Table of Contents

Summary...........................................................................................................................................2

Principles Underpinning Blockchains.................................................................................................2

What are Blockchains Really?...........................................................................................................3

Is Blockchain all about Computers taking Over the World?.............................................................4

Why does Blockchain Generate Excitement?..................................................................................4
  The Double Spend Problem..............................................................................................................4
  Cybersecurity Stemming from the “Immutability” of Recorded Transactions...............................5
  Blockchained Transactions are Transparent....................................................................................5
  Third Party Validators Not Needed..................................................................................................5
  Power Might Be Returned to the Consumer....................................................................................6

Example of Companies Active in the Blockchain Space.................................................................6

Use Cases..........................................................................................................................................7

Public Policy Issues..........................................................................................................................8
  Regulation.......................................................................................................................................8
  Regulatory Access to Source Code................................................................................................10
  Governance....................................................................................................................................10
  Data Privacy....................................................................................................................................11
  Cybersecurity..................................................................................................................................12
  Energy Use.....................................................................................................................................13
  Intellectual Property Rights (IPR) Considerations..........................................................................14
  Regulatory Technology (“RegTech”)...............................................................................................14

Recommendations for Policymakers..............................................................................................15

Endnotes.............................................................................................................................................17
Summary

Blockchains, which are open, closed, or a hybrid ledger technology (DLT), already exist, primarily for cryptocurrencies, and are potentially important for other sectors as well. There is substantial investment in the technology, which is essentially a type of software. Companies, including SIIA member companies, and governments are experimenting extensively with the technology. The UK Government Office for Science says that “we may be witnessing one of those potential explosions of creative potential that catalyze exceptional levels of innovation.”¹ There are skeptics, but some posit that blockchains could prove to be a transformational development. Perhaps the IMF gets it right when it suggests that with respect to Fintech (sometimes conflated with blockchain, although not all Fintech applications necessarily use blockchain), it is hard to judge whether the technology will have “evolutionary or revolutionary implications.”² The more forward-looking idea that blockchain could be a “foundational” technology such as the transmission control protocol/internet protocol (TCP/IP) was for the Internet is also intriguing. But, it is worthwhile recalling that this Internet technology took decades to mature into the Internet we know today.³ This Issue Brief offers a brief description of blockchain technology. However, it does not take a view on how transformational, disruptive, and/or disintermediating blockchains will ultimately prove to be. Instead, this Brief focuses on the public policy issues associated with the development of blockchains. Technological neutrality remains SIIA’s core operating principle and the best policy is developed if blockchain is seen as one of several digital technologies that will transform the world. Having said that, there are some blockchain-specific public policy issues concerning regulation (including access to source code), governance, data privacy, cybersecurity, energy use, intellectual property, and regulatory technology (“RegTech”) worth discussing. The Brief concludes with a number of recommendations for policymakers.

Principles Underpinning Blockchains

Iansiti and Lakhani describe five basic principles underlying blockchain technology.⁴

1) Distributed Database: Each party on a blockchain has access to the entire database and its complete history. No single party controls the data or the information. Every party can verify the records of its transaction partners directly, without an intermediary.

2) Peer-to-Peer Transmission: Communication occurs directly between peers instead of through a central node. Each node stores and forwards information to all other nodes.

3) Transparency with Pseudonymity: Each transaction and its associated value are visible to anyone with access to the system. Each node, or user, on a blockchain has a unique 30-plus-character alphanumeric address that identifies it. Users can choose to remain anonymous or provide proof of their identity to others. Transactions occur between blockchain addresses.

4) Irreversibility of Records: Once a transaction is entered in the database and the accounts are updated, the records cannot be altered because they’re linked to every transaction record that came before them (hence the term “chain”). Various computational algorithms and approaches are deployed to ensure that the recording on the database is permanent, chronologically ordered, and available to all others on the network.

[Note: In a public blockchain like Bitcoin, miners add transaction records, i.e. blocks to the Bitcoin blockchain ledger through a resource intensive “proof of work” calculation that validates the Bitcoin transaction. Other Bitcoin “nodes” verify the proof of work.⁵ Nodes are computer programs attached to the Bitcoin network that are used to verify transactions.
Arriving at verification among several nodes is arriving at “consensus” in the Bitcoin context. The Bitcoin glossary defines this as “When several nodes (usually the most nodes on the network) all have the same blocks in their locally-validated best blockchain.”

5) **Computational Logic**: The digital nature of the ledger means that blockchain transactions can be tied to computational logic and in essence programmed. So, users can set up algorithms and rules that automatically trigger transactions between nodes.”

Iansiti and Lakhani are describing a public blockchain. These principles are at work with Bitcoin, which is the most prominent real-world application of blockchain. Bitcoin is an example of a “public blockchain.” But there is a lot of work being done on “private blockchains” as well. With respect to the difference between public and private blockchains, Praveen Jayachandran writes:

“The sole distinction between public and private blockchain is related to who is allowed to participate in the network, execute the consensus protocol and maintain the shared ledger. [Executing the consensus protocol in this context means verifying each transaction, i.e. each block.] A public blockchain network is completely open and anyone can join and participate in the network. The network typically has an incentivizing mechanism to encourage more participants to join the network. Bitcoin is one of the largest public blockchain networks in production today.”

Although Jayachandran appears to minimize the differences between public and private blockchains, in fact they are very different in principle and in practice. This is why blockchain purists generally do not favor private blockchains. Maybe the most compelling way to understand the difference is that a public blockchain such as Bitcoin does not in theory have a legal character because everything is done on a peer-to-peer basis. Yes, Bitcoin’s protocols have software developers. And yes, those software developers created code used by the “miners” to verify transactions through consensus operations. But even those miners in theory do not bear legal responsibility. Private blockchains, however, have a proprietor and can thus be held legally accountable.

**What are Blockchains Really?**

Blockchains are defined by the UK Science Office as “a type of database that takes a number of records and puts them in a block (rather like collating them on a single sheet of paper). Each block is then ‘chained’ to the next block, using a cryptographic signature. This allows block chains to be used like a ledger, which can be shared and corroborated by anyone with the appropriate permissions.” Ledger accuracy – “consensus” – can be corroborated in many ways. Permissioned (private blockchains) ledgers have one or more owners and unpermissioned (public blockchains) ledgers have no single owner. But blockchains are more than just a database. As the UK Science Office notes: “The real novelty of blockchain technology is that it is more than just a database – it can also set rules about a transaction (business logic) that are tied to the application itself. This is in contrast with conventional databases, in which rules are often set at the entire database level, or in the application, but not in the transaction.”

