KING'S College LONDON

Blockchain vs. The Law: Can Blockchain and Data Privacy Co-exist?

Aparnaa Balamurali

Abstract:

Blockchain technology has taken the digital space by storm, redefining technological efficiency in a number of industries. This development though has come about parallel to drastic regulatory reform in response to growing concerns surrounding data security after large scale data breaches called the effectiveness of privacy regulation into question. The EU General Data Protection Regulation was developed to enforce stringent and wide-reaching protection for the personal data of EU citizens, emphasizing data subject autonomy and data controller obligations. The challenge is that the principles prescribed for by the GDPR are in stark contrast with Blockchain architecture and thus in the conventional sense the two struggle to co-exist. This paper explores the various points of tension, and considers possible alternatives that attempt to seek a compromise that respects effective regulation without hindering technological innovation.

Table of Contents:

1. Introduction 4
2. The Problem 6
3. Understanding Blockchain Technology 9
    3.1 What is "Blockchain"? 10
4. The GDPR: Scope, Key Principles and Initial View of Conflict 17
5. Blockchain vs. GDPR 24
    5.1 Does the GDPR apply to Blockchain Technology? 24
    5.2 Who is the 'Data Controller'? 26
        5.2.1. Data Controller obligations 29
    5.3 Territorial Scope 31
    5.4 Data Protection Principles and Data Subject Right 33
6. Alternative Interpretation 41
7. Conclusion 47
Bibliography 49

1. Introduction

The popularity of Blockchain technology is in the efficiency and reliability it introduces into existing mechanisms. While of incredible utility, technological innovation without the legal infrastructure to validate its function is essentially redundant.

Since the emergence of Blockchain, there has been a considerable focus surrounding its financial regulation in the area of crypto-currencies, the most prevalent application of Blockchain technology, but less has been said about the challenges Blockchain faces in the area of data privacy and effective privacy regulation alongside it. At the forefront of global regulatory reform with the recent enforcement of the General Data Protection Regulation ('GDPR') in the European Union ('EU'), this is an area that calls for greater scrutiny in order to decipher whether the two areas, as prevalent and significant to today's economy as they both are, can effectively co-exist after careful consideration of the particular nuances by both parts.

As will be demonstrated, Blockchain technology has already been recognized to have highly effective capabilities across all industries, but there are many aspects of the GDPR that signal towards considerable tension when applied to the technically effective performance of Blockchain. In essence, the challenge is that the GDPR is designed to regulate on a platform where data is collected, stored and processed in a centralized manner, while Blockchain technology operates through decentralizing the data management processes. This calls into question whether Blockchain can be successful in achieving legal validation within the EU.

This dissertation intends to investigate the areas of conflict between Blockchain and privacy regulation and ultimately to demonstrate that without tailored and specific considerations in Blockchain development and legal interpretation, it is difficult to find a clear correlation between the two. This is most particularly the case when dealing with public and un-permissioned Blockchains. This paper recognized that Blockchain technology cannot be regulated by a blanket regime; while the GDPR in comparison attempts to be as all

encompassing and far-reaching as competing jurisdictions will allow. The risk in its current state is that Blockchain could be deemed unlawful under the governance of the GDPR, which could completely stifle any further technological progression.

Adequate protection of fundamental rights has been a continuous battle within the European Union, and particularly in a period of such extreme innovation this challenge is only intensified. While the GDPR demonstrates a robust commitment by the EU to the protection of fundamental rights, economic interests do not correlate with such extensive protection. This paper discusses that as demands on effective data privacy control continue to expand, and the applicability of Blockchain technology continues to develop, there ought to be bespoke engagement between Blockchain innovators and GDPR enforcement bodies to ensure that specific and particular nuances of Blockchain technology are not subject to the blanket GDPR as it stands. Any such regulation needs to take into account the specifics of Blockchain technology. Varied interpretation of the regulation, and the consideration of technological solutions will lend in achieving some reconciliation.

Considering this problem from a legal standpoint, this paper will conclude that while the current state of Blockchain and GDPR is incompatibility, what needs to be achieved is a level of legal adaptability to facilitate technological development and grant legal validity to further innovation. While it doesn't suggest that the objectives of the GDPR be weakened or the architecture be less robust, varied interpretation of the GDPR in a practical sense could provide avenues for different means of compatibility and will facilitate technological development.

2. The Problem

An analysis of one of the most recent and impactful data breaches paints a very clear picture of the importance of effective data protection. Cambridge Analytica, a firm responsible for data analysis including that related to bot the Trump and Brexit campaigns, was exposed as having harvested the personal data of over 50 million Facebook users, using the data to develop software that would allow the firm to predict trends and influence potential voting outcomes[1].

Before even addressing the breach itself, the development of Artificially Intelligent software already raises significant concerns in the space of data protection. That such as the software being developed in this case, or those used in predictive policing or even the technology brought to question in the Google DeepMind/Royal Free development of predictive diagnosis software[2], raise questions surrounding the GDPR's emphasis on purpose limitation when it comes to data processing. As is explored further in subsequent chapters[3], the GDPR aims to constrain the purposes for which data is processed, requiring demonstration of obtaining consent before processing the same data for further purpose. The challenge with Artificial Intelligence is that purposes are spontaneous as the technology develops and the direction of development becomes clearer. This is a challenge that will be addressed further in the subsequent discussion surrounding data privacy and technological innovation.

Returning to the data harvesting scandal itself, Facebook faces a number of significant altercations with the EU's new data privacy regime. The GDPR imposes strict rules as to how data processors go about collecting, processing and storing data. Storing the personal data of millions of users without adequate data security measures, and further more not

---

[1] Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach' (The Guardian, 17 March 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
[2] 'Royal Free – Google DeepMind trial failed to comply with data protection law' (ICO, 3 July 2017) < https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/>
[3] See Chapter 4: The GDPR: Scope, Key Principles and Initial View of Conflict

bringing the breach to necessary attention within the 72 hours that the GDPR now requires could have put Facebook at regulatory risk. With the extent to which Facebook collects, stores and shares the personal data of not only millions of both Facebook and non-Facebook users for the purpose of market research and data analytics[4], the risk of an extensive punishment only continues to grow. Should the breach have happened post GDPR, they would face a fine of close to $1.6 billion[5]. However, in Britain, the ICO sentenced a £500,000 fine for breach of the Data Protection Act, representing mere pocket change for the social media giant.

It could be argued in Facebook's case, experiencing such an extensive breach just months before the GDPR takes effect is a blessing in disguise. A data breach of this magnitude would not be viewed lightly in the light of the GDPR, and Europe has demonstrated no hesitation in reprimanding such giants it the past. The European Commission forced Apple to pay back some €13million for falling foul of EU rules in their Irish headquarters[6]. Undertakings will no longer be able to benefit from the less stringent regulatory rules in Ireland with the GDPR in force. Post-GDPR, Google has also been fined £3.8 billion by the EU for breaching competition regulations[7]. While this is not pursuant to a data breach or directly related to the GDPR, it highlights the determination by the EU to ensure adherence to EU regulations and demonstrates the punitive confidence the GDPR aims to enhance.

Scandals like those so aptly demonstrated by Facebook/Cambridge Analytica are what the GDPR aims to avoid with its far-reaching and rigorous regulatory policies, and in the case of the conventional centralized storage mechanisms by large organizations like Apple or Facebook (which would typically pose the largest threat to data security), the GDPR will likely be successful in deterring against flimsy security measures and encourage a more proactive attitude towards data protection. This can only genuinely foreseen in

---

[4] Kurt Wagner, 'This is how Facebook collects data on you even if you don't have an account' (Recode, 20 April 2018) <https://www.recode.net/2018/4/20/17254312/facebook-shadow-profiles-data-collection-non-users-mark-zuckerberg>
[5] as 4% of their annual turnover per GDPR Article 83
[6] Rob Price, 'Facebook may be underestimating the challenge is faces in Europe' (Business Insider, 26 April 2018) <https://www.businessinsider.com/gdpr-facebook-legal-challenges-q1-2018-4/?IR=C>
[7] Michael Baxter, 'EU fines Google £3.8 billion, and that's without a data breach' (GDPR:Report, 19 July 2018) < https://gdpr.report/news/2018/07/19/eu-fines-google-3-8-billion-and-thats-without-a-data-breach/>

circumstances where accountability is at the center of its success. With Blockchain technology, the challenge of finding a party to hold accountable for data breaches in the first place begs the question of whether the GDPR can have the same effect in a decentralized environment. With initial analysis, the answer to this question appears to be no.

3. Understanding Blockchain Technology

In order to effectively analyse the challenge that Blockchain faces in the light of the GDPR, it is necessary first to understand in relevant detail how and in what context Blockchain technology operates.

In its standard form, Blockchain is a distributed database, meaning it is not stored at one central source, with the function of maintaining a constantly expanding chronological list of records, referred to as "blocks". It originated in the digital currency space with the creation of Bitcoin; work began on the financial concept in 2007 by the anonymous 'Satoshi Nakamoto', with the original 'genesis' block being mined in 2009[8].

The Blockchain technology that underpinned Bitcoin is what has since been extracted from currency exchange and applied to a multitude of other industries and inter-organizational methods[9]. The "smart contract" has been used to represent other financial instruments such as bonds or loans, rather than merely cash-like applications[10], and allows for prescribed automatic transactions subject to particular conditions being met. In just 11 years the Blockchain landscape has expanded rapidly, continuously advancing its potential, and encroaching a level of everyday applicability. Eliminating error from traditional financial services, Blockchain technology is now being applied to asset management, insurance, and cross-border payments[11]. Beyond this, it applies to registration of tangible and intangible property that has been embedded with smart technology, managing property ownership, access and management[12]. Smart Contracts, designed upon an 'if-this-then-that' code necessary for self-execution negates the need for a third party to confirm conditional actions. This technology is being used to secure health records and in health insurance,

---

[8] 'History of Bitcoin: the world's first decentralized currency' <http://historyofbitcoin.org/>
[9] Vinay Gupta, 'A Brief History of Blockchain' (Harvard Business Review, 28 February 2017) <https://hbr.org/2017/02/a-brief-history-of-blockchain>
[10] ibid.
[11] BlockGeeks, '17 Blockchain applications that are transforming society' <https://blockgeeks.com/guides/blockchain-applications/>
[12] ibid.

management of health care, complex billing and drug administration[13]. It is also being used in the music industry[14] to maintain an accurate database of ownership rights and secure transfer of royalties. This means amount of personal and transactional data being used and stored is only increasing[15]. Blockchain can even be introduced to guarantee greater security in the governmental voting system; recently applied to government elections for the first time in Sierra Leone[16]. This should eliminate the potential for electronic voting systems to be manipulated by encrypting the votes[17].

It is clear that the necessity and applicability of Blockchain technology as it is introduced to new industries is undeniable. The essence of the Blockchain is to allow information to be distributed without being copied, altered or replicated, which is attractive in all forms of technology development.

3.1 What is "Blockchain"?

As the term suggests, the Blockchain is a chain of information stored in the form of blocks. It is a distributed ledger, open to anyone to join. The unique quality of the Blockchain is that once data has been recorded within it, it is near impossible for this data to be modified or altered. Each specific block contains a particular content of data, its own unique "hash", and the hash of the previous block (hence the need for the original 'genesis' block').

