Blockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows

Stan Sater
November 6, 2017

Abstract

Future economic growth is dependent on global data sharing. With the EU's GDPR going into effect May 25, 2018, data privacy law in the EU will be uniform in text. The GDPR applies extraterritorially to any organization that can reach the EU market in terms of access by an EU citizen. While a consistent and coordinated interpretation of the GDPR provides organizations with the requisite assurances needed when operating in an international environment, stricter standards and higher fines require the organizations to rethink their international privacy compliance protocols. Trust-failures in society are the driving force behind such comprehensive regulatory frameworks, but emerging technology like blockchain can aid in minimizing these privacy concerns. Among other things, blockchain properties include decentralization, authentication, confidentiality, accountability, and access control management. By treating data flows as transactions, blockchain applications can work with regulations to facilitate the secure transfer of information. The purpose of this paper is to begin a conversation around utilizing blockchain technology and reducing harmonizing regulations like the GDPR to an automated protocol.

Table of Contents

I. Introduction 2
II. International Data Laws 4
A. The EU General Data Protection Regulation 4
1. General Provisions and Principles 5
2. Rights of the Data Subjects 7
3. Data Controllers and Processors 8
4. Cross-Border Data Transfers 11
B. EU-U.S. Privacy Shield Framework 13
C. APEC Privacy Framework 15
D. BRICS 16
III. Blockchain 19
A. Ethereum 22
1. Smart Contracts 23
2. Metropolis 24
3. Merkel Trees and Pruning 25
4. Enterprise Ethereum Alliance 26
B. Linux's Hyperledger 27
IV. Blockchain Data Transfer Framework 29
V. Conclusion 38

I. Introduction

In an Internet-connected world, data is essential to the global economy.[1] While global trade in goods has leveled off and cross-border capital flows have sharply declined over the last decade, cross-border data flows have increased more dramatically than anticipated.[2] Based on the rapid adoption of new technologies, the use of data, when well managed, can change business models and improve efficiency. While existing economic activity and, to a significant degree, economic growth is dependent on data usage and sharing, some nations are enacting barriers to international data transfers.[3]

Serving as trade barriers, new data localization laws and strict regulations force companies to comply with costly requirements or face even more costly penalties. These high compliance standards particularly impact small firms looking for international growth more than large firms that can spread the costs over more revenue. Further, the nature of these regulations is subject to political uncertainty, and the regulations are often created without a full understanding of their actual impact on targeted markets and relevant processes. In combination, new regulations may in some cases have unintended consequences that alter market incentives and reduce overall efficiency. In the new, rapidly evolving data driven world, both the European Union's General Data Protection Regulation (GDPR) and the emergence of blockchain applications signal a significant change in the way personal data is managed and transferred across the world.

Part I of this paper summarizes and analyzes the current international legal and regulatory framework that serves to structure data flows in an orderly fashion but that may at the same time create significant hurdles to these international data flows. An understanding of the European Union's (EU) GDPR shows how pervasive the Brussels Effect has become.[4] Not only does the GDPR unify data protection regimes among its 28 Member State, but also it has identified 12 countries outside of the EU that have adequate levels of protection thus authorizing personal data transfers to and from them.[5] Additionally, the Asia-Pacific Economic Cooperation (APEC) is exploring methods for interoperability with the GDPR based on its existing Cross-Border

---

[1] JAMES MANYIKA ET AL., DIGITAL GLOBALIZATION: THE NEW ERA OF GLOBAL FLOWS, 1 (2016), http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows [hereinafter DIGITAL GLOBALIZATION].

[2] Sabine Bendiek, The New Global Economy Runs on Free Flow of Data and Trust, THE B20 (Feb. 24, 2017, 12:28 PM), http://www.b20germany.org/priorities/digitalization/digitalization-dossier/digitalization-article/news/the-new-global-economy-runs-on-free-flow-of-data-and-trust/.

[3] See DIGITAL GLOBALIZATION, supra note 1.

[4] See Joanne Scott, Extraterritoriality and Territorial Extension in EU Law, The American Journal of Comparative Law vol. 62, 87, 88 (2014).

[5] Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Advancement of Such Data, and repealing Directive 95/46/EC, 2016 O.J. L 119/1 [hereinafter GDPR]; see also Communication from the Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalised World, at 7, COM (2017) 7 final (Jan. 10, 2017) [hereinafter Exchanging and Protecting Personal Data] (listing the 12 countries approved by the EU as having adequate levels of data protection).

Privacy Rules (CBPR).[6] A harmonizing data protection framework that provides interoperability with other initiatives, including the EU-U.S. Privacy Shield Framework, is a step forward in creating a global governance structure for cross-border data flows. However, key countries like China, India, Russia, and Brazil are not yet a part of this framework. While this paper will mostly focus on the role of the GDPR, it will also briefly introduce the current data protection and data flow dynamics that exist in China, India, Russia, and Brazil.

Part II presents blockchain technology and explores the recent surge in blockchain initiatives. Blockchain technology provides decentralization, shared control, immutability, audit trails, data integrity, and secure asset exchanges. In effect, blockchain is data protection by design and by default. Therefore, blockchain offers significant promise to further unlock the value of globally transferable data. However, a traditional permissionless and publicly accessible blockchain, like Bitcoin, may not always be the most appropriate option for use by corporations because of the scalability issues, the lack of overall infrastructure controls, and the energy-intensive nature of proof of work.[7] Conversely, an entirely private blockchain, one that is not publicly viewable or accessible, is mostly a traditional system with cryptographic capabilities.[8] Because corporations require a hybrid of various configurations, this paper focuses on a consortium blockchain, which is a semi-trusted and permissioned blockchain that allows only an approved group of entities or individuals to create, view, and verify transactions.[9] This configuration is a superior option for organizational collaboration. The Enterprise Ethereum Alliance, which utilizes the Ethereum protocol, and Linux's Hyperledger Project are consortiums of multinational companies building industrial blockchain applications.[10] While Hyperledger is not a protocol like Ethereum, both consortiums share the goal of utilizing a community effort to produce interoperable and modular blockchain solutions across multiple industries.[11]

Part III of this paper seeks to demonstrate how the GDPR framework could be used with a consortium blockchain to enable secure, international data exchanges for enterprises. Corporate practices like outsourcing, freelancing, and unbundling are expected to continue and indeed grow highlighting the need for a technical framework that not only works but also reduces the cost of regulatory compliance. Internet connectivity has largely reduced costs of accessing information and establishing trust across a broad network. Because regulation is mostly a response to a range of perceived risk, the distributed ledger technology and cryptographic capabilities of blockchain can offer a reduction in those perceived risks.[12] The GDPR is the first regulatory framework to

---

[6] Data Privacy Subgroup Meeting with European Union, ASIA-PACIFIC ECONOMIC COOPERATION, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Data-Privacy-Subgroup-Meeting-with-European-Union (last visited Aug. 16, 2017).

[7] See Vitalik Buterin, On Public and Private Blockchains, ETHEREUM BLOG (Aug. 7, 2015), http://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

[8] Id.

[9] Id.

[10] Carlo R.W. De Meijer, Enterprise Ethereum Alliance: A Blockchain Challenger, FINEXTRA (May 15, 2017), http://www.finextra.com/blogposting/14085/enterprise-ethereum-alliance-a-blockchain-challenger.

[11] See id.

[12] The word "risk(s)" is used 75 time in the GDPR's 80 pages of text.

apply modern data protection effort to embed high levels of accountability as well as multiple lower barrier techniques to promote global interoperability. Once adoption of such standards reaches critical mass and different approaches to establishing security and trust have been studied through real-world experience, wide-ranging innovation through broad participation should be possible. This paper is meant to start a conversation around the establishment of a technical framework for data sharing that complies with a data regulatory framework designed to enable efficient data movement, while protecting in all cases a range of proprietary interests and, above all, data confidentiality.

II. International Data Laws

Companies seeking legal options to transfer data globally are met with complex and uncertain regulations. Recent massive data breach examples like Ashely-Madison and Equifax demonstrate that organizations cannot always be trusted to properly manage users' data and have forced regulators to react harshly.[13] The conclusion from many international regulators has been to enact a form of data localization to resolve privacy and cybersecurity issues.[14] The regulators miss the point that data security does not depend on location.[15] Rather, the new laws serve as trade barriers with greater impact on local economic growth than with respect to the protection it seeks to provide for personal data.[16] Going into effect on May 25, 2018, the EU's GDPR is the most promising global harmonizing framework for international data flows because it has an extraterritorial effect for those directly processing EU citizens' data.[17]

A. The EU General Data Protection Regulation

Regulation (EU) 2016/679, or GDPR, replaces the 1995 EU Data Protection Directive, both of which were enacted to provide a regulatory framework for the management of personal data.[18] In EU law, the difference between a directive and a regulation represents a fundamental change in the scope of the new law.[19] Base on the operation of the EU legal system, the previous "directive" resulted in the creation of multiple disparate data protection laws throughout the

---

[13] See Joshua Barajas, Lawmakers are Angry Over Equifax Data Breach. Where do We Go From Here, PBS (Sept. 26, 2017, 7:03 PM), http://www.pbs.org/newshour/updates/lawmakers-angry-equifaxs-massive-data-breach-go/; see also Charlie Osborne, Ashley Madison Hack: How Much User Data did "Paid Delete" Function Obliterate, ZDNET (Aug. 27, 2015, 2:50 PM), http://www.zdnet.com/article/ashley-madison-hack-how-much-user-data-did-paid-delete-function-obliterate/ (revealing that the data breach proved that Ashley Madison failed to delete user accounts even after users paid $19 for a delete account function).

[14] Nigel Cory, Cross Border Data Flows: Where are the Barriers, and What Do They Cost, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION, 4,8 (2017), http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.243328645.1221543554.1505516309-919574101.1504459156.

[15] Id. at 4.

[16] Id.

[17] See Scott, supra note 4, at 89.

[18] Francoise Gilbert, EU General Data Protection Regulation: What Impact for Businesses Established Outside the European Union, GREENBERG TRAURIG: INSIGHTS (Apr. 19, 2016), http://www.gtlaw.com/en/insights/2016/4/eu-general-data-protection-regulation-what-impact-for-businesses-establishe.

[19] Id.

EU.[20] By adopting a "regulation" on data protection that applies directly to each EU Member, individual Member States no longer need to enact a separate local law.[21] The GDPR makes clear that the EU's goal is to harmonize data protection across the Member States by setting consistent, binding rules across the EU for the protection of data as well as flexible standards to facilitate cross-border transfers of data.[22] The comprehensive nature of the GDPR is a significant move towards the EU's broader strategy of encouraging connectivity throughout a Digital Single Market, a market where digital trade occurs seamlessly.

1. General Provisions and Principles

Unquestionably, the GDPR represents a significant shift in the way that individual data is managed by providing data subjects with choice mechanisms and documenting data processing activities. The GDPR sets out principles that facilitate this shift as it specifically applies to the processing of personal data and the movement of such data by organizations operating within the EU.[23] The GDPR also extends to organizations outside of the EU that process personal data in relation to offering goods or services to EU citizens and/or monitor EU citizens' behaviors.[24] In effect, any company operating a website or mobile application that is accessible by EU citizens falls within the scope of the regulation.[25]

The GDPR applies to the processing of personal data.[26] The processing of such data can be considered in the context of six core privacy principles: (1) lawful, fair, and transparent in relation to the data subject; (2) purpose limitation; (3) data minimization; (4) accuracy; (5) storage limitation; and (6) integrity and confidentiality.[27] The principle of the lawful, fair, and transparent management of personal data relates to the data subject. Purpose limitation limits the collection of personal data to specified, explicit and legitimate purposes that the data subject has been made aware of, and the principle prohibits further processing without additional consent.[28] Data minimization limits the data to an amount that is adequate, relevant and limited to what is necessary for the purposes for which they are processed.[29] Additionally, data must be kept up to date and erased or rectified if inaccurate.[30] Entities must also delete data if its purpose has elapsed unless the data is processed for the purposes and under appropriate safeguards per Article 89(1) of the Regulation.[31] As to integrity and confidentiality, personal data processing must be protected against unauthorized or unlawful processing and accidental loss, destruction, or damage using appropriate technical or organizational measure."[32] Further, the data controller,

---

[20] Id.
[21] Id.
[22] Id.
[23] GDPR, supra note 5, at art. 1.
[24] Id. at art. 3.
[25] Id.
[26] Id. at art. 1(1). The GDPR does not apply to deceased persons and leaves the Member States to regulate the personal data of deceased persons. Id. at recital 27.
[27] GDPR, supra note 5, at art. 5(1).
[28] Id. at art. 5(1)(b).
[29] Id. at art. 5(1)(c).
[30] Id. at art. 5(1)(d).
[31] Id. at art. 5(1)(e).
[32] Id. at art. 5(1)(f).

the one who determines the purpose and means of the processing of the personal data, is accountable for complying with the six privacy principles.[33]

Mentioned with the principle of purpose limitation, the right to consent is one of the rights embedded in a data subject. The processing of personal data requires affirmative and unambiguous consent where "silence, pre-checked boxes, or inactivity" is inadequate.[34] When a data subject gives consent by electronic means, the consent request must be "clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."[35] Further, explicit consent is required to make decisions about the data subject "based solely on automated processing, including profiling."[36] Recital 32 of the Regulation provides for a way to obtain consent by "choosing technical settings for information society services."[37] While it has not yet been determined how this phrase will be interpreted, companies must nonetheless obtain opt-in consent rather than opt-out consent. As well, data subjects have the right to withdraw consent, and data controllers must make data subjects aware of this right before the subject gives consent.[38] Moreover, each data processing function requires its own consent.[39] However, separate consent is not needed if the new processing function is compatible with the original consent.[40] Regardless of the designated choice mechanism used to obtain consent, the process must be simplified in a way that demonstrates clear, affirmative, and unambiguous consent or potentially faces repercussions from data authorities.

