



March of the blocks

GDPR and the blockchain



THE CENTER FOR
GLOBAL ENTERPRISE

SLAUGHTER AND MAY

CRAVATH, SWAINE & MOORE LLP



March of the blocks

GDPR and the blockchain



Credits

This paper was written by the Center for Global Enterprise's Digital Supply Chain Institute, and leading international law firms Slaughter and May and Cravath, Swaine & Moore. It is published with thanks to Jody Cleworth and his team at Marine Transport International (MTI), for allowing us to use MTI as a case study.

For further information, please contact:

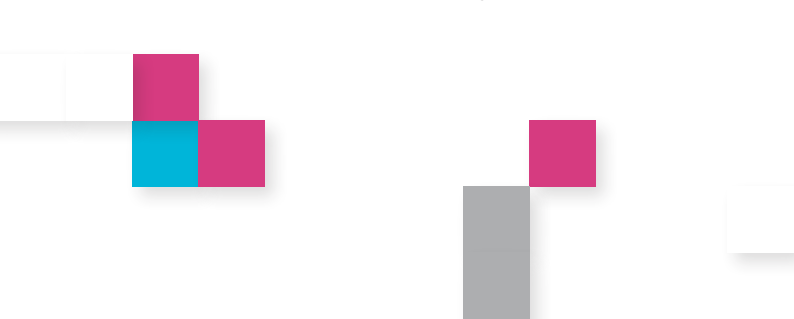
Shawn Muma the blockchain research leader at the CGE's Digital Supply Chain Institute. Enterprise blockchains are a prime focus of his research
e smuma@thecge.net

Rob Sumroy a partner at Slaughter and May, who co-heads the firm's global data protection and privacy practice, as well as leading Slaughter and May's technology, emerging tech and cyber advisory units
e rob.sumroy@slaughterandmay.com

David Kappos a partner at Cravath, Swaine & Moore LLP in New York, one of the foremost lawyers in the field of intellectual property and former head of the United States Patent and Trademark Office
e dkappos@cravath.com

To discover more about MTI's blockchain technology, please visit marinetransportint.com or contact info@askmti.com for any further information.

Other contributors: Jessica Goodman and Ryan Wichtowski from Cravath, Swaine & Moore; Ian Ranson and Duncan Mykura from Slaughter and May; and Sugathri Kolluru and Ira Sager from the CGE.



Foreword

Blockchain and Distributed Ledger Technologies (DLT) have emerged as an effective enterprise transformation tool. They provide capabilities beyond traditional databases to share data and manage workflow throughout an enterprise and across its ecosystem of customers, partners and suppliers in a trusted manner without central control.

Blockchain for the enterprise is a specialised workflow automation tool that, when applied properly, is a powerful cross-enterprise transformation instrument. However, at CGE's Digital Supply Chain Institute (DSCI), our research has shown that success stories remain elusive because of difficulties in forming the blockchain ecosystem or network, determining network and data governance, and complying with government data regulations. It is this last element that forms the basis of this paper.

As with many exciting new technologies, the hype surrounding blockchain has been extreme and prompted a tidal wave of company experimentation that has proven one thing: blockchain is not a good fit for all applications, but for some it is an exceptional fit. This paper examines one such exceptional fit for the shipping industry, in the context of compliance with the European Union's General Data Protection Regulation (GDPR).

Many commentators have written that the GDPR and blockchain technology are fundamentally incompatible.



This paper was prompted by DSCI members who saw this as a clear inhibitor to blockchain adoption and asked for our view. We enlisted Slaughter and May and Cravath, Swaine & Moore LLP, two leading international law firms, to better define the opportunities and challenges as to how the GDPR applies to this nascent technology.