The data in each block is specific and dependent on the Blockchain itself. In the original 'Bitcoin' form, for example, each block would contain detailed information about a particular financial transaction, such as the sender, receiver and the monetary value. The "hash" for each block is similar to a fingerprint, in that each hash is entirely unique, identifying the specific block and all of its contents. Each block includes a unique hash, created

[13] Bernard Marr, 'This is why Blockchain will transform Healthcare' (Forbes, 29 November 2017) <https://www.forbes.com/sites/bernardmarr/2017/11/29/this-is-why-blockchains-will-transform-healthcare/#14ba10a01ebe>
[14] n. 11
[15] Volodymyr Fedak, 'Blockchain and Big Data: The match made in heavens' (Medium, Towards Data Science, 21 February 2018) <https://towardsdatascience.com/blockchain-and-big-data-the-match-made-in-heavens-337887a0ce73>
[16] John Biggs, 'Sierra Leone just ran the first Blockchain-based election' (Tech Crunch, 15 March 2018) <https://techcrunch.com/2018/03/14/sierra-leone-just-ran-the-first-blockchain-based-election/>
[17] n. 11

corresponding particularly to the content of that block at the point of creation. This means that if the content of a block is changed, the hash will be caused to change as well. Therefore the hash in itself is a useful tool in detecting any changes to a block, as once the fingerprint has been changed, the identity of the block is altered. Finally, each block also carries the hash of the preceding block. This feature allows each block to maintain a dedicated connection to the previous block, continuing all the way back to the original 'genesis' block. Thus when a block is tampered with, causing the hash to change as well, this would make all subsequent blocks invalid as the hash they hold for the pre-tampered form of the block, thus no longer applicable as in essence that block no longer exists. Therefore, changing a single block will invalidate the entirety of the remaining chain.

The record of the previous hash is not enough to maintain the thorough security of the chain, as technically computers have the power to rapidly recalculate each subsequent hash to validate the chain once a block has been tampered with. In order to alleviate this possibility, Blockchains also require 'proof-of-work'. This mechanism proves highly effective in slowing the creation of new blocks. Back to the example of Bitcoin, it takes close to ten minutes for each new block to be created[18], in which time the necessary proof of work is calculated and a new block is added to the chain. This means that when a block is tampered with, not only must each subsequent hash be recalculated; the proof-of-work for all the following blocks will need to be recalculated as well, which is a lengthy, complicated and near impossible process.

Both hashing and the proof-of-work mechanism support the reputed high level of security, but one additional feature further ensures that a Blockchain is secure. A Blockchain is characteristically distributed. Instead of one central entity responsible for managing the chain, it operates within a peer-to-peer network, which anyone can join. Each new member gains access to a full replica of the Blockchain, which can be used to verify the validity of the chain. When a new block is created, it is sent to all network members, each of whom will verify the new block to ensure there has been no tampering. So long as this is confirmed, each node will then add the new block to their own Blockchain. This consensus

[18] Simply Explained – Savjee, 'How does a Blockchain work' (13 November 2017) <https://www.youtube.com/watch?v=SSo_EIwHSd4>

mechanism gives all members of the peer-to-peer network the opportunity to agree on the validity of new blocks. Any tampered blocks will be rejected from the chain by other nodes in the network.

The security of a Blockchain is thus enforced through a number of mechanisms. In order for a block to be successfully tampered with, every subsequent block must have their hash re-define, the proof-of-work will have to be recalculated, and a majority consensus must be reached as to the validity of the block, requiring control of more than 50% of the peer-to-peer network[19].

As described by Don and Alex Tapscott[20], the Blockchain can record "virtually anything of value". Its defining principles have driven so many industries to extract it from its originally monetary application to be used in a variety of other means.

Considerably durable and robust, through its distributed architecture a Blockchain is not controlled by a single entity and thus doesn't have a single, identifiable point of failure. Reverting to the Bitcoin example, in the ten operational years, any disruption has been due to mismanagement or hacking rather than any technological flaw[21]. While incidents such as the 2016 DAO hack do demonstrate a vulnerability to Blockchain[22], it demonstrates that Blockchain is only susceptible to human error or malicious intent, but the technology itself has proven entirely secure. Technology Futurist Ian Khan concedes that this property gives Blockchain the means to require the highest degree of accountability. It eliminates error and doesn't allow for progression without consent. Transactions are guaranteed through the distributed secure validation mechanism[23].

---

[19] ibid.
[20] Don Tapscott and Alex Tapscott, 'Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World' (Portfolio/Penguin, 2016)
[21] Blockgeeks, 'What is Blockchain Technology' (June 2016) <https://blockgeeks.com/guides/what-is-blockchain-technology/>
[22] Muhammad Mehar et al., 'Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack' (26 November 2017) <https://ssrn.com/abstract=3014782>
[23] Ian Khan, TEDx speaker, as referenced in 'Bitcoin and Cryptocurrency Technologies' (Christopher Nygaard, R&C Publishing 2018).

Further, in theory, the Blockchain is a transparent and incorruptible network. The necessary stage of consensus described above creates a continuously self-auditing environment. The transparency comes from the peer-to-peer element of the network, and the difficulty in effectively altering blocks due to the hashing and proof of work mechanisms lends to its incorruptibility.

To analyze Blockchain from a data privacy perspective, further technical understanding is necessary. There is a two-step verification process that is necessary for Blockchain to function. Each member has their own unique public key, which is an exclusive combination of numbers and letters by which they are represented. This is synonymous with a pseudonymized account name on any online platform. Combined with the public key, each user also has a private key. This is to the public key as a password is to a username. The public and private keys are combined through a complex mathematical relationship, which provides the means by which the private key can decrypt data originally encrypted by the public key[24]. In practice, the owners of public keys are thus maintained anonymous until combined with the supplementary identifiers.

'Nodes' in the peer-to-peer network refer to the various computers between which the ledger is distributed and stored. These are relevant in understanding the difference between public, permissionless, and private, permissioned Blockchains. Where the Blockchain is public and un-permissioned, the necessary software must simply be downloaded and operated in order to engage the node[25], with no other permission necessary for access to the network.

Notably, data stored on a decentralized ledger can be stored in a variety of ways. The simplest of these is to store the data in the form of plain text[26], but understandably this is the most objectionable means of storage given the ease of access on a permissionless chain. For this reason, encryption or hashing measures are typically put into effect before data is added to a Blockchain. There storage mechanisms are vital to understanding data

---

[24] Michele Finck, 'Blockchains and Data Protection in the European Union' (30 November 2017). Max Planck Institute for Innovation & Competition Research Paper No. 18-01. <https://ssrn.com/abstract=3080322>
[25] ibid.
[26] ibid.

storage on the Blockchain. Returning to the Bitcoin example, data will be stored in two forms: There will be the 'header' in which you will find superficial information such as the timestamp, the source of the data and the hash of the previous block. Such information will typically be stored without encryption. The other form of data can be termed the 'payload', referring to the valuable data contained in the block; which in Bitcoin would be the details of the transaction itself[27]. This data must be encrypted for obvious reasons, and this is where the private key is necessary.

The underlying challenges standing in the way of the legal validation and support of Blockchain stem from the variations in architecture of its numerous applications. Each possesses different features, which must find their own ways to comply with the GDPR.

Bitcoin is the original form; a public, permissionless, decentralized Blockchain that anyone can gain access to with the relevant software. In comparison with the conventional database, the kind most probably in mind during the drafting of the GDPR in relation to data storage, the public and permissionless Blockchain is clearly most at odds with EU data protection standards.

Alternatively though, Blockchains can exist in a private, permissioned form. This means they are distributed within a private network, i.e. an intranet rather than the Internet, where someone attempting to entertain a node on the network must first seek permission from a network administrator. While this is more desirable as a means of respecting data privacy given that the architecture is more inline with that of a traditional database, this paper will maintain focus on the un-permissioned and therefore more risk-prone architecture of Blockchain in its GDPR analysis.

Beyond this, it is necessary also to further differentiate Blockchain application into on-chain and off-chain processing[28]. 'On-chain data' describes the original form of Blockchain technology, cryptocurrency. This term describes a ledger on which the data is only existent so long as the Blockchain itself is existent. This further demonstrates the concern

[27] ibid.
[28] Jacob Eberhardt and Stefan Tai, 'On or Off the Blockchain? Insights on Off-Chaining Computation Data' (European Conference on Service-Oriented and Cloud Computing, Springer, September 2017) pp. 3 - 15

surrounding a public, permissionless Blockchain. Off-chain assets, in contrast, are assets that maintain a tangible existence outside of the Blockchain, with their own legal identity. This refers to Blockchain technology used in management of intellectual property, shares, medical apparatus or even pharmaceuticals. The existence of such assets, unlike the existence of Bitcoin, does not depend on the maintenance of the distributed ledger itself. This is a relevant consideration in the analysis of technical solutions to the legal resistance of Blockchain.

Blockchain technology has been able to eradicate three key points of vulnerability that present in a traditional database; forgery, omission and deletion[29]. However, the choice between a permissionless or a permissioned Blockchain calls for a trade-off between the three. While both maintain the ability to mitigate the risk of forgery given the various validation mechanisms previously addressed, permissionless Blockchains are able to correct the risk of omission given the broad access to the network, while permissioned Blockchains are able to mitigate the risk of deletion given the contained access to the network.

The notion of 'permission' is extremely relevant to the challenge between Blockchain and data privacy. The 'permissioned' concept is characterized through the nature of the consensus mechanism. While each node on a permissionless Blockchain must reach a consensus as to each transaction, only a selected group of nodes have the right to do so on a permissioned network[30]. What these variations demonstrate so far as permission and data storage are concerned is that various designs are necessary for differing responsibilities and priorities of Blockchain application, and each has their own implications where data privacy is concerned.

Practically, enhanced security is a defining and majorly benefitting characteristic of the Blockchain. The decentralized nature of the Blockchain significantly diminishes the risk

---

[29] Robert Sams, 'Blockchain Finance', presentation (March 2015) <https://www.slideshare.net/rmsams/blockchain-finance> as references by Cagla Salmensuu, 'The General Data Protection Regulation and Blockchains' (1 January 2018) <https://ssrn.com/abstract=3143992>
[30] Cagla Salmensuu, 'The General Data Protection Regulation and Blockchains' (1 January 2018) <https://ssrn.com/abstract=3143992>

involved with data being stored in one central location and having one identifiable and targetable source. Without this source, the ease of access and thus the vulnerability of data are removed. On the face of it, this appears to be a guarantee of substantive privacy, but in reality these principles cannot blend effectively with the requirements for data protection, particularly with regards to access, accountability, data minimization, rectification and erasure[31].

[31] GDPR Chapter 3 – Rights of the Data Subject

4. The GDPR: Scope, Key Principles and Initial View of Conflict

Blockchain transactions are designed in such a way that they will be recorded in a ledger, distributed across the entire network and all of its users. Coupled with the consensus mechanism, this means no block or its contents can be altered or deleted[32]. While a key strength of Blockchain technology, it is also responsible for great tension with the GDPR, which calls for data subject autonomy in rights to data rectification and erasure[33], among others. Blockchain provides the means to remove the intermediary from a transaction, so while it is accountable in minimizing room for error, it doesn't represent accountability as the GDPR intends, as there is no intermediary party to be held accountable for data protection.