As noted earlier, the GDPR places specific restrictions on subjecting data subjects to automated decision making as well as individually defines the terms "profiling" and "monitoring." Data processing is considered profiling if it involves automated processing of personal data and using that personal data to evaluate certain personal aspects related to a natural person.[41] Data subjects, though, do not have a right to avoid profiling but rather the right to avoid decision making solely based on automated means.[42] Therefore, there must be some form of human intervention in the data processing. Data subject "monitoring" is when individuals are "tracked on the Internet including potential subsequent use of data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes."[43] The differences in the definitions of the terms suggest that automated decision making or predicting the data subject's behaviors and preferences as forms of profiling are more worrisome from the regulator's viewpoint. This point is prevalent throughout the GDPR in the articles that relate to a data subject's rights and in particular the right to object. The data subject's rights though are not

---

[33] Id. at art. 5(2).
[34] Id. at recital 32.
[35] Id. at recital 32.
[36] Id. at art. 22.
[37] Id. at recital 32.
[38] Id. at art. 7(3).
[39] Id.
[40] Id. at art. 7.
[41] Id. at art. 4(4).
[42] Id. at art. 22(1).
[43] Id. at recital 24.

absolute. Only the right to object to direct marketing is absolute. The data controller may present a "compelling legitimate interest" to override the data subject's right.[44]

2. Rights of the Data Subjects

The GDPR creates new rights for the data subject as well as strengthens some rights that currently exist. The focus put on transparency and accountability about handling personal data puts the data subject's fundamental right to data privacy and protection at the heart of the new Regulation. Data controllers will need to consider the rights of the data subject to be in the best position to demonstrate compliance if a data subject chooses to exercise his rights. The rights afforded to the data subject are still open to some interpretation, and the scope of the restrictions/enforcement is yet to be determined.

It is not enough that data subjects have the right to object, rectify, and erase their data from data controllers, the data controllers must also communicate in a transparent manner with the data subjects about their processing activities. In reality, Article 12 of the Regulation is not very different from the Article 10 of the old Directive that needed to be implemented state by state. The information must be provided "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child."[45] To facilitate the exercise of the data subject's rights, controllers must establish mechanisms so that the data subject may make the proper requests and the controller can respond in a timely manner.[46] Before complying with a data subject's request, a controller may request proof of identification from the data subject.[47] While the "controller should use all reasonable measures to verify" a data subject's identity when access is requested, the controller is under no obligation to gather additional information to validate the identity of the data subject.[48] If the data controller cannot identify the data subject, the data controller is exempt from the application of Article 15-22.[49] However, the controller cannot refuse to accept additional information submitted by a data subject to facilitate the exercise of the data subject's rights.[50]

The core of this portion of the GDPR is that the data subject is entitled to a certain minimum amount of information concerning the use and management of the data subject's data. This minimum includes the right to know who the relevant controllers are as well as their location, the reasons for processing the data in question, and other information necessary to ensure the fair and transparent processing of the data.[51] This principle embodies the implied transparency requirement previously contained in the Directive.

As more data rights shift to the data subject, the data subject also has the right to rectify incorrect data, which includes completing incomplete data through a supplementary statement.[52] The data subject may restrict the processing of their personal data if they chose to contest the

---

[44] Id. at recital 69.
[45] Id. at art. 12(1).
[46] Id. at recital 59
[47] Id. at art. 12(2), (6).
[48] Id. at recital 57, 64.
[49] Id. recital 57; see also id. at art. 12(2) (stating the controller's obligations for identifying a data subject seeking to exercise their rights under Article 15-22).
[50] Id. at recital 57.
[51] Id. at art. 15.
[52] Id. at art. 16.

accuracy of the data, the processing is unlawful, the controller no longer needs the data for the initially stated purpose, or verification of overriding grounds is pending.[53] Additionally, the data subject has the right to know the third parties with their data and the third parties are to be informed when the data subject exercises one of their data rights.[54]

Further, the "right to erasure," commonly referred to as the "right to be forgotten," gives the data subject the authority to force the data controller to permanently erase any or all data held by the controller about the data subject.[55] The right to erasure includes when the data subject withdraws his consent, the data is unlawfully processed, or the data subject objects to the processing as stated in Article 21(1)(2). Article 21(1) allows the data subject the right to object to the processing of his personal data and requires the controller to provide "compelling legitimate grounds" to override the objection.[56] Additionally, the data subject can object to the processing of his data for direct marketing purposes.[57] If the data controller rectifies or erases personal data or restricts the processing of personal data, the data controller must notify those with access to the data and disclose those with access to the data to the data subject.[58] Along with the right to rectify and right to erasure, the data subject also has the "right of data portability."[59] This right allows a data subject to receive, move, and provide access to their personal data as they see fit.[60] While the right of data portability is a new right of the data subject, it is limited to situations when the processing was first based on the data subject's consent or by contract and not when there is a legal obligation by the controller that is in the public's interest.[61]

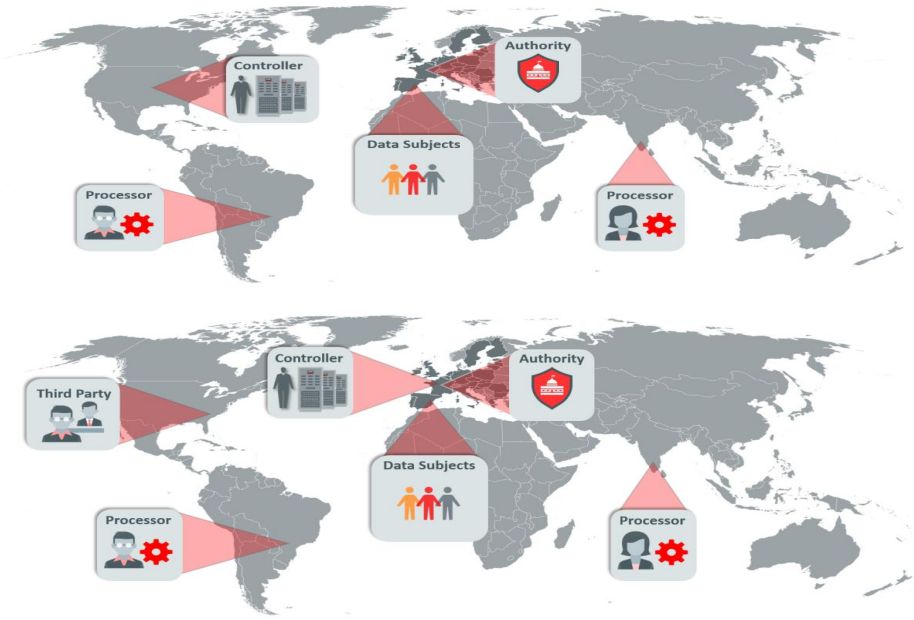
3. Data Controllers and Processors

The GDPR impacts all parties involved in the processing of personal data from the data creators to the data controllers to the downstream processors if the data controllers and the data processors are not the same entity.[62] Formally, a data controller is any person, entity, or group that determines the purposes and means of the processing of personal data.[63] A data processor is the person, entity, or group that processes the personal data on behalf of the controller.[64] Data processors can include a company's internal analysts, developers, or an outsourced processing company. Third parties are those who process data under the authority of the controller or processor.[65] The GDPR recognizes the fluidity of controllers also being processors as well as the

---

[53] Id. at art. 17.
[54] Id. at art. 19
[55] Id. at art. 17.
[56] Id. at art. 21(1).
[57] Id. at art. 21(2).
[58] Id. at art. 19.
[59] Id. at art. 20.
[60] Id. at art. 20.
[61] Id. at recital 68.
[62] Id. at art. 20.
[63] Id. at art. 4(7).
[64] Id. at art. 4(8).
[65] Id. at art. 4(10).

growth in outsourcing processing activities. In some cases, the below figures represent two plausible scenarios that are subject to the GDPR.[66]



The EU Data Protection Directive did not explicitly include privacy by design and default, but Article 8 of the European Convention on Human rights has come to include personal data privacy as a fundamental human right.[67] The GDPR codifies the concept of creating systems that are privacy by design and default in recognition of the right to privacy being a fundamental human right.[68] The restraints put on the entities handling the personal data of EU citizens serve as a baseline for data protection and as a means of avoiding different results from those involved in the processing of such data regardless of location.

Working in conjunction with the data controllers and data processors, a Data Protection Officer (DPO) is to be appointed as an officer of the firm with "expert knowledge of data protection law and practices."[69] The DPO serves as an advisor to the controllers or processors and their employees to ensure adherence to their processing obligations as well as the need to

---

[66] DINESH RAJASEKHARAN ET AL., ACCELERATING YOUR RESPONSE TO THE EU GENERAL DATA PROTECTION REGULATION (GDPR): USING ORACLE DATABASE SECURITY PRODUCTS 4-5 (2017), http://www.oracle.com/technetwork/database/security/wp-security-dbsec-gdpr-3073228.pdf.

[67] Frederick Leentfaar, Privacy by Design and Default, TAYLORWESSING (Nov. 2016), http://united-kingdom.taylorwessing.com/globaldatahub/article-privacy-by-design-and-default.html; see also S. and Marper v. the United Kingdom, App. Nos. 30562/04 and 30566/04, 48 Eur. Ct. H.R. 1169 (2008) (deciding that "the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8"); see also The European Convention on Human Rights, §1, arts. 8, 14, Nov. 4, 1950, 213 E.T.S. 222, available at http://www.echr.coe.int/Documents/Convention_ENG.pdf (specifically titling Article 8 as the Right to Respect for Private and Family Life and Article 14 as the Prohibition of Discrimination).

[68] GDPR, supra note 5, at art. 25.

[69] Id. at art. 37(1), (5).

monitor compliance with the GDPR.[70] Further, the DPO is the officer tasked with performing the data protection impact assessments.[71] Additionally, the DPO cooperates with the supervisory authority established by an EU Member State or an auditing agency, and the DPO is the point of contact for the supervisory authority on issues related to the firm's data processing.[72] The DPO's tasks can be performed by either an employee of the controller or processor or be outsourced to a third-party service.[73] The DPO position is not new in Europe. Germany requires DPOs for organizations with more than ten employees. However, the GDPR does not address the size of the firm, but instead, the GDPR DPO requirement applies to any business processing personal data.

The GDPR also changes the required methods of demonstrating compliance. Rather than filing notifications with the data protection authorities, companies must be able to demonstrate the existence and implementation of a comprehensive data compliance program in case of an audit. Companies will need to develop, implement, and maintain policies, reports, rules, and contracts that demonstrate compliance with the GDPR. It is assumed that these obligations will extend to both data controllers and processors.

As to processing activities, controllers will need to record information such as the purpose of processing, categories of data and data subjects, the categories of recipients to whom the data will be disclosed, and the approximate time limit for the erasure of the different categories of data. When processing certain types of personal data that present a high risk to the data subject, the controller must perform a Data Protection Impact Assessment outlining and evaluating the foundation for preventing gaps and breaches in the system. Upon transfer of data, companies will also be expected to maintain a record of recipients and the documentation of the appropriate safeguards used to legitimize the transfers of personal data. Other obligations include keeping a written description of the technical and organizational measures used to protect the security of the personal data, a responsibility to keep records of activities to document the process of selecting data processors and to keep copies of written contracts with data processors. Techniques such as data mapping will assist controllers in showing such information. Other than record information requirements, data mapping will assist organizations in assessing the risks of its data processing activities as well as track the data flows both intra-organizationally and inter-organizationally. Further, appropriate technical and organizational measures must also be implemented protect against any potential risks.[74]

To prevent unauthorized access to personal data, the GDPR recognizes encryption, anonymization and pseudonymization, privileged access control, and data minimization as viable techniques to use to minimize the risk of attacks. Pseudonymization is not a new term, but it is worth defining as it provides the controllers and processors with incentives encouraging the pseudonymization of data. Under the GDPR, pseudonymization means that data is processed in a way that prohibits the data subject from being identified without additional information.[75] The controller should keep in mind all of the means reasonably likely to be used as well as the costs

---

[70] Id. at art. 39(1)(a)(b).
[71] Id. at art. 1(c).
[72] Id. at art. 39(1)(d)(e).
[73] Id. at art. 37(6).
[74] Id. at art. 25.
[75] Id. at art. 4(5).

and amount of time required to identify the subject to determine whether or not a subject is still identifiable.[76] Recognizing that pseudonymization is an industry practice that can reduce risks to data subjects, the GDPR creates incentives to implement the practice. While pseudonymization is not enough to escape the scope of the GDPR, it may enable processing personal data beyond the original stated purpose. Pseudonymization is part of the GDPR's overall concept of data protection by design.[77] Mentioned with pseudonymization is full anonymization. Full anonymization is not subject to the GDPR; however, fully anonymizing data quickly becomes a high standard to meet.[78] Data minimization is meant to restrict the amount of personal data collected, processed, stored, and accessible to the minimum amount required by the processor. Data minimization is a key issue when thinking about big data analytics because the availability of massive and diverse data sets is crucial for uncovering potential insights driving innovation.