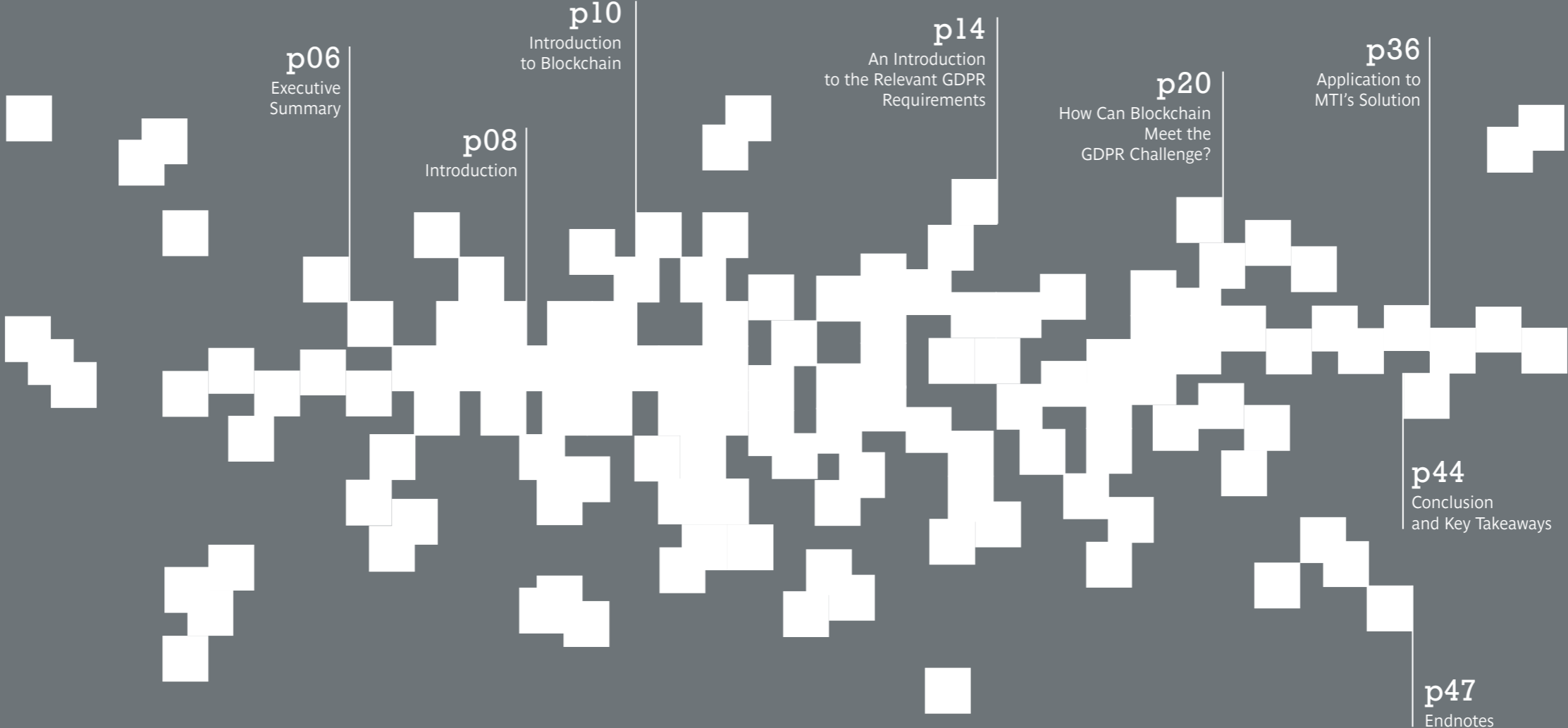
Other countries will, undoubtedly, adopt regulations similar to the GDPR, and hence businesses are unlikely to avoid privacy compliance issues in the future. We also want to emphasise that the GDPR is a pressing concern for all companies, not just B2C companies, as the digital economy is increasingly making B2C and B2B distinctions fade away.

This paper provides a management framework for addressing GDPR compliance in a blockchain network. We examine the power and efficiencies blockchain brings to the shipping industry, and examine the compliance challenges created by the GDPR. We conclude that, with some up-to-date, pragmatic guidance and increased support from regulatory authorities in Europe, there is no fundamental reason why the GDPR and many blockchain solutions cannot happily coexist.

Christopher G. Caine, President
The Center for Global Enterprise



Contents



p06 Executive Summary	p08 Introduction	p10 Introduction to Blockchain	p14 An Introduction to the Relevant GDPR Requirements	p20 How Can Blockchain Meet the GDPR Challenge?	p36 Application to MTI's Solution	p44 Conclusion and Key Takeaways	p47 Endnotes
---------------------------------	----------------------------	--	---	---	---	--	------------------------

1

Executive Summary

Blockchain technology has advanced tremendously over the past decade, and now provides a viable alternative to traditional database solutions. In particular it is suggesting dramatic advancements in solutions for recording, processing and sharing information: offering decentralisation, accessibility and reliability. However, the EU's recently enacted General Data Protection Regulation (GDPR) poses significant compliance hurdles to the ongoing development of blockchain-based solutions involving storing and transacting with data about individuals.

This paper identifies some of these hurdles, such as the GDPR rights to have one's personal data deleted or corrected, which sit at odds with the very concept of an immutable blockchain. This paper will also offer suggestions on how best to implement GDPR-compliant blockchain solutions. Rather than offering a theoretical

discussion on creating a GDPR-compliant blockchain solution, this publication examines a realworld use case developed by Marine Transport International (a UK-based digital logistics enabler) to provide practical solutions to the issues the GDPR poses to blockchain implementers.

What we have identified in writing this publication is that not all of the blockchain challenges posed by the GDPR and other privacy regimes can currently be bridged. However, we do feel that the gap left by those challenges is relatively small, and the fundamental freedoms forming the policy behind such privacy laws can be maintained and protected in particular blockchain environments. However, this will require both lawmakers and regulators to take an active and pragmatic approach to blockchain technology.

