.64

I contend that such a coalition exists for each blockchain (at least, for the surviving ones),65 and I call it the nucleus. The nucleus includes all the participants who have a personal interest (albeit transiently) to collaborate toward the same long-term goal: ensuring the blockchain’s survival.66 Its members do not compete as they are, together, trying to maintain and expand their blockchain. Their short-term interests may diverge from time to time67 - for example, when two miners are racing to mine new blocks.68 Still, they seek to ensure blockchain integrity and systematically promote the same blockchain instead of other ones.

2.2.1.2 Usefulness

Assessing which participants have joined forces and are thus part of the nucleus is essential to determine who ultimately controls the blockchain. Put differently, it leads to identifying the participants that can be held liable for a breach of antitrust law when it is shown that they have anticompetitively exerted their influence.69 Identifying the nucleus amounts to creating a legal fiction to which the law can be applied, but also to which rights can be granted (see Figure 7.2).

The nucleus should indeed become a legal fiction that can be liable for anticompetitive practices, but also able to claim damages. In that regard, determining the nucleus size will prove central. It will prove useful in cases of anticompetitive practices directed at a blockchain nucleus. When a legal entity - whether a blockchain nucleus or a firm - infringes antitrust law and causes damages to another nucleus, the latter must have the means to introduce a legal action, stand by its rights and claim damages. Assigning liability and granting rights to blockchain ecosystems are thus two sides of the same coin.

3 DEFINING THE NUCLEUS SIZE

Courts and antitrust agencies will face the task of determining the nucleus size. The further away a participant will be from the nucleus’s center, the more difficult it will become to genuinely include her or him in the nucleus. With distance, it will prove harder to show that she or he could have influenced other participants’ behavior. Only a case-by-case analysis can elucidate this question. This analysis should nevertheless be based on concrete and quantifiable frameworks to ensure legal certainty, limit legal errors and reduce regulatory costs. To this end, agencies should focus their investigation on economic agents’ ability to exert a horizontal power of command and control. They should also consider their capacity to interfere with the blockchain’s economic value and influence norms.70

Let me be more specific. The first element that should be factored in to determine which participants are part of the nucleus is the technical ability to exert a horizontal quasi-power of command and control. One must assess each blockchain’s architectural characteristics to determine whether a few users may impose such decisions on others. The more a group of users can control others, the more they can single-handedly contribute to the block- chain’s survival, and therefore be considered part of the nucleus. In fact, the original design of a blockchain can give one of the three groups of users more or less power. It can put them in charge of implementing the execution of transactions, designate them as miners or even enable them to change the design a blockchain’s design unilaterally. Some blockchains might also use several mechanisms based on the platform layer to create governance (whether off-chain or side-chain).71

The second element is the ability of each participant to interfere with the blockchain’s economic value.72 When some users govern the pricing structures, the blockchain’s attractiveness or economic incentives, they have indirect control over the blockchain. This ability can be assessed by looking at technical elements. For instance, the capacity to change the size of each block, which may alter the number and types of transactions, is a sign of control. The same goes for the power to propose modifications to the core code to attract new participants. Finally, the more a participant has invested in the blockchain, the more he has an incentive to control its economic value.73 For that reason, previous investments in a blockchain can show agencies where to look for the nucleus.

The third element is the ability to influence a blockchain’s norms.74 Here, “norms” are defined as the “constraints imposed not through the organized or centralized actions of a state, but through the many slight and sometimes forceful sanctions that members of a community impose on each other”75 - that is, the unwritten rules that one often feels compelled to follow.76 The more a participant can incentivize others to behave in a certain way - on pain of rejection from the community - the more they exercise control over the blockchain’s general direction.77 For example, when core developers can influence other participants into accepting all of the modifications they would like to apply to the core (e.g., by arguing about the necessity for technical upgrades, security failures, bugs...), they effectively pilot part of the blockchain.

4 THE THEORY OF GRANULARITY IN ACTION

The theory of granularity would enable agencies to identify a blockchain’s nucleus. It would thus permit the creation of a legal fiction to which antitrust can be applied. In turn, this would impose new obligations upon blockchain participants while simultaneously giving them new means to challenge anti- competitive behavior. This theory would make it possible to analyze relevant markets and market power in antitrust proceedings. The theory of granularity would also make it possible to impute anticompetitive practices to a given set of blockchain participants.

#### Antitrust is limited by application only to the ‘firm’, defined by vertical control---modifying this with targeted prohibitions prevents blockchain centralization.

Dr. Thibault Schrepel 21, PhD in Antitrust Law from Université Paris-Saclay, LLM in International Law and Legal Studies from the Brooklyn Law School, Associate Professor of Law at VU Amsterdam University, Faculty Affiliate and Creator and Director of the Computational Antitrust Project at the Stanford University CodeX Center, Blockchain + Antitrust: The Decentralization Formula, p. 79-94

The second part of this book is dedicated to artificial centralization - namely, anticompetitive behaviors that take place on blockchains or are facilitated by them. 1 contend that studying these practices is essential to make blockchain and antitrust law function as allies; indeed, no sustainable cooperation is possible without addressing (and preparing for) the situations in which mutual aggressions will occur.

To this end, I first analyze the extent to which antitrust laws are currently applicable to blockchains. I show that the theory of the firm is central to modern antitrust (Chapter 6) and that it cannot be transposed to all blockchains. For that reason, I propose a new approach - dubbed “the theory of granularity”- which allows for the creation of a legal fiction, placing blockchain’s activities (back) under the rule of law (Chapter 7). I explain that implementing that approach would benefit all the players in the blockchain ecosystem. This would clear the way for law enforcers to apply the rule of law and, in turn, would help eliminate the most harmful practices and encourage investments. Once the question of applicability has been cleared up, I turn to how antitrust law could be applied to anticompetitive practices. To this end, I begin by looking at collusive practices, whether they concern the blockchain itself (Chapter 8) or make use of the blockchain to affect the “real space” (Chapter 9). 1 explain that these practices tend to centralize decision making power and thus contribute to the “artificial” centralization of different levels of block- chain ecosystems and the economy.

Part 2 closes by examining abuses of market power. I first show that the analysis of market power on blockchain raises several difficulties, and I offer suggestions to overcome them (Chapter 10). I then analyze the practices that may result from such power and show that they are heterogeneous (Chapter 11). I draw a risk map. Finally, I conclude by studying different forms of blockchain concentration (Chapter 12). I draw a distinction between hostile and mutually agreed concentrations and explain how these may recentralize blockchain.

6. The theory of the firm

1 LEGAL FICTIONS

The concept of “legal fiction” is central to all legal systems, although regulation and court decisions refer to it only infrequently. I first explain its meaning by taking a brief detour through... trees and forests. I then show why it is useful for the present study.

1.1 Trees as a Legal Fiction

Christopher D. Stone is a law professor in the United States. In 1965, after a stint at the University of Chicago,1 he joined the University of Southern California Law School, where he taught several subjects, including public international law and property law. One day in the fall of 1971, as he was nearing the end of a class, he asked his students the following question: “What would a radically different law-driven consciousness look like?” As he walked out of the classroom, down the corridor to his office, he wondered why he had asked such a strange thing. “How could a tree have rights,” after all? Days went by, and still he continued to wonder. He soon became convinced that the answer to his question should be positive and decided to make it known.

In October that same year, he got in touch with the Southern California Law Review's editor in chief. The Supreme Court had taken up a case, Sierra Club v. Morton, that touched upon his question. Although Stone did not think he would be able to publish his article before the case went to trial, he hoped that Justice William O. Douglas - who had agreed to write the preface to a symposium issue of the Review - would at least see the draft of his article. His strategy paid off. Although the Supreme Court decision did not follow his thesis, Justice Douglas wrote a dissent in which he held that: “Contemporary public concern for protecting nature’s ecological equilibrium should lead to the conferral of standing upon environmental objects to sue for their own preservation. See Should Trees Have Standing?”2 In 1974, Stone published a book in which he developed his theory further.

1.2 The Concept of Legal Fiction

Christopher Stone’s book is a pillar of modern thinking on the subject. Of course, the argument concerning what is a legal person - or a legal object to which rights are attributed - did not originate in the 1970s. Since medieval times, scholars have considered what rights should be attributed to corpo- rations3 - a debate they centered on the question of legal fictions. A “legal fiction” is presumably defined as a fact created by courts or legislation to help legal ruling.4 Stone poses three conditions for the creation of a new one:

They are, first, that the thing can institute legal actions at its behest, second, that in determining the granting of legal relief, the court must take injury to it into account; and, third, that relief must run to the benefit of it.5

A company meets these criteria. Legal systems have recognized them as a legal fiction for hundreds of years.6 Corporations are, in the words of John Sherman, “artificial person[s] without fear of death, without a soul to save or body to punish;”7 and yet they are at the center of our modern economies. Not only has the law “been able to exploit to its advantage and to maximize for its needs” the fact that corporations are persons; but also, they can file legal actions, suffer from damages and benefit from relief. One can find traces of that recognition in the Rolls of British Parliament in 1444: “they [the Master and Brethren of the Hospital] by that same name mowe be persones able to purchase Londez and Tenementz of all manere persones.” Here, the Hospital was recognized as a legal fiction.

As for the process of establishing legal fictions - once the criteria are known to be met - three methods have been used,8 whether by the courts (in common law) or by the legislature (in civil law). The first is by assertion, where one thing is declared to be true. For instance, one may say that corporations are persons. The second is by assumption - more specifically, by an irrefutable presumption that may morph into a legal fiction. For instance, one may say that corporations are presumed to be persons. The third is by deeming. Here, X is deemed to be Y, which creates a disconnect between the reality before deeming the fact, and after.

1.3 Legal Fiction and Blockchain

If legal fictions are so convenient, why not create a multitude of them? The first objection is the necessity to agree on the desirability of the objective they ought to achieve. When courts use legal fictions to deny minorities their fundamental rights, the objective is achieved, but society does not come out better.9 The second objection relates to the balance of power. Bentham called legal fictions “the stealing of legislative power” when courts create them. The third objection relates to the difficulty of creating a coherent legal system. Companies are legal persons, and although they can be charged with criminal activity, these crimes are committed by physical entities (persons). One must therefore put in place adequate measures to ensure that any illegal activity by a firm can be put to an end (that its perpetrators cease to act). The fourth and final objection concerns the systematization of the law. The creation of legal fictions leads to the elimination of case-by-case analysis, at least partially. For instance, a firm will always be a legal person. That may create difficulties because it entails giving the firm all the fundamental rights given to us, humans.

On the other hand, creating legal fictions significantly improves legal certainty. First, this applies to the entities directly concerned, which as legal fictions may bring actions under their own name and can thus be compensated for any damage they might unjustly suffer. It also creates legal certainty for all those who interact with these legal fictions, as trading partners can indeed bring legal actions against them. It helps when legal fictions rather than individuals benefit from illegal practices and cases where several individuals are responsible for a behavior. In short, although the creation of legal fictions is an exercise that requires precision, it unlocks a range of potential interactions that can greatly benefit society.

I intend to explain that creating a new legal fiction for blockchains is essential to their decentralization. I have argued that decentralization is the capacity of subjects to determine their competence. That requires recognizing their legal existence before transferring such capacity. Doing so will also allow them to introduce proper legal actions and prevent illegal behaviors being turned against them.

2 THE FIRM IN ANTITRUST

Antitrust’s most common legal fiction is the firm. That legal fiction has developed little since the 1930s and Ronald Coase’s work. For that reason, one may wish to understand its premises to get a grasp of modem antitrust law.

2.1 The Theory of the Firm

The economic literature regarding the emergence of firms emphasizes the importance of transaction costs and the ability to reduce them thanks to top-down control. To this day, that theory has provided the bedrock for modem microeconomic analysis.

2.1.1 Highlights of Ronald Coase’s article

In 1937, when he was 21 years old, Ronald Coase published “The Nature of the Firm.”10 It contains no mathematics and is just 20 pages long, but it remains one of the most-cited publications in economic theory today." One can hardly overstate its impact.12

In it, Coase sought to answer the following question: if markets are efficient, why do firms emerge? Coase responded simply and elegantly, stressing that firms make it easier to organize certain exchanges. Coase introduced the concept of transaction costs without naming it - referring to all the expenses the parties must incur to complete a transaction - and explained that firms exist to minimize these costs.13 Indeed, a transaction involves different costs - the costs of finding economic agents on the market, negotiating, drafting a contract and so on. By internalizing these various externalities, firms reduce the cost of economic transactions. Firms were thus seen as an institutional device for the first time.14 Coase opened the firm “black box.”15

He then explained why firms reduce these costs. His explanations came down to the power of command and control.16 Firms are hierarchically organized: orders and directions are given from the top and trickle down the hierarchy. This reduces the scope for costly opportunistic behavior that might otherwise make transaction unprofitable. Put differently, the reduction of these costs is often achieved by collaboration between employees, while market participants outside the firm are compelled to compete.

In Coase’s words, “in place of the complicated market structure with exchange transactions is substituted the entrepreneur-coordinator, who directs production.”17 Reductions of costs follow, as “by forming an organisation and allowing some authority (an ‘entrepreneur’) to direct the resources, certain marketing costs are saved.”18 Coase thus defines the “firm” as “the system of relationships which comes into existence when the direction of resources is dependent on an entrepreneur.”19 On the contrary, this kind of efficiency is not found in the market, where free economic agents compete under emergent orders. One can thus define the boundary between the firm and the market: where control stops, the firm’s perimeter stops.