In the event of a personal data breach, Article 31 of the Regulation requires the controller to notify the supervisory authority within 72 hours of becoming aware of the breach.[79] Notification to the supervisory authority must at least include approximate numbers about the affected data subjects, the DPO's contact information, likely consequences of the breach, and a description of measures to address the breach and mitigate further issues.[80] Notification must also be made "without undue delay" to data subjects that are likely affected by the breach.[81] However, if the data affected by the breach is unintelligible to any person who is not authorized to access it, the data subject does not need to be notified.[82] Unintelligible data forms include encrypted data.[83] While the GDPR introduces more rigorous practices in some areas, there are also ways to minimize the controller's obligations to the data subject provided the controller takes other measures.

4. Cross-Border Data Transfers

The misinterpretation of the regulatory frameworks that govern cross-border data flows is a key issue that has held back such activity.[84] Article 44 through 50 directly deal with the regulation of cross-border transfers of personal data. Under Article 44 of the Regulation, cross-border data transfers can occur if the transfer is made to a country or international organization with adequate protections or the exporter has a lawful transfer mechanism.[85] The adequacy of the level of protection is made by the Commission and is to mean that the level of protection is

---

[76] Id. at recital 26.
[77] Id. at art. 25(1).
[78] See id. at recital 26.
[79] Id. at art. 33(1) (An exception being if it is "the data breach is unlikely to result in a risk to the rights and freedoms of natural persons).
[80] Id. at art. 33(3).
[81] Id. at art. 34(1).
[82] Id. at art. 34(3).
[83] Id. at art. 34(1)(a).
[84] Facilitating Cross Border Data Flow in the Digital Single Market, at xii (Jan. 10, 2017), http://ec.europa.eu/digital-single-market/en/news/facilitating-cross-border-data-flow-digital-single-market.
[85] GDPR, supra note 5, at art. 44.

essentially equivalent level of protection to the EU law.[86] Particularly influenced by Schrems, the factors that are considered include but are not limited to how a particular third country respects "the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defense, national security and criminal law and the access of public authorities to personal data, as well as…judicial redress for the data subjects whose personal data are being transferred."[87] Adequacy decisions are subject to periodic reviews where the Commission may appeal, amend, or suspend a nation's adequacy decision.[88] To date, the Commission has issued 12 adequacy designations.[89] The adequate third countries include Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay, New Zealand, and the U.S.[90] It is interesting to note, the GDPR will go into effect before the conclusion of the negotiations of the terms and conditions of Brexit. Thus, the UK is still bound by the regulation. Currently, the UK is in the process of negotiations with the EU surrounding Brexit, but the UK government has published a policy recommendation paper outlining the continued exchange and protection of personal data with the EU through a UK-EU model based on the existing adequacy methods.[91] Still, the future remains somewhat uncertain as to how the UK will proceed after Brexit is fully performed. The Commission will continue to take the necessary steps to promote international cooperation in personal data protection.[92]

While the GDPR provides certain countries with an adequacy of protection designation, it does not preclude cross-border transfers to nations without an adequacy designation provided the controller or processor uses appropriate safeguards found in Article 49 of the Regulation.[93] Appropriate safeguards include Binding Corporate Rules (BCRs), standard data protection contractual clauses, an approved code of conduct, an approved certification mechanism, or legally binding instruments between public authorities.[94] The GDPR also provides provisions for the transfer of personal data to countries that have not received an adequacy designation. Article 46 of the Regulation provides another option for data controllers and processor to transfer

---

[86] Id. at art. 45(1); see also Judgment of the Court of Justice of the EU of 6 October 2015 in Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650 (invalidating the EU-US Ssfe Harbor Agreement for not providing adequate levels of data protection for EU citizens) [hereinafter Schrems].

[87] GDPR, supra note 4, at art. 45(2)(a); see also Schrems (detailing certain criteria lacking from the Safe Harbor Agreement that invalidated the agreement as being essentially equivalent to EU law and views on data protection).

[88] GDPR, supra note 5, at art. 45(3).

[89] Exchanging and Protecting Personal Data, supra note 5.

[90] Id.

[91] DEPT. FOR EXITING THE EUROPEAN UNION, THE EXCHANGE AND PROTECTION OF PERSONAL DATA – A FUTURE PARTNERSHIP PAPER 2 (2017), http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf.

[92] GDPR, supra note 5, at art. 50.

[93] Id. at art. 49 (1)(a).

[94] Id. at art. 46(2).

personal data is via BCRs that are approved by a supervisory authority.[95] BCRs set out the company's privacy policy that demonstrates how it maintains an adequate level of data protection and necessary safeguards under the GDPR.[96] Once implemented, BCRs are an advantageous form of joint activity among companies as they are allowed to use the same approved BCRs for international data transfers.[97] Today, fewer than 100 companies have obtained approval of their BCRs despite BCRs being a recognized means of cross-border data transfer for the last decade.[98] The standard data protection contractual clauses are adopted by the EU Commission or by a supervisory authority and controllers or processors are free to supplement standard protection clauses provided they do not conflict with the already adopted standard contractual clauses.[99] As to the codes of conduct and certification mechanisms, they are self-regulatory programs that signal a company's compliance with privacy standards. The codes can be established by associations of controllers or processors. Drafts of the codes of conducts must be sent to the supervisory authority for approval.[100] Monitoring of compliance with the approved codes of conduct may be done by an accredited and competent body.[101] Further, the controller must also obtain explicit consent from the data subject to transfer the personal data to a country that has not obtained an adequacy decision.[102] Without explicit consent, the data controller could still transfer the data provided the transfer is necessary to carry out the obligations of a contract in the interest of the data subject either for a contract between the data subject and the data controller or the data controller and another person.[103] If an organization is found to have violated any of the articles of the GDPR mentioned above, the organization will be subject to either a fine of €20 million or 4% of the company's total worldwide annual revenue, whichever is greater.[104]

B. EU-U.S. Privacy Shield Framework[105]

In July 2016, the U.S. Department of Commerce and the European Commission approved the EU-U.S. Privacy Shield Framework (Privacy Shield), which is a data protection framework that allows companies on both sides of the Atlantic to transfer personal data from the EU to the

---

[95] Id. at art. 47(1).
[96] See generally id. at art. 47.
[97] Id. at art. 47(1)(a).
[98] Gilbert, supra note 18; see also European Commission, List of Companies for which the EU BCR Cooperation Procedure is Close, EUROPEAN COMMISSION JUSTICE, http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm (last visited Oct. 29, 2017) (listing the companies with approved BCRs).
[99] GDPR, supra note 5, at recital 109.
[100] Id. at art. 38
[101] Id. at art. 41.
[102] Id.
[103] Id. at art. 49 (1)(b)(c).
[104] Id. at art. 83(5). An entity in "non-compliance with an order by the supervisory authority as referred to in Article 58(2)" may be subject to fines up to €10 million or 2% of the company's total worldwide annual revenue. Id. at art. 83(6).
[105] In alignment with the EU-U.S. Privacy Shield, the U.S. also has a privacy shield with Switzerland.

U.S.[106] Over 2,400 companies have agreed to follow the obligations in the pact requiring U.S. companies to protect EU citizens' personal data.[107] The Privacy Shield is the result of the European Court of Justice (CJEU) invalidating the US-EU Safe Harbor Framework on October 6, 2015 after being in place for fifteen years.[108] The CJEU cited misuses of European citizen's personal data with no judicial means of redress in the US for these European citizens and concerns over US law enforcement having unrestrained access to the transferred data as reasons to invalidate the Safe Harbor agreement.[109] To maintain the transatlantic relationship concerning transfers of personal data, the Privacy Shield was created but with added policing mechanisms and guaranteed data protections for EU citizens.[110]

Since July 2016, the Privacy Shield has allowed the continuation of personal data being transferred from the EU to a US-based company provided that the company handles the data according to the set rules and safeguards.[111] If a US company uses the Privacy Shield to transfer data, the company must first sign up to the Privacy Shield with the U.S. Department of Commerce and self-certify that it has a privacy policy that is in line with the Privacy Principles.[112] Participation with the Privacy Shield is voluntary, but the commitment to the Privacy Shield is enforceable under US law once made.[113] The Privacy Principles overlap with the GDPR as well as address some of the concerns the CJEU put forth in its Schrems judgment about data transfers to third countries. The Privacy Principles include the data subject's right to be informed; limitations on the use of the data subject's data for different purposes; obligations to secure the data subject's data; obligations to protect the data subject's data if transferred to another company; the data subject's right to access and correct their data; the data subject's right to files a complaint and obtain a remedy; and redress in case of access by U.S. public authorities. Certification to the Privacy Shield must be renewed annually.[114] The first annual review of the Privacy Shield was conducted in September 2017 by U.S. and EU official.[115] Following the two-day meeting that analyzed all aspects of the administration and enforcement of the Privacy Shield for the last year, the response was largely positive, but there are still areas of needed improvement from the EU's perspective.[116]

---

[106] Privacy Shield Overview, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/Program-Overview (last visited Oct. 21, 2017).
[107] Allison Grande, What to Watch with EU-US Privacy Shield Under Microscope, LAW360 (Sept. 15, 2017, 9:31 PM), http://www.law360.com/articles/964150/what-to-watch-with-eu-us-privacy-shield-under-microscope.
[108] See Schrems.
[109] See id.
[110] See European Commission Press Release IP/16/2461, European Commission Launches EU-US Privacy Shield: Stronger Protection for Transatlantic Data Flow (July 12, 2016).
[111] Id.
[112] Privacy Shield Overview, supra note 106.
[113] Id.
[114] See generally U.S. Dept. of Comm., EU-US Privacy Shield Framework Principles, http://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg.
[115] European Commission Press Release IP/17/3966, EU-US Privacy Shield: First Review Shows It Works but Implementation Can Improve (Oct. 18, 2017).
[116] Id.

C. APEC Privacy Framework

The Asia-Pacific Economic Cooperation (APEC) was formed with the goal of facilitating economic growth, cooperation, trade, and investment in the Asia-Pacific region.[117] Created in 1989, APEC has 21 member countries that include countries in Asia as well as North America and South America.[118] The APEC Privacy Framework, a set of principles and guidelines with the purpose of creating privacy protections that avoid barriers to information flows thus ensuring continued trade and economic growth, established the APEC Cross-Border Privacy Rules (CBPRs).[119] The CBPR system facilitates international data transfers, increases data subject privacy protections, and serves a demonstration of a company's commitment to data privacy protection.[120]

There are many similarities between the CBPR system and the GDPR.[121] Such similarities include the goal of decreasing barriers to information flows, the same definition of personal data, collection and use of data limitations.[122] Unlike the GDPR, the CBPR system is based on voluntary participation and is not intended to override a nation's domestic laws.[123] The CBPR system does not replace domestic requirements when those legal requirements exceed the CBPR system.[124] Instead, the CBPR system serves as a minimum level of protection when no other domestic privacy protection laws exist.[125]

To date, five nations are CBPR members: U.S., Japan, South Korea, Canada, and Mexico.[126] Additionally, U.S. companies such as Apple, Cisco, Box, IBM, and others have joined the CBPR and are held accountable by TrustArc, Inc.[127] Merck, one of the approved CBPR companies and a US company, took advantage of its CBPR approval to promote interoperability between

---

[117] About APEC, ASIA-PACIFIC ECON. COOPERATION, http://www.apec.org/About-Us/About-APEC (last visited Oct. 13, 2017).
[118] Id
[119] Asia-Pacific Econ. Cooperation, APEC Cross-Border Privacy Rules System Policies, Rules and Guidelines, 2 (available at http://www.cbprs.org/generalpages/apeccbprsystemdocuments.aspx).
[120] Id.
[121] Alex Wall, GDPR Matchup: The APEC Privacy Framework and Cross-Border Privacy Rules, IAPP (May 17, 2017), http://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/.
[122] Id.
[123] APEC Cross-Border Privacy Rules System Policies, Rules and Guidelines, supra note 110, at 2, 10; Cf. GDPR, supra note 5, at art. 2.
[124] APEC Cross-Border Privacy Rules System Policies, Rules and Guidelines, supra note 119, at 10.
[125] Id.
[126] Elaine Ramirez and George Lynch, South Korea Joins Asia-Pacific Data Transfer System, BLOOMBERG LAW: PRIVACY & DATA SECURITY (June 28, 2017), http://www.bna.com/south-korea-joins-n73014460915/.
[127] TRUSTe Privacy Program Participants and Services, TRUSTARC, http://www.trustarc.com/consumer-resources/trusted-directory/#apec-list (last visited Oct. 29, 2017).

privacy protection frameworks.[128] Merck adapted its CBPR policies to retain a BCR approval under the GDPR guidelines.[129] In doing so, the process of BCR approval was significantly faster and less expensive.[130] Because of Japan's and South Korea's commitments to data protection laws and being key trading partners with the EU, the EU Commission will actively engage with these two countries on an adequacy decision to facilitate the free flow of data.[131] However, interoperability between APEC and the EU data transfer laws remain on a case by case basis.