For another introduction, Entrepreneur’s Rob Marvin describes the blockchain as a distributed database that keeps records in blocks tied together with information transmitted using end-to-end encryption. The blocks are chained together through a network of computers sometimes called “nodes.” Transactions can only take place through a “Distributed Trustless Consensus” mechanism that provides “proof of work” that a given transaction has happened, for instance a payment.
There are two kinds of blockchains, and they pose different regulatory and governance challenges. But there are similarities in that both are decentralized peer-to-peer networks where each participant maintains a replica of signed transactions; both maintain the replicas in sync through a protocol referred to as “consensus”; and, both provide certain guarantees on the immutability of the ledger, even when some of the participants are faulty or malicious.

The fundamental characteristic of a public blockchain is that anybody can participate in one. This has transparency advantages but corresponding privacy challenges. Moreover, in order to achieve consensus a substantial amount of energy-intensive computer power is needed.

Private blockchains require an invitation in order to participate, which is why private blockchains are sometimes called “permissioned” blockchains. Because permissioned blockchains offer greater privacy protections and because they require less energy to maintain, it is possible that private blockchains will become relatively more important in the coming years. However, some blockchain advocates consider them less secure than public blockchains because there is a central administrator.

**Is Blockchain all about Computers taking Over the World?**

The vocabulary surrounding the blockchain discussion can sometimes appear to conjure up the image of machines taking over the world, for instance when the role of “nodes” is discussed. But blockchain is very much about people, companies, governments, and NGOs taking advantage of what the technology potentially has to offer. In the case of Bitcoin, for instance, the protocols underlying technology are developed by programmers, as well as users and miners. A user is anybody who buys and/or sells Bitcoins. “Miners” engage in the computer processing necessary to verify transactions. While at the industry’s inception, there were individuals engaged in this activity, mining has become a large corporate activity with large “mining pools” having been created. Pools consist of people or companies who combine their resources in the hopes of verifying transactions first, thus earning Bitcoins. China has 58% of the mining pools and the United States 16%. For a description of how mining actually takes places, this Quartz article on Bitcoin mining in the city of Ordos in Inner Mongolia is interesting.

**Why does Blockchain Generate Excitement?**

Advocates say that the technology (at least as applied to Bitcoin) solves the “double spend” problem, provides better (albeit not perfect) cybersecurity, promotes transparency (although advocates say that the privacy challenges associated with the technology are solvable), eliminates or reduces the need for third party validators, and could conceivably empower consumers.

**The Double Spend Problem**

Blockchain is often associated with Bitcoin and other cryptocurrencies because the first major application of blockchain is Bitcoin, which is essentially digital cash. The 2008 Satoshi Nakamoto White Paper entitled “Bitcoin: A Peer-to-Peer Electronic Cash System” is considered the foundational paper for blockchain technology as a whole even though the first word in the title is “Bitcoin.” Nakamoto solves the double-spend problem by using a peer-to-peer network to “mine” (place) data on blocks and then use a “hash” (a time-stamped link) to create “an ongoing chain of hash-based proof of work, forming a record that cannot be changed without redoing the proof-of-work.” There is a voluntary
community of “miners” that provide the proof-of-work (which requires energy-intensive computer processing) in return for Bitcoins. This proof-of-work concept is at the root of the idea that blockchain can reduce fraud from occurring over the Internet. (Note: Satoshi Nakamoto has not been identified and some speculate that Nakamoto could be more than one individual.)

Cybersecurity Stemming from the “Immutability” of Recorded Transactions

The concept here is that bitcoin transactions (or other data, transactions or contracts) are not “saved” in a conventional computer file. Instead, transactions are recorded in a blockchain that cannot be changed. Each transaction is verified by computers all over the world. There is no central database to hack, which improves security. However, commentators concede that “nothing is completely un-hackable.” 17 There have been blockchain-related cybersecurity incidents. For example, Mt. Gox, 18 Bitfinex, 19 Ethereum, 20 and DAO 21 have been hacked and robbed. Blockchain proponents suggest that attempts to centralize blockchains, deficient code, and smart contract loopholes explain the vulnerabilities. PC Magazine’s Rob Marvin says: “These issues all stemmed from vulnerabilities in systems connected to the blockchain, not the blockchain itself.” 22 Perhaps, but given that systems will have to connect to blockchains, cybersecurity will continue to be an important consideration as more blockchains are created, and they are scaled up.

Blockchained Transactions are Transparent (but privacy can still supposedly be accommodated)

Blockchains can be viewed by the public so there is transparency as a result. But privacy is still desirable for many reasons and it is legally required in many cases. Nakamoto solves this problem by “keeping public keys anonymous.” He analogizes to stock exchanges. The public can see that a transaction has happened. The time and size of individual trades are made public, but the identity of the parties is not revealed. 23 This is essentially the difference between a public and a private blockchain. Public blockchains are open to all who wish to participate. Bitcoin is the most well-known example. Private blockchains are operated by a company or perhaps several organizations (this is known as “consortium” blockchain). The operator(s) of the private blockchain verifies each transaction and, crucially, the company can “also choose who has read access to their blockchain’s transactions, allowing for greater privacy than a public blockchain.” 24

Third Party Validators Not Needed

This is probably where most of the excitement around blockchain has been generated. The idea is that if information, including transactions, are inherently correct and secure, then there might not be a need for banks to process payments, titling companies to register land transactions, or companies to provide information for know your customer compliance requirements. This is why blockchain is considered disruptive: because of its potential power to disintermediate. Perhaps. For an interesting example of some of the disintermediation discussion surrounding blockchain, there is a Harvard Business Review article suggesting that “The Blockchain Will Do to the Financial System What the Internet Did to Media.” 25 However, the reality is that banks are major blockchain investors. And major technology companies are offering blockchain services. For example, IBM is building a blockchain for seven European banks in the area of trade finance. 26 There is a major consortium called R3, which describes itself as an “enterprise software firm”. R3 is building a distributed ledger technology called Corda. 27 R3 is working with over 100 banks, financial institutions, regulator, trade associations,
professional services firms and technology companies to develop Corda. Banks and financial institutions are engaged in a number of other blockchain-related initiatives as well such as the Enterprise Ethereum Alliance and the Hyperledger Project, which is led by the Linux Foundation. Ripple is a company that uses blockchain technology to provide cross-border payments. Investors include Accenture, CME Ventures, Google Ventures, SBI Group, Seagate, Andreessen Horowitz, Core Innovation Capital, Santander, Digital Ventures, and Standard Charter.  