Coase particularly emphasized the firm’s ability to deal with contingencies during the performance of a contract. While firms manage long-term relationships, the market mainly permits short-term contracts based on the price mechanism.20 Thus, Coase argued, “it seems improbable that a firm would emerge without the existence of uncertainty”21 in the market. This assumption is based on the theory of incomplete contracts, according to which the contracting parties cannot anticipate all the situations that may arise during their contract’s performance.22 The firm helps in creating a way to settle disputes, which as a result reduces all the upfront costs related to the management of potential conflicts. Here again, Coase put the firm’s ability to exercise control at the center of his demonstration. He was awarded the 1991 Nobel Prize in Economics for “his discovery and clarification of the significance of trans- action costs and property rights for the economy’s institutional structure and functioning.”23

2.1.2 Coase’s impact

Coase’s article put transaction costs at the center of modem economics, making them “the ultimate unit of microeconomic analysis.”24 Although Coase complained in 1988 that the concept was “largely absent from current economic theory,”25 it has transformed the perception of the firm from a pro- duction function into a governance structure.26

This transformation of economic thinking heavily influenced Oliver Williamson, among many others.27 He researched the optimal design of firms28 and helped to open the firm “black box” even further, putting the firm’s “control instruments”29 and the “means by which to infuse order”30 at the center of his analysis. Williamson was awarded the Nobel Prize in Economics in 2009.

Alternative theories to those of Coase have also developed. For instance, incentive theory portrays the firm as an incentive system that uses various instruments combining authority, ownership and compensation to ensure that all employees contribute their best to the firm’s interests.31 The theory holds that firms must adopt institutional arrangements that ensure survival by aligning these incentives. They are thus a nexus of written and unwritten contracts between different economic actors in which each contractual relationship is an agency relationship, whose optimal configuration must be discovered. According to the proponents of this theory, there is no difference in nature between firms and the market. Both are said to depend on contractual relationships that do not imply any exercise of authority or control. As I will explain, none of these alternative theories is currently being used in antitrust and competition law.32

2.2 A Pillar of Modern Antitrust

Although Coase’s theory was developed in the 1930s, modem antitrust is still constructed on the basis of this theory and has not adapted to changes in the nature of firms. Why is that? One may find a satisfying explanation in the fact that the nature of economic hierarchies has changed little to this day. Even the apparition of online platforms and aggregators has not changed the structure consisting of minimizing transaction costs thanks to vertical power. In a nutshell, Coase’s theory is here to stay. As a matter of fact, and as we are about to see, all modem antitrust case laws and regulations are based on the above-mentioned article, whether in the United States or Europe. More specifically, Coase’s theory helps point out where control is being exercised and, therefore, where the firm’s boundaries are. Antitrust and competition law applies to all entities defined accordingly.

2.2.1 The firm’s boundaries in antitrust and competition law

The Sherman Act in the United States and the TFEU in Europe are both the subject of extensive case law. The vast majority of the jurisprudence is not concerned with the question of the firm - that is, the person that is the subject of antitrust and competition law. The firm’s structure has transformed very little since the introduction of these two texts; it has become more complex, but has not changed in nature.33 For that reason, litigation generally involves other issues subject to further disagreement. Nevertheless, blockchain’s emergence forces us to reassess the definition of a “firm,” to analyze whether decentralized groups can be captured by antitrust law as currently conceived or if blockchains should be captured through another theory. In the United States, antitrust provisions apply to all “persons”34 affecting trade and commerce by unlawful restraints and monopolies.35 According to Section 7 of the Sherman Act:

the word ‘person,’ or ‘persons,’ wherever used in sections 1 to 7 of this title shall be deemed to include corporations and associations existing under or authorized by the laws of either the United States, the laws of any of the Territories, the laws of any State, or the laws of any foreign country.36

The text does not further define the term “person”; it simply establishes exemption regimes for which antitrust is not applicable - mainly concerning federal government agencies and instrumentalities.37

The case law is more informative. In *Copperweld*,38 the Supreme Court stressed that although “[n]othing in the literal meaning of [the Sherman Act] excludes coordinated conduct among officers or employees of the same company,”39 there is “general agreement that § 1 is not violated by the internally coordinated conduct of a corporation and one of its unincorporated divisions.” On that basis, the Court held that “there can be little doubt that the operations of a corporate enterprise organized into divisions must be judged as the conduct of a single actor,” therefore exempting these operations from Section 1 of the Sherman Act.

The Supreme Court was dealing with possible intra-group collusion for the first time with this decision.40 One can only guess what would have been its reasoning before Coase’s article (1937). The fact remains that *Copperweld* follows a Coasian logic:41 the firm uses vertical control to save transaction costs; antitrust law must recognize the fact and exempt from Section 1 of the Sherman Act all agreements between two legal entities bound by such a control relationship42 In the words of the Supreme Court:

The intra-enterprise conspiracy doctrine looks to the form of an enterprise’s structure and ignores the reality. Antitrust liability should not depend on whether a corporate subunit is organized as an unincorporated division or a wholly-owned subsidiary. A corporation has complete power to maintain a wholly-owned subsidiary in either form. The economic, legal, or other considerations that lead corporate management to choose one structure over the other are not relevant to whether the enterprise’s conduct seriously threatens competition.

In the end, “courts must examine whether the conduct in question deprives the marketplace of the independent sources of economic control that competition assumes” “when making a single-entity determination.”43 Only when “general corporate actions are guided or determined” by “separate corporate consciousnesses” can two entities be seen as two separate firms in antitrust law.44 One must make no mistake about it: only control makes the firm and defines its scope.45

In Europe, the theory of the firm as defined by Coase is also the basis of modern competition law.46 Article 1 of Protocol 22 to the European Economic Area Agreement defines the “firm” as “any entity carrying out activities of a commercial or economic nature,” but the concept is not properly delimited in the black letter of EU law. However, the case law defines “undertakings” as “every entity engaged in an economic activity, regardless of the legal status of the entity and the way in which it is financed.”47 The legal form of the entity offering the economic activity does not matter.48 In fact, as the CJEU made clear in Shell, “undertakings” are economic units rather than legal units.49 Here again, the concept of undertaking takes Coase’s path-breaking article as a starting point.50

That definition of the “firm” is still incomplete, as it does not define its boundaries. For instance, in Imperial Chemical Industries, the CJEU ruled that the degree to which it carried out “the instructions given” by a company was essential in analyzing the independence of a subsidiary; and that “where a subsidiary does not enjoy real autonomy in determining its course of action in the market,” the prohibitions set out in Article 101 of the TFEU were inapplicable.51 The CJEU further held in Akzo Nobel that “the actual exercise of decisive influence”52 defines firm limits in competition law; and that “it is sufficient for the Commission to prove that the subsidiary is wholly owned by the parent company to presume that the parent exercises a decisive influence over the commercial policy of the subsidiary.”53 In the end, a firm encompasses all the elements over which control is exercised, as in the United States.54 For instance, in Hydrotherm, the CJEU found that a natural person, a limited partnership and another undertaking made up a single economic unit when they were all controlled by the same natural person.55 That logic derives from Coase’s “The Nature of the Firm.”56

2.2.2 The firm as a pillar of antitrust and competition law

The definition of the firm’s boundaries helps in three fundamental steps of antitrust and competition law: (1) determining whether the law should apply; (2) assessing practices; and (3) and assigning liability. First, establishing the firm’s boundaries helps determine the extent to which antitrust and competition law applies. U.S. antitrust law provides several exemptions to different types of entities, which require both the identification of the firm and an understanding of its activities. European competition law applies only to undertakings that carry out an economic activity. Once again, it is then necessary to identify the firm’s boundaries to determine the activities carried out.

Second, establishing the firm’s boundaries is essential when agencies assess the legality of business practices.57 In terms of collusion, U.S. and European courts have recognized that two legal entities that are part of the same eco- nomic unit - that is, the same firm - cannot be held guilty of collusion, as one cannot agree with oneself.58 Antitrust prohibits several forms of cooperation outside the firm, while it always permits cooperation within the firm. The logic is similar in terms of monopolization and abuse of a dominant position. As a company cannot abuse its market power against itself, abuses of power are illegal only when they affect other firms. Above all, defining the boundaries of firms is essential to analyze market power (and thus whether Section 2 of the Sherman Act or Article 102 of the TFEU is applicable to a given case) and the ability to engage in anticompetitive practices. Control indeed confers the firm with the power to implement practices - including the ability to raise prices, which is often central in antitrust cases.

Finally, identifying the boundaries of firms is essential to assign liability.59 Liability for anticompetitive practices rests with the parent company that ultimately controls other entities if such control has been exercised.60 This logic stems from the classic distinction between ownership and control.61

It is safe to assume that antitrust law will capture the activities of blockchain participants at their individual level.62 For example, one could imagine that a miner is considered a company on his own; after all, miners are operating an economic activity. Nevertheless, analyzing whether the entire blockchain layer 1 could be deemed a firm for the purpose of antitrust law is essential if agencies are to understand and apprehend anticompetitive practices that are carried out beyond the simple framework of the individual. For example, suppose a blockchain is implementing practices to exclude another blockchain from the market. In that case, one will want to punish these practices rather than each individual action leading to the entire scheme. I will return to these practices in the coming chapters.

In other words, defining the firm’s boundaries is a necessary step in understanding competitive dynamics, in analyzing practices and eventually, in assigning antitrust liability to the blockchain when, as an entity, it seeks to achieve survival through anticompetitive ways. It is thus essential to carefully consider the elements that are taken into account when defining “firms” under antitrust law. I showed that in the United States, as in Europe, only one element matters: control. This reasoning is problematic when it comes to blockchain.

# 2AC

## Blockchain ADV

### AT: Democracy Bad Turn

#### Backsliding causes global nuclear war

Corr ’17 (Anders Corr – PhD in Government and International Relations @ Harvard, Principal at Corr Analytics, Political Risk Analysis, “The New Cold War: Democracy Vs. Autocracy,” 21 May 2017, https://www.forbes.com/sites/anderscorr/2017/05/21/the-new-cold-war-democracy-vs-autocracy/2/#)

Over the past 8 days, North Korea successfully tested two nuclear-capable missiles, making a mockery of President Trump’s tough approach on North Korea. He has meanwhile opened his arms of friendship to Russia and China, the biggest global threats to democracy. His public excuse is the need to work with Russia on terrorism, and with China on North Korea. That help has not materialized, which will be a test of Trump’s mettle. If he fails to take action against North Korea, and leaves his many concessions to China in place, he got played.

The North Korean launches are the latest in decades of events that show an animosity of authoritarian rulers toward democracies. Shortly after the Soviet Union disintegrated in the 1990s, many U.S. analysts saw democracy and liberalism as triumphant over autocracy, and even presaged the “end of history.” Russia and China were proceeding toward market liberalization and democratization. The democratic peace would soon take hold and the world would evolve in a utopic manner, they thought.

But that dream now seems far-flung, with low-grade Russian and Chinese offensives in Eastern Europe and Asia respectively. These offensives are calibrated in such a manner as to make territorial gains, while not provoking a military response. They utilize alliances with Iran and North Korea to encourage rogue state action that distracts global public attention from Chinese and Russian territorial offenses.

Conversely, the United States, Japan, South Korea, Australia, the European Union and others are in a relatively loose alliance based on the common values of democracy, human rights, and freedom of speech. But the alliance is divided by the strong democratic desire for peace, and domestic elites with individual incentives to value trade and investment over the defense of values like democracy. It is subject to free riding, which President Trump has successfully pushed, including at an upcoming meeting in Brussels on May 25.

What could be called an autocratic bloc is provoking, through territorial expansion and destabilizing nuclear development, an interrelated set of conflicts developing in the direction of a New Cold War between autocracies on one side, and democracies on the other. As with the old Cold War, the locus of the conflict is everywhere, including the South China Sea, East China Sea, North Korean and Iranian nuclear and ballistic missile development, the Russian occupation of Crimea in Ukraine, Russia’s attempt to reclaim influence in the former Soviet Union, including through occupation of part of Georgia, China’s attempt to push the U.S. out of Asia and claim it as a sphere of influence, the Arctic, space, undersea exploration, and Russian and Chinese attempts to influence politicians and even voting outcomes in democratic countries.

To institutionalize its growing power and leadership of autocratic countries, and many democratic hangers-on, China attempts to reform global governance not through democratization that might help countries like Japan, India, Brazil and Germany to positions of greater influence in places like the U.N. Security Council, but to uniquely reflect and accommodate China’s own growing economic and military power.

Democracies are being challenged worldwide by this autocratic bloc. If democracies do not have a clear-eyed understanding of the threat, and a grand strategy to defeat or at least deflect the challenge, democracies will be weakened in such a way as to make future challenges even more difficult to overcome. The outcomes of the challenges that democracies face today will determine future outcomes, in a process that is increasingly path dependent.