We believe that a blockchain solution that respects the fundamental principles of data protection and privacy is achievable if the following four guiding principles are followed.

1 Use a private, permissioned blockchain.

While the most common vision of blockchain is of a fully public, permissionless network, there are a wide variety of blockchain solutions, many of which are in fact private and require permission to join. Because anyone can join a public permissionless blockchain, it is impossible to ensure participants agree to necessary rules around the protection of personal data. As a result, the only clearly effective way of achieving a GDPR-compliant blockchain solution is by using a private, permissioned blockchain.

2 Avoid, if possible, the storing of personal data on the blockchain.

The most obvious way to avoid GDPR compliance issues is, predictably, to employ a blockchain solution that avoids processing any personal data. While keeping a blockchain completely free of personal data will be very difficult to achieve, this should not prevent efforts being made to keep personal data off-chain (as far as it is possible to do so). This may be done, for example, by storing an encrypted anonymous hash of the personal data on-chain, with the underlying and identifiable personal data being kept off-chain, and also by minimising free form data.

3 Implement a detailed governance framework.

Given: (a) the need to ensure that personal data is adequately protected; (b) the requirements under the GDPR to establish contractual relationships governing the processing of personal data between parties; and (c) the legal obligations on data controllers to provide individuals with privacy notices and a means to uphold their personal data rights, a GDPR-compliant commercial blockchain solution will require a detailed governance framework that is contractually binding on all participants and clearly sets out each party's rights and responsibilities.

4 Employ innovative solutions to data protection problems.

The immutable nature of blockchain data is the one element of the technology which clashes most obviously with data subjects' rights under the GDPR, especially the right to erasure (the so-called right to be forgotten) and the right to rectification (i.e. to have incorrect personal data corrected). However, through reliance on innovative solutions such as the use of advanced irreversible encryption as a means of deletion, it is possible to comply with the spirit and (we argue) the policy of data protection legislation, if not yet fully the word.

Ultimately, we are calling on regulatory authorities and technology providers to take any reasonable remaining steps necessary to address the outstanding privacy challenges posed by blockchain.

If these steps are not taken, there is a risk of a stall in (or even end to) investments in blockchain companies who are developing innovative solutions that could, in the long-run, benefit the world as a whole.

2

Introduction

Over the past decade, blockchain-based technologies have evolved in a wide range of directions. As businesses have developed increasingly innovative blockchain solutions to an increasingly broad range of problems, governments, regulators and organisations have become more active in creating meaningful support for blockchain's huge potential. Indeed, the European Commission announced plans last year to increase funding for projects drawing on blockchain technologies by up to 340 million euros by 2020.¹ The European Union's Blockchain Roundtable in November 2018 further highlighted the desire to create a comprehensive European strategy to boost innovation and exploitation of blockchain technology.²

There remains, however, significant concern about the application of the GDPR to blockchain technology, and the difficulty of achieving a GDPR compliant blockchain solution. Indeed, a number of recent publications have discussed at length the tensions between the GDPR and blockchain technology.³ Some commentators have even gone as far as to call blockchain fundamentally incompatible with the GDPR.⁴ While we take a more optimistic view, their concerns are not entirely misplaced.

"... the development and uptake of this new technology requires close cooperation between the public and private sectors. Governments and economic actors must work together to overcome regulatory obstacles, increase legal predictability, lead international standardisation efforts and accelerate research and innovation..." EU Blockchain Roundtable report, 20 November 2018,⁵

Some of the most revolutionary aspects of blockchain technology, such as the distribution of ledger data and its generally immutable nature, do not sit neatly with key obligations in the GDPR. These features may lead to many applications of blockchain technology (such as most public, permissionless blockchains) not being compliant with the GDPR. However, in our view, they do not necessarily render GDPR compliance impossible. In particular, we believe it should generally be possible to deploy a blockchain solution in compliance with the GDPR, at least where that solution involves a defined group of participants, all of whom agree to a common contractual governance framework.

In this paper we analyse some of the key requirements of the GDPR that present a compliance challenge for blockchain solutions. We then consider how a blockchain solution can be deployed to meet that challenge. We then progress beyond discussion in the abstract by looking at how these issues apply to a realworld use case developed by Marine Transport International (**MTI**), a UK-based digital logistics enabler. By analysing the compliance challenge and considering various means of meeting that challenge in the context of MTI's blockchain solution, this paper aims to be of practical use to those looking to deploy blockchain solutions in their business.

Finally, it should be noted that this publication is intended for general information only and is not intended to provide legal advice.

3 Introduction to Blockchain

A blockchain is a series of blocks of data that are linked together by a cryptographic hash. Each block of data in the chain includes a hash of the previous block. Because the previous block in the chain includes a hash of the block before that one (and so on back to the first block), the blocks form a continuous chain.