D. BRICS

While the Privacy Shield and the CBPR system demonstrate the progression of data protection through cooperation, the free flow of information has other challenges to overcome. BRICS stands for Brazil, Russia, India, China, and South Africa.[132] In the coming years, these countries are projected to be the world's dominant suppliers of manufactured goods and services as well as the dominant suppliers of raw materials. China and Russia are both members of APEC but maintain controversial data localization laws as a means to preserve sovereignty over the internet.[133] Meanwhile, India, despite expressed interest, is struggling to secure membership with APEC but continues to modernize its digital infrastructure. Not a member of APEC or located in Asia, Brazil is working on new data protection laws and is a part of the Mercosur bloc that has expressed interest in working with the EU Commission to obtain an adequacy decision.[134] These four nations, if acting in unison, have the power to influence the development of global issues.

Brazil is a member of the Mercosur trading bloc that includes Argentina, Uruguay, and Paraguay with Bolivia, Chile, Colombia, Ecuador, and Peru as associate members.[135] Interestingly, Brazil does not have a data protection framework. However, under various principles in the country, international data transfers are permitted subject to informed consent of the parties involved.[136] Currently, legislation has been widely discussed in the country, and it is

---

[128] Hilary Wandall and Daniel Cooper, How to Align APEC and EU Cross-Border Transfer Rules, LAW360 (April 12, 2016, 3:10 PM), http://www.law360.com/articles/783482/how-to-align-apec-and-eu-cross-border-transfer-rules.

[129] Id.

[130] Id.

[131] Exchanging and Protecting Personal Data, supra note 5, at 8.

[132] Since 2010, South Africa has been a member of the BRICS. While the EU is one of South Africa's largest trading partners, South Africa's POPI Act is largely in line with the GDPR with the exception of some additional requirements. Therefore, it is not difficult for South Africa to be compliant with the GDPR compared to the other BRICS nations. See Russell Nel, GDPR Matchup: South Africa's Protection of Personal Information Act, IAPP (Sept. 5, 2017), http://iapp.org/news/a/gdpr-matchup-south-africas-protection-of-personal-information-act/.

[133] See Levi Maxey, The Worldwide Struggle to Claim Cyber Sovereignty, THE CIPHER BRIEF (Sept. 26, 2017), http://www.thecipherbrief.com/worldwide-struggle-claim-cyber-sovereignty.

[134] Exchanging and Protecting Personal Data, supra note 5.

[135] Claire Felter and Danielle Renwick, Mercosur: South America's Fractious Trade Bloc, Council on Foreign Relations, http://www.cfr.org/backgrounder/mercosur-south-americas-fractious-trade-bloc (last updated Sept. 13, 2017).

[136] Further restrictions may be applied to medical data.

expected that Brazil will enact its first data protection regulation soon. Still, the EU Commission identified Mercosur as having conveyed interest in obtaining an adequacy decision.[137]

In 2015, Russia passed a data localization law that requires companies to store data concerning Russian citizens on databases located in Russia. Similar to China, companies face backlash for not complying with the data laws. For example, LinkedIn is banned in Russia because the company refused to store user data in the country.[138] Russia is mostly concerned with the processing and storing of its citizens' data staying in Russia. It has yet to be determined if the storing and processing of personal data of a Russian citizen can be compliant with the Russian data protection laws based on mirroring databases.[139] The Russian regulators have stated that storing and processing of personal data of Russian individuals outside of Russia may still be compliant provided the primary storage and processing of the data is done in Russia.[140] Transferring data outside of Russia requires the recipient state to have adequate levels of protection of personal data, the data subject consents, the transfer is under an international treaty that Russia is a signatory too, or the transfer is for the performance of a contract that the data subject is a party to.[141] Like China, Russia is concerned with its sovereignty over the internet.

India is engaged in an IT overhaul moving towards greater digitization, experimenting with a cashless economy, and liberalizing its laws to attract foreign investments. When it comes to privacy and data protection, India does not have specific legislation addressing the issue. However, India adopted the Information Technology Rules in 2011, which introduced data protection regulation to the country.[142] The rules require companies to comply with certain procedure when collecting, processing, and storing personal data.[143] When transferring personal data, contractual agreements following the Rules' guidelines are an accepted practice.[144] Despite efforts to modernize its digital infrastructure, India has been unsuccessful to date in securing a membership with APEC despite showing a clear interest in joining.[145]

In 2017, China updated its data protection laws, and the updates are having tech companies rethinking their strategies in the region. China has continually been open about its goals to exert sovereign control over the internet.[146] For example, the new draft states that the goal is to protect

---

[137] Exchanging and Protecting Personal Data, supra note 5. Argentina and Uruguay are two of the twelve countries with adequacy status under the GDPR. Id.

[138] Ingrid Lunden, Russia Says "Nyet," Continues LinkedIn Block After It Refuses to Store Data in Russia, TECHCRUNCH (Mar. 7, 2017), http://techcrunch.com/2017/03/07/russia-says-nyet-continues-linkedin-block-after-it-refuses-to-store-data-in-russia/.

[139] Data Protection Laws of the World: Russia, DLA PIPER, http://www.dlapiperdataprotection.com/index.html?t=law&c=RU (last modified Jan. 26, 21017).

[140] Id.

[141] Id.

[142] Data Protection Laws of the World: India, DLA PIPER, http://www.dlapiperdataprotection.com/index.html?t=law&c=IN (last modified Jan. 24, 21017).

[143] Id.

[144] Id.

[145] Rani Singh, What's Stopping India From Joining the Asia Pacific Economic Forum, FORBES: AISA (Mar. 17, 2016, 8:26 PM), http://www.forbes.com/sites/ranisingh/2016/03/17/whats-stopping-india-joining-the-asia-pacific-economic-forum/#6aa015fc5dad.

[146] Maxey, supra note 133.

cyberspace sovereignty, national security, public interests, and citizens' lawful interests.[147] A shift in the law also comes from a change in the distinctions of data. Instead of classifying important data as important personal data, important business data, and important national data, the phrasing combines the distinctions into "important data," which indicates a recognition of how big data can be used to blur the lines between the previous three distinctions.[148] By exerting greater control over internet related activities within its country, the Chinese government requires data related to Chinese citizens or business operations to be stored on servers within the country.[149] The localization law puts an added burden on doing business in China particularly on companies that do not have data centers in China. For example, Apple opened its first data center in China in response to the data localization requirements.[150] Additionally, Facebook is rumored to be looking for an office in Shanghai.[151] Currently, Facebook is blocked in China.[152] Despite this fact, Facebook sells advertising to Chinese businesses through its Hong Kong office.[153] China's data protection regulation, at the core, is similar to the GDPR in its goal to protect its citizens' personal data. However, China goes another step further by requiring localized data storage as well as broader government access to data generated in China for national security purposes.[154] Cyberlaw change in China is still ongoing, but it is clear that barriers to data flows will exist.

It is clear that considerable challenges remain to resolve the tension between national sovereignty and international data flows. Economic trade data indicates the negative impact on local economies that enact barriers to trade. Countries enacting forms of data localization regulations will lag behind while countries adopting pluggable data transfer regulations like BCRs, CBPRs, and Privacy Shields will drive global innovation forward. Rather than undermining data protection, common data protection approaches through collaboration are slowly gaining traction.

---

[147] Yanquing Hong, THE CROSS-BORDER DATA FLOWS SECURITY ASSESSMENT: AN IMPORTANT PART OF PROTECTING CHINA'S BASIC STRATEGIC RESOURCES, Yale Law Sch.: Paul Tsai China Center (June 20, 2017) (working paper) (on file with Yale law School).

[148] Id.

[149] Id.

[150] Apple to Build First China Data Center to Comply with Law, BLOOMBERG NEWS (July 12, 2017, 5:16 AM), http://www.bloomberg.com/news/articles/2017-07-12/apple-to-build-first-china-data-center-to-comply-with-local-law.

[151] Paul Mozur, Blocked in China, Facebook is Said to Seek a Shanghai Office, THE NEW YORK TIMES (Sept. 6, 2017, 5:02 PM), http://www.nytimes.com/2017/09/06/technology/facebook-china-shanghai-office.html?mcubz=1.

[152] Id. The Chinese government recently blocked Facebook owned WhatsApp as well. Keith Bradsher, China Blocks WhatsApp, Broadening Online Censorship, THE NEW YORK TIMES (Sept. 25, 2017), http://www.nytimes.com/2017/09/25/business/china-whatsapp-blocked.html?mcubz=1.

[153] Mozur, supra note 157.

[154] See Hong, supra note 147.

III. Blockchain

Gartner forecasts that "the business value-add of blockchain will grow to slightly more than $176 billion by 2025, and then it will exceed $3.1 trillion by 2030."[155] Subsequently, industries are exploring blockchain applications and are quickly moving from the proof of concept phase to pilot programs. When most people think of blockchain, they often think of Bitcoin, which is partially justified. Bitcoin, a cryptocurrency and a protocol, was the first decentralized and permissionless peer-to-peer payment system to implement blockchain. Blockchain, a subset of distributed ledger technology (DLT) is a decentralized peer-to-peer network that maintains a distributed digital ledger of transactions.[156] In other words, blockchain includes a protocol that bundles data in a defined size (blocks) and then stores the grouped data in a chained sequence on a distributed, global network of computers.

Before explaining how a transaction takes place, some terminology must be explained. Blockchain is sometimes referred to as a state transition system where a state is a set of all the stored information in the system and a transaction, which transitions the state, is a piece of data in the form of an operation that a party wants to execute.[157] Transaction data includes the sender's public key, the receiver's public key, the payload, and a cryptographic signature.[158] A block is a list of transactions that references the previous block and some other information that shows the validity of the block.[159] Simply, the blockchain is a chain of verified blocks that goes back to the genesis state, the beginning of the blockchain.[160] Part of the process of verifying transactions is through consensus algorithms.[161] In any consensus model including proof of work (PoW), there are two core processes: (1) a fork choice rule, which is a process to check what the current main state of blockchain is and (2) an updating process, which is a universally accepted updating process to produce a new block to extend the blockchain.[162] There are many different consensus models, but the two commonalities are checking the current state of the blockchain and applying the agreed upon process to append the valid current state.[163]

Going through the life cycle of a transaction in the Bitcoin blockchain, it begins with someone creating a transaction, which can involve cryptocurrencies, contracts, records, or other sets of information.[164] The sender creates a message that includes the asset amount being

---

[155] John-David Lovelock et al., Forecast: Blockchain Business Value, Worldwide, 2017-2030, GARTNER (Mar. 2, 2017), http://www.gartner.com/doc/3627117/forecast-blockchain-business-value-worldwide.

[156] JOSIAS N. DEWEY ET AL., THE BLOCKCHAIN: A GUIDE FOR LEGAL AND BUSINESS PROFESSIONALS 2 (2016).

[157] VITALIK BUTERIN, NOTES ON SCALABLE BLOCKCHAIN PROTOCOLS (VERSION 0.3.2) 4 (2015), http://github.com/vbuterin/scalability_paper/blob/master/scalability.pdf [hereinafter NOTES ON SCALABLE].

[158] Id. at 5.

[159] Id. at 5.

[160] Id. at 6.

[161] Id.

[162] Id.

[163] See id. at 3, 6.

[164] A Gentle Introduction to Blockchain Technology, BITS ON BLOCKS (Sept. 9, 2015), http://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology/.

transferred and the receiver's address.[165] The sender signs this message with his private key.[166] The transaction request is broadcast to all of the computers on the network, also called the nodes.[167] The miner nodes work to validate the transaction using known algorithms to verify the transaction before appending it to the blockchain.[168] The mining process begins with miners bundling pending transactions to create a new block.[169] Each block has a header that contains the timestamp of the block, which includes a cryptographic hash of the block's items characterized by a 256-bit hash number beginning with a set number of zero bits.[170] Along with the new block's cryptographic hash, the header also includes a reference to the previous block's hash, which creates the chain of verified transactions.[171] A nonce is also added in the header. A change in the nonce results in a different hash value.[172] The miners do not know which nonce will produce the correct hash value.[173] Thus, a consensus algorithm is used which forces them to solve computationally-intensive puzzles to unlock the nonce that allows them to verify the transaction.[174] This process is called PoW, and it ensures the high level of difficulty required to re-write transactions previously appended to the blockchain.[175] The difficulty of the PoW is adaptively set so that a block is created every 10 minutes. The miner that solves the PoW and verifies the block that is added next to the blockchain receives a reward.[176] Once created, blocks are propagated to the majority of the nodes before another block is created. Finally, once successfully added to the blockchain, anyone on the network can query the transactions and know with a high degree of certainty that the obtained results are accepted by the entire network.[177]

Because of the transaction process, the blockchain is an append-only, immutable, and timestamped chain of information. In order for someone to change a transaction, they would have to redo all of the previous miner's work to produce a different winning nonce and redo the work for all the subsequent blocks to keep the chain intact.[178] The work must be done before the network is alerted and the nodes reject all the blocks that the majority now views as

---

[165] SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 2 (2008), http://bitcoin.org/bitcoin.pdf.
[166] Id.
[167] Id.
[168] Id. at 3.
[169] Id.
[170] Id.
[171] Id.
[172] Id.
[173] Id.
[174] Id.
[175] Id.
[176] Id. at 4. The current reward for successfully mining a block on the Bitcoin Blockchain is 12.5 Bitcoins (BTC).
[177] ARIEL EKBLAW ET. AL, A CASE STUDY FOR BLOCKCHAIN IN HEALTHCARE: "MEDREC" PROTOTYPE FOR ELECTRONIC HEALTH RECORDS AND MEDICAL RESEARCH DATA, 2.2 (2016), http://dci.mit.edu/assets/papers/eckblaw.pdf.
[178] NAKAMOTO, supra note 165, at 3.