Nowhere are the challenges and path dependence greater than in defending democratic voting processes from autocratic influence, and in defending front-line democratic territory in places like Eastern Europe, the East China Sea, the South China Sea, the Himalayas, and Taiwan. Decisions on defensive actions or inactions by allied democracies on these fields of economic, diplomatic, and military battle will profoundly affect the future of democracy, peace, and stability for decades, if not centuries, to come. Positive outcomes will require not just grand strategies by major powers, but comprehensive citizen involvement by people of many nations who care about a future that is democratic and at peace.

## FTC ADV

### AT: LIO Bad Turn

#### Leadership is sustainable---multipolarity’s not inevitable

Michael E. O'Hanlon 10/28, Director of Research - Foreign Policy Co-Director - Center for Security, Strategy, and Technology, Africa Security Initiative Senior Fellow - Foreign Policy, Center for Security, Strategy, and Technology The Sydney Stein, Jr. Chair, “China is definitely on the rise. But don’t write off American dominance just yet.,” Brookings, 10-28-2021, https://www.brookings.edu/blog/order-from-chaos/2021/10/28/china-is-definitely-on-the-rise-but-dont-write-off-american-dominance-just-yet/

China is definitely on the rise. But don’t write off American dominance just yet.

Even if the trade wars between the United States and China that dominated the Trump era have receded slightly, many other issues have intensified.

China tested a hypersonic and potentially globe-spanning weapon this summer. It conducted dozens of sorties by combat aircraft that touched on Taiwan’s Air Defense Identification zone and otherwise menaced the island of 23 million (plus much of the world’s semiconductor production capacity) that it claims as its own. The Pentagon’s artificial intelligence guru, Nicolas Chaillan, recently resigned with a warning that the United States is losing the AI race to China. Intelligence and military officials warn that China may be expanding its nuclear arsenal by up to several hundred warheads. And commanders of U.S. Indo-Pacific Command in Hawaii have estimated that China might well attempt to take Taiwan within a half-dozen years or so, given its military modernization trends.

We should not overreact to these troubling trends. They are serious. They are, however, far from truly foreboding.

China is flexing its muscles more than preparing for war; this is not the equivalent of Europe in the late 1930s, given how much China depends on a stable international order for its continued success. We do need to stay vigilant, remember the art of war even in this age of (relative) peace, and expand our economic as well as military toolkit for crisis management. We need not and must not panic, however, because doing so could turn manageable crises into truly scary ones.

CHINA WON’T TAKE THE RISK

First, let’s remember America’s many strengths. Our military budget is about three times’ China’s, and our allies in Europe and East Asia together outspend China themselves (even if not all would fight in a war in the Pacific, admittedly).

The loose coalition of European nations and the U.S. also represents the consumer market of more than a billion comparatively wealthy individuals whom China needs in order to sustain its still-export-driven economy. That means we have many tools of economic, as well as military, warfare if needed.

Since 1945, seven Democratic and seven Republican U.S. presidents have collectively upheld a rules-based international order that has established a very strong norm against interstate aggression, making any Chinese attack on Taiwan hugely problematic for President Xi Jinping and his fellow leaders in Beijing.

The world’s response to an actual attack against Taiwan — and this is the scenario that is truly the most worrisome for its potential to shake world peace — would likely be rather unified and strong. China knows it. For this reason, I believe that U.S. Indo-Pacific Command and other parts of the government need to be careful and restrained with their rhetoric (as most but not all are). China may have growing capacity to attempt to seize Taiwan, but it knows that actually making the attempt would be a cosmic roll of the dice, to be attempted only under the most extreme of circumstances.

AMERICA’S OPTIONS AGAINST CHINA

Beyond these broad advantages are a number of specific factors working in our favor to direct China’s rise in a generally peaceful direction:

Even if our AI efforts, at the Pentagon and elsewhere, could be better focused, we enjoy numerous advantages in high technology vis-à-vis China, including in stealth, submarine technology, and long-range strike platforms like aircraft carriers. Even if China’s military is bigger than ours in some ways — total troop count, total ship count — ours is much better (and battle-hardened). Also, just to take one frequently misused statistic, if China’s navy has more ships than ours, we have a fleet with larger vessels, meaning the U.S. Navy wields twice the total ship tonnage, based on calculations my colleagues and I have done.

Every time China fortifies another artificial island, should it continue down that path, we can respond. We can add bases in the Indo-Pacific region ourselves, or tighten various security partnerships, as with India. We should do this with restraint, and proportionality, to be sure — but the bottom line is that the United States has lots of allies and China does not. We also have a globally capable military that can, for example, continue to uphold our access to the South China Sea even when Beijing wrongly and dangerously claims it as territorial waters.

If China does attack Taiwan, with the goal of reunification, I believe it is far more likely to attempt a blockade (combined with cyberattacks) than an outright invasion. Moving big ships near the coasts of a vigilant adversary is very hard to do in the era of precision-strike weaponry and advanced mines. In a blockade scenario, we have other options besides fighting right next to Taiwan — we can, for example, use economic warfare backed up by our military to interfere with China’s access to oil and other commodities coming from the Persian Gulf and Africa.

MANAGING CHINA’S RISE

To be sure, the United States needs to stay vigilant — and to keep getting “stronger” ourselves, as Brookings Institution scholar Ryan Hass argues in a new book of that very title. Our military command and control must be more resilient in order to makes sure our “kill chain” is robust. Our armed forces need more long-range strike platforms, including more bombers and long-range unmanned systems operating off aircraft carriers and attack submarines, given China’s ability to threaten nearby U.S. bases.

Nations need to diversify and harden their economies, and the global supply chains that undergird them, so that China does not have the upper hand in any future economic warfare scenarios.

Managing China’s rise is going to be a challenge for America and her allies for a generation. But if we stay calm in crises, and make ourselves stronger and more resilient militarily and economically, we should have the tools needed to sustain the peace.

## OFF

### New Plan---2AC

### NFT---2AC

### T Per Se---2AC

#### ‘Prohibition’ is injunction. That can happen after review.

Sarah E. Light 19, Assistant Professor of Legal Studies and Business Ethics at the The Wharton School at the University of Pennsylvania, “The Law of the Corporation as Environmental Law”, Stanford Law Review, 71 Stan. L. Rev. 137, Lexis

Section 1 of the Sherman Act prohibits "every contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce." 159 There are certain kinds of actions that are per se illegal under the antitrust laws, rendering antitrust law an absolute bar. 160 Such actions include price fixing, horizontal boycotts, and output limitations. 161 Courts apply the per se rule when firms aim to "disadvantage competitors by "either directly denying or persuading or coercing suppliers or customers to deny relationships the competitors need in the competitive struggle.'" 162 In the per se unreasonableness context, the plaintiff need not show anticompetitive effect, as harm to competition is presumed. 163

Before the enactment of the Clean Air Act, the federal government invoked antitrust law to end a collusive agreement among major automakers and their industry association to keep pollution control technology from reaching the California market. By 1952, authorities addressing air pollution in Los Angeles County had accepted scientific findings that motor vehicle emissions were the major source of the smog that blanketed the Los Angeles basin. 164 Local officials began to reach out to the major automobile [\*173] manufacturers about research on emissions-control technology. 165 In 1953, the Automobile Manufacturers' Association (AMA), an industry trade group, began a campaign to study the issue and committed to funding research. 166 In 1955, several automobile manufacturers, including the four major manufacturers - General Motors, Ford, Chrysler, and American Motors - entered into a formal cross-licensing agreement to share technological information and data on the development of emission-control technology, 167 an action that later became the subject of antitrust litigation. 168 They announced their decision publicly, garnering some praise for addressing the smog problem. 169

In 1960, California passed the California Motor Vehicle Pollution Control Act. 170 The Act mandated that manufacturers of new cars install emissions-control devices; however, the mandate was only triggered once such devices had been certified by the newly created Motor Vehicle Pollution Control Board. 171 By 1964, the Board had certified four emissions-control devices as meeting the state's standards, triggering the mandate under the Act. 172 Independent firms, rather than the major automakers, had developed these devices. 173 Shortly after the state certified these devices, the major automakers announced that they, too, had developed their own emissions-control technology, 174 arguably so that they would not be required to license technology from other firms. This sequence of events led some officials in California to conclude that the major automakers had conspired to delay making their own technologies publicly available. 175 After Los Angeles County officials asked the U.S. Attorney General to investigate possible collusion, a grand jury was convened. 176

Although the Department of Justice did not file criminal charges, in January 1969 it filed a civil antitrust suit against the AMA and the four major [\*174] automakers, alleging that the defendants had conspired among themselves and with smaller motor vehicle manufacturers "to eliminate competition in the research, development, manufacture and installation of motor vehicle air pollution control equipment, and in the purchase from others of patents and patent rights, covering such equipment," in violation of section 1 of the Sherman Act. 177 In response to the complaint, the defendants argued that their cooperation had actually accelerated the development of emissions-control devices and noted that collaboration was required to ensure that all manufacturers would be able to comply with the increasingly stringent standards. 178 After the lawsuit was filed, a partner in the law firm representing the AMA penned an article 179 explaining that individual consumers had been "unwilling to spend the additional small amount" necessary to purchase vehicles equipped with emissions-reducing devices. 180 Thus:

So far as the installation of devices was concerned, therefore, the manufacturers had a substantial and legitimate interest in cooperating. No company wanted to incur a cost disadvantage, either in terms of an increase in sales price or an adverse effect on vehicle driveability, without some assurance that all manufacturers were incurring similar disadvantages in the marketplace. 181

Arguably, this was as much a problem of the interaction between corporate law and antitrust law in competitive markets as it was one of antitrust law alone. If firms had a broader mandate beyond profit maximization, including to contribute to the public interest, perhaps they would have been more willing to incur a short-term cost disadvantage, even in a competitive market, rather than enter into an agreement to limit competition.

The parties resolved the suit by entering into a consent decree, which required the defendants not to conspire to delay the development of emissions-control devices and to make available without royalties both patent licenses and data on the emissions-control devices they had developed. 182 However, the decree did not require the defendants to admit liability or pay monetary penalties or damages for environmental harm; nor did it require the [\*175] retrofitting of vehicles. 183 Despite the lack of damages or penalties, in this case antitrust law served as a mandate to promote environmental goals, preventing collusion in the market when firms feared that developing an environmental product would put them at a competitive disadvantage.

A second, more recent example of antitrust law serving as an environmental mandate comes from the European Union, not the United States, but the example offers a similar lesson about the potential confluence, rather than conflict, between antitrust principles and environmental goals. In 2011, the European Commission fined two consumer products firms, Unilever and Procter & Gamble, more than 300 million euros combined for entering into an agreement to maintain prices for laundry detergent while the firms switched to selling a more concentrated, environmentally preferable formulation. 184 The firms switched to the more environmentally friendly formulation as a result of their participation in a voluntary industry initiative called the "Code of Good Environmental Practice for Household Laundry Detergents," 185 a classic example of private environmental governance. The voluntary initiative included reducing the amount of detergent needed for each load of laundry, as well as overall product weight and packaging. 186 The industry initiative appropriately did not include any commitments regarding price fixing. 187

However, the firms privately "agreed to keep the price unchanged" when the "products were "compacted'" in a way that might appear to a consumer that he would be able to wash fewer loads of laundry than the compacted product was capable of cleaning. 188 In addition, they engaged in other forms of price collusion, including "restricting their promotional activity" and "deciding not to pass the benefit of cost savings (reduced raw materials, packaging and transport costs) on to consumers." 189 The firms further agreed on direct price [\*176] increases and "exchanged sensitive information on prices and trading conditions, thereby facilitating the various forms of price collusion." 190

In this case, just as in the case of the automakers, antitrust law enforcement served as an environmentally positive mandate. Relying on antitrust law, the European Commission fined these firms for seeking to avoid passing cost savings from an environmentally beneficial product onto consumers. The motivations of the consumer products firms mirrored those of the automakers: In both cases, the firms feared that being the first to market an environmentally preferable product would reduce profits or create a competitive disadvantage vis-a-vis other firms in the marketplace. This example likewise suggests the importance of viewing antitrust law in connection with other fields, such as corporate law. Firms driven by a profit motive experience that motive in the context of a competitive environment. 191

B. Prohibitions and Disincentives: The Antitrust Per Se Rule and the Rule of Reason

While antitrust law can serve as an environmental mandate by prohibiting collusive behavior that keeps environmentally preferable goods from the market, there is also conflict between antitrust law's goals of promoting competition and environmental law's goals of promoting [\*177] conservation. 192 Because antitrust law's per se rule and rule of reason operate on a somewhat fluid continuum, 193 this Subpart discusses the two doctrines together. The per se rule operates as a prohibition, whereas the rule of reason operates as both a prohibition and a disincentive.

As noted above, antitrust law generally prohibits certain types of market activity - price fixing, horizontal boycotts, and output limitations - as illegal per se, and harm to competition is presumed. 194 For example, if an industry association declines to award a seal of approval necessary for a product's sale without any good faith attempt to test the product's performance, but rather simply because that product is manufactured by a competitor, such an action would be illegal per se. 195 Under this Article's framework, a per se violation is thus a prohibition.