**Power might be returned to the consumer**

Proponents say that blockchain could lead to a “decentralized Internet.” What that theoretically could mean is that the transactions associated with services and apps used by consumers could be recorded by computers not controlled by the companies offering those services. That could conceivably increase competition and presumably effectively enable consumer-owned data stemming from the use of those services.

**Example of Companies Active in the Blockchain Space**

RedHat, a global software open source software development company, notes the many use cases for blockchain such securities settlement, insurance policy/document management, public records, supply chain management, and patient records. RedHat focusses on providing open source products for the enterprise and cloud-based solutions. The company offers the Red Hat Open Shift Blockchain Initiative application platform that enables blockchain application and service developments from ISVs, Startups, Financial Services Firms, and Individual developers. RedHat also participates in the Hyperledger project. This project seeks “to create an open-source initiative to create an open, standardized, and enterprise-grade distributed ledger framework and code base to be used across industries.” The group recently released Hyperledger Fabric, which can be used to build blockchain apps.

Intuit, a major financial services firm, has been experimenting with blockchain since 2014. Intuit QuickBooks customers can send international payments via blockchain payment provider Veem as an alternative to traditional wire transfers. Intuit’s Peter Horadan says that the potential implications for tax professionals are extensive. Although there are significant obstacles the potential is large because if companies record transactions in a public blockchain, tax authorities would have real-time access to the ledgers. As a result, the delay between transactions and remittances could potentially be eliminated.

RELX, a data analytics, risk-solutions and publishing company, is active in this space. The firm announced on August 5, 2016 that it will integrate its anti-money laundering data into Elliptic’s Bitcoin transaction monitoring system. This is interesting because one of the criticisms of Bitcoin is that it enables criminal activity (Silk Road). The RELX product helps legitimate users of Bitcoin (which in turn is a blockchain technology) because they will be more confident in the legitimacy of the Bitcoin transactions in which they engage. LexisNexis Risk Solutions Senior Vice President of U.S. Commercial Markets and Global Market Development Thomas C. Brown says: “More banks, Fintech startups, payments companies and eCommerce businesses can further consider the usefulness of the permissionless blockchain because as of today they are able to deploy best-of-breed money laundering screening against Bitcoin.”
Thomson Reuters, which describes itself as the “answer company,” announced on June 14, 2017 that it was making “a smart oracle available in the blockchain ecosystem for lean experimentation purposes.” The oracle is called BlockOne IQ and enables Thomson Reuters customers that are developing blockchain proof of concepts to include market data within their applications with cryptographic proof that Thomson Reuters is the source. BlockOne IQ is currently compatible with Corda and Ethereum but will soon be available to Hyperledger and other technologies. The service will be released to R3 and Enterprise Ethereum Alliance members and will also be available to developers.

Google’s DeepMind is working with the UK’s National Health Service (NHS) to create a secure system for health data using blockchains. The idea is that each view of the data is recorded so unauthorized views can be prevented. This is still at the development stage and there is no reporting on when this initiative will go live.

Use Cases

The Chamber of Digital Commerce study - “Smart Contracts: 12 Use Cases for Business & Beyond” lists a number of varied “smart contract” use cases. Nick Szabo writes in the foreword that he conceived of smart contracts over 20 years ago and posits that “the humble vending machine is the original form of the smart contract.” Today’s smart contracts are typically deployed on a blockchain, but they do not have to be. The study then goes on to describe possible smart contracts for digital identity; records; securities; trade finance; derivatives; financial data recording; mortgages; land title recording; supply chains; auto insurance; clinical trials; and, cancer research. However, these still remain mostly possibilities. Work on trade finance is probably furthest along. The Chamber suggests that smart contracts may be developed most quickly for business uses involving insurance, escrow, and royalty distributions. But the Chamber acknowledges that contracts involving subjective judgment (and many do) will be more difficult to automate.

With respect to trade finance, Comerzbank AG, the Bank of Montreal, Erste Group Bank AG and Caixabank SA announced that they were joining UBS and IBM in the “Batavia” project, which is aimed at creating and using blockchain technology to conduct trade finance. The participants are working among themselves to use the IBM Blockchain Platform, which in turn is powered by the Hyperledger Fabric Blockchain framework. The idea is for Batavia to allow “transacting parties to view the progress of a shipment as it leaves the warehouse, is loaded onto a plane, truck or boat and arrives at the receiving port, automatically releasing payments incrementally along each step of the process.” There will be live pilot transactions starting in early 2018.

For another example of how so many different players view blockchain as an opportunity (but also a threat), the U.S. Postal Service Office of the Inspector General commissioned Swiss Economics (a consulting firm) to conduct a study on the technology and identify possible Postal Service blockchain opportunities. Swiss Economics suggests that the Postal Service could expand its international money transfer business through the creation of a blockchain-based “Postcoin” transactions system. This would require the cooperation of other national post offices as well. The USPS Office of the Inspector General says the Postal Service is also well placed to verify identities by using an ID card, a driver’s license or some sort of biometric ID such as a fingerprint and then link those identities within a blockchain to, for example, an individual’s mailing address. Postal Service customers could then use the verified identity to login into secure websites, notarize documents or participate in smart
contracts. The technology could conceivably be used to support the Postal Service’s passport application work for the Department of State. It is possible the technology could be used to help with making the Postal Service’s operations more efficient through device management, for instance by making it possible to predict postal vehicles’ maintenance needs. Maybe the most exciting potential use for the Postal Service is the potential for using blockchain to make supply chain management by using blockchains to verify actions taken by Postal Service partners such as other post offices, customs agencies, shipping partners, contractors, long-haul trucking drivers etc.  