unverified.[179] The nodes are able to do this because every node on the network has a full replication of the valid transactions on the ledger that dates back to the first block, the genesis block.[180] Successfully tampering with the chain quickly becomes very cost prohibitive and computationally intensive.[181]

Along with the blockchain, the other innovative aspect of Bitcoin was the use of cryptoeconomics. Cryptoeconomics is the use of cryptography, network theory, computer science and economic incentives to create applications that singular disciplines could not achieve on their own.[182] With cryptoeconomics, there are two layers: (1) cryptography and (2) economics. Through the cryptography layer, computational efficiency and scalability are sacrificed to force participants to use computational resources to maintain relationships between strangers. The economics adds another security layer through incentives to promote good behavior and deter malicious network participants.[183] As seen in the above transaction lifecycle example, the goal is to reward those who participate in furthering the system and penalize those who harm the system. The economics are aligned in such a way that the system encourages properties to hold into the future. If an actor tries to add blocks or attacks the network maliciously, it quickly because very expensive to expend the resources necessary to do so before others are alerted and block further malicious efforts. These tradeoffs to ensure security is the cryptoeconomics premise for public blockchains like Bitcoin and public Ethereum that operate in a trust-minimized and permissionless environment.[184]

While numerous applications are being built on top of the Bitcoin protocol, a further discussion on Bitcoin, as a permissionless blockchain, is outside the scope of this paper. Permissionless and permissioned blockchains have the same underlying technology, that is a method of data storage, transmission and proof in a decentralized way that is based on a distributed structure, and the continuous grouping of transactions into linked blocks chaining the data records together and adding the new blocks to the chain based on a consensus mechanism. Ethereum will be discussed in the sense that Ethereum protocols are being adapted to private blockchains through the consortium blockchain, the Enterprise Ethereum Alliance. The Enterprise Ethereum Alliance (EEA) and Hyperledger are consortium blockchain platforms that have pluggable and extendable frameworks for various blockchain use cases. Further, both utilize smart contracts to automate transactions that also prevent the transacting parties from not abiding by the terms. These two consortiums represent a new generation of enterprise collaboration.

Applying cryptoeconomics to consortium blockchains is slightly different than applying cryptoeconomics to public blockchains. Consortium blockchains share similarities but are not

---

[179] Id.
[180] DEWEY, supra note 156, at 3.
[181] Id. at 8.
[182] Josh Stark, Making Sense of Cryptoeconomics, COINDESK (Aug. 19, 2017, 9:40 PM UTC), http://www.coindesk.com/making-sense-cryptoeconomics/.
[183] NOTES ON SCALABLE, supra note 157, at 8.
[184] As demonstrated, trustlessness on the blockchain is slightly exaggerated and more accurately means trust minimized. Nick Szabo, Money, Blockchains, and Social Scalability, UNENUMERATED (Feb. 9, 2017), http://unenumerated.blogspot.mx/2017/02/money-blockchains-and-social-scalability.html.

full cryptoeconomics models. There is just as much of a need to establish cryptography tools to maintain privacy, security, etc. as well as economic incentives in the form of rewards/penalties or privileges. At the start of the consortium blockchain though, the level of trust among participants is higher than zero. Trust is introduced via some authority that approves members to the consortium and the members, for the most part, already have some form of public reputation in the off blockchain (off-chain) world. As well as the off-chain reputation, these entities are subject to legal ramifications. Because damage to public reputation and legal remedies serve as disincentives to malicious activities, a small amount of trust among consortium members is introduced. Therefore, the assumption can be made that actors within a consortium blockchain are altruistic, meaning they will follow the protocol exactly, or rational, meaning they will follow or deviate from the protocol to maximize their own benefits.[185] Thus, the consensus model, while still needing to exist to process new, valid transactions, does not have to be as computationally intensive as models like PoW.

However, fault accountability is just as important in a consortium blockchain as it is in a public blockchain. Fault accountability means that a problem in the blockchain is traceable to the party that caused it. In thinking through the future of many consumer Internet of Things (IoT) devices, provenance becomes essential. All parties involved in the device need access, on some varying level, to see how the device passes through the supply chain to the end consumer to properly assign fault if there is a flaw in the device. Beginning with an introduction to Ethereum and through selected examples, this paper will highlight some of the technology used and how consortiums deal with the blockchain concepts previously discussed.

A. Ethereum

Ethereum, a cryptocurrency and a protocol, takes the blockchain technology behind Bitcoin and builds a generalized framework that allows for others to develop decentralized software applications (Dapps).[186] While Dapps are free to use any number of consensus algorithms, Ethereum transactions currently use PoW as its consensus algorithm like Bitcoin.[187] Other than the ability to create Dapps, Ethereum also has the ability to run complex smart contracts through its Turing complete Ethereum Virtual Machine (EVM).[188] A Turing complete virtual machine enables the programming of any conceivable computation.[189] Turing completeness allows creators to create smart contracts based on their own arbitrary rules.[190] The ability to run

---

[185] See STEFAN THOMAS AND EVAN SCHWARTZ, A PROTOCOL FOR INTERLEDGER PAYMENTS 3 (2015), http://interledger.org/interledger.pdf.

[186] VITALIK BUTERIN, ETHEREUM WHITE PAPER: A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM 1, http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf [hereinafter ETHEREUM WHITE PAPER].

[187] VITALIK BUTERIN ET AL., CASPER THE FRIENDLY FINALITY GADGET 1 (2017), http://github.com/ethereum/research/blob/master/papers/casper-basics/casper_basics.pdf [hereinafter CASPER].

[188] ETHEREUM WHITE PAPER, supra note 186, at 28.

[189] Id. at 29.

[190] Id. at 13.

complex smart contracts through a Turing complete EVM makes Ethereum an attractive technology for broader industry adoption.

1. Smart Contracts

In the 1990s, Nick Szabo, a legal scholar and a cryptographer, first introduced the concept of smart contracts, which are programmable contracts that self-execute on the blockchain (on-chain) based on the occurrence of pre-specified conditions.[191] In 2015, Ethereum became the first real implementation of the concept as it is the most advanced use case for the coding and processing of smart contracts.[192] Because smart contracts are self-executing and code-based, they are less expensive, faster, and less ambiguous than traditional contracts.[193] However, it is important to note that smart contracts are not legal contracts.

There are difficulties in assessing the merger of law and code through smart contracts. Law is considered wet code because it is interpreted by the brain and is highly subjective.[194] Software, on the other hand, is considered dry code because it is interpreted by computers and is mostly deterministic.[195] Solely using dry code to execute contracts creates a drawback regarding interacting with the off-chain world that is highly non-deterministic. It is impossible to write a complete contract that accounts for unspecified, emergent phenomenon that would disrupt the execution of the contract.[196] As any first-year law student or economist knows, all ownership rights cannot be contracted away due to high transaction costs.[197] Thus, the notion of residual rights of control is necessary, which presents mechanisms to fill in the ownership gaps over time.[198] The shift from implicit contracts to more explicit smart contracts will inevitably also involve trusted intermediaries overseeing performance and adjudicators resolving disputes.[199] Still, the underlying idea behind smart contracts is that contractual clauses are embedded in the software and performed in an automated fashion where transaction costs are significantly reduced, and it becomes prohibitively expensive to breach the contract.[200] Consequently, certain conditions included in the smart contract are still left to normal, off-chain remedies. While the limitations of smart contracts are still being explored, a developer could not run on-chain automated data analytics like machine learning using them today. A level of human intervention

---

[191] Nick Szabo, Smart Contracts: Formalizing and Securing Relationships on Public Networks, 2 FIRST MONDAY (1997), http://ojphi.org/ojs/index.php/fm/article/view/548/469).

[192] See id.; see also Massimo Bartoletti & Livio Pompianu, An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns, CORR abs/1703.06322, 1, 4 (Mar. 18, 2017) (noting that smart contracts can be written on the Bitcoin protocol using the OP_RETURN function. However, Bitcoin smart contracts have far less functionality than Ethereum partially because Bitcoin is a Turing incomplete language).

[193] Szabo, supra note 191.

[194] Nick Szabo, Wet Code and Dry, UNENUMERATED (Aug. 24, 2008), http://unenumerated.blogspot.com/2006/11/wet-code-and-dry.html.

[195] Id.

[196] Szabo, supra note 191.

[197] See Oliver D. Hart, Incomplete Contracts and the Theory of the Firm, Journal of Law, Economics, & Organizations, Vol. 4 No 1 (1988) 119, 123.

[198] Id.

[199] Szabo, supra note 191.

[200] Id.

is still needed despite the automatic execution of the contract itself. Despite the limitations being explored, smart contracts are a highly useful tool for automating deterministic elements of transactions today. Ultimately, it is important to understand how humans and computers are evolving together based on the strengths and weaknesses of each.[201]

2. Metropolis

Ethereum is in the process of its penultimate phase with its Metropolis update that addresses scalability, safety, and privacy concerns. The Metropolis update will be implemented with two hard forks, Byzantium and Constantinople.[202] Released in October, the Byzantium hard fork introduced zk-SNARK, early support for the switch to a proof of stake (PoS) consensus model, more robust smart contract features, and account abstraction.[203] One of the new contract features revolves around reverting contracts to the previous state without using all of the gas for the transaction.[204] The account abstraction feature brings Ethereum's two account types closer which allows individual accounts to be defined similarly to smart contract accounts.[205] The second hard fork of the Metropolis update, Constantinople, has yet to launch but is expected in 2018.[206] For this paper, zk-SNARKs and the PoS consensus model will further be discussed.

The first new feature with the Byzantium hard fork, Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK), is a zero-knowledge cryptography technology introduced by Zcash, a privacy-centric cryptocurrency.[207] In zero-knowledge proofs, the prover can prove to the verifier that a statement is true without revealing the underlying data.[208] Mathematical functions are performed against the fully encrypted data while the data remains encrypted, and the results of the proofs are validated without decrypting the data. The succinctness of the proofs allows for short and relatively easy verifiability. In effect, the data can be verified by any observer, but the raw data is not revealed. Along with the Metropolis upgrade, zero-knowledge technology has spread to the enterprise realm via an integration with JPMorgan's Quorum, which is discussed in the EEA section of this paper below.[209] While still

---

[201] Szabo, supra note 194.

[202] A hard fork is a change in the base protocol that creates a new path and requires all nodes to update their software to the new protocol in order to participate in the new blockchain. A soft fork is when part of the network agrees to place additional restrictions on what constitutes a valid block. KEIR FINLOW-BATES, ADDING TRUST TO CAP: BLOCKCHAIN AS A STRONG EVENTUAL CONSISTENCY RECOVERY STRATEGY 4-5 (2017).

[203] What is Ethereum Metropolis: The Ultimate Guide, BLOCKGEEKS, http://blockgeeks.com/guides/ethereum-metropolis/ (last visited Oct. 29, 2017).

[204] Id.

[205] Id.

[206] Id.

[207] Zooko Wilcox, Ethereum Adoption of zk-SNARK Technology, ZCASH BLOG (Sept. 20, 2017), http://z.cash/blog/ethereum-snarks.html.

[208] What are zk-SNARKs, ZCASH: TECHNOLOGY, http://z.cash/technology/zksnarks.html (last visited Sept. 27, 2017).

[209] Michael del Castillo, JPMorgan Integrates Zcash Privacy Tech into Quorum Blockchain, COINDESK (Oct. 17, 2017, 13:00 UTC), http://www.coindesk.com/jpmorgan-integrates-zcash-privacy-tech-enterprise-blockchain/.

being developed and put into practice, the use of zero knowledge proofs would allow for smart contracts to run on encrypted data.

As noted before, Ethereum, like Bitcoin, currently uses a PoW system to reach consensus to verify transactions before transactions are appended to the blockchain.[210] Due to the costly and energy-intensive nature of PoW that contributes to scalability issues, Ethereum is changing to a PoS system called Casper.[211] Caper is "a security deposit based economic consensus protocol."[212] Nodes must place a security deposit, or stake, to participate in the validation process. Validators bet on consensus meaning they bet on how they think other validators will bet regarding the validity of the block.[213] Rather than security coming from miners expending significant energy to reach validation, security comes from the economic loss if a validator violates the Casper commandments.[214] There are more incentives involved in Casper to address things like the potential of a Sybil attack, a 51% attack, and the Byzantine Generals Problem, but a further technical explanation is outside the scope of this paper. Casper is used in this paper to highlight another consensus blockchain model and to show how Ethereum is evolving its consensus model to address trade-offs found in blockchain technology.