The more fact-intensive inquiry under the rule of reason tests "whether the restraint imposed is such as merely regulates and perhaps thereby promotes competition or whether it is such as may suppress or even destroy competition." 196 While this extremely broad statement might suggest that any fact is relevant to the inquiry, the salient facts under the rule of reason are "those that tend to establish whether a restraint increases or decreases output, or decreases or increases prices." 197 If an anticompetitive effect is found, then the action is illegal and the rule of reason operates, like the per se rule, as a prohibition. 198 The rule of reason can also operate as a disincentive, even if no [\*178] court finds an anticompetitive effect, as uncertainty and litigation risk may discourage firms from undertaking legally permissible, environmentally positive industry collaborations. 199

#### ‘Practices’ can be singular.

Justice Clinton 82, Supreme Court of Nebraska, Justice. Opinion in MID-SOUTH, ETC. v. Platte Valley Livestock, 315 NW 2d 229 - Neb: Supreme Court 1982

Most words, including the word "practice," encompass more than one meaning, and the particular meaning intended must be determined from the context in which it is employed. Only two of the multiple meanings of the word practice, as found in the dictionary, can possibly apply in the context of the statute. In Webster's Third New International Dictionary, Unabridged (1968), one meaning is "to make use of: use, employ." Another meaning is "to do something habitually," or "repeated or customary action." 233\*233 The words of the statute, "and every unjust, unreasonable, or discriminatory regulation or practice is prohibited and declared to be unlawful," § 208(a), do not suggest that the word practice includes only that which is done habitually or repetitively by the particular stockyard or marketing agency. (Emphasis supplied.) Rather, as we will later attempt to demonstrate from an analysis of the cases upon which the parties rely, repetition may be important only in determining whether a particular act is an unjust or unreasonable practice included within the evils which the act was intended to cure.

#### Coherence---it’s impossible to apply to ‘anticompetitive’ conduct

Donald L. Beschle 87, Associate Professor of Law at The John Marshall School of Law, B.A. from Fordham University, J.D. from the New York University School of Law, LL.M. from Temple University School of Law, “"What, Never? Well, Hardly Ever": Strict Antitrust Scrutiny as an Alternative to Per Se Antitrust Illegality”, Hastings Law Journal, March 1987, 38 Hastings L.J. 471, Lexis

This Article argues that the defenders of per se analysis have assigned themselves an impossible task. Arguing that types of activity can [\*476] be identified as invariably anticompetitive is futile; counterexamples can almost always be put forward. Consequently, defenders of per se categorization are reduced to one of two unattractive alternatives. First, they can concede that per se categories may in some instances prohibit procompetitive activity, but argue that the overall benefits of per se categorization justify the result. Such an argument is unsatisfying because it explicitly sacrifices particular blameless defendants in order to search for an increase in general welfare. Second, per se defenders can narrow their categories to eliminate procompetitive counterexamples. This strategy, however, threatens to destroy those categories entirely. And if most of the once-condemned activity is returned to the realm of the rule of reason, the insight that certain types of behavior are particularly dangerous is lost.

### Capitalism K---2AC

#### Profit-centric innovation solves their impacts---BUT, limits are wrong.

---T = dirty technology.

---A = affluence.

Stijn Bruers 21, PhD, Researcher, Physics & Philosophy, KU Leuven, "The Case Against Degrowth," Stijn Bruers – Word Press, 12/29/2021, https://stijnbruers.wordpress.com/2021/12/29/the-case-against-degrowth/.

Economic degrowth is not necessary, because it targets the wrong enemy. GDP is not the enemy; environmental impact is the enemy. Environmental scientists are able to determine upper bounds on environmental impacts such as pollution. For example, climatologists have determined the carbon budget: how much greenhouse gases can still be emitted that keep the atmospheric temperature increase below 1,5°C. But GDP is measured in dollars, a totally different quantity than kg CO2. Hence, none of the economic degrowthers are able to say what is the upper bound or true limit on affluence. There are no scientific studies that estimate the maximum level of GDP that is still permissible.

In the very end, it all comes down to computation (information processing). Everything we value, such as the feelings of well-being created by our computing brains or the biological diversity created by ecosystem processes, is based on computation. The true limits to growth, are the limits of computation, and these are extremely far away. GDP can still grow by an extremely huge amount before hitting these limits.

Economic degrowth is not an effective strategy to reduce environmental impact. First, from a global social justice perspective, economic degrowth should apply only to the high-income countries. Poorer countries should be allowed to grow in order to reduce poverty. However, most (more than 50%) of the global environmental impact (for example global greenhouse gas emissions) occurs in non-high-income countries with high levels of poverty, where degrowth is not appropriate. Suppose degrowth results in a reduction of 50% of the average GDP per capita in the high-income countries. This will reduce the total impact with less than 25%. Such a small reduction in greenhouse gas emissions is not sufficient to meet climate targets and keep the temperature increase below 1,5°C. Hence, reducing affluence has only a small potential. In general, reducing the total impact all the way to zero by only reducing affluence requires a 100% reduction of affluence, which is not feasible.

Economic degrowth is not so politically feasible, as it requires a lot of international cooperation between high-income countries. Reducing GDP is an objective of economic degrowth, but that does not immediately translate into a concrete policy. To study the effectiveness and feasibility of economic degrowth, we have to look at specific policy proposals made by degrowthers.

The most obvious degrowth policy proposal that targets economic growth and affluence, is the implementation of an income ceiling or maximum income level (e.g. a 100% income tax rate above a certain threshold). Degrowthers argue that the relationship between what is measured (income or GDP per capita) and what matters (e.g. well-being, life satisfaction, flourishing), is non-linear and concave. That means increasing the income or wealth of a poor person strongly increases that person’s well-being, but increasing the income of a rich person does not much increase that person’s well-being. If a population becomes very rich, increasing GDP is no longer an effective means to increase the well-being of those people. Hence, setting a maximum income level where the relationship between income and well-being breaks down, should be feasible. But degrowthers neglect the also non-linear and concave relationship between environmental impact (e.g. ecological footprint per capita, greenhouse gas emissions per capita) and GDP per capita. Richer people have a higher propensity to save, which means a smaller fraction of their income goes to consumption. Richer people also make use of more clean technologies that are more expensive. Hence, someone with twice as much income, has less than twice as much environmental impact. This non-linear relationship between GDP and environmental impact means that choosing a high maximum income level does not reduce the total environmental impact that much.

In general, choosing the maximum income level is difficult. If the maximum income level is high, it still allows for a lot of growth, as many people can increase their incomes. If on the other hand the maximum income level is low, it becomes politically unfeasible, as many people will consider that income level as poverty.

A more problematic aspect of a maximum income, is that it can decrease innovation and technological progress, because it reduces the incentive to earn more money by taking risks and invest in innovation. The same goes for another degrowth proposal: a maximum size on (for-profit) companies. This regulation would imply that companies cannot grow and take advantage of their increasing returns to scale. This reduces efficiency. Many small companies are often not able to produce the same things as efficiently as a fewer number of larger companies.

Another degrowth policy proposal that intends to target affluence, is a reduction of working hours. Income and affluence can be reduced by reducing hourly wages, but this faces political resistance, or reducing working hours. However, in free market capitalist societies, we already see a reduction in working hours per worker. Due to increasing productivity and income levels, which corresponds with economic growth, people increasingly value leisure time and prefer to work fewer hours. As a consequence, further government interventions to regulate working hours, for example by setting a maximum that people are allowed to work, would be less effective. And such regulations are too economically disruptive. For example, some highly productive people are willing to work more hours and employers are willing to pay them for those extra hours, but they would be prevented from doing so. This is an infringement on liberty.

Finally, economic degrowth can be harmful. A policy to reduce economic growth risks having negative economic side-effects, for both richer and poorer countries. The rich countries that degrow could face for example increased unemployment and increased government debt (due to lower tax revenues). There are at present no economies that show a decrease in their GDP while at the same time not increasing unemployment or government debt. There is no clear consensus among economists how to safely degrow as a country. Degrowth can be considered as a risky experiment to figure out how to avoid unwanted economic problems while reducing GDP. Also poorer countries can be harmed if richer countries degrow, because of reduced international trade and decreasing export levels towards degrowing richer countries.

Reducing resource consumption: the resource degrowth objective

A third strategy to reduce environmental impact, is to reduce the resource consumption intensity C. This can be very cost-effective, as it saves energy and resource costs, but it has limited feasibility. Just like the previous two factors, reducing the impact all the way to zero by reducing consumption intensity to zero, is not feasible. This unfeasibility is not because of political reasons, but because of physical limits (in particular the second law of thermodynamics).

Due to its cost-effectiveness, we already see a decrease in the global average energy intensity (kWh energy used per dollar GDP) with 1% per year over the past two decades.

Instead of focusing on the factors A and C separately, the degrowth movement focuses on the product AxC. What is needed according to resource degrowth, is neither merely a reduction in economic activity as measured in GDP, nor merely a reduction in consumption intensity, but a reduction in resource throughput, as measured in GDP times consumption intensity.

As with economic degrowth, resource degrowth is not necessary, not effective, not politically feasible and potentially harmful.

The major criticism against resource degrowth policies, is its lack of necessity. First, the real limits to growth are still far away. Consider energy scarcity. The amount of solar energy that hits the earth is almost 10.000 times more than the energy used by all humans. Add the solar energy that can be captured in space (e.g. on the moon), all geothermal energy that can be captured, and nuclear energy from both fission and fusion, and it becomes clear that there is an abundance of energy. Limits on materials (e.g. metals and minerals) are less stringent, because given enough energy, materials can be recycled or mined at hard-to-reach places (e.g. the ocean floor, the moon, asteroids,…). The physical limits of resource use are not yet reached, so why would we need a self-declared, political limit on resource use that is much lower than the physical limit that sets the true boundary?

Second, even if we hit the limits, planned policies are not required. Private property rights on resources (energy, land, minerals) are feasible. These rights are already in place or easily implementable. With such property rights, there is no market failure, which means that free markets solve the scarcity problem through the price mechanism. In other words; markets will automatically indicate whether resource growth and GDP growth are no longer possible. In particular, if the prices of resources increase so fast that resource use or GDP no longer grow, then the market indicates that the limit to growth is reached. As the market will not let the economy grow any further, extra government interventions to stop the growth are superfluous.

But at this moment, there are no indications that we are near the limit. For example, energy expenditure accounts for less than 10% of GDP in high-income countries. That means that the energy prices need to increase really a lot before they impact economic growth. But the prices of resources do not increase so fast that growth becomes impossible. In fact, the prices of most resources (adjusted for inflation) are not even increasing. There is more evidence for a general decreasing trend of resource prices the past decades. This is the opposite of what one would expect if we reached the limits to growth.

Next to their lack of necessity, the resource degrowth policy proposals are not so effective. The two most relevant proposals are an advertisement ban and a resource taxation.

Suppression of advertisements from the public space might be effective, as it could decrease overconsumption. However, this effectiveness is very limited. First, there is some economic evidence that advertisement does not increase consumption that much. Second, an advertisement ban could decrease the prices of products, which results in higher consumption levels. Commercial advertisement is economically inefficient, because it is a zero-sum game: if one company advertises, the competing companies have to spend advertisement budgets to promote their products. In the end, the competing companies are pulling on a rope in opposite directions. The rope is not moving that much and the rope pullers waste energy. Similarly, the competing companies waste costs on advertisement. An advertisement ban would save the companies these costs, which means they can lower their prices.

Degrowthers argue that technological innovations that increase resource efficiency and decrease resource use are not so effective, due to possible rebound effects. For example, households save energy costs when they use more energy efficient appliances. That means they have more money left for extra consumption of other things. Their use of energy efficient appliances also decreases energy demand, which means the price of energy decreases, which means other people will buy (and waste) more energy. These concerns for rebound effects are legitimate. But degrowthers underestimate or neglect similar rebound effects of their policy proposals, such as an advertisement ban.

A second resource degrowth policy proposal is a resource taxation. We have to make a distinction between a resource tax and a pollution tax. When there are negative externalities, such as pollution, a taxation is very effective (although its effectiveness is mitigated due to a lower political feasibility, as it requires international cooperation). A pollution tax internalizes the external costs of pollution into the price of the product. However, when there are property rights on resources, there are no such negative externalities. Furthermore, the supply of resources is inelastic (independent of the price). Consider a tax on land use. As the land is already there (i.e. it is not being produced), a land tax does not decrease land use (unless the tax would be really high, which is politically unfeasible). In general, a resource taxation does not decrease resource use and hence is not effective to reduce the environmental impact.

But a resource tax remains important, though, because it increases fairness through redistribution. A resource tax allows to redistribute the unearned income (resource rent) from owning resources. A resource tax-and-dividend system, where resource tax revenues are distributed to all citizens as a universal dividend, is both fair and efficient. A resource tax is efficient, because resources are created by nature and not by the resource owners. The resource owners will not be disincentivized by the tax: they will not produce less resources when resources are taxed, because the resources are not produced by the owners. And a resource dividend makes the system fair: as no-one produced the resources, the value of the resources belongs equally to everyone. A dividend is a method to equally distribute the value (resource rent) of the resources among citizens.

Improving technology; the ecomodernist objective

In contrast with the degrowth movement, the ecomodernist and effective environmentalist movements primarily focus on the fourth factor in the ImPACT-equation. This T-factor represents technology. A high T-factor means a lot of dirty technology is being used in the economy. Ecomodernists and effective environmentalists campaign for increased government funding in clean technology research and development.