The hash stored in each block of the chain operates like a fingerprint of the previous block. It is possible to run the hash function over the previous block to confirm that it generates the correct hash. If the previous block is changed in any way, it will not generate the correct hash and the chain will be broken. Therefore, the data of any block in the chain cannot be modified without changing the hash of every block that comes after it in the chain.

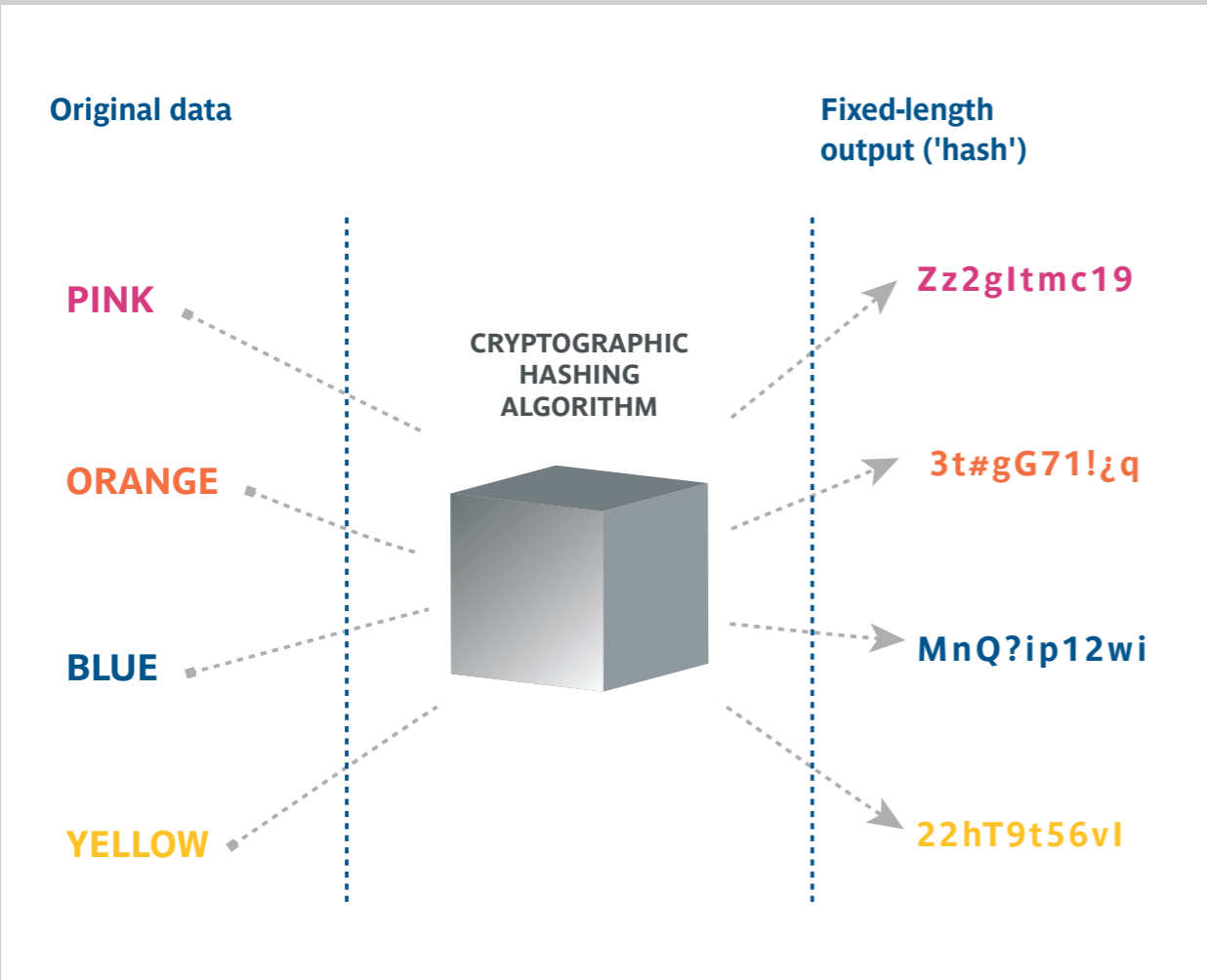
Separately, there is the concept of a distributed ledger. A distributed ledger is a database that is stored separately and maintained independently yet synchronously by a consensus mechanism, across multiple points (nodes) on a network. Most, but not all, distributed ledgers are implemented using a type of blockchain.

While the concepts of a “blockchain” and a “distributed ledger” are distinct, in this paper we use the term “blockchain” to refer to a distributed ledger which is implemented using blockchain technology.

Where a distributed ledger is implemented as a blockchain, each copy of the blockchain serves as a copy of the ledger and multiple nodes on the network will each have a copy of the blockchain. This means that where one copy of the blockchain is modified, everyone else with a copy of the blockchain (i.e. every other node on the distributed ledger network) can detect that modification, because the hash of the latest block of the modified chain will be different to that of the latest block of their own chain.