Data is increasingly essential to today's global and technology dependent economy. Cross-border data transfers have seen a significant incline in recent years[34] parallel to economic development, which has begun to spark considerable tension. Barriers to data flow can suppress the extent of potential economic growth, but such free-flow cannot persist without effective privacy protection, which is what calls for a balance between data flow and data privacy to be struck[35].

There are currently at least 34 jurisdictions with stringent 'data localization' policies, which includes a number of major economic influencers such as China and Russia[36]. Data localization policies intend to legislatively require that any data belonging to citizens of a particular country be collected, stored and processed at a domestic level, subject to strict requirements, notifications and permissions prior to any international transfer[37]. These

---

[32] n. 30
[33] see GDPR Articles 16 and 17
[34] Globalization has been redefined through the trade of data rather that the trade of goods of cross-border capital flows. See James Manyika et al., 'Digital Globalization: The New Era of Global Flows', (McKinsey, January 2016) < https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows>
[35] Sabine Bendiek, 'The New Global Economy Runs on Free Flow of Data and Trust', (The B20, 24 February 2017) <http://www.b20germany.org/priorities/digitalization/digitalizationdossier/digitalization-article/news/the-new-global-economy-runs-on-free-flow-of-data-and-trust/>
[36] Sam Pfeifle, 'Is the GDPR a data localization law?' (International Association of Privacy Professionals, 29 September 2017) < https://iapp.org/news/a/is-the-gdpr-a-data-localization-law/>
[37] Courtney Bowman, 'Data Localization: an Emerging Global Trend', (Jurist, 6 January 2017) < https://www.jurist.org/commentary/2017/01/Courtney-Bowman-data-localization/>

policies can be seen as the result of policymakers "mistakenly believing that data is more secure if kept within a country's borders"[38]. This was raised at the 2017 International Conference of Data Protection and Privacy Commissioners in Hong Kong, asking how this ties into the adequacy requirements put forward by the GDPR, and whether or not the GDPR itself is a form of localization[39]. Gencarelli of the European Commission notes that the increase in the number of countries party to the Council of Europe's Convention 108 shows Europe is not the only region to view privacy as a fundamental right[40]. The diverse range of signatories to the Convention, which is an instrument designed to enforce data privacy in regulating cross-border transfer, signifies a convergence of data protection standards globally. He stresses that the GDPR is simply further demonstration of the EU working to influence a commonly robust standard for data privacy globally. It is clear that the intention is to facilitate rather than inhibit cross-border data transfer with greater consideration for fundamental rights.

The international reach of the GDPR is unquestionable. It is thus the most relevant instrument for analysis Blockchain technology and its relationship with data protection standards. The 'Brussels Effect' is a term that suitably demonstrates the extra-territorial effect of the GDPR[41]. While EU Regulations are formally an instrument designed to unify legal systems among EU member states, the GDPR's calls for adequacy and obligations on all controllers and processers regardless of location to abide so long as EU citizen data is involved extends the scope tremendously. Blockchain holds the potential to multiply the utility of internationally transferable data, but this must be effectively regulated in order to be effectively unlocked.

Prevalent in the architecture of global data transfer are highly complex privacy regulations from varying jurisdictions all aiming to set a standard for suitable and reliable protection[42].

---

[38] Nigel Cory, a trade policy analyst at the Information Technology and Innovation Foundation, as referenced by Pfeifle, n. (36).
[39] n. (36)
[40] ibid.
[41] Joanne Scott, 'Extraterritoriality and Territorial Extension in EU Law' (American Journal of Comparative Law, Vol. 62, No. 1, 2014, June 8, 2013) <https://ssrn.com/abstract=2276433>
[42] See for example the 2005 APEC Privacy Framework, and the EU-US Privacy Shield 2016

There have been numerous demonstrations in recent years, Uber[43] or Equifax[44] being two of a number of examples, which clearly highlight the practical purpose and imminent necessity of effective data security. It is incidents such as these that have motivated the aggressive modification of European data protection standards by way of the GDPR. A previously common misconception in cyber-security is that data localization is the only effective means of containing any risk of breach[45]. The aim was to maintain restrictive policies, making cross-border data transfers unfeasible. This lacks recognition of the current nature of transaction and communication. Data security cannot and should not be dependent on tangible location-based boundaries. Such restrictive regulations only hinder economic growth due to the limited scope for data flow, but the data itself would still be subject to breach risks[46].

This is where the GDPR distinguishes itself from most other jurisdictional data privacy regulations[47]. The GDPR intends to be a globally harmonizing regime, replacing the 1995 EU Data Protection Directive with the aim of enforcing a more robust and globally reaching framework for data security so far as the personal data of EU citizens is concerned. An EU directive requires member states to implement their own laws corresponding to the directive. This inevitably results in diverse legislations with varying levels of severity and effect. In updating the EU regime, enacting a regulation rather than a directive gives direct effect and has a harmonizing function in that it is implemented directly for each member

---

[43] The magnitude of the 2016 Uber data breach was such that 20 million Uber customers' personal (identifiable) information was exposed such as names, email addresses and phone numbers after considerable misleading users as to their privacy and security practices: Bloomberg, 'Uber Data Breach Exposed Personal Information of 20 Million Users' (12 April 2018) <http://fortune.com/2018/04/12/uber-data-breach-security/>

[44] The breach was originally reported to the FTC as exposure of 143 million affected people, and was actually found to be that 146.6 people were subject to the exposure of their name and date of birth, which 145.5 of those incidences also included the exposure of social security numbers. Matt Weinberger, Business Insider US 'The Equifax breach results in the leak of 56,200 drivers' licenses, passports and other forms of ID' (15 September 2017) <https://www.businessinsider.sg/equifax-breach-check-details-update-2018-5/?r=US&IR=T>

[45] Stephen J. Ezell, Robert D. Atkinson, and Michelle A. Wein, 'Localization Barriers to Trade: Threat to the Global Innovation Economy' (Information Technology and Innovation Foundation, September 2013), <http://www2.itif.org/2013-localization-barriers-to-trade.pdf.>

[46] Stan Sater, Blockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows (6 November 2017). <https://ssrn.com/abstract=3080987>

[47] Though there is some common ground with California State Law

state[48]. The GDPR clearly demonstrates European intention to harmonize the level of data management standards across participating member states, while extending its scope to protect EU citizens beyond European boundaries.

The substantial premise is to provide data subjects with greater autonomy and control in the processing of their personal data[49], through emphasised data subject rights and more stringent obligations upon data controllers' and processers' data-protective practices in collection, storage and processing of personal data. The GDPR is designed to achieve extraterritorial effect by targeting bodies outside the EU whose data processing activities are in relation to EU citizens, typically in the provision of goods and services[50]. By outlining explicit application to the "processing of personal data… regardless of whether the processing takes place in the Union or not"[51], the EU makes clear it's intention to extend citizens' data protection to the broadest limits. The vigor of this framework has been heavily criticized for attempting jurisdictional overreach with calls for a balance allowing the GDPR to operate in 'peaceful coexistence' with other jurisdictions[52]. Its extensive scope already points towards conflicting implications for the ever-growing application of Blockchain technology.

Per Art 1(1) of the GDPR, the regulation relates to the 'processing of personal data'. There are six fundamental principles which the GDPR intends to implement with regards to data privacy; lawful, fair, and transparent processing activities, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality[53], and further required accountability by which the "controller shall be responsible for, and be able to demonstrate compliance with" the principles outlines above[54]. These principles are to be applied collectively and in a cumulative fashion in order for the particular data processing

---

[48] Francoise Gilbert, 'EU General Data Protection Regulation: What Impact for Businesses Established Outside the European Union', (Greenberg Traurig: Insights, 19 April 2016)<http://www.gtlaw.com/en/insights/2016/4/eu-general-data-protection-regulation-what-impactfor-businesses-established>
[49] n. 46
[50] GDPR Article 3
[51] ibid.
[52] Graham Smith, Peaceful coexistence, jurisdiction and the internet (Cyberleagle, 2018) <https://www.cyberleagle.com/2018/02 >
[53] GDPR Art 5(1)
[54] GDPR Art 5(2)

activity to be deemed valid[55], but each of these holds their own point of tension with Blockchain operation.

Processing in a fair, lawful and transparent manner respects the data subjects themselves, in that the data subject must be kept fully informed as to the nature and purpose of such activities, compliant with GDPR requirements[56]. It clearly extends the EU Charter of Fundamental Rights which requires that all data be processed "fairly"[57].

Purpose limitation intends for the purpose of data collection and processing to be made clear to data subjects beforehand, and should not be subsequently extended without notification of the data subject. The GDPR specifically outlines that personal data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."[58] Notably though, the language of the GDPR does not prohibit all further processing, just that which is incompatible with the initial purpose. This may be a point at which to ease tension between Blockchain and the GDPR.

Data minimization requires that data be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"[59], clearly demonstrating the aforementioned cumulative nature of these principles. Accordingly, processing should only take place if there were no other reasonable means by which to achieve the desired purpose[60]. This prohibits what would otherwise be the sheer continuous collection of data pursuant to a 'just incase' mentality, thus conflicting with a number of new data reliant methodologies such as big data and artificial intelligence[61], and particularly with the means of data collection on a Blockchain.

---

[55] Bart Sloot and Frederick Zuiderveen Borgesius, 'The EU General Data Protection Regulation: A New Global Standard for Information Privacy' (15 April 2018). <https://ssrn.com/abstract=3162987>
[56] Luke Irwin, 'The GDPR: Understanding the 6 data protection principles', (IT Governance, 31 January 2018) < https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles>
[57] EU Charter of Fundamental Rights, Art 8(2)
[58] GDPR Art 5(1)(b)
[59] GDPR Art 5(1)(c)
[60] GDPR Recital 39
[61] n. 55

Accuracy demands that data be "accurate and, where necessary, kept up to date"[62]. Further expanded through the language of article 5 and the recitals, it is expected that controllers take "every reasonable step… to ensure that personal data that are inaccurate, having regard for the purposes for which they are processed, are erased or rectified without delay"[63]. Data controllers are obliged to actively preserve data accuracy and to afford data subjects the facility to demand rectification should this not be the case[64]. Parallel to Blockchain technology a clear conflict can be identified. The process of updating or amending a particular block in a chain is a highly technical and practically impossible option to conduct in order to comply with the GDPR.

Storage limitation further promotes the principle of data minimization, and vice versa. The GDPR emphasizes that personal data be "kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed."[65] Data controllers should establish time frames throughout processing activities at which to consider erasure or to carry out periodic review[66]. Such a requirement, particularly at the stage of erasure, can throw a spanner into the effective workings of Blockchain in a similar manner by which alteration of data for the purposes of accuracy poses a challenge.