There are several reasons why ecomodernists and effective environmentalists focus on reducing the T-factor by increasing government spending on clean tech innovation.

A first reason is that of all factors in the ImPACT-equation, T is the only factor that can feasibly (according to the laws of physics, without much political resistance) be reduced all the way to (almost) zero, such that the environmental impact becomes (almost) zero. For example, there are clean energy technologies, such as nuclear energy and renewable energy, that have (almost) zero greenhouse gas emissions per energy unit.

Due to technological innovation (research and development of clean technology that has a low environmental impact), we already see a decoupling of climate impact and economic growth in most high-income countries. The consumption-based per capita CO2-emissions in almost all high-income countries (e.g. EU, US,…) dropped by about 25% the past 15 years (since 2005), whereas their levels of GDP per capita kept increasing. Degrowthers are skeptical about such decoupling, and argue that such decoupling is not fast enough to meet climate targets and avoid 1,5°C global warming. But at least we have evidence that decoupling due to technological innovation is possible. In contrast, degrowthers believe in the feasibility of another kind of decoupling, between economic wealth and human well-being or life satisfaction. But there are no countries that show an increase in well-being (e.g. an increase in living standards or flourishing) and a decrease in GDP or resource use. There is strong evidence that GDP is positively correlated with measures of well-being. Degrowthers should be more skeptical about the decoupling of well-being and GDP, than about the decoupling of GDP and environmental impact.

A second reason for the effectiveness of reducing the T-factor, is the interdependence between the factors A and T. In particular, with appropriate policy, the T-factor can be made a decreasing function of A. And this function could even be steeper than 1/A. That means an increase in A could reduce the total environmental impact, because the factor T decreases stronger than the increase in A. Suppose the affluence A increases with 10% (which can be reasonably expected after 5 years of growth at the average growth rate of the past two centuries). If only 1% of that increase in GDP is used for funding of clean technology innovation, which should be politically feasible, the global budget for clean technology R&D more than doubles (currently less than 0,1% of global GDP goes to clean tech R&D). A doubling of R&D could roughly correspond with having the clean technologies on the market twice as fast. If a clean technology has zero CO2 emissions per kWh energy or dollar GDP, it doesn’t matter if the economy grows with 10%, because zero times 10% is zero. Reducing GDP, on the other hand, is dangerous, because there will be less money available for funding of clean tech R&D and for paying for the new clean tech infrastructure.

Third, technological innovations have positive returns to scale. Technology has large spillovers: once invented, the whole world population can adopt the clean technology without extra R&D costs. The innovation is a public good. The provision of public goods is a market failure, because markets are not sufficient providers of public goods. Therefore, it is important that governments invest in this public good by increased funding of clean tech R&D.

Fourth: technological innovation is politically feasible. It does not require international cooperation. It does not face much societal resistance.

Degrowthers argue that clean tech innovation introduces rebound effects that make this policy less effective. For example more clean tech could decrease the price of dirty technology and hence increase the use of dirty technology. However, a rebound effect is mitigated if a pollution tax (or a tax on dirty technologies) is introduced, and if the R&D focuses on clean technologies that are sufficiently substitutable (instead of complementary) with dirty technologies. If clean tech is a good substitute, it can automatically outcompete dirty technologies from the market. Compare it with the transition from horse carriages to motorized cars. The cars outcompeted the horse carriages from the market, even without a horse carriage tax or other government policies to regulate horse carriage use. Horse carriages were considered a big environmental problem in 19th century cities, because of the horse manure and horse cadavers on the streets. And these carriages created other negative externalities, such as the noise of the horse hooves and accidents by unexpected movements of horses. But economic or resource degrowth policies were not necessary to solve these problems. Technological innovation, in particular the invention of the car, solved it.

#### 1. It solves climate mitigation.

Eduard Soler et al. 21, Senior Research Fellow, CIDOB. PhD, International Relations, Universitat Autònoma de Barcelona; Hannah Abdullah, Senior Research Fellow, Global Cities Programme, CIDOB; Inés Arco, Visiting Fellow, CIDOB; Anna Ayuso Pozo, Associate Professor, Public International Law, Universitat Autònoma de Barcelona, "The World In 2022: Ten Issues That Will Shape the International Agenda," Barcelona Centre for International Affairs, December 2021, https://www.cidob.org/en/publications/publication\_series/notes\_internacionals/265/the\_world\_in\_2022\_ten\_issues\_that\_will\_shape\_the\_international\_agenda.

Are we better prepared for a new way of doing things? Time will tell if the reassessment of the priorities of public administrations and societies that occurred in the pandemic has lasting effect. The measures imposed to tackle the health emergency accelerated processes of economic and social transformation. Readjustments may occur when it comes to teleworking, but the change of habits that has taken place in mobility, consumption and information processing and the intensive process of learning digital tools will be difficult to reverse. Another of the legacies of the health crisis has been the focus on science. Ostensibly contradictory phenomena have emerged. Science’s social prestige has grown (the latest global State of Science Index (SOSI) suggests that 79% of people believe that science will improve life in the next five years), but so have the dynamics of politicisation and contestation mentioned above.

If this trend continues it may have a densifying effect, with more collaboration projects between research teams, alliances forming between public administrations, scientists and the private sector, and a closer relationship between the public and science. Meanwhile, science budgets will be notably larger: the Next Generation EU funds allocate 37% and 20% to financing the green and digital transitions, respectively, while the US stimulus plans will spend $250 billion on innovation.

On the other hand, this will exacerbate the concentration of scientific production in just a few countries. Global investment in artificial intelligence (AI) and quantum computing is led by the United States, China and a small group of developed countries, as well as India in certain fields. When it comes to new patents China is the undisputed leader and a wider shift towards Asia is underway. This scientific asymmetry adds a new dimension of inequality to a world advancing at multiple speeds, even in innovation.

Alongside health, the environment is the second major field where efforts are being concentrated. In 2022, pressure will rise on scientific communities, businesses and public administrations to find innovative solutions to the climate crisis. This includes research into advanced technologies to reduce emissions associated with energy use, such as carbon capture and storage, small modular nuclear reactors and options for decarbonising energy-intensive industries. Another challenge is the search for technical solutions to anticipate and prevent the worst impacts of natural disasters and increase resilience.

#### 2. It caps numerous existential risks.

Philip Trammell 21, PhD, Economics, Oxford University. Researcher, Global Priorities Institute, Oxford University, "Existential Risk and Exogenous Growth," ResearchGate, 01/17/2021, pg. 12-13.

Aschenbrenner (2020) explores the possible relationship between economic growth and existential risk, using an endogenous growth model in which sustained output growth requires sustained population growth, and an existental risk model in which the production of consumption goods increases existential risk and the production of “safety goods” lowers it. He finds that, as society grows richer, it should allocate ever more of its resources from consumption to existential risk mitigation efforts. Furthermore, he finds that this policy can render (at least anthropogenic) existential catastrophe permanently avoidable under circumstances in which it would be inevitable under a “rule of thumb” policy in which a fixed proportion of output is spent on risk reduction. Finally, he finds that if there is a sufficiently large “scale effect” of existential risk, existential catastrophe is unavoidable: lowering the hazard rate steeply enough to render the probability of long-run survival positive would require a consumption sacrifice so large that life would no longer be worth living, and which would therefore in itself constitute a kind of existential catastrophe.

Here, we have seen that the last of these findings, but not the rest, disappears when we use the same risk model but move to a simple exogenous growth model. The intuition for this divergence is straightforward. Fixing consmption at some positive-utility level, exponential exogenous productivity growth allows for an exponential increase in risk-mitigation efforts, which delivers a positive probability of survival. Exponential population growth with fixed consumption per capita, on the other hand, creates exponential increases in output only at the expense of corresponding exponential increases in the risky production of consumption goods.

Since we are unlikely to sustain population growth in coming centuries, but may nonetheless sustain productivity growth, the above is good news for those concerned with humanity’s long-term survival. It also illustrates the potential importance of growth theory from a longtermist perspective, even if we believe with Bostrom (2003) that existential risk is the primary determinant of the expected value of the future. Our beliefs about the feasibility of containing existential risk may be sensitive to our beliefs about the mechanisms driving economic growth.

### State Courts CP---2AC

#### State control of blockchain will be preempted

Patricia Fry 18, Former Chair of the Uniform Electronic Transactions Act Drafting Committee, Former Professor of Law at the University of Missouri-Columbia School of Law, JD from the Southwestern University School of Law, MA from California State University, Northridge, et al., “Joint Statement in Response to State "Smart Contracts" Legislation”, 4/4/2018, https://esignrecords.org/wp-content/uploads/2018/04/Joint-Ltr-State-Smart-Contracts-Legislation.pdf

Cryptographic signatures fall squarely within the definition of "electronic signature" set forth in UETA and ESIGN. Thus, if blockchain technology or smart contract code is used to create or effect an electronic signature, electronic record, or electronic contract, UETA and ESIGN ensure it is valid. Therefore, legislation seeking to define blockchain technology or smart contracts or to ensure smart contracts are legally enforceable, while well-intentioned, is harmful for the following reasons:

1. Redundancy. Redundancy is confusing, unnecessary, and potentially harmful if courts determine the legislature intended a different effect.

2. Inconsistency. Bills introduced in California, New York, Illinois, Nebraska, and Tennessee this year contain definitions of blockchain and smart contract inconsistent with each other (in some cases) and the definition published by the Chamber of Digital Commerce. The potential for a network of conflicting state laws is obvious.

3. Federal Preemption. ESIGN provides that any state law giving special effect to a specific technology is preempted. Moreover, conflicting state laws provide additional incentive for Congress to preempt those laws to remove barriers to interstate commerce.

#### The CP is meaningless. It leaves Supreme Court precedent unchanged, overriding anything done by states.

Richard A. Matasar 86, Professor of Law, University of Iowa College of Law. B.A. 1974, J.D. 1977, University of Pennsylvania, and Gregory S. Bruch, Associate, Shea & Gardner, Washington, D.C. A.B. 1982, Stanford University; J.D. 1985, University of Iowa College of Law, “Procedural Common Law, Federal Jurisdictional Policy, and Abandonment of the Adequate and Independent State Grounds Doctrine”, Columbia Law Review, 86 Colum. L. Rev. 1291, November 1986, Lexis

The second finality justification for the advisory opinion ban -- the requirement of an actual controversy -- also does not require the adequate and independent state grounds doctrine. The argument that the advisory opinion ban requires the adequacy doctrine rests on the assumption that the Supreme Court's opinion on a federal question will not affect the ultimate disposition of the case because on remand the state court will reinstate the original result as a matter of state law. 56 Thus, it is argued that the Supreme Court's decision on the federal question is advisory. The argument is unsound for several reasons.

First, it is based upon a false premise. The adequacy doctrine is premised upon a lack of federal review of state law grounds; in order to prevent an advisory opinion on the federal law ground, the adequacy doctrine precludes review of the federal ground. However, the premise that the Court cannot review state law grounds is false. As shown above, article III grants the Court power to reach some state law questions contained in the same "case" as federal questions. 57 Only the Court's refusal to exercise its power to review state law grounds, which is not constitutionally compelled, is the basis for this premise. Therefore, the claim that reviewing the federal ground would be an advisory opinion is a result merely of the Court's own self-restraint.

Second, the non-finality argument proves too much. If it violates the advisory opinion ban for the Supreme Court's opinions on federal law to have no effect on the ultimate judgment rendered by a state court, one would expect the Court always to avoid such a possibility by finally deciding and rendering judgments in appeals from state courts rather than vacating and remanding cases. Vacating and remanding allows state courts to make the Supreme Court's dispositions of federal issues irrelevant to the outcome of a case because it permits state courts to assert dispositive, unreviewable state grounds after the Supreme Court has acted. Yet, the Court frequently does permit state courts to avoid the disposition of cases apparently compelled by its resolution of federal issues either on the basis of new state law issues, 58 or unclearly resolved state issues, 59 or even state issues that previously had been determined differently. 60 Similarly, the Court sometimes takes interlocutory review of cases before final judgment, rendering decisions that might be unnecessary in light of future developments in the action. 61

Third, it may well be that no degree of certainty by the Supreme Court is sufficient to demonstrate the independence of state grounds when a state court purposely chooses to decide a case on state and federal grounds. 62 As the independent state grounds cases 63 demonstrate, the Supreme Court's decision whether to review a state court's judgment always involves a prediction of how the state court will react to the Court's disposition of the case. 64 Sometimes the Court will correctly predict that its review of the federal grounds of a state court's judgment will alter that court's decision on state grounds after remand; 65 however, the Court may also predict incorrectly. 66 Surely a presumption of jurisdiction by the Supreme Court based on its belief that a state ground is not independent does not make its opinion in the case advisory if on remand the state court asserts the independence of the state ground and reverses. 67 The conclusion is equally true outside the independent state grounds cases. That the Court sometimes expresses certainty about a state court's action after remand does not preordain the state court's behavior. Even clear predictions may go awry. 68 That they do suggests that state grounds ought not be treated as adequate, and hence eliminates the argument that the advisory opinion ban requires the adequate and independent state grounds doctrine.