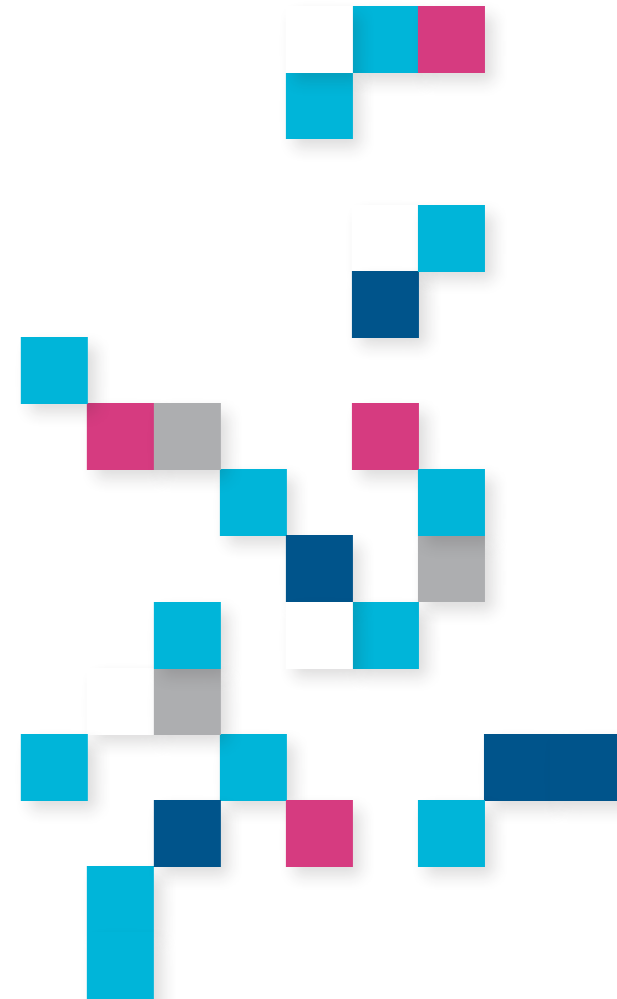
The ultimate source of truth (the true ledger) is the ledger recorded by the blockchain as maintained by a majority of the nodes on the network. It is therefore generally only possible to modify a ledger by having that majority of the nodes adopt the modified blockchain. The greater the number of nodes, the more difficult it would generally be for anyone to modify the blockchain maintained by a majority of them, and therefore modify the ledger. So, once included in a blockchain, data is generally immutable: it cannot be changed and it cannot be deleted (at least not in the traditional sense of the word). It is this aspect of blockchain technology that most obviously runs against the aims of the GDPR, which has individuals’ rights to correct and delete their own personal data at its very core. Detailed analysis of the interplay between the GDPR and blockchain technology follows in section 4 and section 5.

Hashing (simplified)



Cryptographic hashing is one of the cornerstones of blockchain technology and is at the heart of what guarantees the reliability and integrity of blockchains. Cryptographic hashing involves the running of a cryptographic algorithm (a hash function) to turn a block of data of any length into a fixed-length output (a hash). Computing the hash function for a small amount of input data, such as a short string of characters making up a single word could produce, for example, a 40 character string (hash). Similarly, computing the same hash function for terabytes of input data would also produce a 40 character string. Computing the hash function for the same input data will always generate the same hash. But even a very small change to the input data (such as changing a single byte in a terabyte of data) produces a significantly different hash as an output. Generally, the only way to effectively reverse the hash function (to start with the hash and determine the input data that was used to generate the hash) is to compute the hash function for all possible input data until a particular input generates the same hash.

Salting and peppering are two methods that increase the security of hashed data by adding random values to the data being hashed. By enlarging the amount of data being hashed, these methods increase the amount of computational energy required to reverse the hash function. The difference between salting the data and peppering the data is that while salt is stored with the underlying data off-chain by the hash generating user, pepper is stored separate from the data or not at all.⁶



4

An Introduction to the Relevant GDPR Requirements

4.1 What is the GDPR?

The GDPR is a European Union regulation on data protection and privacy for individuals within the European Economic Area (the **EEA**). The GDPR was implemented in May 2018 and marked a significant evolution in data protection law in Europe. This paper will not summarise every aspect of the GDPR, but will instead highlight those aspects of the Regulation we consider to be most relevant to the question of GDPR compliance for blockchain solutions.

While the GDPR governs how personal data relating to individuals inside the EEA may be processed, it also has a wide-ranging extra-territorial application. The GDPR applies first and foremost to entities that are processing personal data in the context of a European establishment, regardless of whether or not the processing takes place in the EEA. However, the GDPR also applies to entities established outside the EEA that are offering goods or services to (or monitoring the behaviour of) individuals in the EEA.