In integrity and confidentiality however, the GDPR and Blockchain are aligned. This data security principle[67] imposes an obligation on data controllers to take the necessary and appropriate steps to guarantee the security of subjects' personal data, further expanded within the article to require "protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures"[68]. In an initial comparison with Blockchain technology, given the various mechanisms such as hashing and consensus requirements, integrity and confidentiality are intentionally guaranteed.

---

[62] GDPR Art 5(1)(d)
[63] Ibid. and GDPR Recital 71
[64] GDPR Art 16
[65] GDPR Art 5(1)(e)
[66] GDPR Recital 39
[67] n. 55
[68] GDPR Art 5(1)(f)

Finally the underlying principle of accountability[69]; this is a considerable point of tension between Blockchain and the GDPR. This principle calls for compliance with the aforementioned principles, by demonstrable means through which data controllers can thus be held accountable. In comparison with the preceding Directive[70], this highlights that the modification in EU data protection standards intends a stronger emphasis on compliance by calling for a demonstrable quality thus enforcing accountability. This challenge is that by its very nature, the Blockchain is decentralized and consensus driven. Being able to find the particular point at which privacy is jeopardized and to dictate accountability is thus extremely challenging.

Beyond this, the GDPR extends a number of rights to data subjects in order to facilitate autonomy and control over personal data. Pursuant to Chapter 3 of the GDPR, data subjects have the right to access, rectification and erasure of their personal data[71]. They are granted the power to gain access to and request to be updated any personal data stored about them, and have also been granted a 'right to be forgotten'[72], permitting the erasure of personal data upon the data subject's request, though circumstantially dependent. The challenge in executing these rights is that access and amendment of data is inherently challenge due to its secure architecture.

[69] GDPR Art 5(2)
[70] EU Data Protection Directive 1995
[71] GDPR Articles 15, 16 and 17
[72] A term coined by the groundbreaking Google Spain case

5. Blockchain vs. GDPR

Correlation between the GDPR and Blockchain technology has been a major area of contention. Debate has suggested that perhaps Blockchain technology should be entirely exempt from GDPR governance. The argument is that the clear incompatibility between the two should encourage Europe to excuse Blockchain technology in order to allow for effective development and thorough application of Blockchain technology[73]. It is the opinion of this paper however that such an exemption only drives a deeper wedge between technological innovation and fundamental rights. To support long term innovation and application of Blockchain technology it must obtain legal validity; there shouldn't be exemption but rather there should be compromise. Per Berberich and Steiner, the technological neutrality respected by the GDPR is intended to enable 'innovation to continue to thrive under the new rules', and giving effect to this simply means Blockchain and the GDPR must reach a point of compromise[74].

5.1 Does the GDPR apply to Blockchain Technology?

The first step is to establish on a technical and architectural level why is it is necessary for the GDPR to be the appropriate governing regulation of data processing in Blockchain. The EU data privacy reform has strongly emphasised the need to protect personal data. Thus for Blockchain to fall within the remit of the GDPR it must encompass the processing of personal data. This begs the question: do the public keys and supplementary data recorded on Blockchain fall within this scope?

---

[73] See for example Shannon Liao, 'Major Blockchain group say Europe should exempt Bitcoin from new data privacy rule' (The Verge, 5 April 2018) <https://www.theverge.com/2018/4/5/17199210/blockchain-coin-center-gdpr-europe-bitcoin-data-privacy>. Also considered: Tom Pritchard, 'Crypto Group Claims Blockchain Should Be Exempt From EU Data Protection Rules' (Gizmodo, 6 April 2018) <http://www.gizmodo.co.uk/2018/04/crypto-group-claims-blockchain-should-be-exempt-from-eu-data-protection-rules/>

[74] Matthias Berberich and Malgorzata Steiner, 'Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers', 2 Eur. Data Prot. L. Rev. 422, 426 (2016)

The GDPR defines 'personal data' as 'any information relating to an identified or identifiable natural person'[75]. 'Identifiable' is determined through use of an identifier such as the data subject's name, ID number, location, economic, cultural or social identity[76]. This means that any anonymous (note not pseudonymous) data is not governed by the GDPR. Understanding Blockchain technology, it is possible that there are two types of personal data stored on a Blockchain. These are the public keys that relate transactions to a particular user, and the transaction data itself.

Transactional data refers specifically to a particularly party to the transaction. As demonstrated, such data is maintained through three different means of storage: either in the form of plain text, or as encrypted data requiring a decrypting key, or through the hashing mechanism, which links it to the previous block.

While anonymity would exclude this data from the GDPR, the Article 29 Working Party suggests that a high threshold should be maintained in qualifying for an anonymous status of data storage. It stipulates that data is only anonymous once processed by means that 'irreversibly prevent identification'[77].

Transactional data that is stored on-chain, in plain text, undeniably identifiable and thus clearly and simply within the scope of the GDPR, not requiring any more detailed analysis. Moving on to encrypted personal data, it requires the mechanism of public and private keys in order to be decrypted. This is reversible anonymity and thus also pulls encrypted data within the scope of the GDPR. Effective encryption is at best a pseudonymisation measure rendering the data subject identifiable through the used of supplementary data.

Finally, the hashing process. As an intamperable mechanism, the hash function in itself is technically irreversible. That being said, the Article 29 Working Party has confirmed that hashing is to be considered a pseudonymisation technique rather than a means of successful anonymisation. This is because the data set can still be related to the data

[75] GDPR Art 4(1)
[76] ibid.
[77] Article 29 Working Party, Opinion 04/2014 on Anonymisation Techniques, 0829/14/EN

subject through accurate analysis[78]. This confirms that transactional data stored by any means is to be targeted as personal data within the scope of the GDPR.

The analysis of the 'personal data' quality of public keys is much more straightforward. It is a pseudonymisation method, relying on the same lock-and-key methodology as a username and password. Blockchain founders Satoshi Nakamoto maintain that privacy is preserved not through a simple measure of encryption but instead through 'breaking the flow of information… : by keeping public keys anonymous'[79]. So the question is whether public keys are considered to be anonymous. The GDPR recognises pseudonymisation where personal data cannot be 'attributed to a specific data subject without the use of additional information, provided that such information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable person'[80]. The mechanism of public and private keys fits nicely within this definition, where the public key is the pseudonymised data that cannot be directly attributed to a particular data subject, while the private key serves as the 'additional information' that, combined with the public key, renders it identifiable.

Consequently there is very little room for doubt that Blockchain, particularly in the on-chain, permissionless, public form, is within GDPR jurisdiction. Having established the clear necessity for governance, Blockchain technology must find ties to each of the major components of the GDPR.

5.2 Who is the 'Data Controller'?

Subsequently, the 'data controller' must be identified. As defined by the Article 29 Working Party, the data controller is the party who makes the decision as to the purpose and means of data processing[81]. Thus not defined by title, the role is fit by the actual activity that warrants their controlling capacity. This is something that clearly has to be determined on a

[78] ibid.
[79] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2009) <https://bitcoin.org/bitcoin.pdf.>
[80] GDPR Art 4(5)
[81] Article 29 Working Party, 'Opinion 01/2010 on the concepts of "controller" and "processor"'

case-by-case basis rather than by contractual designation, identified by contributory decision as to the purpose of data processing activity.

The challenge is that for the GDPR to be applicable, the language assumes the existence of an identifiable data controlling or processing party engaging in the relevant activity. This contrasts with Blockchain in that the language of the GDPR is not tailored to regulate in a space where there is no identifiable processor[82].

That being said, Article 4 of the GDPR makes one reference to a "decentralized" system; the "filing system" required by the GDPR refers to "any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis"[83]. This broad definition could possibly pull a Blockchain within the remit of the GDPR. Most notably, the language in this article uses the words "functional and geographical". Pertaining to the qualification that the structure be functionally organized, interpretation can lend itself towards the decentralized nature of a permissionless Blockchain being a functional characteristic of its architecture thus requiring that Blockchain to be governed by the GDPR.

Regardless of the above however, the recitals demonstrate a requirement for technology neutrality[84] in the interpretation of the GDPR, so although not legally binding, this is enough to presume that it intends to regulate Blockchain technology, mitigating any exemption due to architectural variation.

The greatest hurdle is thus clearly the unidentifiable source of control that is so unique to Blockchain technology. Without identifying a specific data controller it is not clear how the essence of the GDPR can be executed. In their analysis, Berberich and Steiner suggest that where the data controller is the party who contextually has control over the data pursuant to the GDPR, there are two ways in which the controller could be interpreted within Blockchain architecture. The decentralized structure could mean that either no nodes will be classed as data controllers, or that all nodes are individually regarded as data

[82] n. 30
[83] GDPR Article 4(6)
[84] GDPR Recital 15

controllers[85]. In practice however, it is difficult to see how either would be feasible within the GDPR framework. De Filippi has broached the topic with a more viable solution, noting that "regardless of how much effort has been put into the design of a secure decentralized architecture, there is no guarantee that people's privacy will never be compromised": she suggests that each user should be should be individually responsible for the particular data contributed by that node[86]. The approach is so favourable as it is consistent with the GDPR's aim to promote personal autonomy.

Take for example the Bitmark Blockchain. This affords individuals the opportunity to affirm ownership of their own personal data and digital assets[87]. The technology company has applied Blockchain technology to turn digital assets into digital property, allowing any individual to records, track and trade the property rights to their digital assets and data[88]. By recording data by means of property titles referred to as "Bitmarks", registries hold proof not only of authenticity but of ownership, meaning individuals can use this to maintain total control of their data promoting trust and transparency in data management[89].

Entrusting each node with the protection of their own privacy is theoretically more manageable, but it also assumes each user has the knowledge and technical expertise so far as effective data protection technology is concerned to ensure this is effectively ensured. Each node makes an autonomous decision to engaged in the peer-to-peer network, and each has it's own intentions and objectives within the chain. Although there will be a technological barrier to the efficiency of this approach it does make sense that each node be considered a data controller in itself.

The challenge of liability in Blockchain technology is widely recognized[90], and the urgency

---

[85] n. 74
[86] Primavera Di Filippi, 'The interplay between decentralization and privacy: the case of blockchain technologies' (2016) Journal of Peer Production, Alternative Internets, 7. <https://hal.archives-ouvertes.fr/hal-01382006/document>
[87] Bitmark Inc., 'Bitmark raises $1.7M to establish property rights for user generated content and data' (PR Newswire, 17 November 2016) <https://www.prnewswire.com/news-releases/bitmark-raises-17m-to-establish-property-rights-for-user-generated-content-and-data-300364688.html>
[88] Bitmark <www.bitmark.com>
[89] Bitmark Inc. 'With Bitmark your data can now become your most valuable asset' (28 November 2016) <https://www.prnewswire.com/news-releases/with-bitmark-your-data-can-now-become-your-most-valuable-assetintroducing-bitmarks-next-generation-property-system-build-on-a-blockchain-300562071.html>
[90] European Data Protection Supervisor Annual Report 2016 <https://edps.europa.eu/data-protection/our-work/publications/annual-reports/2016-annualreport-state-privacy-2017-edps_en>

in understanding the privacy implications of Blockchain technology is prevalent. Inability to assign liability accurately would be a crucial to technological down fall due to legal invalidity.