There is substantial discussion on how blockchains might be helpful in the health sector. Broadly speaking, blockchain-related use cases fall into five main categories: Clinical Health Data Exchange and Interoperability; Claims Adjudication and Billing Management; Drug Supply Chain Integrity and Provenance; Pharma Clinical Trials and Population Health Research; and, Cyber Security and Healthcare IoT.  Becker’s Hospital Review recently published a list of 25+ companies in healthcare to know with a description of the services they provide. Essentially, they are all active in the categories mentioned above. But the reality is that the potential for blockchain to make healthcare more efficient, safe, and or secure will require a great deal of experimentation and investment. As Mike Orcutt puts it: “Technologists and health-care professionals around the globe see blockchain technology as a way to streamline the share of medical records in a secure way, protect sensitive data from hackers, and give patients more control over their information. But before an industry-wide revolution in medical records is possible, a new technical infrastructure – a custom-built ‘health-care blockchain” – must be constructed.” This is likely several years away.

There are intriguing possible uses in education as well. Some of these uses could be highly disruptive, although it is too soon to say whether the blockchain truly will “change the relationships among colleges and universities and, in turn, their relationship to society.” But it is possible and even likely that blockchain applications for identity and student records; new pedagogies (customized teaching); costs; and, new models for higher education will be developed. To take just one example, why should institutions charge for providing degree validations? If qualifications were listed on a secure blockchain, they could be easier and cheaper to access for students.

Public Policy Issues

Regulation

People are asking many questions about blockchain and regulation. How do you regulate permissionless blockchains controlled by technical software code organized by developers working in an open source setting? Are permissioned blockchains fundamentally different because they have a proprietor? What is desirable in this context? Light touch regulation? Regulatory “sandboxes,” i.e. jurisdictions where companies can experiment at a small scale relatively free from regulation? Would more detailed approaches be appropriate, for instance New York State’s BitLicense? Is it appropriate at all to talk about regulation of blockchain? After all, blockchains are fundamentally a kind of software. Software per se is not regulated. Moreover, public policy is fundamentally concerned about outcomes, for instance with respect to anti-money laundering laws, not necessarily what kind of software is used to process a payments transaction.

One way to think about the issue is to what entity would regulation be directed to? In a permissionless system such as Bitcoin, who is responsible for complying with financial regulation? The UK
Government Chief Science Advisor notes that with respect to Bitcoin, regulators have focused on “regulating the businesses that deal with Bitcoin, such as exchanges and wallet providers.” What this means is that the wallet provider can be prevented from stealing customers’ money or ensuring indirectly that the blockchain is not used to launder money. Recently, the Chinese government’s decision to move against Bitcoin has received considerable press. But it is worth noting that the government is reportedly not shutting down Bitcoin per se but is rather considering whether to shut down domestic Bitcoin exchanges such as Bitfinex, OkCoin, and TCC. It some sense this is a distinction without meaning, but it is worth noting that the Chinese authorities had to act this way because as Sergii Shcherbak puts it: “Bitcoin can neither be classified as a credit institution nor an e-money institution, as Bitcoin is not a legal entity.” (Note: Bitcoin has generated a tremendous amount of press recently because the price has risen 600% over the last 12 months. However, at least one observer believes that the price will collapse, but that the technology underpinning Bitcoin will thrive.)

Should regulators determine that they need to intervene directly with respect to the technical code underpinning a blockchain, there are precedents from the Internet for the public sector to engage in developing protocols. For example, Internet (TCP/IP) and the HTTP World Wide Web standards emerged from the public sector. It is not clear, however, whether this precedent is replicable or indeed even desirable with respect to blockchain given IPR and business confidentiality concerns. However, it is one option among others, to ensure that laws and regulations are respected.

In this context, it is worth noting that regulatory technology, otherwise known as “RegTech,” has the potential to assist, rather than hinder regulators. If a regulator can “see” all the transactions in a network in real time, that could potentially be of use to financial institutions and their regulators in complying with disclosure requirements such know your customer (KYC) and anti-money laundering (AML). Nitin Gaur, Director at IBM Blockchain Labs, argues that blockchain can make a significant contribution in this regard.

Sometimes the question of whether blockchains should be regulated gets conflated with the debate in the United States as to how or whether Fintech companies should be regulated. The Office of the Comptroller of the Currency (OCC) is currently determining whether there should be a possibility of OCC offering special purpose national bank charters for Fintech companies. The OCC is also somewhat open to experiments along regulatory sandbox lines, but has said that “any program we pursue will be voluntary for banks and cannot provide a safe harbor from many compliance requirements.” In contrast, the UK’s Financial Conduct Authority (FCA) appears to be further along in this regard and announced on June 15, 2017 the names of 24 companies that have been accepted for the “Cohort 2” sandbox.

Private blockchains have a proprietor, which makes it easier for regulators. For instance, the R3 Consortium is producing a blockchain platform called Corda. The Consortium itself can be regulated and/or the companies and institutions that make up the Consortium. The UK Science Advisor analogizes private blockchains to conventional private financial networks such as the Visa Core Rules and suggests that they are not very different from software-as-a-service (SaaS) systems. This seems like a reasonable analogy, which suggests that there may be relevant recommendations for policymakers that can be derived from SIIA’s 2011 White Paper on Cloud Computing. As that paper notes, SaaS is one of three cloud computing service delivery models.
SIIA’s long-standing view is that regulation should be technology neutral so blockchain-specific regulation is likely not desirable and could be counter-productive even if regulation is motivated by a desire to stimulate blockchain innovation. This seems to be a widespread view with respect to the Bitlicense offered by New York’s Department of Financial Services. The 44-page regulation appears to have generated excessive legal fees to obtain the license with the result that a number of virtual currency companies have decided to establish themselves outside New York.

Regulatory Access to Source Code

The Chamber of Digital Commerce suggests that in some cases regulators “may demand a peek behind the proverbial curtain and a deep look into the source code of the proffered ledger-hosted contract.” This is a real possibility. The U.S. Commodities Futures Trading Commission (CFTC) proposed in 2015 a rule that would have given it access to source code. The proposal is known as “Regulation AT.” SIIA joined with a number of other trade association in a June 24, 2016 letter opposing the provision. Public policy issues identified by SIIA and other participating trade associations included the due process rights of rightsholders, the possibility of “copycat” measures from other countries; and, the possibility of cyberattacks against government-mandated data repositories. Regulatory access to algorithms is not needed for validation purposes or for assessing compliance with regulatory requirements such as conformity to fair lending laws. Proposed legislation would require independent court review (due process) before granting regulatory access to proprietary algorithms in extraordinary circumstances.