Fourth, the Supreme Court's decision is in fact always final with regard to federal questions. Under the supremacy clause, the Court's disposition of any federal question -- even in a case containing an adequate and independent state ground -- cannot be questioned by the state court either in the very case being remanded or in any subsequent litigation.

#### Minimally, the result is mass confusion and inconsistency that destroys the credibility of law

M. Jason Hale 7, JD Candidate at Case Western Reserve Law School, MBA from Belmont University, BA from Middle Tennessee State University, now Vice President of Risk & General Counsel at Lee Company, “Federal Questions, State Courts, and the Lockstep Doctrine”, Case Western Reserve Law Review, 57 Case W. Res. 927, Summer 2007, Lexis

Introduction

State courts have adopted the doctrine that if presented with a federal question, they are not bound by the decisions of any federal court interpreting that law except the United States Supreme Court. The theory is that federal courts were originally created to be coordinate with state courts; with the exception of the highest court in the land, federal courts were not seen as superior to their state counterparts. As such, state courts are presumed to be free of precedent of the federal courts that decided federal law in the jurisdiction in which the state court sat, even if the circuit court had ruled on the matter. State courts adopted several approaches in their interpretation of the law, some more deferential to federal decisions than others, but the overwhelming majority of courts viewed the federal decisions as merely persuasive.

In 2004, the Pennsylvania Supreme Court addressed the issue of whether Pennsylvania state courts would be bound by the pronouncements of federal law by inferior federal courts or whether the courts would decide these issues independently. In Hall v. Pennsylvania Board of Probation and Parole, 1 the prisoner Hall filed a pro se petition for a review in the nature of a request for mandamus to challenge application of the 1996 amendments of the Federal Parole Act. Hall had been serving time for a variety of assault-related convictions. 2 From 1996 through 1999, Hall appeared before the Parole Board, each time having his parole request rejected. 3 In 2002, Hall filed his pro se petition in the Pennsylvania Commonwealth Court, claiming that the Parole Board's application of the 1996 amendments to the Parole Act to his parole requests violated the constitutional prohibition against ex post facto laws. 4 The Commonwealth Court ultimately denied the petition, and Hall appealed to the Pennsylvania Supreme Court for review. 5 Pennsylvania courts had rejected the ex post facto argument raised by the prisoner in Winklespecht v. Pennsylvania Board of Probation and Parole 6 and in Finnegan v. Pennsylvania Board of Probation and Parole. 7 Seven weeks after Winklespecht, the Third Circuit Court of Appeals rejected the Winklespecht rationale in a case with an identical substantive contention, holding that applying the 1996 amendments of the Parole Act to the defendant violated the ex post facto prohibitions of the United States Constitution. 8 Hall, recognizing the divergence in state and federal rulings, asked the Pennsylvania Supreme Court to consider his ex post facto argument in light of the Third Circuit's recent decision. 9

The Pennsylvania Supreme Court, in considering the merits of the appeal, was faced with the question of whether or not their court--a state court--had any responsibility to treat the pronouncements of inferior federal courts on matters of federal law as binding, namely the amendments to the Parole Act at issue. 10 The Pennsylvania Supreme Court recognized that states had varying approaches to this issue, with only a very small minority of states treating lower federal court's rulings as binding on federal matters. 11 As for Pennsylvania's historical approach to the issue, the court considered its ruling in Commonwealth v. Negri 12 in 1965. In Negri, the court had to decide whether it would follow a state interpretation of Escobedo v. Illinois 13 or the conflicting analysis of the Third Circuit Court of Appeals. The Negri court considered some of the policy implications of not treating the Third Circuit's pronouncements as binding and therefore dispositive:

If the Pennsylvania courts refuse to abide by [the Third Circuit's] conclusions, then the individual to whom we deny relief need only to "walk across the street" to gain a different result. Such an unfortunate situation would cause disrespect for the law. It would also result in adding to the already burdensome problems of the Commonwealth's trial courts, which look to us for guidance. Finality of judgments would become illusory, disposition of litigation prolonged for years, the business of the courts unnecessarily clogged, and justice intolerably delayed and frequently denied. 14

Despite these concerns of unevenness in the law, lack of judicial economy, judicial confusion, and overall disrespect for the federal law, the Pennsylvania Supreme Court in Negri chose to dispense with the Third Circuit's interpretation of Escobedo and stick with the state's version of the law. 15 Since Negri, a number of decisions affirmed Negri's conclusion that Pennsylvania state courts were not bound by lower federal courts' rulings on matters of federal law brought into a state courtroom. 16 As such, the Pennsylvania Supreme Court in Hall elected to continue the doctrine that the court could decide federal matters independently of the Third Circuit, or any federal circuit courts of appeals for that matter, 17 for reasons of keeping continuity with precedent. 18 The Hall court affirmed the order of the Commonwealth court and its use of the Winklespecht analysis.

This Note argues that there is a better way for state courts to interpret federal law when a federal question is presented to a state court than the one the Pennsylvania Supreme Court has adopted. This approach is called the Lockstep Doctrine. This doctrine is premised on the idea that one court will treat as binding another court's interpretation of a law not because it has to, but because of the benefits that such an approach generates. When state courts follow the decisions of an inferior federal court on an issue of federal law, the federal law sees improvement: a reduction in the abuses of forum shopping, better consistency in the application of the federal law, a higher quality in the adjudication of federal laws generally, and the promotion of equal protection of the law.

### Spending DA---2AC

#### Nothing in the budget will become law.

Margot Sanger-Katz 3/28, Domestic Correspondent for The New York Times, M.A. in Journalism from Columbia University, Knight-Bagehot Fellow in Economics and Business Journalism from Columbia University, B.A. from Columbia University, “Missing From Biden’s Budget: His Signature Policy Agenda,” The New York Times, 3/28/2022, https://www.nytimes.com/2022/03/28/upshot/budget-biden-policy-agenda.html≥/

Administrations normally detail their biggest policy dreams in their annual budgets. The Biden administration tucked its into the footnotes instead

Months after congressional talks stalled on the president’s expansive climate and social safety net bill known as Build Back Better, the White House simply declined to include its fine print in its annual budget proposal that was released on Monday.

The budget included a slew of smaller policy specifics, including a new minimum tax for the very wealthy; a change to the way the government pays for vaccines for adults; and new money to ensure clean drinking water. But it did not include the key provisions in Build Back Better — the legislation that President Biden has spent much of his time in office promoting.

White House budgets are always largely symbolic documents, unlikely to become law without substantial changes from Congress. But without details about many of Mr. Biden’s top priorities, the budget this year is unusually unhelpful in even understanding the administration’s budgetary goals.

“Ironically, what you are seeing in the budget is things that are not going to happen,” said Marc Goldwein, the senior policy director at the Committee for a Responsible Federal Budget. “And what you are not seeing are things that possibly are going to happen.”

In a call with reporters on Monday, Shalanda Young, the White House budget director, said the administration had left out the specifics to help the continuing congressional negotiations on the package.

“I understand their political calculus, but it makes their budget not a very useful document for understanding their priorities,” Mr. Goldwein said.

Such vagueness is not utterly without precedent, but the scope of the omissions this year is unusual.

During the Obama administration’s first year in office, as it was developing the health care proposal that would become the Affordable Care Act, it also skipped including key policy details from its budget tables. Similarly, the Trump administration’s first budget offered scant specifics about its ambitions for overhauling the tax code, a priority that came to fruition later that year.

But both of those omissions occurred in the administrations’ early months, before White House policy officials or congressional negotiators had time to develop the finer points. Mr. Biden’s domestic policy agenda, in contrast, has been the subject of extensive white papers, policy speeches and legislative text — including a bill that passed the House in November.

The tax overhaul and Obamacare were major projects for those administrations, but they did not represent the range of their domestic ambitions in quite the way that Build Back Better does for the Biden White House.

The Biden administration’s plan, drawn up as a single piece of legislation that could pass through a special process without requiring Republican votes, included a range of tax, social welfare and climate policy ideas, rolling in much of Mr. Biden’s presidential campaign agenda. Depending on the details, the proposal is likely to increase both spending and revenues by $1 trillion or more over a decade.

And while the Trump budget office declined to specify tax details in 2017, it did commit to including substantial cuts to Medicaid and the Affordable Care Act as part of its plan to “repeal and replace” the health law.

Ironically, the Biden administration’s budget does include proposals, like an increase to the corporate tax rate, that lawmakers have already trimmed from the legislation in their recent negotiations.

Last year’s budget featured more of Mr. Biden’s domestic policy plan, detailing programs to combat climate change and expand child care, for example, that did become a part of the Build Back Better proposal.

This year, the agenda was briefly described in broad terms in the budget’s introductory text. But its role in the document’s detailed breakdowns was limited to footnotes in the summary tables and a line item with no corresponding dollar amount. That budget line allows for unlimited spending and unlimited revenue related to the legislation, so long as it does not increase the federal deficit.

#### Biden has no PC.

David Winston 3/30, Writer at Muck Rack, President of The Wilson Group, “Biden: Crisis of credibility,” Muck Rack, 3/30/2022, https://rollcall.com/2022/03/30/biden-crisis-of-credibility/

It’s been another bad week for the president, as White House staffers, and Biden himself on Monday, tried to clean up a string of troubling gaffes made during his crucial trip to meet with NATO leaders as the Ukraine war continued to rage.

With Russian President Vladimir Putin hinting that a nuclear response was possible if NATO directly intervenes in Ukraine or threatens Russia itself, Biden’s misstatements couldn’t have come at a worse moment. Yet, when asked about his ad-lib remarks to American servicemen in Poland, his response to the possible use of chemical weapons by Russia, and now, famously, his barely nuanced call for the ousting of Putin, incredulously, Biden told reporters, “None of the three occurred.”

It was a mind-boggling moment.

Even the president’s supporters in the media are having trouble excusing Biden’s latest attempt to explain away his gaffes, which sent shock waves across international diplomatic and security circles. The world is wondering who is in charge. It has come to that.

After months of verbal stumbles, what is most worrisome is that we don’t know whether Biden actually believes what he’s saying when he makes a gaffe, which in and of itself is problematic. Or whether it’s a cynical tactic to move on from what has been one major misstatement after another by this president, the gravest of these this past week.

Since Biden’s return from Europe, there has been a lot of hand-wringing over his leadership and his ability to govern, with many pundits suggesting that the problem is the president’s tendency to drift from the script. If only Biden would stick to the prepared text and teleprompter, they argue, his problems go away.

But even a brief analysis of his prepared budget remarks, delivered just ahead of taking questions from reporters, is a better explanation of why Biden has taken such a hit in the polls personally and on almost every major issue likely to drive the outcome of the November elections.

Simply put, this president hasn’t been straight with the American people, and it has cost him his credibility. A quick fact check of a few of Biden’s assertions on the economy Monday is a perfect example.

# 1AR

## Blockchain ADV

### AT: Democracy Bad---1AR

#### The alternative will be reactionary populism, not benign ecological autocracy---that worsens every response to climate.

Dr. Daniel J. Fiorino 21, Director of the Center for Environmental Policy at American University, PhD in Political Science from Johns Hopkins University, “Democracy is Suited to Tackle Climate Change”, Democracy Without Borders, 9/22/2021, https://www.democracywithoutborders.org/20869/democracy-is-suited-to-tackle-climate-change/

The cases for and against democracy

The case made by critics of democracy goes something like this: Democracies exist to serve the needs and preferences of their citizens. They are built on notions of individual freedom and private property rights. Voters lack the needed scientific literacy to be able to understand the causes and consequences of climate change, and they are too focused on enjoying and expanding their affluence. Handling climate change calls for drastic action, perhaps a suspension of individual rights, hard controls on population and economic growth, and more modest lifestyles.

No benign ecological autocracy has ever existed

Given these flaws, critics argue that what is needed is top-down, centralized, and authoritarian governance by scientific (or at least scientifically enlightened) elites. With the appropriate concentrations of authority and ability to set aside constraints like private property rights and economic freedoms, enlightened autocrats can make hard choices and overcome vested interests.

There are many problems with this conception. The first is that no such benign ecological autocracy has ever existed. Although many critics hold out hope that an authoritarian China will lead the way, there are many reasons to doubt that scenario. Another is that the research does not support the view that democracies are less suited to handling climate change than authoritarian regimes. Indeed, the reverse is more likely. It also is hard to imagine how these enlightened ecological autocrats will establish legitimacy and be able to make and carry out the tough decisions that have to be made.

Finally, the emergence of authoritarian populism in countries like Hungary, Poland, Venezuela, and even the United States do not bode well for a climate action agenda. As the quality of democracy and governance decline, so will capacities for dealing with climate change. Climate policy has suffered in regimes that reject scientific evidence, focus narrowly on the short term, assert extreme nationalism, and ally themselves strongly with established economic interests. With liberal democracy breaking down in many places, these barriers to action will only increase. The quality as well as existence of democracy will matter for tackling climate change.

## FTC ADV

### AT: LIO Bad---1AR

#### Biden is actively containing Russia.

Brahma Chellaney 3-7, Professor of strategic studies at the Centre for Policy Research in New Delhi, "The New Us-Russia Cold War Will Accelerate China’s Rise," Hill, 03/07/2022, https://thehill.com/opinion/national-security/597062-the-new-us-russia-cold-war-will-accelerate-chinas-rise/.