Given the characteristic peer-to-peer architecture and the consensus mechanism, it is worth considering what the GDPR refers to as 'joint controllers'[91]. Per Article 26, joint controllers are those who 'jointly determine the purposes and means of processing'; this is identified by a clear allocation of responsibility[92]. The freedom that each node has in its decision to join a chain and to decide in what capacity it choses to participate mean a clear and transparent allocation of responsibility to be essentially non-existent. There is no common and prescribed determination of responsibility in this context and each node, though driven by consensus, is essentially independent in its participation[93].

The most reasonable approach to the data controller requirement is to allocate each participating node as a data controller in itself, but this introduces further complications. On the effective protection side, each node requires the necessary technological knowledge, so as not to jeopardize data security. The other challenge is identifying each and every controller and each being able to execute their responsibility. It would be very difficult to identify in any detail the number, location or particular identity of each of the nodes[94]. This is a major obstacle to respecting accountability for protecting each particular set of data. Further to this, the encryption and hashing techniques that give the Blockchain it's secure character mean that nodes are unable to access and make chances to data on a block without great difficulty. This makes it near impossible to give effect to the various data subject rights prescribed by the GDPR. Where nodes are considered to be the data controllers, they are unable to identify, rectify or delete data in response to a data subject exercising their right, and are not even able to access data to satisfy a subject access request[95]. It is clear that in their current capacity and under conventional interpretation of the GDPR, nodes within a public, permissionless Blockchain are not equipped to fulfill the tasks which the GDPR required of a data controller or processor.

5.2.1. Data Controller obligations

[91] GDPR Art 26(1)
[92] GDPR Recital 79
[93] n. 24
[94] ibid.
[95] GDPR Article 15

Drawing this to a practical example of Bitcoin, there are currently approximately 9,500 nodes active nodes running on the Bitcoin network (this number takes into account and omits any duplicated or non-listening nodes)[96]. In a network of this scale and distribution, data controller challenges are inevitable. The lack of a single, centralized controller means each of these nodes must be contacted individually to comply with a data subject right. In the interest of respecting data subject rights per the GDPR, the risk in a network of this scale is that the Blockchain might have to be entirely terminated if such requests can't be achieved through simpler or less extensive means[97].

Proportionality is a key proponent within the EU jurisdictional framework, particularly with regards to the protection of fundamental rights. In a situation where no other means can successfully respect a data subject right and the solution is to terminate an entire Blockchain, while this is the minimum action necessary to respect data subject rights to erasure, this pulls the proportionality discussion into play surround balancing respective fundamental rights. The age-old imbalance between privacy and free expression must be taken into account at this juncture. The EU Charter of Fundamental Rights protects on the one hand, respect for private and family life[98] and the protection of personal data[99], and on the other, freedom of expression and information[100] and freedom to conduct a business[101]. The GDPR calls for Member States to reconcile the two sides, adopting measures that effectively balance fundamental rights[102]. Terminating a Blockchain to protect the rights of an individual data subject contrary to the operation of an entire Blockchain reliant business is not a proportionate reconciliation of fundamental right.

Further to this, the GDPR has also escalated penalties for data security breaches. Dependent on the extent of the breach and the size of the undertaking, the GDPR now prescribes for two tiers of punitive fines. Tier 1 is a fine of up to 10,000,000 EUR or 2% of annual turnover[103], or Tier 2 calls for up to 20,000,000 EUR or 4% of annual turnover[104], in

---

[96] Bitcoin nodes summary – see https://coin.dance/nodes
[97] n. 24
[98] EU Charter of Fundamental Rights (CFR), Article 7
[99] EU CFR, Article 8
[100] EU CFR, Article 11
[101] EU CFR, Article 16
[102] GDPR Article 85 and Recital 153
[103] GDPR Article 83(4)
[104] GDPR Article 83(5)

both cases "whichever is higher". The GDPR has considerably extended punitive capabilities to enforce more stringent data security regimes[105].

The challenge in Blockchain is who pays such fines. Article 83 targets the data controller or processor responsible for the data that has been subject to breach. As considered, within a peer-to-peer network with each individual node responsible for their own data, the process of identifying the responsible data controllers becomes near impossible. It also stands to reason that where several data controllers contribute individually to the protection of portions of the involved data, very few or potentially none are equipped to satisfy the punitive prescriptions of the GDPR in the way it is intended[106].

The conventional GDPR scope of a 'data controller' does not reflect the architecture of Blockchain technology proportionately, or give effect to the intention of the GDPR. Without the means to assign liability there is no way to give effect to the increased level of accountability that the GDPR intends to promote.

5.3 Territorial Scope

Beyond the challenges in allocating liability, there are further challenges in marrying the territorial scope of the GDPR with the extensive reach of Blockchain. The GDPR applies to 'the processing of personal data in the context of the activities of an establishment of a controller or processor in the European Union, regardless of whether the processing takes place in the Union or not'[107]. The language of this clause makes it very clear that the GDPR intends to be as far-reaching as possible, with no loophole in moving their processing activities outside of the union. It further extends it's scope with the Article 3(2); where data processors or controllers are not established within the EU, so long as their processing

[105] see Bernard Marr, 'GDPR: The Biggest Data Breaches and The Shocking Fines (That Would Have Been)' (Forbes, 11 June 2018) <https://www.forbes.com/sites/bernardmarr/2018/06/11/gdpr-the-biggest-data-breaches-and-the-shocking-fines-that-would-have-been/#66afbc8a6c10> which reassess some of the largest and most damaging data breaches through the eyes of the GDPR. Yahoo would have been fined potentially $160 million for the data breach of '13/'14 which was the largest of it's time, and the famed Equifax breach which compromised the personal information of 143 million consumers could have faced close to $130 million in fines pursuant to the highest extent of the rule. Notably though they did demonstrate proactive cooperation post breach to assist consumers, and this would be taken into account.
[106] n. 24
[107] GDPR Article 3(1)

activities relate to the offering of goods or services to a data subject within the EU[108], or monitoring of data subjects activities that take place geographically within the EU territory[109], the GDPR is the governing regulation.

An un-permissioned Blockchain has the capacity to operate on a peer-to-peer network of nodes spanning the entire globe. The ten countries with the highest proportion of the 9,500 currently reachable Bitcoin nodes are the USA, China, France, Germany, the Netherlands, Canada, Russia, the UK, Japan and Singapore respectively[110]. This demonstrates no geographical barrier to Blockchain operation, engaging a large number of jurisdictions, inclusive, be it directly or indirectly, of the GDPR.

Beyond this, the GDPR also provides for regulation over the extra-territorial transfer of personal data to third countries. Pursuant to Article 44 of the GDPR, transfer to a 'third country or to an international organization' can only proceed subject to the satisfaction of a number GDPR compatibility provisions[111]. Nodes can join a Blockchain from any location (particularly in the permissionless context). Once this takes place, the entire distributed ledger is then informed and consequently updated in order to reflect the further addition to the chain. This requires the international transfer of personal data between nodes, albeit in an encrypted or hashed format, qualifying as a third-country transfer.

The adequacy mechanism of the GDPR has been under considerable scrutiny, particularly in the wake of Schrems, the subsequent declaration of the US Safe Harbour as invalid[112], and the consequential establishment of the EU-US Privacy shield, demonstrating further the intention of the European union to extend the protection of EU citizens' fundamental rights beyond jurisdictional borders. As a reflection of this, the GDPR's adequacy mechanism involves a declaration of an adequate level of protection by the third country[113], demonstrated by provision of suitable safeguards by the controller or processer, such that 'enforceable data subject rights and effective legal remedies… are available' for the data

[108] GDPR Article 3(2)(a)
[109] GDPR Article 3(2)(b)
[110] Global Bitcoin Nodes Distribution (as of Monday 6th August 2018) – see https://bitnodes.earn.com/
[111] GDPR Article 44
[112] Case C-362/14 Maximillian Schrems v Data Protection Commissioner ECLI:EU:C:2015:650
[113] GDPR Article 45(1)

subject[114]. Beyond this, undertakings are encouraged to introduce Binding Corporate Rules to facilitate appropriate intra-organizational personal data transfers across jurisdictional borders. These are approved by a 'competent supervisory authority', must be legally binding, confer enforceable data subject rights, and must specify applicability to the necessary data protection principles[115].

Within a private and controlled corporate structure, it is clear how such mechanisms are intended to work, but the nature Blockchain architectural development challenges the conventional adequacy mechanisms. Approving each node's facilitation of data protection and ensuring effective compliance on this scale is an impossible task where public, permissionless Blockchains are concerned. Private Blockchains though could engage Article 49 of the GDPR. It provides for derogations in 'special situations', namely where there is 'absence of an adequacy decision'. In such cases, the data subject once informed of the possible risks of such data transfers can provide explicit consent[116]. While this is straightforward on a private chain, thus far it is clear that the GDPR is designed for centralized data collection, processing and storage. It is not clear how to execute this on a permissionless Blockchain without technically altering the underlying architecture.

A consistent theme in EU data protection reform has been emphasis on data subject rights and autonomy, which is considerably at odds with Blockchain technology. Having established that it involves personal data, data subjects should be able to enforce the rights prescribed to them by the GDPR. Given the accountability motive, it is highly debatable whether the node itself, and the technology itself, is equipped and allows for the enforcement of data subject rights. The above analysis suggests that only feasible procedure is for data subjects to contact each individual node to effectively exercise their rights along the entire chain, but this technically highly impractical. That is not to say that there is no technical solution, but in Blockchain's current state it is difficult to see how data subject rights can be accurately protected.

---

[114] GDPR Article 46(1)
[115] GDPR Article 47
[116] GDPR Article 49(1)(a)

5.4 Data Protection Principles and Data Subject Rights

The data minimization and purpose and storage limitation principles[117] do not correlate with the nature of storage on a Blockchain. As demonstrated, the language of the corresponding article is such that data must only be 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes'[118]. However, once data is added to extend a Blockchain, it essentially reaches a state of perpetuation. The function of a Blockchain is to constantly grow and given the hashing functions this is entirely defined by the make up of previous blocks. Given its distributed architecture, the Blockchain can grow consistently thus accruing more and more personal data. Beyond this, each node also stores a complete copy of the chain and thus the personal data within it.

This technology entirely contradicts both principles. In Bitcoin, each new transaction adds personal data to the chain, for the purpose of that particular transaction. This is maintained indirectly though the hashing sequence for further transaction, entirely contrary to purpose limitation. Further to this, the inability to remove data from a chain and the permanence of its architecture call the principle of data minimization into question. The impossibility of deletion, while contradicting more literally with other data subject rights, essentially contradict with the respect for storage limitation in itself.

It is important at this stage to recognize that the conflict between data minimization/purpose limitation and the furtherance of innovation and technology are not unique to Blockchain architecture, and have been explored in the space of big data analytics, which will be further discussed.

In contrast with the American privacy regime, the EU data protection framework is both procedural and substantive, accounting for both autonomy and governance. Alongside the substantive obligations placed upon controllers and processors to implement protective efforts, data subjects also have extensive autonomy in the protection of their own information. Personal data must be accurately maintained, and should it not, the GDPR prescribes that 'every reasonable step' be taken in order to ensure that 'inaccurate (data),

[117] see GDPR Articles 5(1)(b) and (c)
[118] GDPR Article 6

having regard to the purposes for which they are processed, are erased or rectified without delay'[119]. Thusly data subjects have the right to request amendments. "The data subject shall have the right to obtain from the controller without undue delay the rectification (or completion) of inaccurate (or incomplete) personal data concerning (them)…"[120].