SIIA further explored this issue in an Issue Brief on Algorithmic Fairness. Besides the proprietary nature of algorithms, SIIA notes that divulging the formula publicly could allow outside parties to defeat the purpose of legitimate programs, for instance in selecting who to audit for taxes or who to choose for terrorist screening. There is also the possibility that source code disclosure could make it easier for hackers to game the system, thereby creating security risks. In the credit scoring context, at least one company uses trade secrets to protect its algorithms. The company patents certain functionality in their software but not all of it as that would require disclosing too much source code. The company is committed to developing explainable algorithms. This seems to strike the right balance between letting companies choose what makes sense from a business development perspective: seeking a patent that provides for exclusive use for a limited time but requires disclosure (including of source code) or using trade secret protection. At the same time, the company is committed to developing explainable algorithms, which is consistent with SIIA’s position that it is reasonable for companies to provide a “narrative” of what underlies their algorithms.

Governance

Governance is distinct from regulation in that it essentially deals with the development of the software underlying the development of the blockchain. Private blockchains are relatively straightforward in this regard as their proprietors, usually companies, develop them.

Public blockchains, however, are different. The protocols governing Bitcoin were developed collaboratively among several coders. These include Satoshi Nakamoto (he might be a pseudonym or actually several coders), Jeff Garzik, Gavin Andresen, Mike Hearn, Vinnie Falco, Wladimir J. van der, and Peter Wuille, and likely others. This reportedly worked well for a number of years. However, as Bitcoin has scaled up, disagreements have emerged and Bitcoin is now reportedly splitting in two. The disagreement has to do with whether to create larger blocks in the chains. Creating larger blocks speeds up transaction time. However, it would put greater stress on the “miners” that use
computers to verify transactions in exchange for Bitcoins. That would likely mean that larger companies would take a greater share of the mining business, which Bitcoin purists consider contrary to the more distributed vision they have for Bitcoin. Whatever the merits of the argument, it illustrates that a blockchain is not an end in itself. It is a piece of software designed to accomplish a business process or government function.

For those who support unpermissioned public blockchains with strong peer-to-peer characteristics, the Internet governance model is potentially attractive. The World Economic Forum (WEF) released a White Paper in June 2017 entitled “Realizing the Potential of Blockchain: A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies.” 70 White Paper authors Don Tapscott and Alex Tapscott suggest that in order for Blockchain to thrive, it could benefit from replicating where possible the multistakeholder approach to Internet governance. The WEF describes the players in the blockchain ecosystem as blockchain innovators, venture capitalists, banks/financial services companies, coders/developers, academics, NGOs, governments/regulators/law enforcement, and users. 71

The key problem is how to get these players to work with each other. How can incentives be created for collaboration? The WEF advocates for the creation of “Global Solution Networks (GSNs). There are different kinds of networks organized around knowledge, policy, advocacy, operations/delivery, networked institutions, global standards, and watchdogs. The WEF is likely correct in arguing that standards development is probably the most urgent task facing blockchain. 72 From a public policy perspective, one way government and regulators can help would be to permit as much regulatory flexibility as possible in order to incentivize players to work together. It is questionable, however, just how deep this multistakeholder approach to blockchain development will be. It is true that the Internet governance model has been many years in the making. However, there was and is an external driver in incentivizing workable Internet governance: the threat that if the model does not work, the Internet could be placed under United Nations control. This external driver is not present (and should not be) with respect to blockchain. Moreover, the multistakeholder Internet governance model does not mean that governments are absent. They are very much present and influential both formally through the Internet Corporation for Assigned Names and Numbers’ (ICANN) Governmental Advisory Committee (GAC) and informally.

Data Privacy

It is at least superficially puzzling as to why this technology gives rise to privacy concerns. After all, as Iansiti and Lakhani write, principle number three on how blockchain works is yes, transparency, but with pseudonymity as well. They say: “Users can choose to remain anonymous or provide proof of their identity to others.” 73 However, there are skeptics regarding whether privacy can really be safeguarded in public blockchains. As Cade Metz writes in the context of using blockchains to register stock market transactions: “Researchers have shown that even if you hide behind anonymous addresses, there are ways of determining who you are.” 74 The current consensus seems to be that private blockchains can accommodate privacy concerns better because the proprietors determine who can “see” a given transaction(s).

A clear description of how to manage privacy in public and private blockchains can be found in a White Paper put out by Baker McKenzie. 75 The reality is, as indicated earlier, public and private blockchains are very different in this regard, especially from a legal and compliance perspective. As Baker McKenzie notes, the two existing notable public blockchains that currently exist – Bitcoin and
Ethereum – operate in a way that is not fully compatible with the needs of the regulated financial industry. Because each computer on the Bitcoin and Etherium networks receives a record of every single transaction, every participant in the blockchain can “see” the transaction. This is a problem with respect to data privacy.

Baker McKenzie posits that the next generation of distributed ledgers for the financial industry will not be, strictly speaking, blockchains. Instead, they will be “inspired by blockchains, but solve for the privacy and scalability needs of the industry.” So, whereas in the past, financial industry services parties each maintained their own records, with a distributed ledger, they essentially operate shared records. But those records are shared only among the relevant parties, not the public at large, on a need-to-know basis. Baker McKenzie puts it in the following way.

With broadcast blockchains, all data including commercially sensitive data (e.g., prices) and data the dissemination of which is restricted by regulation (e.g., personally identifying) is passed to all participants in whichever jurisdiction their servers are held. This has legal implications: How can a system that broadly distributes personal information comply with laws prohibiting dissemination of personal information? Who is liable if your server suddenly has data on it that is prohibited by regulation from being there, sent by someone else?

Private distributed ledgers run by known participants will be subject to contractual agreements such as service level agreements and limitations of liability, so the existing legal framework can be referred to when there are issues.

Another technical way of looking at this is that in public blockchains, each “node,” (i.e. computer broadcasting messages) handles the data it receives as a fully autonomous operator. What that means from a legal perspective is that each node (there is a person or company running each node) has a compliance obligation. In contrast, in a distributed ledger or private blockchain, each node receives only the data that is relevant to it. This has two practical implications. First, fewer parties have compliance responsibilities. Second, regulators and consumers have identifiable parties they can deal with.

It is also worth mentioning in this context the General Data Protection Regulation’s (GDPR) “right to be forgotten.” After all, one of the main characteristics of a blockchain is that each transaction is “immutable.” The idea is that each transaction or “block” registered on a chain can never be changed. With respect to public blockchains, this is possible but technically complex and likely expensive. This is another reason that the use of public blockchains could be quite limited. Baker McKenzie says that “because permissioned DLT systems involve known and trusted parties, historical entries can be amended provided the required number of parties agrees to an erasure.”