President Biden has made clear that the United States has embarked on a strategy of Containment 2.0 against Russia with what he calls “the broadest sanctions in history.” But Biden is unlikely to have factored in the possibility of a boomerang effect. The unintended consequences could bifurcate the global economy, polarize international politics and strengthen China at America’s expense.

Over the years, the relative ease of imposing economic sanctions has turned them into a grossly overused tool of American diplomacy. The efficacy of U.S. sanctions has been eroding with the relative decline of American power, and a growing body of evidence suggests that such measures have often proved counterproductive to America’s own economic and geopolitical interests.

The U.S. has virtually ejected Russia from the Western-led financial order at a time when economic power is moving east. Expelling the world’s 11th-largest economy from an order that the U.S. seeks to uphold could intensify the search for a viable alternative system that isn’t dominated by the West.

What is more certain is that the new U.S.-led hybrid war against Russia, centered on unparalleled sanctions, will help deepen the undeclared Beijing-Moscow axis against Washington and make China the big winner financially and geopolitically, thereby aiding its expansion of economic and military power.

The West’s heavy economic penalties on Moscow, including unplugging key Russian banks from the international SWIFT payments system, are set to turn China into Russia’s banker, enabling it to reap vast profits. In structural terms too, Russia’s sanctions pain will be China’s gain: To help insulate itself from similar Western sanctions if it were to invade Taiwan, Beijing is seeking to boost the payments and reserve role of the yuan and the international use of its competitor to the SWIFT network — the Cross-Border Interbank Payment System, or CIPS. The West’s Russia sanctions are likely to provide a fillip to both efforts.

#### AND China.

Michael D. Swaine & Sarang Shidore 3-7, Director of QI’s East Asia program; Director of Studies at the Quincy Institute, "Biden pursues China-containment in new Indo-Pacific strategy," Responsible Statecraft, 03/07/2022, https://responsiblestatecraft.org/2022/03/07/biden-pursues-china-containment-in-new-indo-pacific-strategy/.

Even as the Ukraine crisis continues to escalate, the security situation in Asia remains far from calm. However, the Biden administration’s recently-released Indo-Pacific Strategy is both disappointing and dangerous in the manner in which it doubles down on containing China. By doing so, the United States is enhancing the risk of great power war and missing a major opportunity to engender economic prosperity and tackle the existential threat of climate change.

The depiction of the relationship with Beijing presented in the two documents that spell out the strategy is almost entirely negative and zero-sum in nature. When China is mentioned directly, it is described as using all dimensions of its power to engage in “coercion and aggression” across the globe. It is cast as pursuing “a sphere of influence in the Indo-Pacific and seeks to become the world’s most influential power.” Beijing is supposedly committed to undermining international law and “transforming the rules and norms that have benefitted the Indo-Pacific and the world.”

The broad-brush, unqualified message conveyed is very clear: China presents a dire threat to the Indo-Pacific region and the world that must be countered on all fronts by the U.S and its allies and partners.

The Indo-Pacific Strategy makes no attempt to provide a vision or program for how an authoritarian China can coexist peacefully and productively with the U.S. over the long term, other than as a subordinate or compliant power. The document merely states that the U.S. objective “is not to change China but to shape the strategic environment in which it operates, building a balance of influence in the world that is maximally favorable to the United States, our allies and partners, and the interests and values we share.”

According to this approach, actually engaging with Beijing to reach understandings on a host of contentious issues from trade and investment to cyber norms and regional maritime disputes is apparently fruitless.

Moreover, there is no sign whatsoever in the Indo-Pacific strategy of an attempt at meaningful cooperation with China, most consequentially on solving the critically important climate problem. Other than a passing reference to working with China, there is no substantive discussion of how to actually engage Beijing in this critical area, whether in research and development, scientific and educational exchange, disaster relief, resilient infrastructure, or any of the other activities essential to combating the climate threat.

## T Per Se

### We Meet---1AR

#### The rule of reason does that. Legally, ‘unreasonable’ restraints are absolutely forbidden. This satisfies the test!

Srikanth Srinivasan 94, JD and MBA Candidate at the Stanford Law and Business Schools, “College Financial Aid and Antitrust: Applying the Sherman Act to Collaborative Nonprofit Activity”, 46 Stan. L. Rev. 919, April 1994, Lexis

Section 1 of the Sherman Act states that "every contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce … is declared to be illegal." 21 Interpreted literally, this provision could prohibit all commercial contracts. But courts have instead interpreted the Act to prohibit only "unreasonable" restraints on competition. 22 Courts normally assess the reasonableness of a competitive restraint by applying a "rule of reason" test that evaluates the competitive effect of the contested conduct in light of all relevant circumstances. 23 Some categories of activities are so likely unreasonable, however, that courts determine them per se unreasonable without analyzing their competitive implications. 24 For example, courts generally invalidate horizontal agreements to fix prices, the crux of the Justice Department's allegations [\*923] in Brown University, as per se illegal. 25 Courts ask three questions when evaluating agreements under Section 1: Does the activity constitute trade or commerce so that the Sherman Act applies? If so, is the activity in a category that evokes application of a per se presumption against its validity? If not, is the activity unreasonable under the rule of reason? Both Brown University decisions followed this general scheme.

#### ‘Anticompetitive’ behavior is outcome dependent

Janusz A. Ordover 85, Professor of Law at the University of Columbia School of Law, A.O. Sykes, and R.D. Willig, “Nonprice Anticompetitive Behavior by Dominant Firms Toward the Producers of Complementary Products”, in Antitrust and Regulation: Essays in Memory of John J. McGowan, Ed. Fisher, p. Google Books

In a variety of market settings dominant firms have an incentive to engage in anticompetitive practices that disadvantage the producers of complementary products. (Here, we define "anticompetitive practices" as practices that exclude other producers from markets, to the detriment of economic welfare.) These incentives arise as a result of com- plementarities in consumption and in production. For example, cameras and film are complements in consumption, whereas basic and pay programming for cable television are complements in production, at least at the distribution level. Thus, contrary to conventional think- ing, a firm with market power at one stage of production or over one component of a product may nonetheless have an incentive to extend its market power to other stages of production or to other product components.

#### It's a prohibition because conduct incompatible with the standard is illegal

John G. Koeltl 7, United States District Judge, “United States Baseball v. City of New York”, United States District Court for the Southern District of New York, 509 F. Supp. 2d 285, 297, 2007 U.S. Dist. LEXIS 63234, 8/27/2007, Lexis

The City responds that its home rule and police powers are broader pursuant to Article IX, Section 2(c) of the New York State Constitution, New York Home Rule Law § 10(1)(a)(12), and New York General City Law § 20(13) than the plaintiffs suggest. These provisions give the City the power to enact laws for the "safety, health, well-being, and welfare" of its residents. The City asserts [\*\*29] that the Bat Ordinance does not constitute a "prohibition" because it does not condemn all use of non-wood bats. It bars their use in competitive high school baseball games, but not for example in high school practices, junior high school games, "pick up" games, or youth league games that are not school-sponsored. Moreover, the City persuasively argues that the suggested distinction between "prohibitions" and other "regulations" is artificial and untenable, because all regulations prohibit some conduct that is incompatible with the regulatory standards and all "prohibitions" leave some conduct untouched. For example, a New York court upheld as a valid exercise of the police power a New York City law banning the possession in a public place of a knife with a blade of at least four inches in length in People v. Ortiz, 125 Misc. 2d 318, 479 N.Y.S.2d 613, 620 (Crim. Ct. 1984). The plaintiffs suggest the law at issue in Ortiz was a not a "prohibition," but it appears to be at least as complete a prohibition as the Bat Ordinance, which prohibits only certain uses of bats with certain defined characteristics.

#### ‘Increase’ isn’t immediate

Judge Tucker 9, Supreme Court of Virginia, Reno's Ex'rs v. Davis, 14 Va. 283, 289, 1809 Va. LEXIS 53, 11/8/1809

Thursday, November 23. On the merits, Wickham argued that, by the word "increase," children born after the death of the testator only passed; for at the time of the death and not until then, the will speaks. This is a question of intention. If the children living when the will was made had names, it would have been more natural to describe them by name, than by the word increase. But according to the general usage of the country, the word "increase" means the same as "future increase." Parol testimony on this subject is improper, as it goes to prove what the testator meant by particular words.

#### It prohibits a practices---the rule is simply a test to determine whether conduct violates that prohibition

Todd Fishman 19, [Allen & Overy LLP](https://www.jdsupra.com/profile/Allen_Overy_docs/), January 31st, 2019, “The Rule of Reason as a Bar to Criminal Antitrust Enforcement”, https://www.jdsupra.com/legalnews/the-rule-of-reason-as-a-bar-to-criminal-87406/

Antitrust law’s rule of reason was born of technical necessity. By its terms, §1 of the Sherman Act prohibits “[e] very contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade.” 15 U.S.C. §1. Despite the expansive language of the statutory prohibition, the Supreme Court has held that §1 prohibits only agreements that unreasonably restrain trade. *Board of Trade of Chicago v. United States*, 246 U.S. 231, 238 (1918); *Standard Oil Co. of N.J. v. United States*, 221 U.S. 1, 58-60 (1911). With the rule of reason, antitrust courts assumed a prudential role in administering the scope of antitrust violations, applying a factual inquiry weighing legitimate justifications for a restraint against any anticompetitive effects. Under the rule of reason, “the factfinder weighs all of the circumstances of a case in deciding whether a restrictive practice should be prohibited as imposing an unreasonable restraint on competition.” *Continental T.V. v. GTE Sylvania,* 433 U.S. 36, 49 (1977).

#### Prohibition includes per se and rule of reason.

Anu Bradford 18, and Adam S. Chilton. Anu Bradford Henry L. Moses Professor of Law and International Organization, Columbia Law School. Adam S. Chilton. Assistant Professor of Law and Walter Mander Research Scholar.

Before discussing our data and the coding of the CLI, it is important to recognize that there are limitations to any index that attempts to quantify competition regulation. This is because it is difficult to produce a single metric that tells the comprehensive story of country’s competition regime. For example, if a specific type of conduct is prohibited, is it prohibited always (per se) or sometimes (rule of reason)? This seems like a relevant distinction to code, but it turns out to be difficult to capture systematically in many jurisdictions. For instance, Article 101(3) of the Treaty on the Functioning of the European Union (TFEU) seems to regulate anticompetitive agreements under the rule of reason standard in the European Union, but, in practice, cartels are per se prohibited. This highlights the challenge of coding even just the law in books, let alone accounting for all the nuances of a country’s competition policies.20

### C/I---1AR

#### It can hinder, rather than be absolute

Sandra L. Lynch 2, Judge on the United States Court of Appeals, First Circuit, “Second Generation Props., L.P. v. Town of Pelham”, 313 F.3d 620, 634, 2002 U.S. App. LEXIS 25904, 12/17/2002, Lexis

§ 332(c)(7)(B). We start with the fact that Congress used "services" and not "service." A straightforward reading is that "services" refers to more than one carrier. Congress contemplated that there be multiple carriers competing to provide services to consumers. That one carrier provides some service in a geographic gap should not lead to abandonment of examination of the effect on wireless services for other carriers and their customers. Next, the phrase "have the effect of prohibiting" may well refer to actions that mostly prohibit. For example, B.A. Garner, A Dictionary of Modern Legal Usage 256 (2d ed., 1995), gives as the first definition of effective "having a high degree of effect." (emphasis added). Accord B.A. Garner, A Dictionary of Modern American Usage 237-38 (1998). Moreover, a common reading of the word "prohibition" standing alone would apply to a situation of denial of services to the vast majority of users. See, e.g., Oxford English Dictionary (2d ed. 1989) (defining [\*\*33] "prohibit" as "to prevent, preclude, hinder") (emphasis added). Thus Congress may well have meant the effective prohibition clause to reach certain situations in which there is some coverage in a gap.

## Capitalism K

### Sustainability---1AR

#### Best study confirms it.

Hideo Noda & Shigeru Kano 21, Tokyo University of Science; The Shoko Chukin Bank, "Environmental Economic Modeling of Sustainable Growth and Consumption in a Zero-Emission Society," Journal of Cleaner Production, Vol. 299, 05/25/2021, pg. 1-2.

Manufacturing activities that pollute the soil, atmosphere, and water have adversely affected the environment. The abatement of pollution is therefore essential to maintaining environmental standards in the future. The purpose of this paper is to examine what kind of economic conditions should be satisfied if an economy adopts a rule stating that pollution must be cleaned up when it is produced, and whether the zero net emission of pollution flow (in the sense of a zero residual amount of pollution created minus pollution abated) is compatible with the continued growth of gross domestic product (GDP) and consumption when the economy experiences cyclical fluctuations.

A detailed understanding of the economic implications of cyclical fluctuations is crucial because actual economies inevitably undergo cycles of expansion and recession. In this respect, on the basis of the laboratory equipment model of Rivera-Batiz and Romer (1991), Matsuyama (1999) constructed a useful model that generates endogenous fluctuations. Notably, under specific conditions, an economy can perpetually oscillate between a capital-accumulation-based (no-innovation) growth phase and innovation-led growth phase. The former phase is called the Solow regime, after the work of Solow (1956), while the latter phase is called the Romer regime, after the work of Romer (1990) and Rivera-Batiz and Romer (1991).