Initial interpretation suggests that what is expected is for data subjects to submit a request to each node individually. In reality however, this is not a feasible interpretation. The first challenge is for the data subjects themselves. Returning to the distributed Bitcoin network of approximately 9,500 nodes, there is no feasible way for the data subject to correctly identify all or in fact any of the necessary nodes. Beyond geographical complexity, nodes are not always online or active, and it is possible that when the user changes location the IP address of the node also changes[121]. Further, Blockchains are immutable. Along with the unbreakable security and transparency of the technology, this is seen as a reason why law and regulation are unnecessary for the technology[122], but as for the EU data subject privacy standard this jeopardizes effective regulation.

That being said, however, both Articles 5 and 16 maintain the language "having regard to the purposes for which they are processed". This directs all parties to have regard for the particular technology at stake. This suggests that there could be other acceptable ways to indicate a correction or modification of particular data without amending the original block. The GDPR permits rectification through 'providing a supplementary statement'[123]. This can be viewed as another attempt by the GDPR to adapt to developing technology for a framework such as Blockchain where the conventional means of correction isn't possible. It could be possible to simple add another block to the chain that acts to represent a correction or update of any previous data without the need to edit or delete the original data. It supports the notion of a 'supplementary statement' and gives effect to the GDPR in the functional sense. While the incorrect data cannot itself be corrected, it is addressed in the most effective way for both the technology and the law.

---

[119] GDPR Article 5(1)(d)
[120] GDPR Article 16
[121] n. 24
[122] Dirk A. Zetzsche, Ross P. Buckley, Douglas W Arner, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (13 August 2017, University of Illinois Law Review, 2017 – 2018) <https://ssrn.com/abstract=3018214>
[123] GDPR Article 16

The distinction was made previously between on- and off-chain storage, as well as between transactional data and public keys as the two forms of personal data this paper is concerned with. It has been suggested that pursuing off-chain storage of data could overcome the challenge of editing data on a Blockchain, as the data itself could be changed without having to tamper with the chain itself[124]. This however would only be feasible with regards to transactional data. Public keys must be stored within the block on the relevant chain.

A further Article to consider pursuant to this right is Article 19 of the GDPR. The Article requires that controllers 'communicate any rectification or erasure… to each recipient to whom the personal data have been disclosed'. While this again would prove extremely difficult in a public, permissionless Blockchain, the language of the GDPR again demonstrates some leniency by including the words 'unless this proves impossible or involves disproportionate effort'[125]. Given the near impossibility of identifying each node within a chain that holds the copy of the chain within the distributed network, this demonstrates again a space where the GDPR recognizes data subject rights potentially getting in the way of technological advancement and permits lack of performance of the right due to infeasibility.

Essentially, though rectification in the traditional sense cannot be respected in Blockchain. There is a middle ground that can be identified through the language of the GDPR to provide some means of correction, but it remains to be seen whether this would be to the satisfaction of the data subject given that the original, incorrect data still remains within the chain. This should not be a point of contention so long as supplementary statements are thorough and effectively executed.

The GDPR also provides data subjects with a Right to Access their personal information held or processed by a data controller[126]. Pursuant to the language of the Article, the data subject can request access to information regarding the purpose of processing, the recipients of the relevant data, the time frame during which the data will be stored, information as to the source of the data, and which categories of personal data are held

---

[124] n. 24
[125] GDPR Article 19
[126] GDPR Art 15(1)

about the data subject. It is of course not limited only to these criteria. Having established that each node should be a data controller in itself, each data controller doesn't not have knowledge of the actual content data for each particular data subject request. As has already been demonstrated, the data is typically stored in a hashed or encrypted format. This provides a further challenge should the data subject actually be successful in targeting the relevant nodes with their request.

While this proposes enough challenges in the Blockchain context, the Article further complicates the obligation my requiring that data subjects also be entitled to information regarding transfer of their personal data to third parties, particularly with regards to which safeguards have been put in place to effectively protect this data[127]. As has already been addressed, the distributed and potentially perpetual nature of a Blockchain mean that such an obligation is a difficult one to fulfill. Though the block may be validated in the EU with data pertaining to an EU citizen (pulling that data within the jurisdiction of the GDPR), once this happens the information must be shared with all nodes within the network, regardless of their location, in order to maintain accurately the copy of the Blockchain for all network members.

While similarly the proposal of off-chain storage is one to consider here[128], again it can only apply to transactional data, and the challenges of encryption, hashing and pseudonymisation still play their part. It is difficult to see how the Right to Access can accurately be reconciled with Blockchain technology.

In the wake of the iconic Google Spain[129] case, one of the more important provisions of the GDPR is the right to be forgotten. Pursuant to Article 17 of the GDPR, data subjects have the ability to ensure that a data controller 'eras[es] personal data concerning him or her without undue delay'[130]. Required by the language of the article, controllers must fulfill the obligation to delete in a number of particular circumstances, including where the data is no longer necessary for the purpose for which it was collected, the processing occurred unlawfully, a lack of legitimate grounds in a situation where the data subject has objected,

---

[127] GDPR Article 15(2)
[128] n. 24
[129] Google Spain v AEPD and Mario Costeja González C-131/12
[130] GDPR Article 17(1)

or where the data subject has exercised their right to withdraw their consent[131].

As has been recognized as the biggest challenge with respect to other data subject rights, the undeniable immutability feature is definite downfall for the right to be forgotten from Blockchain technology. Satoshi Nakamoto intended for one of the defining feature of Blockchain technology to be censorship resistance; it is designed to promote autonomy and control and 'fight against oppression and censorship'[132]. The permanence and unalterable nature of a Blockchain is intended to prevent third parties from have any control over the original content and purpose of data[133]. This makes a Blockchain, by definition, impossible to forget[134]. The technological features behind this characteristic have been explained previously, but there is a greater urgency in finding a way to overcome this challenge. Subsequent to the iconic Google Spain decision of 2014, Google has since received 2.4 million 'Right to be Forgotten' requests, all considered and 43.3% complied with[135]. Though still awaiting the Google v CNIL decision as to whether such delisting efforts should have global effect, the GDPR has given data subjects the power to demand such delisting from any data controller, which, given that it involves the data of an EU citizen, could still potentially have global effect. The origin, scale and extent of this right demonstrated the need to reconcile with the GDPR in order to give it effect.

The means of overcoming this challenge again depend on which form of personal data is being considered; transactional data or public keys. As with all other rights, transactional data can be salvaged through off-chain storage, and the chain itself won't need to be tampered with in order to delete the relevant data. But as has also been previously encountered, this is not the case with public keys.

As with all data subject right, though some to a lesser extent than others, the GDPR provides qualifications with regard to the purpose of processing and the feasibility of performance, permitting some account for the technology at stake as previously discussed.

---

[131] GDPR Article 7(3)
[132] Paul Andrew, 'Bitcoin Censorship Resistance Explained', (23 April 2018, Coin Central) <https://coincentral.com/bitcoin-censorship-resistance/>
[133] ibid.
[134] n. 24
[135] Michee Smith, 'Updating our "right to be forgotten" transparency report' (26 Feb 2018, Google Transparency Report) <https://blog.google/around-the-globe/google-europe/updating-our-right-be-forgotten-transparency-report/>

The same goes for the right to be forgotten; the GDPR does not prescribe an absolute right here. It permits for the data controller to take 'account of available technology and the cost of implementation'[136]. While it is yet to be seen how this may unfold, it is possible to interpret this language as recognizing the technical exertions encountered by Blockchain technology in exercising this right. While the language doesn't excuse Blockchain from the GDPR, it does propose that consideration of 'available technology' lead to alternative means of achievement. De Filippi, for example, suggests that this be achieved through a formalized procedure by which the key is transmitted to the data subject in order to provide autonomy, or the key is deleted in a technologically supervised environment, which should substantially achieve deletion the way the GDPR entails[137]. The most efficient technical solution may be to limit or disable access to that particular data, potentially through the use of a private key that allows only the data subject, or possibly no one at all, to access the data intended for erasure through the exercise of data subject rights[138].

Beyond this, Ateniese et al. have also proposed the use of 'chameleon-hashes' to afford only particular authorized parties the means to change the content of a block[139]. However, Finck rightfully highlights a number of technical faults with a solution of this nature; loss of the particular authorization key is a frivolous but guaranteed way to return the Blockchain to its immutable state. Further this solution requires the introduction of a third party to act as the authorized party permitted to perform such re-writes. This entirely contradicts the intention of Blockchain to provide autonomy and negate external interference.

While there is not yet a decided means to achieve erasure, a flexible construal of the GDPR is necessary. Finck recognizes that it does not provide any particular or specific definition for the term 'erasure', and this could lead to alternative interpretations[140] as to the limiting or removal of access to the data (as 'delisting' works in the context of search engines) instead. So perhaps this opens the door for alteration in order to meet the demands of the GDPR without traditional execution of 'erasure'.

---

[136] GDPR Article 17(2)
[137] n. 86
[138] n. 24
[139] Giuseppe Ateniese, 'Redactable Blockchain – or – Rewriting History in Bitcoin and Friends' (2017 IEEE European Symposium on Security and Privacy (EuroS&P) 3 July 2017) <https://ieeexplore.ieee.org/document/7961975/>
[140] n. 24

Analysis so far has demonstrated for Blockchain technology to adjust or supplement its functioning in order to comply with the GDPR framework. This can be further demonstrated through the consideration of the Data Protection by Design and Default mechanisms. These are two all-embracing principles that draw a consistent theme throughout the GDPR. The GDPR requires that 'controller[s] shall… implement appropriate measures which are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this regulation and to protect the rights of data subjects'[141]. This language alludes to the accountability principle that the GDPR aims to promote. It encourages controllers to bring such demonstrable safeguards into their architectural design to demonstrate an inherent priority for data privacy. The recitals expand on this to require that such systems account for minimizing the processing of personal data, pseudonymisation at the earliest possible point, providing data subject autonomy, and improving the effectiveness of data protection and security features[142].

[141] GDPR Article 25(1)
[142] GDPR Recital 78

6. Alternative Interpretation

It has been demonstrated clearly that there is an undeniable tension between Blockchain technology and the GDPR. The case remains that the former should not be entirely exempt from the latter, and current analysis has attempted to explore solutions on the technical side that would allow Blockchain to respect the requirements of the GDPR, particularly where it comes to the performance of data subject rights. It is clear that this is a challenging endeavor that either complicated the already complex operation of the technology itself, or only satisfies the GDPR so far as technological adaptation allows, which is no cases reaches the robust capacity of GDPR protection as conventional interpretation currently stands.