Cybersecurity

The jury appears to still be out regarding whether blockchains will prove to be a net benefit for cybersecurity. The consensus seems to be that the technology is promising in this regard. However, as Deloitte’s Cillian Leonowicz puts it: “blockchain’s characteristics do not provide an impenetrable
panacea to all cyber ills, to think the same would be naïve at best, instead of as with other technologies blockchain implementations and roll outs must include typical systems and network cyber security controls, due diligence, practice and procedures.”  

And again, the reality is that the security challenges faced by public (unpermissioned) blockchains are not the same as those faced by private (permissioned) blockchains. As the British Science Advisor puts it: “The security advantages of the decentralized systems identified above – specifically, resilience and robustness – only apply completely to unpermissioned ledgers that subscribe to a global trust theory. For permissioned ledgers, or examples with other centralized functions, there will be less resilience and robustness, but a better ability to assure central trust and/or functions.”

Blockchain technologies or technologies that mimic aspects of blockchain can be used to enhance cybersecurity. Google does this through its Certificate Transparency (CT) system which uses a distributed ledger that allows users to determine that the certificate they use is, in fact, in the ledger and correctly issued. This helps address the problem that while browsers are quite good at detecting forged or false SSL certificates, they are not good at detecting mistakenly issued certificates. This could make a contribution to increasing confidence in the Public Key Infrastructure (PKI) that establishes that “a public key belongs to a service that a user wishes to use.”

The National Institute of Standards (NIST) is looking at how fundamental blockchain features and resource requirements relate to the Internet of Things (IOT), i.e. proof of work. The European Union Agency for Network and Information Security (ENISA) has released a report on Distributed Ledger Technology & Cybersecurity. The report is focused on the financial sector. The document is worth reading because it describes that while blockchain technology can help with cybersecurity, many, if not most, of the best practices cybersecurity professionals should practice remain relevant. ENISA identifies “traditional challenges” as key management, privacy, and code review. ENISA considers “technology specific challenges” to be using recovery keys, using multiple signatures for authorizing and processing transactions, and using a library of standardized smart contracts. The Agency says that there are “challenges that may require further development” such as anti-money and anti-fraud tools, interoperability of blockchain protocols, and legal provisions and tools for implementing privacy and the right to be forgotten.

Energy Use

One of the lesser known attributes of the Bitcoin operation is that it is very energy-intensive. This is because of the distributed nature of Bitcoin with every transaction being recorded in perhaps thousands of different accounting ledgers. Each of these transactions is verified by what is known as a “miner.” Miners (actually computers) analyze information on the ledger (which is list of blocks) to create a shorter “hash” that can be described as a digital wax seal. Miners compete with each other to create this seal, which is the last entry on a block. In return for creating this digital seal, miners receive Bitcoins. This works in the Bitcoin context, but it is very energy intensive. The Digiconomist blog explores energy consumption for Bitcoin and Bitcoin cash. The numbers (and these are borne out by other research as well) are striking. Bitcoin and Bitcoin cash consume electricity equivalent to Syria’s consumption. If Bitcoin were a country, it would rank 71 among countries in terms of consumption. Maybe the most relevant statistical comparison is that Bitcoin’s energy consumption is higher by orders of magnitude than Visa’s payment operation even though Visa processes many more transactions. There is speculation that algorithms based on “proof-of-stake,” rather than the current “proof-of work,” could reduce consumption, but this is not proved yet. Private blockchains where
transactions are verified by the proprietor are more energy efficient so that is another reason for why private blockchains may, at least in the short run, become more prevalent than public blockchains.

The question of the energy consumption by existing blockchain applications is different from the conversation of how blockchain could make energy consumption more efficient and benefit consumers. There is quite a bit of discussion on this topic, but it is speculative for now. 89

**Intellectual Property Rights (IPR) Considerations**

As with energy and other sectors, there is an extensive conversation on how blockchains might affect IPRs. The general sense is that blockchains have the potential to help rightsholders. Managing Intellectual Property recently put out a piece on how blockchains could help the fashion industry and other IP-intensive industries. Blockchains could be used for record-keeping; to register and clear IP rights; to control and track the distribution of (un-) registered IP rights; to provide evidence of first use in commerce/trade and/or (genuine) use of a trade mark; to establish and enforce IP contracts, licenses through smart contracts; to transmit payments in real-time to IP owners; for authentication: detection and retrieval of stolen goods; detection of grey or parallel imported goods; and, enforcements of exclusive distribution networks. 90 Similar arguments are made for the music industry. 91

With respect to what IP rules and regulations work best to develop the blockchain industry, there is not yet a lot of research, although current law in the United States and elsewhere appears to be working. Blockchains are being developed primarily through a mix of open source and patent-based models. The software underlying Bitcoin was developed through an open source model. The law firm, Marshall IP Gerstein has developed information on IP Considerations for Blockchain Technology in the United States. 92 In the United States, there are 250 blockchain-related patents, 1,592 published patent applications, and 1,843 total filings. 93 Most of the patents are related to the financial industry, which is logical given that blockchain applications have so far been concentrated in the financial sector. So far, no patent infringement suits related to blockchain have been filed. It appears that patent filers have been able to describe the real-world problem they are solving in order to obtain a patent. And companies use both patents and open source models. For example, IBM has filed for blockchain-related patents. But it also contributes to the Linux Foundation’s Hyperledger Project through a modular-based protocol for recording and accessing transactions on a private ledger, which is called “Open Blockchain.” 94 The idea behind the Project is for developers to work together to create new blockchain applications in an open source fashion. 95

**Regulatory Technology (“RegTech”)**

RegTech encompasses a variety of technologies, not just blockchain. Besides blockchain, RegTech means machine learning, robotics, artificial intelligence, cryptography, biometrics, application programming interfaces (APIs), and shared utility functions and cloud applications. 96 Blockchains could “give regulators direct, instant, and full transparency.” 97 This could be quite useful with respect to anti-money laundering, tax compliance, and other activities. There are technical hurdles such as current blockchain applications’ limited scalability and speed of execution. 98 Private blockchains can accommodate privacy concerns because they limit the number of entities that can “see” individual transactions. However, there are still impediments to the sharing and use of data for regulatory purposes, which IIF suggests should be removed. 99 Effective use of RegTech (and other technologies such as those mentioned above) presuppose a privacy assessment to ensure that the collection and
analysis is consistent with privacy laws. This is a complex undertaking given that cross-border data flows are typically involved and those flows cross borders with different laws. The IIF suggests therefore that the RegTech market requires collaboration between “unlikely partners” such as regulators and regulatory experts, technology and software developers, and entrepreneurs willing to invest.