As the GDPR became effective within the past twelve months, there remains much ambiguity and uncertainty as to how it will be enforced, especially in relation to innovative technologies such as blockchain. After all,

the GDPR was not designed with distributed ledger technology in mind. It is however possible to gauge, to some extent at least, the likely approach of European regulators to blockchain technologies. This can be achieved by assessing regulators' public statements and policies related to blockchain, which are considered later in this paper.

Given that the GDPR is generally perceived as a high-watermark of international data protection laws (and becoming a template for increasing numbers of countries' own data protection laws), engineering a blockchain solution that is GDPR compliant will help efforts aimed at achieving worldwide data protection and privacy compliance.

4.2 What is personal data?

In relation to the GDPR, personal data is any information relating to an identified or identifiable natural person. It includes data such as names, addresses, identification numbers, location data, and IP addresses.

The GDPR also sets out special categories of personal data, the processing of which is subject to stricter regulation. These more sensitive categories of personal data include personal data revealing racial or ethnic origins, political opinions, religious beliefs and health data.



4.3 Processing of personal data under the GDPR

The GDPR regulates the “processing” of personal data. Processing is defined extremely broadly as:

“any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”

This effectively captures almost anything one might do with data, including merely storing it. Blockchain solutions with the functionality to store or share personal data will inevitably be involved in the “processing” of that personal data.

The GDPR requires that personal data must be:

- processed lawfully, fairly and transparently;
- collected (and processed) for specified, explicit and legitimate purposes (**the purpose limitation**);
- adequate, relevant and limited to what is necessary for the purpose for which they are processed (the principle of **data minimisation**);
- accurate and kept up-to-date;
- retained (i.e. kept in an identifiable form) for no longer than is necessary for the purpose for which they are processed (**the storage limitation**); and
- processed securely.

The GDPR also requires that all processing of personal data must have at least one of a defined list of legal bases. These bases include:

- processing based on the relevant individual’s specific, informed, unambiguous, freely given and revocable consent;
- processing necessary for the performance of a contract with the relevant individual;
- processing necessary for compliance with a legal obligation; and
- processing necessary for the legitimate interests pursued by the controller or a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject).

Even higher thresholds apply to processing of special categories of personal data.⁷

4.4 Controllers and processors

Entities processing personal data under the GDPR fall into one of two categories: data controllers or data processors. A data controller is an entity that, alone or with another data controller, has primary responsibility over the processing of personal data, and who determines the manner in which, and the purposes for which, the personal data is processed. A data processor, on the other hand, processes personal data on behalf of a data controller, under mandatory contractual provisions set out in the GDPR.

The legal terminology used in the GDPR, including the notion of data controllers and data processors, was designed with a clear division of responsibilities in mind. However, in a blockchain ecosystem, where decentralisation is key, the variety of stakeholders makes the controller/processor differentiation particularly complex. This is considered further in the following section of this paper.

4.5 Privacy by design

In addition to the above principles, the GDPR includes an overarching obligation on data controllers to move towards data protection by design and by default (so-called **privacy by design**).⁸ To achieve privacy by design, data controllers under the GDPR must implement appropriate technical and organisational measures which ensure that, by default, data protection is integrated into all personal data processing activities and business practices, from the initial design stage onwards.

The GDPR’s aim through privacy by design is to change organisational attitudes to the protection of personal data, by making it a pervasive issue that is considered by organisations as a matter of course during their business as usual practices. In that light, it should also be noted that:

... when creating solutions based around new technologies (such as blockchain) that pose a potential high risk to individuals’ rights or freedoms, there is a specific obligation to conduct a risk assessment known as a Data Protection Impact Assessment (DPIA).

4.6 Rights of individuals

The GDPR builds upon the principles discussed above in a set of detailed rights for individuals. Within the context of blockchain applications, the most pertinent of these are:

- the right to erasure (commonly referred to as the **right to be forgotten**), which gives individuals a right to request that certain (usually outdated) information about them be deleted; and
- the right to rectification, which allows individuals to have incorrect data referring to them corrected.

A The right to erasure

Article 17 of the GDPR gives individuals a qualified right to request that a data controller erase personal data about them without undue delay. There is a defined list of circumstances in which a controller will be obliged to erase personal data about an individual who submits an erasure request. Most commonly, the right to erasure applies where the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed. As a result, personal data that are still required for the purposes for which they were originally collected can, in most instances, be retained by the data controller.

The obligation to erase personal data also includes a number of exceptions, among them:

- where retention is required by EU or EU Member State law (for example, statutory record keeping obligations);⁹ and
- where retention is necessary for the establishment, exercise or defence of legal claims.¹⁰

B The right to rectification

Article 16 of the GDPR provides data subjects with an unqualified right to “obtain from the controller without undue delay the rectification of inaccurate personal data concerning” them. It is important to note that the article goes on to say: “[t]aking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement,” which may well be helpful in the context of blockchain solutions struggling with the concept of rectification.