3. Merkel Trees and Pruning

The immutability of blockchain poses a significant data storage issue. As more transactions take place, the database grows with each transaction containing data about account balances, contract code, and account nonces.[215] Remember, everything in blockchain is linked. The chain of transactions appended to the blockchain is longitudinal. But, the underlying data about the transactions is stored using a Merkle Tree. Going back to the lifecycle of a transaction on the Bitcoin blockchain, each block has a header that contains the hash of the previous block, a time stamp, a proof of work nonce, a mining difficulty value, and a root hash for the Merkle Tree containing all the transactions in the block.[216] Merkle trees are data structures for data verification through the use of hashes instead of full files. The use of hashes allows for faster verification times and less data stored on-chain.[217] Additionally, with the Merkle tree leading all the way back to the root hash, a user could query the database for data in a particular position by asking for a Merkle proof.[218] A Merkle proof can prove the existence of a piece of data located at some point in the Merkle tree based on the root hash and the hash being proved.[219] The reasoning behind storing such a large amount of individual transaction data is so that any node on the

---

[210] ETHEREUM WHITE PAPER, supra note 186, at 18.
[211] CASPER, supra note 187.
[212] Vlad Zamfir, Introducing Casper "the Friendly Ghost," ETHEREUM BLOG (Aug. 1, 2015), http://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/.
[213] Id.
[214] See CASPER, supra note 187, at 5-6.
[215] Vitalik Buterin, State Tree Pruning, ETHEREUM BLOG (June 26, 2015), http://blog.ethereum.org/2015/06/26/state-tree-pruning/
[216] Bitcoin uses a Binary Merkle tree. Ethereum uses a Patricia Merkle tree. A further technical explanation of Merkle Trees is outside the scope of this paper.
[217] Vitalik Buterin, Merkling in Ethereum, ETHEREUM BLOG (Nov. 15, 2015), http://blog.ethereum.org/2015/11/15/merkling-in-ethereum/.
[218] Id.
[219] Id.

network can look to the last block and know that it is synchronized with the blockchain by seeing that all the previous hashes match up.[220]

Because Ethereum allows for more dynamic transactions than Bitcoin, it uses three Merkle Trees in its blocks: one for transactions, one for receipts, and one for the state. The transaction tree signifies the transactions in the block. The state tree shows current account states, if the account exists at all, and runs a Merkle state transition proof to see the outcome of the transaction. Finally, the receipt tree demonstrates all instances of an event. Along with the hash of the previous block, these four things make up a block header in Ethereum. Because Ethereum uses a Patricia tree, a form of a Merkle tree, data inside the tree can be added, removed or modified by only making a few changes to the structure.[221] To allow nodes to remain constantly in sync with the current state of the system while decreasing storage, the approach is called state tree pruning.[222] References are used as pointers to where the data is in the tree structure, and the unnecessary data is queued to be permanently deleted after some blocks are appended to the chain.[223] As a fail-safe, a few archive nodes storing the entire network without any deletions are maintained to help the rest of the network when needed.[224] This hybrid strategy keeps every block but not every piece of data related to the state tree.[225] By structuring the data in this way, Ethereum can run more advanced light clients, which are nodes that do not process every transaction but instead hold the valid block headers.

4. Enterprise Ethereum Alliance

In February 2017, the Enterprise Ethereum Alliance (EEA) was formed to connect Fortune 500 businesses, startups, academics, and blockchain experts to research and develop industry grade blockchain technology through Ethereum's platform.[226] Industries represented in the alliance include but are not limited to technology, banking, government, healthcare, energy, pharmaceuticals, marketing, and insurance.[227] For example, JPMorgan released Quorum, which is a permissioned implementation of Ethereum that focuses on industry-grade data privacy.[228] Because Quorum is a permissioned network where all participants are trusted and approved, it is unnecessary to use intensive consensus algorithms like PoW or PoS.[229] Instead, Quorum uses a

---

[220] Buterin, supra note 215.
[221] Vitalik Buterin, On Abstraction, ETHEREUM BLOG (Jul. 5, 2015), https://blog.ethereum.org/2015/07/05/on-abstraction/.
[222] Buterin, supra note 215.
[223] Id.
[224] Id.
[225] Id.
[226] Hewlett Packard Enterprise and 47 Organizations Join 200-Member Strong Enterprise Ethereum Alliance, ENTERPRISE ETHEREUM ALLIANCE (Oct. 18, 2017), http://entethalliance.org/hewlett-packard-enterprise-47-organizations-join-200-member-strong-enterprise-ethereum-alliance/.
[227] Id.
[228] JPMORGAN CHASE, QUORUM WHITEPAPER 1 (2016), http://github.com/jpmorganchase/quorum-docs/blob/master/Quorum%20Whitepaper%20v0.1.pdf.
[229] Id. at 2.

smart contract based, majority voting consensus model called QuorumChain.[230] QuorumChain designates certain nodes as voting nodes who vote "which block should be the canonical head at a particular height. The block with the most votes will win and is considered the canonical head of the chain."[231] Additionally, like miners in PoW, certain nodes are given the maker role, which permits them to create blocks.[232] When a maker node creates a block, they sign it, and other nodes compare the signature with a list of approved maker nodes to verify that the maker node has permission to create a block.[233] Quorum is also integrated with Porosity, which is an EVM decompiler that makes it easier to detect bugs in smart contract code by reverting it to the source code.[234] Another example of a consortium blockchain initiative is Microsoft's Coco Framework.[235] Coco uses trusted execution environments (TEE) to enable a high scale, confidential blockchain network.[236] Coco is not a protocol but rather an administrative ledger that sits on top of other protocols like Ethereum, Quorum, and Hyperledger's Sawtooth.[237] As such, the network constitution sets out to define minimum network policies including the membership list, the code manifest of all approved code, the TEE manifest, the validating nodes list, and the voting policy.[238] Additional policies standards developed could include approved GDPR contractual clauses and model BCRs.[239] Also supporting pluggable consensus algorithms like Paxos and Caesar, Coco is an easily deployable blockchain platform for enterprises.[240] These are just two examples of applications from EEA members that are pushing forward industry adoption of blockchain. With over 200 members, the EEA is the world's largest open-source blockchain initiative.[241]

B. Linux's Hyperledger

Hyperledger is a permissioned and shared ledger designed for the implementation of industry-specific blockchain use cases.[242] Started in 2015 by the Linux Foundation, Hyperledger

---

[230] Id. at 4.
[231] Id. at 2.
[232] Id.
[233] Id.
[234] Michael del Castillo, "First" Ethereum Decompiler Launches with JP Morgan Quorum Integration, COINDESK (July 27, 2017, 21:15 UTC), http://www.coindesk.com/first-ethereum-decompiler-launches-jp-morgan-quorum-integration/.
[235] MICROSOFT, THE COCO FRAMEWORK 4 (Aug. 10, 2017), http://github.com/Azure/coco-framework/blob/master/docs/Coco%20Framework%20whitepaper.pdf.
[236] Id.
[237] Id. at 5.
[238] Id. at 10.
[239] See id.
[240] See id. at 15, 24.
[241] Hewlett Packard Enterprise and 47 Organizations Join 200-Member Strong Enterprise Ethereum Alliance, ENTERPRISE ETHEREUM ALLIANCE (Oct. 18, 2017), http://entethalliance.org/hewlett-packard-enterprise-47-organizations-join-200-member-strong-enterprise-ethereum-alliance/.
[242] Brian Behlendorf, Meet Hyperledger an "Umbrella" for Open Source Blockchain & Smart Contract Technology, HYPERLEDGER BLOG (Sept. 13, 2016),

is an open source project comprised of a consortium of more than 100 enterprises with the goal of developing industry-specific blockchain frameworks.[243] Like Ethereum's smart contracts, Hyperledger uses the term "chaincode" to refer to its executed on-chain code.[244] Hyperledger's chaincode functionality allows members to encode arbitrary rules based on the type of transaction, the operating protocols for a private channel, or the protocols to endorse and validate transactions.[245] Hyperledger's modular framework allows for the development of enterprise-grade blockchain applications among its members.[246] As a blockchain framework for enterprises, Hyperledger hosts different blockchain frameworks created by these institutions under its umbrella with the one-day goal of interoperability with multiple blockchain ledgers.[247]

1. Fabric

Fabric is Hyperledger's primary infrastructure. It is a modular framework that supports pluggable implementations of various components that allows members of any industry to participate in the network.[248] Through Fabric, members are known based on the issuance of digital certificates and IDs.[249] Transaction privacy and confidentiality are achieved through the use of private channels as well as transaction level keys.[250] The private channels coincide with the permissioned network but require another permission to view and access the channel information.[251] The transactions on Fabric are constructed in such a way that only the parties to the transaction can see the details.[252] Consensus is still reached using pluggable consensus protocols.[253] With consortiums, another level of obscuring transaction information is needed to maintain privacy. If a consortium participant has unique or large volumes of transaction data, it would not be difficult to identify the party despite pseudonymization. Therefore, different transactional keys are generated for each transaction. To generate new transaction keys, a centralized key issuing authority would be tasked with doing so and would map the transaction keys with the party's core key. The core private key and the transaction keys mappings are never made public. Despite shared resources going into the development of the consortium, the privacy of its participants in the ordinary course of business is still maintained.

---

http://www.hyperledger.org/blog/2016/09/13/meet-hyperledger-an-umbrella-for-open-source-blockchain-smart-contract-technologies.

[243] Diana Ngo, Hyperledger Project Hits 100 Members with Addition of China's SinoLending, Gingkoo, ZhongChao, BITCOIN MAGAZINE (Nov. 30, 2016, 1:30 PM), http://bitcoinmagazine.com/articles/hyperledger-project-hits-members-with-addtion-of-china-s-sinolending-gingkoo-zhongchao-1480530607/.

[244] CHRISTIAN CACHIN, ARCHITECTURE FOR HYPERLEDGER BLOCKCHAIN FABRIC 2 (July 2016), http://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf.

[245] Id.

[246] Id.

[247] Id.

[248] Id.

[249] Id.

[250] Id.

[251] Id.

[252] Id.

[253] Id.

Another contribution to Hyperledger is Sawtooth, which is a platform for building, deploying, and running distributed ledgers.[254] Sawtooth is based on a new consensus algorithm called Proof of Elapsed Time (PoET).[255] PoET, requiring far fewer resources compared to PoW, constructs consensus among parties regardless of the data type and language.[256] One of the key elements of PoET is that these transactions are executed within a trusted execution environment.[257] Another feature of Sawtooth's design is to integrate more easily with Burrow, Monax's implementation of the Ethereum Virtual Machine (EVM).[258] Burrow's permissioned EVM is a general purpose smart contract machine that allows users to run smart contracts compiled by any EVM language compiler in their permissioned blockchains.[259] Because of this integration, Ethereum developers with existing smart contracts are expected to be able to "transition their work to the Hyperledger Sawtooth platform."[260] This integration establishes a strong upstream-downstream relationship between the Sawtooth and Burrow projects.[261] The projects being created under the Hyperledger umbrella show that there is no universal blockchain model.[262] The mentioned examples and developments throughout this section highlight the critical role that industry-wide collaboration plays in the advancement of blockchain technology.

IV. Blockchain Data Transfer Framework

With the proliferation of internet connectivity and new technologies that constantly capture personal data, it is only natural that the laws have responded to the new, globally connected information economy. With a change to an information economy, the GDPR moves the regulatory framework to an information access model. Blockchain facilitates such a change by creating and connecting networks to securely share information. Data, like currency, is a valuable asset that can be transferred digitally and recorded to show who has possession of what assets and where. As seen, the benefits of blockchain include distributed ledgers, secure transactions, and consensus models while the limitations for mainstream adoption include time to reach consensus in the protocols, compatibility of ledgers, and nascence of blockchain government regulations.

Companies can largely comply with the GDPR through proprietary database systems and customer identity and access management solutions currently on the market. However, the underlying push toward a digital single market requires a different technical approach centered on connecting disparate systems. The aim is to create a consortium blockchain for data flows

---

[254] HYPERLEDGER ARCHITECTURE WORKING GROUP (WG), INTRODUCTION TO HYPERLEDGER BUSINESS BLOCKCHAIN DESIGN PHILOSOPHY AND CONSENSUS 13 (Hyperledger Architecture, Vol. 1), http://www.hyperledger.org/wp-content/uploads/2017/08/HyperLedger_Arch_WG_Paper_1_Consensus.pdf.
[255] Id.
[256] Id.
[257] Id.
[258] Adam Ludvik and Casey Kuhlman, Hello World, Meet Seth (Sawtooth Ethereum), HYPERLEDGER (Aug. 22, 2017), http://www.hyperledger.org/blog/2017/08/22/hello-world-meet-seth-sawtooth-ethereum.
[259] Id.
[260] Id.
[261] Id.
[262] DEWEY ET AL., supra note 156, at 80.

based on granular access controls and real-time analysis. The cost prohibitive nature of exploratory technology makes consortiums an ideal organizational structure for organizations to collaborate to improve regulatory compliance. Via smart contracts, organizations can use, produce, and distribute data across boundaries, while ensuring that data remains up-to-date and accurate across all nodes. Blockchain access controls would allow auditors the ability to peer into the network to make sure participants are honest and in compliance.