The IIF further explores the ideas discussed above in another report on deploying RegTech against financial crime. It suggests closing gaps in the AML/CFT framework; improving data quality and data sharing policy; creating a proper environment for RegTech experimentation; allowing shared utilities to be able to carry responsibility and liability (banks report that currently know your customer utilities are of limited use to them because banks remain liable); making regulation and supervision resilient to continuous technological innovation (focus regulation on the activity, not the technology); and, changing supervisory focus as automation alters the nature of risk in the financial sector.

The Atlantic Council, City UK, and Thomson Reuters discuss similar recommendations in its “The Danger of Divergence” report. Perhaps the most important recommendation there is to make the G20 the preeminent body for coordination on financial regulation. The G7 could also play an important role.

Jeff Bandman notes in testimony before the Securities and Exchange Commission (SEC) that regulators may well be among the biggest users of distributed ledger technology. But there are sometimes obstacles (procurement and ethics rules) that stand in the way of regulators making full use of RegTech solutions. He therefore proposes a “Sandbox for Regulators,” which does appear to be worth considering. The “Sandbox for Regulators” would allow regulators to use blockchains themselves in a limited way without applying the full procurement and ethics rules. Bandman suggests that a simple solution might be to establish de minimis dollar threshold limits that would allow regulators to implement small scale experimental FinTech and RegTech procurements outside of existing procedures. He is careful to say that he is “definitely not advocating a carte blanche exception to either procurement or ethics rules.”

Recommendations for Policymakers

Blockchain is a promising technology but not so different from cloud computing, artificial intelligence, the Internet of Things and other digital technologies so as to merit its own distinct policy approach. SIIA’s recommendations are consistent with previous recommendations on cloud computing, data-driven innovation, the Internet of Things, artificial intelligence and the future of work, algorithmic fairness, and principles for ethical data use. See below for suggestions that could assist in providing an enabling environment for this promising technology.

1. Maintain a technologically neutral stance to blockchain while at the same time remain open to the potential inherent in blockchain and other digital technologies.
2. Regulators should allow space for experimentation. Specifically, the OCC should consider the regulatory sandbox approach adopted by the British FCA and Singapore’s financial authorities.
3. Consider “Sandboxes for Regulators.”
4. Privacy and Financial regulators should engage in a dialogue to ensure that regtech’s potential to assist with regulatory compliance is combined with appropriate privacy safeguards.
5. Privacy regulators should work with industry in crafting guidance on how to realize the potential of blockchains, while at the same time complying with privacy legislation.

6. Given that blockchains are inherently international, include cross-border data flow obligations and prohibitions against data server localization in trade agreements.

7. Promote international interoperability agreements such as the APEC Cross-Border Privacy Rules and EU-U.S. Privacy Shield.

8. The general respect for intellectual property rights in the blockchain space should be extended to source code, often a critical trade secret. Public disclosure of source code should not be required. Regulators should have access only under extraordinary circumstances and subject to independent court review. In any event, blockchain software should not be treated differently from other software. Countries should commit to these ideas in trade agreements.

9. Ensure that electronic authentication and signatures commitments in trade agreements include blockchain applications.

10. Promote open and industry-driven software and data interoperability standards.

11. Strive for global stakeholder-shaped approaches to cybersecurity and explore how blockchains could improve cybersecurity.

12. To the extent policymakers consider the promotion of blockchain solutions to be beneficial, they should also promote cloud computing as cloud computing underpins many blockchain applications.

13. Besides trade fora, because the G20 is relatively small yet includes the world’s most important economies, the forum should be used to promote regulatory cooperation to enable technological innovation, including in the blockchain space. The G7 countries could perhaps encourage the G20 to work on this matter.
Endnotes

2 IMF Staff Discussion Note, “Fintech and Financial Services: Initial Considerations,” June 2017, page 5
   https://hbr.org/2017/01/the-truth-about-blockchain
4 Harvard Business Review Article, pages 2-3
5 Bitcoin wiki
   https://en.bitcoin.it/wiki/Mining
6 Bitcoin glossary consensus
   https://bitcoin.org/en/glossary/consensus
8 UK Government Science Report, page 17
9 UK Government Science Report, page 17
10 Entrepreneur, “Just What the Heck is Blockchain? Watch this Explainer Video,” Rob Marvin, September 19, 2017
   https://www.entrepreneur.com/article/300555
14 Quartz, “The lives of bitcoin miners digging for digital gold in Inner Mongolia,” Zheping Huang & Joon Ian Wong, August 17, 2017
15 Bitcoin: A Peer-to-Peer Electronic Cash System,” Satoshi Nakamoto, satoshi@gmx.com, www.bitcoin.org
   https://bitcoin.org/bitcoin.pdf
16 Nakamoto White Paper, Abstract, page 1
   https://www.pcmag.com/article/351486/
19 Quartz, “The $65 million Bitfinex hack shows that it is impossible to tell a good bitcoin company from a bad one,” Josh Horwitz, August 9, 2016
20 Quartz, “A coding error led to $30 million in Ethereum being stolen,” Joon Ian Wong, Uly 20, 2017


https://www.pcmag.com/article/351486/blockchain-the-invisible-technology-thats-changing-the-world

23 Nakamoto White Paper, page 6


26 CNBC, “Blockchain technology is moving into the financial mainstream with IBM and seven European banks, Arjun Kharpal, June 26, 2017

27 R3 Website
https://www.r3.com/about/

28 Ripple Website
https://ripple.com/company/

29 Marvin video

30 Red Hat, Open Shift Blockchain Initiative, page 2
https://blog.openshift.com/blockchain-work-openshift/


32 Hyperledger Fabric Website

33 Coindesk, Wolfie Zhao, “Blockchain Payments Startup Veem Integrates with Intuit QuickBooks,” June 27, 2017
https://www.coindesk.com/blockchain-payments-startup-veem-integrates-intuit-quickbooks/


36 Thomson Reuters Press Releases, “Thomson Reuters Releases BlockOneIQ into Blockchain Developer Community,” June 14, 2017