At this juncture this paper proposes that perhaps the compromise needs to be extended from the side of the GDPR, rather than through the technical adaptation of Blockchain technology. Though the GDPR clearly intends an extra-territorial effect in order to provide the most thorough and secure protection and afford extensive and autonomous control to the citizens of the EU, the language of the GDPR can still be interpreted as highly geographically stunted. It calls for consideration of aspects such as the location of both data subjects and controllers, and the adequacy of specific third-party cross border transfer subject to safeguards provided by that particular jurisdictions. While the intention of this language is clear in demonstrating a proactive and preventative approach to data protection, it is also language that acts in start contrast with the global nature of the Internet and of the currently rapid state of technological development.

The Internet is thoroughly global. Take for example the scale of the Facebook/Cambridge Analytica scandal, the extent of Wikileaks, or even Russia's interference in the 2016 US elections. The Internet in itself is not hindered by geographical limitation; it works to facilitate transactions, communications, and economic growth through providing the platform and the architecture for cross-border development. This is clearly enhanced further in the development of Blockchain technology, which in it's traditional, decentralized, permissionless, public format as in the operation of Bitcoin, is encompassed within a peer-to-peer network that spans the entire globe. While the GDPR intends to support this at a

superficial level of interpretation, the reality is that the extensive requirements and obligations put forward by the GDPR do not correlate with an international developmental motive the way that the internet and more specifically Blockchain, in this particular case, are designed to do so.

It is now necessary to draw back to the space of Big Data and Artificial Intelligence that was previously referred to. There has been extensive literature in this area that has alluded towards an entirely different mentality than that of the conventional EU data protective legislation relied upon in other fields of technological development.

To set the scene, there is a stark contrast in the American and European approaches to data privacy. At a constitutional level, the European Union provides for a constitutional right to both respect for private and family life[143], and the protection of personal data[144]. The United States on the other hand, does not. The closest constitutional recognition of privacy in the US is the 4th Amendment to the United States Constitution, which affords the 'right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizure'. This is a vertical level of protection against the state, interested in the traditional sense in prevention of trespass.

The European Union has cultivated a continuous and growing shift towards the protection of privacy as a fundamental right for the citizens themselves. Article 16 of the Treaty of the Functioning of the European Union, which reads that 'everyone has the right to the protection of personal data concerning them'[145], has altered the pillar framework of the EU, giving data protection the important from a fundamental rights perspective rather than purely in the interest of market harmonization[146]. The approach in the US however, is more commercially driven. The U.S. Federal Trade Commission is one of the most significant bodies of American authority for data protection, though their jurisdiction pursuant to the Federal Trade Commission Act of 1914 is to act in the commerce space to prohibit unfair methods of competition and unfair or deceptive acts or practices, challenging business

[143] Charter of Fundamental Rights of the European Union, Article 7
[144] Charter of Fundamental Rights of the European Union, Article 8
[145] Treaty of the Functioning of the European Union, Article 16
[146] Article 29 Working Party Opinion 168

conduct harms competition, or misleads or injures consumers[147]. In respect of this, given growing consumer concerns regarding personal data privacy, the FTC issued recommendations in 2012 for business and policy makers with regards to protecting consumer privacy in a rapid area of change[148]. They promote privacy by design, which draws some parallels with the current European framework, and simplified consumer choice, to draw away from the previously overwhelming American consent system that is the result of the American attitude to notify in order to avoid deception. It also promotes transparency in an attempt to push market practices in a more fair and comprehensive direction.

Hoofnagle, however, recognizes a major issue with an overly transparent approach. He notes that the end-result is a perverse one, in that disclosure becomes a one-way ratchet. More transparency acts as a safety blanket, washing the business' hands of any wrong doing with the ability to argue 'after all, the consumer was informed'[149]. This is where the European framework demonstrates the upper hand, in requiring a more sophisticated means of prior consent and an opt-in mechanism[150].

The two jurisdictions paint two very different pictures of the approach towards data protection. There are two strands to data privacy; autonomy, which gives rise to personal agency through the actions of notice and consent, and governance, which introduces the element of paternalism through obligations on data controllers and processors. Autonomy is very strong in American law in the procedural sense[151]; there is considerable emphasis on personal agency and the guarantees of notice, choice and consent. Governance, on the other hand, distinguishes the EU from the US. Substantive principles of data minimization and purpose limitation provide a more overarching influence to data protection attitudes,

---

[147] Federal Trade Commission Act 1914, Section 5
[148] see FTC Reports, 'Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers' (5 March 2012) < https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>
[149] Chris Hoofnagle, 'Federal Trade Commission Privacy Law and Policy' Chapter 6 Online Privacy (Cambridge University Press, 2016)
[150] see GDPR Article 7
[151] Helen Nissenbaum, 'Privacy as contextual integrity' (Washington law review,79(1), 2004) <https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf>

with greater consideration for the fundamental rights motive rather than the commercial procedural motive.

It is this American attitude that comes into play when considering information governance in the space of big data and artificial intelligence. There is no question that algorithms, given the extensive level of data accumulation, need governance and accountability. In an area so quickly developing in parallel with growing concerns about data privacy, this is a field where a delicate balance must be struck between achieving genuine and effective data protection, alongside avoiding any considerable limitations on technological development. Artificial intelligence and machine learning challenge transparency and the substantive principles of the GDPR, which are essential to the notion of accountability. This then begs the question: does the GDPR provide suitable mechanisms for the collective accountability that is ideal to technological development? Or is it so focused on the individual through the protection of fundamental rights that it is pointed in the wrong direction?

Three of the most distinctive aspects of big data analytics are the mass collection of data, the distinct opacity of analysis, and the relatively spontaneous repurposing of data as analysis develops. Even at a superficial level of consideration, these aspects are in undeniable contrast with the GDPR's focus on consent, transparency, data minimization, and purpose/storage limitation. Referring back to the Google DeepMind/Royal Free research venture, it is clear that in an ideal world for algorithmic training and development, the goal is to collect as much data as possible, and to have the scope to repurpose this data as and when research results lead to further applications (similar to the perpetual nature of data storage on a Blockchain). It is difficult to see where consent can effectively come into play here, and also where information falls into the remit of personal data when it comes to profiling and inferred data that may not necessarily be identifiable.

There has been considerable American literature that calls for reconsideration of the approach taken towards information governance in the Big Data space. In Anupam Chander's consideration of 'The Racist Algorithm', which has been an inherent challenge in the US development of predictive policing techniques, he described the algorithms at work as 'the Black Box', in that the data inputs and outputs are transparent and subject to notice

and consent, but the algorithm itself is behind closed doors. He proposes that this is what should be opened up to explanation[152]. Applying this view to Blockchain technology, in respect of data protection in this context, greater concern should be put towards to security of the technology itself rather than the inputs and outputs of personal data. Through the decentralization, encryption, validation, hashing and immutability features of Blockchain, the technology itself is extremely secure[153]. Where it has been observed that the language of the GDPR does make reference to technological considerations in the performance of data subject rights, this language could potentially be more widely interpreted to greater encourage demonstration of data privacy by design as an alternative means of GDPR satisfaction, under which Blockchain technology clearly qualifies.

Such a viewpoint is further elaborated by Zarskey; He recognised that the GDPR and Big Data are inherently incompatible. Purpose specification in particular leads to a great clash with Big Data analysis and essentially undermines the intention and utility of the entire process[154]. A very similar argument can be said of the GDPR and Blockchain. Zarskey proposes that data minimization requirements be loosened in the area of Big Data analytics. It undermines the success of Big Data initiatives, the same way that it undermines the success of effective Blockchain application. What should instead be introduced is a form of ex-post interpretation[155], rather than the currently ex-ante interpretation of the GDPR.

The language of the GDPR essentially frames a near-explicit rejection of big data initiatives. In the area of automated decision-making, including profiling, 'data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects'[156]. While Blockchain technology doesn't necessarily fit within this template, its decentralized nature demonstrates the same lack of accountability that the GDPR rejects in big data analytics. This is another demonstration of the lack of coherence

---

[152] Anupam Chander, 'The Racist Algorithm?', (13 June 2016) 115 Michigan Law Review 2017 <https://ssrn.com/abstract=2795203>
[153] Michelle Orolet, '4 reasons Blockchain could improve your data security', (5 June 2018, CSO Online) <https://www.csoonline.com/article/3279006/blockchain/4-reasons-blockchain-could-improve-data-security.html>
[154] Tal Zarskey, 'Incompatible: The GDPR in the Age of Big Data' (8 August 2017). Seton Hall Law Review, Vol. 47, No. 4(2), 2017. <https://ssrn.com/abstract=3022646>
[155] Ibid.
[156] GDPR Article 22

between the GDPR and technological development.

Former Commissioner of the US FTC, Julie Brill, sums up quite illustratively what the solution could be to this legal and technological tension. She recognizes that too much attention is being paid to the dashboard issues with regards to data inputs and outputs, but similarly to what Zarskey and Chander suggest, more emphasis should be placed on what is 'under the hood'[157]. This is an embodiment of the American attitude that could form the bridge between Blockchain technology and data protection; instead of overly analysing the procedural issues and concern for individual rights, permit the processing in the interest of technological innovation and focus primarily on the ethics and security of processing. The intamperable security of Blockchain technology is one of its defining and most attractive features. This attitude could permit effective technical development while ensuring data is protected through the means of processing and the operation of the technology itself. The language of the GDPR can thus be interpreted to reflect this as an acceptable alternative to its traditional views on data protection, in that demonstrable data protection by design are inherent in Blockchain architecture and there are technical means by which to satisfy data subject rights which have been previously addressed.

[157] Julie Brill, 'A Call to Arms: the role of technologists in protecting privacy in the age of big data' (FTC, 23 October 2013) < https://www.ftc.gov/public-statements/2013/10/call-arms-role-technologists-protecting-privacy-age-big-data>

7. Conclusion:

The value in Blockchain technology is undeniable. It promotes transactional efficiency, and contributes towards transparency, neutrality and security in the digital space. But it is clear that these benefits come at a price. They have fuelled a legal tension that questions the validity of their operation entirely. Analysis so far suggests that for Blockchain technology to be thoroughly and effectively utilized, some social trade-off must be managed between effective regulation and technological development.

As was explored, this challenge is much more significant in the original permissionless Blockchain architecture, but the possibility of a permissioned chain does serve as an alternative solution to mitigate this challenge while continuing to support technological innovation. It is clear that while the language of the GDPR does provide some clear obstructions to business fluidity and technological innovation, the intention is purely to harmonize a more robust level of EU citizen privacy protection.

A consideration often overlooked is that all applications of Blockchain technology are essentially in the interest of providing for consumers[158]. As far as the GDPR is concerned, the consumer is the EU citizen the regulation aims to protect. This emphasizes a need for compromise that gives data subjects the autonomy intended for them, rather than an exclusion of regulation altogether, in the interest of concurrently supporting technological innovation. This could be through broad use of purely permissioned Blockchain, warranties for access and authentication, and limitation of personal data exposure. As Salmensuu reframes, rather than what is simply a 'GDPR problem', the case is actually a 'design-solution mismatch'[159]. This paper has explored a number of design-focused and interpretation-fuelled options that would structure a common ground between Blockchain technology and data security.

What should not occur is thorough dismissal of the technology pursuant to stringent and traditional interpretation of the GDPR. This is disproportionate and contrary to business and

[158] n. 30
[159] ibid.

technological progression.