There are other technical solutions that may be less expensive to perform cross-border data transfers. However, the costs of running afoul is significantly more expensive with the ability to go as high as 4% of the company's worldwide revenue.[263] Thus, with the GDPR's enhanced fiduciary responsibilities to the data subject, it presents the need to demonstrate the ability to run reliable and secure fiduciary code on the blockchain chain. As the blockchain protocol is distributed in nature, the fiduciary code spans the global network of participants regardless of traditional borders increasing reliability and decreasing vulnerability.[264] The goal of establishing a regulatory compliant consortium blockchain is so that companies can freely transfer data across the world through a technological protocol that also alleviates regulators' perceived data protection concerns. Continued blockchain collaboration could lead to a standardized data store allowing companies to transact with each other for data analysis and a dashboard for individuals to track their data. In order to reach the business value-add that data is forecasted to have on the economy, data must be removed from silos and interoperable services built. Combining on-chain and off-chain data storage methods, disparate networks could transact with one another based on coded laws and regulations.[265]

The GDPR requires systems to be privacy by design. Blockchain's infrastructure is privacy by design.[266] The new protocols are putting forward the notion of trusted environments through transparency and traceability while maintaining privacy with cryptographic tools and incentives designed to prevent malicious actors from diverging from the protocol. The first assumption that this paper makes is that the growing trend toward a digital single market will also coincide with individuals having a digital identification. Blockchain companies like uPort and Civic are focusing on creating digital identities.[267] Another private initiative is between Microsoft and Accenture.[268] Currently in the prototype phase, Microsoft and Accenture are developing a blockchain based ID network designed to allow individuals with direct control over who has

---

[263] See GDPR, supra note 5, at art. 83(5).

[264] Nick Szabo, The Dawn of Trustworthy Computing, UNENUMERATED (Dec. 11, 2014), http://unenumerated.blogspot.com/2014/12/the-dawn-of-trustworthy-computing.html.

[265] See GUY ZYSKIND ET AL, DECENTRALIZING PRIVACY: USING BLOCKCHAIN TO PROTECT PERSONAL DATA 5 (2015), http://web.media.mit.edu/~guyzys/data/ZNP15.pdf [hereinafter DECENTRALIZING PRIVACY].

[266] MEDHI BENCHOUFI AND PHILLIPPE RAVAUD, BLOCKCHAIN TECHNOLOGY FOR IMPROVING CLINICAL RESEARCH 3 (2017).

[267] DR. CHRISTIAN LUNDKVIST ET AL., UPORT: A PLATFORM FOR SELF-SOVEREIGN IDENTITY 2 (2017); see also CIVIC 3 (2017) (explaining the current and future developments of Civic).

[268] Accenture, Microsoft Create Blockchain Solution to Support ID2020, ACCENTURE: NEWSROOM (Jun. 19, 2017), http://newsroom.accenture.com/news/accenture-microsoft-create-blockchain-solution-to-support-id2020.htm.

access to their personal information.[269] Along with an aggregated dashboard, the prototype uses off-chain solutions to maintain the data rather than storing everything on-chain and only calls on the data when the data subject grants access.[270] As well, countries are launching pilot programs for state backed blockchain ID platforms. Estonia, an EU Member State, has been a leader in becoming an electronic country and it has led the way in terms of implementation.[271] Estonian citizens have digital id cards and majority of interactions in the country are authenticated using digital signatures.[272] Further, Estonian citizens can access a site to see a log of who has accessed their personal data and can report suspicious activity.[273] In the realm of blockchain, Estonia now allows health patients to control their data access through "Keyless Signature Infrastructure."[274]

Having a digital ID would aid a data subject's efforts to maximize his rights under the GDPR. Article 12(2) and 12(6) are not difficult to implement via blockchain and methods of identity verification are already in practice. While society is still years away from every citizen having a digital ID, cryptocurrency exchanges use required identification methods to stay in compliance with Know Your Customer (KYC) and Anti-Money Laundering (AML) laws.[275] For example, if you start an account on Coinbase, you will be asked for additional information beyond a log in email address and password. The additional information is an ID and photo verification. The ID can be a driver's license or passport. The photo is taken via your webcam prior to uploading it. More robust security could additionally add a Two Factor Authentication (2FA) along with the photo taken prior to submitting an identity verification request.[276] 2FA is commonly used when logging into accounts once past the verification process and is just one method of multi-factor authentication. Similarly, Sony has a patent application for a blockchain based multi-factor authentication system for user login that could also support user identification

---

[269] Id.
[270] Id.
[271] Ben Hammersley, Concerned about Brexit? Why not Become an E-Resident of Estonia, WIRED (Mar. 27, 2017), http://www.wired.co.uk/article/estonia-e-resident. Unfortunately, Estonia discovered a vulnerability in their system and suspended approximately 760,000 ID cards used for voting, filing taxes, and encrypting sensitive documents. Dann Goodin, Flaw Crippling Millions of Crypto Keys is Worse than First Disclosed, ARS TECHNICA (Nov. 6, 2017, 4:10 PM), http://arstechnica.com/information-technology/2017/11/flaw-crippling-millions-of-crypto-keys-is-worse-than-first-disclosed/?utm_source=dlvr.it&utm_medium=twitter.
[272] Id.
[273] Id.
[274] Martin Ruubel, Estonian eHealth Authority Partners with Guardtime to Accelerate Transparency and Auditability in Health Care, GUARDTIME: BLOG & NEWS (Feb. 12, 2016), http://guardtime.com/blog/estonian-ehealth-partners-guardtime-blockchain-based-transparency.
[275] KYC is a term for the processes used to confirm customers' real identities as required by government regulations outlining these processes. AML refers to processes designed to prevent money laundering and illegal income generating activity. The purpose of KYC and AML is to prevent crimes such as financial fraud, identity theft, money laundering, etc.
[276] 2FA is a two-step verification process that asks for a user name and password as well as a randomly generated code that is only accessible on the user's device for a very short period of time. For example, the Google Authenticator app uses a six-digit one-time password.

verification for data transfers, contract generation, and other asset transfers.[277] The system is not limited to blockchain but rather any form of distributed database system.[278] Also, Comcast has a patent application that describes two distributed databases for user ID management.[279] The first distributed database would be a master ID database for each user's private and identifiable information and would maintain a log of every time someone accessed the user's data.[280] This database would resemble a blockchain database.[281] The second database, more like a distributed platform, would contain location information for the user's data on the first database serving as a reference guide for those accessing the user's data.[282] Comcast's goal is to organize user's habits from different content provider platforms into a searchable repository of data.[283]

It is clear that digital IDs will be used throughout society going forward. A move toward self-sovereign digital IDs combined with smart contracts would allow the full maximization of the data subject's rights under GDPR. Current technical issues in identifying individuals are subject to expensive and time-consuming KYC processes; are reliant on third parties for data storage; and are subject to high liability to safeguard data subject's personal data as it presents a clear single point of failure and thus a target for malicious actors. With the identity controlled by the data subject, the data subject controls his data and counterparties to transactions will not retain sensitive data to verify the transactions. The change would reduce liability while allowing frictionless KYC.

Other than more efficient identity verification, secure data sharing on a global scale is possible in a transparent and auditable manner using blockchain. Blockchain allows for differential privacy. As more and more people are working on machine learning and AI, data sharing can lead to better models. As well, with testing the data, audit trails on the data and models would lead to more people having trust in the machine learning outcomes. Blockchain enables auditability and provenance of data by default. As it stands, the GDPR is clear that data subjects have a right not to be subject to automated decision making in some form or fashion. Still, with the large swaths of data, human intervention on some level is necessary to sort, clean, and standardize data from multiple sources before applying a new machine learning model to the data.

Allowing data subjects more rights of control over their data also requires the subjects to know who has access to their data. Filecoin, a file storage blockchain, uses two proofs-of storage schemes that allow users to prove that the data storage providers are in fact storing their data.[284] The two of the proof-of-storage schemes are proof-of-replication and proof-of-spacetime

---

[277] U.S. Patent Application No. 15/419182, Publication No. 20170310653 (published Oct. 26, 2017) (Sony Corp., applicant).
[278] Id.
[279] U.S. Patent Application No. 15/436240, Publication No. 20170322992 (published Nov. 9, 2017) (Comcast Cable Communications, LLC, applicant).
[280] Id.
[281] Id.
[282] Id.
[283] See id.
[284] PROTOCOL LABS, FILECOIN: A DECENTRALIZED STORAGE NETWORK 10 (2017), http://filecoin.io/filecoin.pdf.

(PoSt).[285] Proof-of-Replication allows a prover "to convince a user that some data has been replicated to its own uniquely dedicated physical storage."[286] PoSt allows a prover to convince a verifier that the prover is storing the outsourced data for some time.[287]

When transacting in data today, the process is largely irreversible. Once the data is sent, it is hard to further control it. However, blockchain, through private and secure computations, could allow access controls through digital signatures and programmable permissions to facilitate data transactions.[288] A promising initiative is the Enigma project, which combines on-chain and off-chain data storage using hashes as pointers to the stored location of the data.[289] Data collected is encrypted and a pointer to the off-chain distributed hash table is located on the chain, which store references to the data but not the raw data.[290] The data can be queried based on permission to access the data.[291] This particular data storage for international organizations allows for internal compartmentalization and greater productivity because more employees could securely access the data through pre-coded access rules that are compliant with the law.[292] Connecting multiple data sources could as well create a marketplace allowing individuals and organizations to freely transact in data.[293]

The vision of connecting multiple data sources is shown through a working prototype of MedRec, a blockchain for medical data access and permission management.[294] MedRec, building on Enigma's work, uses hashed pointers to keep raw data from being stored on-chain. APIs are used to provide interoperability among provider databases.[295] Using Ethereum based smart contracts, the contracts contain metadata about the records and a cryptographically signed message with instructions on how to manage ownership, permissions and data integrity.[296] Smart contracts can be encoded with any desired arbitrary policies to achieve the desired transaction type. Additionally, miners are incentivized in another way to contribute computational resources to keep the system honest. In Ethereum and Bitcoin, the reward is a monetary reward for expending computational resources. Understanding that rewards for maintaining trustworthiness of the system do not need to only be monetary rewards, MedRec offers the validators receive access to aggregated, anonymized medical data.[297] Because MedRec also provides querying capabilities and API libraries, future iterations could include an option for miners to request

---

[285] Id.
[286] Id.
[287] Id. at 11.
[288] See GUY ZYSKIND ET AL., ENIGMA: DECENTRALIZED COMPUTATION PLATFORM WITH GUARANTEED PRIVACY 2, 4 (2015), http://www.enigma.co/enigma_full.pdf [hereinafter ENIGMA].
[289] See DECENTRALIZING PRIVACY, supra note 265, at 1.
[290] Id. at 2.
[291] Id.
[292] ENIGMA, supra note 288, at 12
[293] Id.
[294] EKBLAW ET. AL, supra note 177, at 1-2.
[295] Id. at 1.
[296] Id. at 2.2.
[297] See id. at 2.6.

specific sets of data.[298] The goal is to build a comprehensive medical record based on data from all medical providers as well as Fitbit, Apple HealthKit, and more that allows the patient to permit and restrict access to their data.[299] Although MedRec is designed for medical record management, the data concerns outlined within the MedRec white paper are among those data concerned outlined in the GDPR.

Additionally, security of the network grows as the number of nodes and miners participating in the network increases. With more participants, more people are storing the continuously growing database of transactions thereby increasing the costs of creating fraudulent transactions and decreasing the likelihood of a successful malicious attacker. Public blockchains support extrinsic incentives because operating honestly yields monetary rewards. In a regulated consortium, the incentives can be both intrinsic and extrinsic. Thus, non-profits, research labs, and universities could serve as validators in exchange for non-monetary extrinsic incentives through access to certain data that could be queried in its encrypted state. Other than being a proposed validator reward in medical blockchains, there are real world examples of large corporations donating data to these institutions.[300] For example, when Brewster Kahle, founder of the Internet Archive, sold Alexa Internet to Amazon, he included a contractual provision that Amazon donate Alexa Internet data to the Internet Archive.[301] Ideally, non-profits, like Internet Archive, could join the consortium blockchain as a validator node in exchange for data from a variety of sources that align with its efforts as a digital archive. Doing this form of data philanthropy under the GDPR would also require affirmative consent from the data subject and the data subject's dashboard would be updated in this event to represent a new entity that has access to his personal data. Further, the for-profit organizations have intrinsic incentives because their participation in the network ensures auditable data flow compliance.[302]

The GDPR permits data transfers based on contractual clauses and BCRs. If written with the intent to automate the execution of compliant data transfers outside of the EU, the contracts can take the form of smart contracts. Contract design requires observability by the principals, verifiability by third parties, and privity by those involved in the contract.[303] Observability is the ability of the parties to a contract to observe each other's performance of that contract or to prove their performance to the other party.[304] Verifiability is the ability of a party to prove to a third-party arbitrator that a contract has been performed or breached.[305] Privity is the idea to minimize the number of parties given access to the information about a contract and the contract's performance.[306] In smart contract design, the problem is that observability and verifiability

---

[298] Id. at 2.3.2, 2.5.1, 5.
[299] Id. at 4.
[300] See id. at 2.6.
[301] Recode Staff, Full Transcript: Internet Archive Founder Brewster Kahle on Recode Decode, RECODE (Mar. 8, 2017, 11:30 AM), http://www.recode.net/2017/3/8/14843408/transcript-internet-archive-founder-brewster-kahle-wayback-machine-recode-decode.
[302] See TRENT MCCONAGHY ET AL., BIGCHAINDB: A SCALABLE BLOCKCHAIN DATABASE 29 (2016).
[303] Szabo, supra note 191.
[304] Id.
[305] Id.
[306] Id.

require exposure to information while privity seeks to minimize vulnerabilities to third parties.[307] Minimizing information leaks to third parties during the performance of a contract is where zero knowledge proofs can be invoked.[308] Once the smart contracts are executed and transactions are verified, the information is stored in a post-unforgeable transaction log that can be published using cumulative hashes of the transaction stream.[309]

When parties to a private contract require cryptographic state consensus evidence, a distributed application can retrieve the private contract state hash for a specified block and share this value with the parties to the contract either off chain or through an on-chain transaction. The regulators should only have access to the minimum amount of information required to ensure that the data transfers comply with the GDPR and the fundamental rights of the data subjects are protected. This limited access to information to verify compliance can be achieved through the use of zero knowledge proofs.