37 Wired, Cade Metz, “Google Deepminds: Untrendy Play to Make the Blockchain Actually Useful,” March 11, 2017
https://www.wired.com/2017/03/google-deepminds-untrendy-blockchain-play-make-actually-useful/


39 Chamber Smart Contracts Study, page 3
40 Chamber Smart Contracts Study, page 10
41 Chamber Smart Contracts Study, page 43
42 IBM News Release, “Bank of Montreal, CaixaBank, Comerzbank, Erste Group, IBM and UBS Collaborate to Advance an Open Blockchain-based Trade Finance Platform, October 4, 2017
44 Forbes, “Does Blockchain Have a Place in Healthcare?,” Reenita Das, May 8, 2017
https://www.forbes.com/sites/reenitadas/2017/05/08/does-blockchain-have-a-place-in-healthcare/#728939f01c31
45 Becker’s Hospital Review, “25+ Blockchain Companies in Healthcare to know,” Laura Dyrda, August 17, 2017
46 MIT Technology Review, “Who Will Build the Health-Care Blockchain?,” Mike Orcutt, September 15, 2017
47 Educausereview, Don Tapscott and Alex Tapscott, “The Blockchain Revolution and Higher Education,” March 13, 2017
48 Educausereview, page 2
49 UK Science Office Report, page 44
50 “China is shutting down domestic Bitcoin exchanges: Beijing is increasingly hostile to Bitcoin,” The Verge, Shannon Liao, September 11, 2017
51 European Journal of Legal Studies, Volume 7, No. 1, Sergii Shcherbak, “How Should Bitcoin be Regulated?,” page 55
http://cadmus.eui.eu/handle/1814/32273
52 Project Syndicate, Crypto-Fool’s Gold?,” Kenneth Rogoff, October 9, 2017
53 UK Science Office Report, page 45
54 “Blockchain for Enterprise – Focus on KYC, AML, and Regulatory Compliance – Are We Calling it RegTech?,” Nitin Gaur, Director at IBM Blockchain Labs
http://infocastinc.com/insights/technology/blockchain-for-enterprise-focus-on-kyc-aml-and-regulatory-compliance-are-we-calling-it-regtech/
56 See FCA Website
57 See R3 website
https://www.r3.com/about/
58 UK Science Office Report, page 44
https://www.siia.net/Admin/FileManagement.aspx/LinkClick.aspx?fileticket=PJv7cHdxGTw%3D&portalid=0
61 New York State, Department of Financial Services, Title 23. Department of Financial Services, Chapter I. Regulations of the Superintendent of Financial Services, Part 200. Virtual Currencies.
62 Chamber Smart Contracts Study, page 49
64 Multi-Trade Association Letter to Secretary of the Commodities Futures Trading Commission Christopher Kirkpatrick, June 24, 2016
http://www.siia.net/Portals/0/pdf/Policy/Algorithmic%20Fairness%20Issue%20Brief.pdf
67 SIIA Issue Brief, Algorithmic Fairness, September 22, 2016, page 13
http://www.siia.net/Portals/0/pdf/Policy/Algorithmic%20Fairness%20Issue%20Brief.pdf
68 UK Science Advisor Report, page 43
70 World Economic Forum, White Paper, Don Tapscott and Alex Tapscott, “Realizing the Potential of Blockchain: A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies,” June 2017
71 WEF Report, pages 26-27
72 WEF Report, page 29
73 Harvard Business Review article, page 2
74 Wired, “Bitcoin May Never Make it to Wall Street, but its Tech Will,” Cade Metz, May 12, 2015
https://www.wired.com/2015/05/nasdaq-bringing-bitcoin-closer-stock-market/
76 Baker McKenzie White Paper, page 5
77 Baker McKenzie White Paper, page 6
78 Baker McKenzie White Paper, page 12
79 Baker McKenzie White Paper, page 18
80 Lexology, CMS Cameron McKenna Nabarro Olswang LLP, “Data Protection Aspects of Blockchain,” September 1, 2017
https://www.lexology.com/library/detail.aspx?g=329a9745-885e-4621-8c99-af5e81e81e41
https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf
82 UK Science Office Report, page 48
83 See the Certificate Transfer website.
https://www.certificate-transparency.org/what-is-ct
84 UK Science Office Report, page 47
85 See NIST website.
https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot
https://www.coindesk.com/information/how-bitcoin-mining-works/
88 Digiconomist, Bitcoin Energy Consumption Index, consulted on October 3, 2017 (the index is updated periodically)
https://digiconomist.net/bitcoin-energy-consumption


https://hbr.org/2017/06/blockchain-could-help-musicians-make-money-again


https://www.slideshare.net/NelsonRosario2/ip-considerations-for-blockchain-technology

93 Marshall Gerstein Slide Presentation, slide 22

94 Open Blockchain, IBM


95 There are 150-plus members of Hyperledger. See below for a list of members.

https://www.hyperledger.org/members

96 Institute of International Finance (IIF), “Regtech in Financial Services: Technology Solutions for Compliance and Reporting, March 2016, pages 3-4


97 IIF Report, page 12

98 American Banker, “Can blockchain tech really unclog the capital markets?” Glen Fest, February 24, 2016


99 IIF Report, page 4


http://www.atlanticcouncil.org/images/publications/Big_Data_A_Twenty-First_Century_Arms_Race_web_0627.pdf

101 IIF Report, page 5


104 Written Testimony of Jeff Bandman, Principal, Bandman Advisors, Securities and Exchange Commission, Investor Advisory Committee, October 12, 2017, page 7


105 Bandman Testimony, page 10


https://www.siia.net/Admin/FileManagement.aspx?LinkClick.aspx?fileticket=PJv7cHdxGTw%3D&portalid=0


https://www.siia.net/Portals/0/pdf/Policy/Reports/Empowering%20the%20Internet%20of%20Things.pdf


http://www.siia.net/Portals/0/pdf/Policy/Artificial%20Intelligence%20and%20the%20Future%20of%20Work%20SIIA%20Issue%20Brief.pdf


http://www.siia.net/Portals/0/pdf/Policy/Algorithmic%20Fairness%20Issue%20Brief.pdf

111 SIIA Issue Brief, “Principles for Ethical Data Use,” September 15, 2017

http://www.siia.net/blog/index/Post/73551/SIIA-Releases-Issue-Brief-on-Ethical-Use-of-Big-Data-and-Artificial-Intelligence