However, Matsuyama (1999) did not pay attention to environmental aspects in a society. We therefore extend the model of Matsuyama (1999) by considering pollution abatement from the perspective of the kindergarten rule model of Brock and Taylor (2005). We thereby expect to obtain meaningful findings by analyzing endogenous fluctuations with pollution abatement, which has not been tackled in earlier studies. The term “kindergarten rule” originates from the title of a book written by Fulghum (1990) and implies that messes be cleaned up as they are created. Brock and Taylor (2005) referred to the proportion of pollution abatement expenditure in GDP for achieving zero net emissions of pollution (i.e., completely eliminating the amount of pollution created minus pollution abated) as the kindergarten rule level of abatement (or just the kindergarten rule).

Ono (2003) extended Matsuyama’s (1999) model to analyze endogenous fluctuations by accounting for environmental variables. Specifically, Ono (2003) incorporated the production structure of Matsuyama (1999) into the framework of the overlapping generations model on the basis of the work of John and Pecchenino (1994) and examined environmental taxation that maximizes the environmental quality and economic growth rate. It is found that there is a critical level of tax, and the economy achieves higher growth rates of GDP and environmental quality by raising (or reducing) tax if the initial tax is below (or above) the critical level. That is to say, the purpose of the present study differs from that of the study of Ono (2003). We analyze the feasibility of the positive growth of GDP with zero net emission that reflects the kindergarten rule of pollution abatement, while Ono (2003) focused on taxation for improving environmental quality and promoting economic growth. Recent efforts toward a zero-emission society, which are an important topic of the Paris Agreement that came into force on November 4, 2016, have received worldwide attention (see, for example, Pauli, 1997; Baumgartner and Zielowski, 2007; Tokimatsu et al., 2014). The present study is therefore of social importance and relevant. Additionally, we consider that the notion of environmental quality is vague and hence difficult to capture empirically. In contrast, the zero net emission of pollution has clear meaning.

Related studies of environment-growth models with endogenous fluctuations include those conducted by Zhang (1999), Chen and Li (2011), and Palivos and Varvarigos (2017). Zhang (1999), for example, examined the possibility of nonlinear dynamics in the model of John and Pecchenino (1994) and showed that cyclically or chaotically fluctuating equilibria are more likely to exist when people’s concerns are more towards greener preferences and the maintenance efficiency relative to degradation is not sufficiently high. Chen and Li (2011) introduced the habit formation of environmental quality and consumption tax to the model of John and Pecchenino (1994). The habit formation of environmental quality in the model of Chen and Li (2011) means that people get used to the environment while they grow up and will compare environmental quality in their old age with that when they were young. As a result, Chen and Li (2011) showed that cyclical fluctuations and entropic chaos may exist if households have a preference towards environmental quality and the maintenance efficiency is sufficiently low relative to degradation and the tax rate. The economy moves from complex to simple dynamics as the tax rate increases. Using an overlapping generations model where life expectancy is positively affected by the provision of public health services and by the environmental quality, Palivos and Varvarigos (2017) showed that, despite the presence of an aggregate learning-by-doing externality, the economy cannot sustain a positive growth rate in the long run if resources are not devoted to environmental preservation. Moreover, an active policy of environmental preservation is not only an important complementary engine of long-run growth but also a powerful tool of stabilization.

Zhang (1999), Chen and Li (2011), and Palivos and Varvarigos (2017), however, did not consider the role of innovation in economic growth. When we consider issues related to recent economic growth, it is noteworthy that the economic activities of industries in developed countries and some developing countries have increasingly become knowledge intensive. The economies of these countries are often termed knowledge-based economies. An important feature of such an economy is that it emphasizes innovation, including the creation of new products and production processes through industrial research and development (R&D), and the innovation is accompanied by accumulated knowledge that drives sustained growth. Accordingly, any study on the actual economic problems of a knowledge-based economy needs to construct a model that endogenously incorporates R&D and innovation. From such a perspective, the above-mentioned earlier studies are inadequate in terms of understanding the relationship between contemporary economic growth and environmental problems.

Our model leads to the theoretical possibility that the zero net emission of pollution flow is compatible with sustainable growth and consumption. In this regard, however, the economy requires GDP above a certain level. Moreover, to simultaneously achieve a zero net emission of pollution and sustained economic growth, the economy requires variability of the kindergarten rule level of abatement. In other words, the kindergarten rule level of abatement must not be fixed at a specific value. The present study makes two main contributions. First, we shed light on the relationship between the zero net emission of pollution and economic growth, which is not well understood, and address theoretically an important subject interesting environmental scientists, economists, and policy makers: whether both a zero net emission of pollution and sustained growth of GDP (consumption) are achievable when economies implement a zero net emission policy. In terms of the association with Sustainable Development Goals (SDGs), which were adopted by the United Nations General Assembly in September 2015 and have received international attention, our considerations are conducive to providing a theoretical basis for a part of SDG 8 (“Decent Work and Economic Growth”). Second, we present a dynamic macro-environmental modeling approach based on an extension to Matsuyama’s (1999) model with the idea of the kindergarten rule of Brock and Taylor (2005). To the best of our knowledge, there have been few studies on the environmental economic modeling of endogenous growth with cyclical fluctuations in a zero-emission society. That is to say, our dynamic macroenvironmental modeling approach can be interpreted as a methodological contribution in the research field of economic growth and the environment.

#### War warrant is wrong.

Fritz Dufour 21, MBA, DESS, "The Origins and Causes of War," in The Realities of 'Reality' – Part IV: The Reality Behind Achieving World Peace, Chapter 1, pg. 33-34, 10/27/2021, SSRN.

The weakness of the theory was that the two major expected types of war, the intracapitalist and the capitalist-socialist, did not materialize as frequently as Soviet theoreticians had predicted. Further, the theory failed to adequately analyze the situation in the Soviet Union and in the socialist camp. Even in communist countries, nationalism seems to have proved more powerful than socialism: “national liberation” movements appeared and had to be forcibly subdued in the Soviet Union, despite its communist regime. Also, war between socialist states was not unthinkable, as the doctrine indicated: only the colossal preponderance of Soviet forces prevented a full-scale war in 1956 against Hungary and in 1968 against Czechoslovakia; war between the Soviet Union and the People’s Republic of China was a serious possibility for two decades after the Sino-Soviet split in 1962; and armed conflict erupted between China and Vietnam after the latter country became the most powerful in Southeast Asia. Finally, the theory did not provide for wars of liberation against socialist states, such as that conducted by the Afghan mujahideen against the Soviet Union from 1979 to 1989. Other causes of war are external and are worth analyzing. The following are among the most common.

### Growth Good---1AR

#### AE is coming AND achieves absolute decoupling.

---AE = alternative energy.

Klaas Lenaerts et al. 21, Research Assistant, Bruegel; Simone Tagliapietra, Senior Fellow, Bruegel; Guntram B. Wolff, Director, Bruegel, "Can Climate Change Be Tackled Without Ditching Economic Growth?" Bruegel, Working Paper No. 10, 2021, pg. 11-13.

A decline in energy demand/real GDP can be driven by improvements in energy efficiency from using better technologies for production, transport, isolation etc; by behavioural change towards less energy-intensive consumption (eg increased use of public transport, a larger sharing economy and more re-use of durable goods); and by a changing economic structure towards a more ‘immaterial’ service-oriented economy. A decline in CO2/energy demand is mostly driven by the shift from fossil fuels to renewable energy sources. Changing behaviour also plays a role (choosing to travel by rail rather than by air for example).

So far, energy demand/real GDP has declined more since 1995 than CO2/energy demand. Perhaps this is somewhat surprising as in the long run it seems more likely that energy would be almost completely decarbonised than that the global economy would be completely ‘de-energised’: goods still need to be produced somewhere and transport, heating and lighting will remain necessary. In practise, both factors will have to decline simultaneously to sufficiently reduce gross CO2 emissions. This is also visible in Tables 1A and 1B, which show that if energy demand/real GDP continues to decline at its current rate, a very steep drop in CO2/energy demand will be necessary for both the world and the EU. If energy demand/real GDP is also addressed more strongly, the ‘burden’ can be spread over both factors of the Kaya identity (see for example the different rates depending on which reference period is used for energy demand/real GDP).

The data presented here suggest that an absolute decoupling of CO2 and GDP is possible, but that it is currently still too slow to reach net zero. Note that while the required decoupling rate is higher for the EU than for the world, the EU is closer to its goal: while the overall decoupling rate must increase around five-fold for the whole world, the EU itself only needs less than a three-fold acceleration.

The historical decoupling rate against which to compare also increases if one takes a more recent reference period, as is visible in the table. Speeding-up will still take tremendous effort: if the energy intensity of GDP decreases at the same speed as in the last few decades, even the EU would need to speed up its decarbonisation of energy by a factor of around 11 to reach its required decoupling rate.

The drastic decline in prices of renewable energy technologies suggests that such an accelerated decarbonisation of energy may be feasible. Figure 3 shows that over the last decade, the cost of generating electricity with solar panels has decreased by 85 percent, while the cost of doing so with wind turbines has decreased by 68 percent. The costs of energy from solar and wind have become lower than fossil fuel alternatives even without subsidies. Firms and governments all over the world would therefore have economic incentives to make the necessary investments to save money and at the same time reduce their emissions.

Investment decisions are of course not based solely on market prices but also on government policies and strategies. Money is still being invested in fossil fuels, but volumes are declining. Meanwhile global investments in renewable energy generation have been on the rise uninterruptedly since 2017, even during the pandemic in 2020. Moreover, it takes time before lower costs are translated into larger investments, and other key investments must be made before renewable energy can be used at a massive scale, notably in energy storage capacity and more reliable distribution and transmission. As investments in battery storage are surging while costs are declining and investments in grids are set to recover in 2021, we can expect that the upward trend in renewable energy investment will continue for the foreseeable future (IEA, 2021d).

[Figure omitted]

Already in the earlier literature rejecting degrowth pessimism, the central role of technology was highlighted. Stiglitz (1974) and Kamien and Schwartz (1978) did not yet address GHG emissions, but rather whether continued consumption growth is possible in a world with exhaustible resources. They found that technology-driven efficiency gains allow the limits set by nature to be pushed forward so that continued expansion is possible. Later papers, including Weitzman (1999), Acemoglu et al (2012) and Aghion et al (2016), discussed endogenous and directed technical change with more optimistic outlooks.

#### Anthropogenic risks are numerous, existential, AND compounding.

Nathan A. Sears 20, PhD, Political Science, University of Toronto. Former Professor, International Relations, Universidad de Las Américas, "Existential Security: Towards a Security Framework for the Survival of Humanity," Global Policy, Vol. 11, Issue 2, April 2020, pg. 256.

The ‘anthropogenic’ and ‘existential’ criteria highlight an important class of threats. Put simply, an ‘anthropogenic existential threat’ is a threat that has its origins in human agency and could cause civilizational collapse or human extinction. The spectrum of anthropogenic existential risks is potentially broad and growing, including persistent threats to international security (e.g. nuclear and biological warfare), looming dangers from the large-scale intervention in the natural environment (e.g. climate change, biodiversity loss, and geoengineering), and prospective risks from emerging technologies (e.g. biotechnology, nanotechnology, and artificial intelligence).4

The threats to humanity are exacerbated by the complexity of social, technological, and natural systems, which create lethal combinations (e.g. nuclear war and ‘winter’) (Baum et al., 2013; Ehrlich and Sagan, 1985; Liu et al., 2018), feedback loops (e.g. ‘runaway’ climate change) (Steffen et al., 2015, 2018), small triggers (e.g. cyberattack and nuclear escalation) (Acton, 2018; Gartzke and Lindsay, 2017), chance accidents (e.g. viruses escaping from laboratories) (Merler et al., 2013; Rees, 2003; Torres, 2017), ‘normal’ accidents (e.g. human and/or technical glitches in nuclear command and control) (Blair, 1985; Sagan, 1995; Schlosser, 2013), epistemic uncertainties (e.g. about ‘planetary boundaries’ and climate ‘tipping points’) (Baum and Handoh, 2014; Rockstrom et al., 2009; Steffen et al., 2018), technological diffusion (e.g. terrorists employing advanced biotechnology to release ‘bioengineered pathogens’) (Posner, 2004; Rees, 2003; Torres, 2017), technological disruption (e.g. artificial intelligence destabilizing nuclear deterrence) (Boulanin ed., 2019; Geist and Lohn, 2018; Scharre, 2018), control problems (e.g. an ‘intelligence explosion’ in artificial intelligence) (Bostrom, 2014; Russell, 2019; Shanahan, 2015; Tegmark, 2017), and the cascading collapse of complex systems (e.g. ‘synchronous failure’ of interdependent ecological and social systems) (Diamond, 2005; Homer-Dixon et al., 2015; Kareiva and Carranza, 2018; Manheim, 2018). Perhaps it was this growing spectrum of threats that led the late Stephen Hawking to conclude, ‘I don’t think the human race will survive the next thousand years unless we spread into space. There are too many accidents that can befall life on a single planet.’ 5