4.7 International transfers of personal data

Given the global nature of many blockchain solutions, it is also important to consider restrictions on international transfers of personal data under the GDPR. The GDPR provides that personal data may only be transferred outside the EEA where the transfer is:

- to a country that the European Commission has determined provides an adequate level of protection for individuals’ personal data (known as an **adequacy decision**);¹¹
- to a third party subject to appropriate safeguards under the GDPR, which is usually established by the transferor and the transferee agreeing to a contract containing the European Commission’s model international data transfer clauses;
- to a company that is subject to binding corporate rules approved by a European data protection regulator; or
- in one of a defined list of specific situations set out in the GDPR, such as where the data subject has explicitly consented to the transfer or where the transfer is necessary for the performance of a contract with the data subject.

In practice, commercial parties seeking to transfer personal data outside the EEA to a country that is not the subject of an adequacy decision will usually enter into an agreement that includes the European Commission’s model data protection clauses.

A GDPR governed blockchain solution which transfers personal data to participants around the world should therefore provide for the transferor and transferee agreeing to the model data protection clauses as part of the governance provisions.



5

How Can Blockchain Meet the GDPR Challenge?

5.1 How to meet the GDPR challenge, part 1: keep personal data off the blockchain

The most obvious way to avoid the application of the GDPR to a blockchain solution is to avoid processing any personal data as part of that solution. Indeed, one crucial aspect of distributed ledger technology, that data should be replicated and maintained by various participants rather than stored centrally, is somewhat at odds with the GDPR's principles of data minimisation, storage limitation, and purpose limitation.

The ideal means to resolve this dilemma is to avoid it altogether. The breadth of the definition of personal data in the GDPR, however, makes the keeping of all personal data off the blockchain difficult in many circumstances.

We will look firstly at the problems associated with (1) unique identifiers and (2) the inadvertent addition of personal data to a blockchain.

A The problem of unique identifiers

1 - The challenge

As discussed earlier, personal data can include unique identifiers assigned to an individual such as an IP address or, on a blockchain network, the address assigned to a participant on the network. So, if:

- a participant on the network is an individual;
- the participant is assigned a particular address that will be recorded against transactions on the network involving the individual; and
- there is any reasonable way to link the individual's address on the network to the identity of the individual (for example, by linking that address with the individual's IP address and then obtaining the identity of the individual from the individual's internet service provider by a court order),

then, the participant's address on the blockchain network will be considered personal data under the GDPR. Given the expanded definition of personal data under the GDPR, it is also important to consider the data environment within which the personal information sits, rather than only focusing on information that is clearly, on its face, personal data. After all, personal data under the GDPR also includes information relating to an indirectly identifiable individual, and this means that information which on its own may not be personal data, can quickly become personal data when brought together with other data points to build a profile of an identifiable individual.

2 - Potential solution: Avoiding the use of persistent identifiers for individuals

If a blockchain solution is being deployed in a business context, one way to avoid addresses being treated as personal data is to ensure that (if practicable) all participants on the network are bodies corporate rather than individuals.

Another possibility is to employ a blockchain technology that avoids using persistent public addresses for participants. Some blockchain technologies use cryptography to generate a different address to refer to a participant for each transaction. This helps to obfuscate the identity of participants, making it much more difficult to piece together different transactions undertaken by those participants which, when combined with other information, could uncover the identity of the individual.

B The problem of inadvertent addition of personal data

1 - The challenge

In addition to addresses on the network, another way personal data can land on the blockchain ledger is where substantive data uploaded to the blockchain as part of a transaction on the network (the transaction payload data) contains personal data. A transaction payload containing an individual's name, address, phone number, email address, or other contact or identifying details will result in that personal data being added to the blockchain. Even if the network is operating purely in a business context, this can occur incidentally, for example, if the ledger is used to record:

- an email address for invoicing, and that email address includes a person's name;
- a copy of a receipt for a commercial transaction identifying the individual who completed that transaction;
- a photograph where the image happens to also include an identifiable living person; or
- a copy of a contract that includes the name of an individual signing the contract on behalf of one of the parties.

So while a blockchain solution may be designed to avoid storing personal data, there are numerous instances where personal data may nevertheless be added to the ledger.

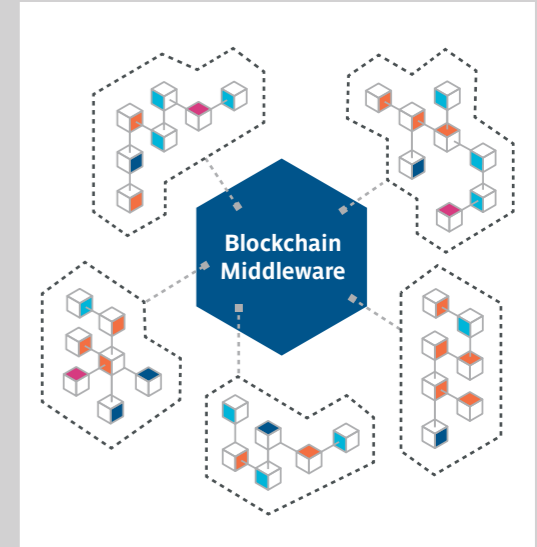
2 - Potential solution: Governance

A first line of defence to help avoid personal data being included on the blockchain would be to implement a contractual governance framework that obliges individuals not to upload personal data to the network and minimises free form data. We will come back to this in the next section but, given the possibility of personal data inadvertently making its way onto the network, this is not necessarily a perfect solution.