To quote Lawrence Lessig, "we are not usually trained to think about all the different ways technology could achieve the same ends through different means"[160]. As explored in this paper, what should be seen is an altered interpretation of the GDPR in order to give validity to the technology while achieving data security through alternate means.

This paper has sought to demonstrate that to find legal validity for Blockchain technology under the GDPR, the following must be considered: An altered perception of the data controller, considering means through which data controllers might be responsible for their own data (though the challenges of this interpretation cannot be ignored), consideration of alternative means to achieve 'rectification' and 'erasure' that still given genuine effect to the intention of the GDPR, and an alternative attitude to data security, in that while some technologies satisfy conventional means of preventing data vulnerability, given the durability and inherent security of Blockchain technology, an altered attitude could view this as satisfactory to the high standard of data security intended by EU regulatory reform.

[160] Lawrence Lessig, Code version 2.0, 2006 Basic Books

Bibliography:

Cases:

Case C-362/14 Maximillian Schrems v Data Protection Commissioner ECLI:EU:C:2015:650
Google Spain v AEPD and Mario Costeja González C-131/12

Legislation:

APEC Privacy Framework 2005
EU Charter of Fundamental Rights, Articles 7, 8, 11 and 16
EU Data Protection Directive 1995
EU-US Privacy Shield 2016
General Data Protection Regulation 2016/679, Articles: 3, 4, 5, 6, 7, 15, 16, 17, 19, 22, 25, 26, 44, 45, 46, 47, 49, 83 and 85
General Data Protection Regulation 2016/679, Recitals: 15, 39, 71, 78, 79 and 153
Treaty of the Functioning of the European Union 1957, Article 16

Bibliography:

Article 29 Working Party, Opinion 04/2014 on Anonymisation Techniques

Article 29 Working Party, Opinion 01/2010 on the concepts of "controller" and "processor"'

Article 29 Working Party Opinion 168

Anupam Chander, 'The Racist Algorithm?', (13 June 2016) 115 Michigan Law Review 2017 <https://ssrn.com/abstract=2795203>

Bart Sloot and Frederick Zuiderveen Borgesius, 'The EU General Data Protection Regulation: A New Global Standard for Information Privacy' (15 April 2018). <https://ssrn.com/abstract=3162987>

Bernard Marr, 'This is why Blockchain will transform Healthcare' (Forbes, 29 November 2017) <https://www.forbes.com/sites/bernardmarr/2017/11/29/this-is-why-blockchains-will-transform-healthcare/#14ba10a01ebe>

Bernard Marr, 'GDPR: The Biggest Data Breaches and The Shocking Fines (That Would Have Been)' (Forbes,
11 June 2018) <https://www.forbes.com/sites/bernardmarr/2018/06/11/gdpr-the-biggest-data-breaches-and-the-shocking-fines-that-would-have-been/#66afbc8a6c10>

Bitcoin nodes summary – see https://coin.dance/nodes

Bitmark Inc., 'Bitmark raises $1.7M to establish property rights for user generated content and data' (PR

Bitmark <www.bitmark.com>

Bitmark Inc. 'With Bitmark your data can now become your most valuable asset' (28 November 2016) <https://www.prnewswire.com/news-releases/with-bitmark-your-data-can-now-become-your-most-valuable-assetintroducing-bitmarks-next-generation-property-system-build-on-a-blockchain-300562071.html>

Blockgeeks, 'What is Blockchain Technology' (June 2016) <https://blockgeeks.com/guides/what-is-blockchain-technology/>

Bloomberg, 'Uber Data Breach Exposed Personal Information of 20 Million Users' (12 April 2018) <http://fortune.com/2018/04/12/uber-data-breach-security/>

Cagla Salmensuu, 'The General Data Protection Regulation and Blockchains' (1 January 2018) <https://ssrn.com/abstract=3143992>

[1]Chris Hoofnagle, 'Federal Trade Commission Privacy Law and Policy' Chapter 6 Online Privacy (Cambridge University Press, 2016)

Courtney Bowman, 'Data Localization: an Emerging Global Trend', (Jurist, 6 January 2017) < https://www.jurist.org/commentary/2017/01/Courtney-Bowman-data-localization/>

Dirk A. Zetzsche, Ross P. Buckley, Douglas W Arner, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (13 August 2017, University of Illinois Law Review, 2017 – 2018) <https://ssrn.com/abstract=3018214>

Don Tapscott and Alex Tapscott, 'Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World' (Portfolio/Penguin, 2016)

European Data Protection Supervisor Annual Report 2016 <https://edps.europa.eu/data-protection/our-work/publications/annual-reports/2016-annualreport-state-privacy-2017-edps_en>

Francoise Gilbert, 'EU General Data Protection Regulation: What Impact for Businesses Established Outside the European Union', (Greenberg Traurig: Insights, 19 April 2016)<http://www.gtlaw.com/en/insights/2016/4/eu-general-data-protection-regulation-what-impactfor-businesses-established>

FTC Reports, 'Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers' (5 March 2012) < https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>

Giuseppe Ateniese, 'Redactable Blockchain – or – Rewriting History in Bitcoin and Friends' (2017 IEEE European Symposium on Security and Privacy (EuroS&P) 3 July 2017) <https://ieeexplore.ieee.org/document/7961975/>

Global Bitcoin Nodes Distribution (as of Monday 6th August 2018) – see https://bitnodes.earn.com/

Graham Smith, Peaceful coexistence, jurisdiction and the internet (Cyberleagle, 2018) <https://www.cyberleagle.com/2018/02 >

Helen Nissenbaum, 'Privacy as contextual integrity' (Washington law review,79(1), 2004) <https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf>

Ian Khan, TEDx speaker, as referenced in 'Bitcoin and Cryptocurrency Technologies' (Christopher Nygaard, R&C Publishing 2018).

Jacob Eberhardt and Stefan Tai, 'On or Off the Blockchain? Insights on Off-Chaining Computation Data' (European Conference on Service-Oriented and Cloud Computing, Springer, September 2017) pp. 3 - 15

James Manyika et al., 'Digital Globalization: The New Era of Global Flows', (McKinsey, January 2016) < https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows>

Joanne Scott, 'Extraterritoriality and Territorial Extension in EU Law' (American Journal of Comparative Law, Vol. 62, No. 1, 2014, June 8, 2013) <https://ssrn.com/abstract=2276433>

John Biggs, 'Sierra Leone just ran the first Blockchain-based election' (Tech Crunch, 15 March 2018) <https://techcrunch.com/2018/03/14/sierra-leone-just-ran-the-first-blockchain-based-election/>

Julie Brill, 'A Call to Arms: the role of technologists in protecting privacy in the age of big data' (FTC, 23 October 2013) < https://www.ftc.gov/public-statements/2013/10/call-arms-role-technologists-protecting-privacy-age-big-data>

Lawrence Lessig, Code version 2.0, 2006 Basic Books

Luke Irwin, 'The GDPR: Understanding the 6 data protection principles', (IT Governance, 31 January 2018) < https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles>

Matt Weinberger, Business Insider US 'The Equifax breach results in the leak of 56,200 drivers' licenses, passports and other forms of ID' (15 September 2017) <https://www.businessinsider.sg/equifax-breach-check-details-update-2018-5/?r=US&IR=T>

Matthias Berberich and Malgorzata Steiner, 'Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers', 2 Eur. Data Prot. L. Rev. 422, 426 (2016)

Michee Smith, 'Updating our "right to be forgotten" transparency report' (26 Feb 2018, Google Transparency Report) <https://blog.google/around-the-globe/google-europe/updating-our-right-be-forgotten-transparency-report/>

Michele Finck, 'Blockchains and Data Protection in the European Union' (30 November 2017). Max Planck Institute for Innovation & Competition Research Paper No. 18-01. <https://ssrn.com/abstract=3080322>

Michelle Orolet, '4 reasons Blockchain could improve your data security', (5 June 2018, CSO Online) <https://www.csoonline.com/article/3279006/blockchain/4-reasons-blockchain-could-improve-data-security.html>

Muhammad Mehar et al., 'Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack' (26 November 2017) <https://ssrn.com/abstract=3014782>

Newswire, 17 November 2016) <https://www.prnewswire.com/news-releases/bitmark-raises-17m-to-establish-property-rights-for-user-generated-content-and-data-300364688.html>

Nigel Cory, a trade policy analyst at the Information Technology and Innovation Foundation, as referenced by Pfeifle, n. (36).

Paul Andrew, 'Bitcoin Censorship Resistance Explained', (23 April 2018, Coin Central) <https://coincentral.com/bitcoin-censorship-resistance/>

Primavera Di Filippi, 'The interplay between decentralization and privacy: the case of blockchain technologies' (2016) Journal of Peer Production, Alternative Internets, 7. <https://hal.archives-ouvertes.fr/hal-01382006/document>

Robert Sams, 'Blockchain Finance', presentation (March 2015) <https://www.slideshare.net/rmsams/blockchain-finance> as references by Cagla Salmensuu, 'The General Data Protection Regulation and Blockchains' (1 January 2018) <https://ssrn.com/abstract=3143992>

Sabine Bendiek, 'The New Global Economy Runs on Free Flow of Data and Trust', (The B20, 24 February 2017) <http://www.b20germany.org/priorities/digitalization/digitalizationdossier/digitalization-article/news/the-new-global-economy-runs-on-free-flow-of-data-and-trust/>

Sam Pfeifle, 'Is the GDPR a data localization law?' (International Association of Privacy Professionals, 29 September 2017) < https://iapp.org/news/a/is-the-gdpr-a-data-localization-law/>

Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2009) <https://bitcoin.org/bitcoin.pdf.>

Simply Explained – Savjee, 'How does a Blockchain work' (13 November 2017) <https://www.youtube.com/watch?v=SSo_EIwHSd4>

Shannon Liao, 'Major Blockchain group say Europe should exempt Bitcoin from new data privacy rule' (The Verge, 5 April 2018) <https://www.theverge.com/2018/4/5/17199210/blockchain-coin-center-gdpr-europe-bitcoin-data-privacy>

Stan Sater, Blockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows (6 November 2017). <https://ssrn.com/abstract=3080987>

Stephen J. Ezell, Robert D. Atkinson, and Michelle A. Wein, 'Localization Barriers to Trade: Threat to the Global Innovation Economy' (Information Technology and Innovation Foundation, September 2013), <http://www2.itif.org/2013-localization-barriers-to-trade.pdf.>

Tal Zarskey, 'Incompatible: The GDPR in the Age of Big Data' (8 August 2017). Seton Hall Law Review, Vol. 47, No. 4(2), 2017. <https://ssrn.com/abstract=3022646>

Tom Pritchard, 'Crypto Group Claims Blockchain Should Be Exempt From EU Data Protection Rules' (Gizmodo, 6 April 2018) <http://www.gizmodo.co.uk/2018/04/crypto-group-claims-blockchain-should-be-exempt-from-eu-data-protection-rules/>

Volodymyr Fedak, 'Blockchain and Big Data: The match made in heavens' (Medium, Towards Data Science, 21 February 2018) <https://towardsdatascience.com/blockchain-and-big-data-the-match-made-in-heavens-337887a0ce73>