Transacting in data is different than transaction in currency. With currency, we are worried about the double spend problem. The double spend problem is one of the reasons why Bitcoin and Ethereum add a step in the transaction process to look at the global state to make sure that the transacting party has the amount of coins they state they have and that they have not already spent the same coins on another transaction. Data does not have the same problem because the transactions could allow for both full transfer of ownership or temporary access to the data. With data, the ability to trace each party that has access to the data is more important than the double spend problem.

Thus, the data records can utilize two transaction types: a creation transaction and a transfer transaction.[310] The creation transaction creates the record of the data, which could include mechanisms found in the GDPR like affirmative consent, purpose limits, the pseudonymized data subject ID, and additional conditions for when consent is needed.[311] A transfer transaction, along with transferring the data, could show who now has access to the data and under what specified conditions or subject to what contract provisions covering access questions. Everything inside of the transactions are of course hashed and timestamped.[312]

The biggest challenge in using blockchain with the GDPR is the right to erasure. Blockchain is commonly referred to as being immutable.[313] In theory, data stored on-chain can be changed.[314] Immutability is used more as a term of art.[315] Multiple factors are used in the protocols that make blockchain practically immutable such as full replication of all the data, nodes monitoring changes, public viewing of the chain, economic incentives as seen in PoW and

---

[307] Id.
[308] Id.
[309] Id.
[310] See TRENT MCCONAGHY ET AL., supra note 302, at 17-18.
[311] See id.
[312] See id.
[313] How BigchainDB is Immutable, GITHUB: BIGCHAINDB, http://github.com/bigchaindb/bigchaindb/blob/master/docs/root/source/immutable.md (last updated Aug. 9, 2017).
[314] Id.
[315] Id.

PoS, node diversity, and cryptographic signatures.[316] Under some interpretations of blockchain, the techniques used to achieve mutability may transition the system from being blockchain based to simply a general distributed ledger system. Based on varying approaches, adding pre-approved, limited, and transparent methods to alter data on an immutable system is a trade-off necessary to be able to utilize the advantages of the technology.

In recognition that the append-only nature of the blockchain is not a viable option for every situation, Accenture has developed re-writable blockchain system.[317] Accenture, a member of both the Enterprise Ethereum Alliance and the Hyperledger Project, uses a chameleon hash to make a permissioned blockchain editable.[318] The ability to edit would be used in a transparent manner by authorized entities under specific constraints to rewrite one or more blocks, compress blocks, and insert blocks.[319] All blockchains are chains of hashed. A trapdoor is created; however, the chain is still collision resistant without knowing trapdoor.[320] A hash function is collision resistant if it is difficult for two inputs to have the same output. By knowing the trapdoor, one could, with transparency and accountability, find the collisions and unlock the door to make the necessary edits to the data without breaking the rest of the blockchain.[321] The change would be represented by a permanent scar that could not be deleted by any party once the scar is made.[322] It is important that the ability to make edits is limited to a small number of pre-approved entities including authorities based on pre-approved conditions like developing a right to erasure request.[323] In the case of a consortium, all members could hold the trapdoor key and redactions would be verified using multi-party computation protocols.

Such a system within a permissioned blockchain would be compliant with the GDPR giving regulators and consumers assurances that the data has been deleted or corrected. However, the method also has trade-offs. Accenture has received criticism over its method because it takes away the immutability and trust feature that blockchain promotes. The point of blockchain is to establish trust through a transparent ledger of transactions verified by trustless consensus algorithms that people can interact with a high level of certainty that previous verified data is still correct. Other than using Accenture's solution, permissioned nodes could transparently annotate the record with the required change and stating the reasoning behind the change similar to version control systems commonly in use. Using IPNS within IPFS, a small amount of mutability can be introduced.[324] The data is stored with a reference to the on-chain has. A change in content

---

[316] Id.
[317] Accenture Debuts Prototype of 'Editable' Blockchain for Enterprise and Permissioned Systems, ACCENTURE: NEWSROOM (Sept. 20, 2016), http://newsroom.accenture.com/news/accenture-debuts-prototype-of-editable-blockchain-for-enterprise-and-permissioned-systems.htm.
[318] See id.
[319] GIUSEPPE ATENIESE ET AL., REDACTABLE BLOCKCHAIN OR REWRITING HISTORY IN BITCOIN AND FRIENDS 2 (2016), http://eprint.iacr.org/2016/757.pdf.
[320] Id. at 3.
[321] Id.
[322] Id. at 6.
[323] Id. at 4.
[324] JUAN BENET, IPFS – CONTENT ADDRESSED, VERSIONED, P2P FILE SYSTEM 3.7 (2014), http://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf.

is rehashed and tied to the original, immutable hash.[325] The erroneous data would still be there, but parties would ignore the data marked incorrect because there would nothing to gain from acting on clearly erroneous data. This way, the data subject or an auditor could track all of the state changes with the data until the finality. Doing so maintains the integrity of the data stored off-chain and on-chain. Another way would be to write a smart contract that allows arbitrary changes outside of the normal business logic if a certain number of signatures approves of the change.[326] Such an outcome makes sense when participants are incentivized to not let erroneous information be on-chain. The process of rectifying data in blockchain is subject to further debate that is outside the scope of this paper.

As for deletion, this is a policy question about revocation of access to the data subject's data. Smart contracts could be used. The GDPR requires controllers and processors to specify the purposes of the data processing and to erase the data once its purpose has been met. In theory, a smart contract could be deployed so that the personal data becomes unsearchable or irretrievable after its purpose has been fulfilled. This solution is more speculative than Accenture's solution because it requires an interpretation or legal decision as to whether or not data would be considered legally destroyed if all traces of it are rendered unsearchable or irretrievable rather than fully erased from the ledger. Conversely, the GDPR only offers protection to living identified or identifiable natural persons. Deceased persons are not protected under the regulation. With this in mind, a smart contract could be deployed that time locks the personal data from anyone accessing it until the data subject's death is verified by an outside, trusted party. However, this would be an unacceptable solution under the GDPR because Recital 27 specifically leaves post-mortem data protection laws to Member States, and many Member States already recognized post-mortem data rights.[327] The right to erasure is an obstacle for blockchain technology. However, introducing limited mutability, based on strict, pre-approved rules, to a fundamentally immutable system is more attractive to regulators than system of rigid immutability.

This paper does not deal with the security of the databases of the individual consortium members. It is assumed that the individual systems store the data securely. However, in the event of data tampering or leakage, the detection process can attribute the damaging activity to the last controller or processor with access to the data. Nor does the paper address undesired data copying as it is assumed that such actions are governed by other off-chain regulations that serve as incentives for the participants to remain trusted. Blockchain initiative are still in their infancy as this year in particular has marked the shift from proof of concepts to pilot programs. Blockchain solutions to the problems discussed are still being contemplated as well as the technology's limitations. It is clear, though, that there is growing interest in embedding blockchain characteristics into enterprise distributed databases.[328]

---

[325] Id.
[326] See ETHEREUM WHITE PAPER, supra note 186, at 23-24.
[327] See GDPR, supra note 5, at recital 27; See also J.C. Buitelaar, Post-Mortem Privacy and Informational Self-Determination 135 (Ethics Inf. Technol., Mar. 29, 2017), http://link.springer.com/content/pdf/10.1007%2Fs10676-017-9421-9.pdf (noting the countries that recognize post-mortem data rights).
[328] See TRENT MCCONAGHY ET AL., supra note 302, at 1.

V. Conclusion

This paper is meant to start a conversation around using blockchain to work with regulations to facilitate the free flow of personal data in a highly secure environment. Transacting in personal data will always be a highly bureaucratized issue, and this paper is not advocating for a complete decentralization of the way countries, individuals, and companies think about data flows. However, better technology can serve as a baseline to decrease transaction and compliance costs while minimizing risks in as efficient a manner as possible. Rather than focusing on regulating unknown risks, multiple stakeholders should come together to focus on the fundamental benefits that blockchain technology has to offer. Similar to how the internet has become a necessity to doing business, access to data is beginning to have the same impact. As important as data security and confidentiality are to this entire effort, misguided regulations can drive up costs unnecessarily resulting in information being trapped in national silos. If governments remain on the current path, networks might remain disparate meaning that data flow markets will to remain largely regional rather than truly global.

The GDPR shows that the EU is moving in the direction of grappling with the reality of a Digital Single Market. The shift in data protection requirements continued in the GDPR enables individuals to have an ownership interest in the data that is being collected by the companies with which they interact. Blockchain is a technology that, among other things, highlights notions of user control around an individual's digital identity. Undoubtedly, Europe is leading the world regarding blockchain innovation and legislative initiatives. Estonia, Switzerland, Slovenia, and Finland are quickly becoming hubs for blockchain innovation by establishing legislation embracing the technology. Further, the EU Commission will spend €30 billion on research and innovation under the Horizon 2020 program that included blockchain as a technology at the core of today's most promising innovation breakthroughs.[329] This program will also invest in 30 initiatives based in non-EU nations so as to increase global collaboration in research and innovation.[330] As with previous globalized technological breakthroughs coming from the European region like the World Wide Web, Europe is again creating the infrastructure for further technological advancement.[331]

Still, there is a need to adopt flexible policies that allow for the continued growth of the technology and inclusion of others in support of long-term sustainability. "Cooperation is the basis for productivity."[332] Harmonizing frameworks such as the GDPR with other jurisdictions could serve as a basis to for establishing a protocol for international data flows. The EU has set out to promote four freedoms: the free movement of capital, people, goods, and services.[333] With the commoditization of the Internet, the free flow of data in a secure fashion should be added to this list of freedoms.[334] As with Blockchain, the GDPR, at the core, is a means to transcend the

---

[329] European Commission Press Release IP/17/4122, Commission to Invest €30 Billion in New Solutions for Societal Challenges and Breakthrough Innovation (Oct. 27, 2017).
[330] Id.
[331] See History of the Web, WORLD WIDE WEB FOUNDATION, http://webfoundation.org/about/vision/history-of-the-web/ (last visited Oct. 21, 2017).
[332] Polk Bros. v. Forest City Enters., 776 F.2d 185, 188 (7th Cir. 1985).
[333] Estonia Ministry of Economic Affairs and Communications. Estonian Vision Paper on the Free Movement of Data – the Fifth Freedom of the European Union, 2017.
[334] Id.

borders of EU Member States to set the stage for further innovation. This premise is the subject of a study being launched by the EU Commission exploring how to create an EU blockchain infrastructure and which services are suitable to run on blockchain.[335]

As the GDPR goes into effect, companies are expending significant resources to meet the minimum compliance standards.[336] Corporations will continually exhaust resources going forward to stay in accordance with the regulation or so as not to incur unnecessary fines. What's needed is a clear base layer that allows for innovations on top. It is essential to keep in mind that the optimal outcome is not for the data collected to be in silos. Regulations are meant to be rational rules for people to follow and are intent on trying to regulate emergent phenomena through a simple system that is then fixed in time once passed into law. The problem is that the world is not ergodic and conditions change. Even without technological advancements, radical uncertainty persists. Therefore, collaboration with regulators, technology providers, and data subjects is necessary to develop global interoperability and industry standards so this technology can live up to its promises.

The blockchain initiatives discussed are part of an effort to achieve social scalability. Social scalability is "the ability of an institution – a relationship or shared endeavor, in which multiple people repeatedly participate, and feature customs, rules, or other features which constrain or motivate participant's behavior – to overcome shortcomings in human minds and in the motivating or constraining aspects of said institution that limit who or how many can successfully participate."[337] "The more an institution depends on local laws, customs, or language, the less socially scalable it is."[338] The blockchain protocols being developed seek to decrease our vulnerabilities to outside forces while enabling us to explore more beneficial forms of innovation.[339] The conversation then shifts from worrying about information breaches to the value of information sharing.

As we continue to build more IoT devices, blockchain technology is set to provide immutable identity, authentication, authorization and access control to business processes in smart contract form. The more people are interacting with Internet-connected devices that are capturing and transmitting personal data, the more critical it becomes to strengthen the sense of trust. Blockchain technology closes the trust gap through cryptography and economic incentives, or cryptoeconomics. Through the examples discussed, blockchain technology can be incorporated into regulatory systems. There will be many blockchain networks that will not stand alone. Rather, these disparate networks will interoperate within the increasing distributed ecosystem.

---

[335] Study on Opportunity and Feasibility of a EU Blockchain Infrastructure, EUROPEAN COMMISSION: DIGITAL SINGLE MARKET, http://ec.europa.eu/digital-single-market/en/news/study-opportunity-and-feasibility-eu-blockchain-infrastructure (last visited Nov. 12, 2017).

[336] Pulse Survey: US Companies Ramping Up General Data Protection Regulation (GDPR) Budgets, PWC, http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-gdpr-series-pulse-survey.pdf (last visited Oct. 29, 2017).

[337] Nick Szabo, Money, Blockchains, and Social Scalability, UNENUMERATED (Feb. 9, 2017), http://unenumerated.blogspot.mx/2017/02/money-blockchains-and-social-scalability.html.

[338] Id.

[339] See id.