3 - Potential solution: Technical measures to redact personal data (design considerations)

Another principal means of keeping personal data off the blockchain network is to implement technological measures in blockchain middleware. Blockchain middleware applications can seek to prevent personal data being added to the network by avoiding the inclusion of specific data fields for personal data such as fields for names, phone numbers or email addresses. These applications can also employ more advanced techniques to recognise and remove personal data from information submitted to the blockchain network. AI or machine learning-based tools can, for example, be employed to recognise and blur faces in images before they are submitted to the network.

Middleware



Blockchain middleware is software that sits on top of one or more underlying blockchain networks and facilitates the application of those blockchain networks to particular use cases. Almost all interactions with blockchain networks will occur via blockchain middleware. Some of the most exciting innovation in the blockchain arena is occurring in blockchain middleware.

4 - Potential solution: Hashing personal data

A third useful way to keep personal data off the blockchain is to ensure that any data containing personal data is communicated via a side channel, with only a hash of that personal data then stored on the blockchain. These side channels could be managed by middleware, as discussed above, and made transparent to the user.

This enables those in possession of the personal data sent via the side channel to confirm that the data they have is correct by running the hashing function over that personal data and checking that the result matches the hash recorded on the blockchain. However, as outlined earlier, anyone who has only the hash generally cannot use it to obtain the underlying personal data.

There is, however, some debate as to whether a hash of personal data is truly anonymous (and so not subject to the GDPR), or whether it is in fact merely pseudonymous (and therefore within the scope of the GDPR by virtue of being re-identifiable as personal data). In particular, the Article 29 Data Protection Working Party, the EU advisory body charged with issuing guidance on the application of the former EU Data Protection Directive (95/46/EC),¹² identified in a 2014 opinion¹³ that hashing was a means of pseudonymisation rather than a means of anonymisation.

This view seems to have been reached in part on the basis that a hash function can effectively be reversed by trying all possible input values to find the one that produces the sought-after hash. In some cases this may be feasible, such as where the data that has been hashed is a name or a phone number – it may be possible to compute a hash of many possible names or phone numbers and identify the matching hash. In many cases, however, if the input data is sufficiently complex (such as a paragraph of text or a digital file such as a pdf document or a JPEG image), trying all possible input values in the hopes of achieving the same output hash would be practically impossible. Some hashing techniques, such as salted or peppered hashes (as discussed earlier in this publication) can also help to increase the complexity of input data and thus reduce the susceptibility of the hash to a brute force attempt at reversal.

Importantly, the European Data Protection Board (the body that replaced the Article 29 Data Protection Working Party under the GDPR) did not formally endorse this particular opinion of the Article 29 Data Protection Working Party in its formal endorsement statement.¹⁴ The Article 29 Data Protection Working Party's opinion also perhaps relied, in part, on the wording of Recital 26 of the former EU Data Protection Directive, which somewhat equivocally, suggested that data is only anonymous if re-identification of the individual is "no longer possible". The same wording is not present in Recital 26 of the GDPR, which states that:

"... To determine whether a natural person is identifiable [and therefore whether data is personal data that is the subject of the GDPR], account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments ...,"

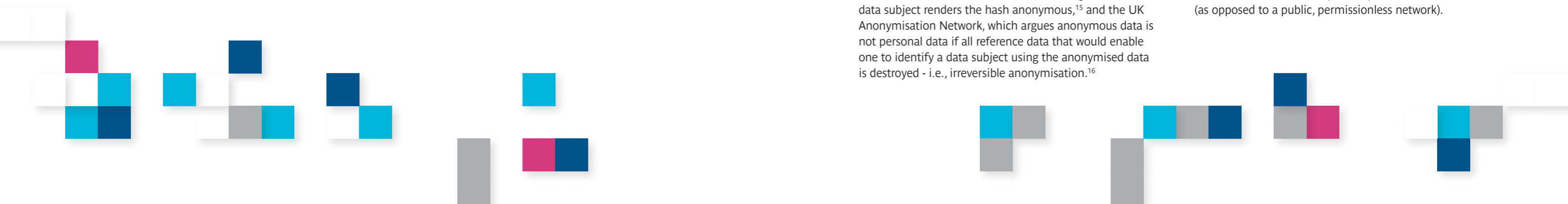
Given the above background, we would suggest that whether a hash is personal data and so within the scope of the GDPR will depend on the circumstances of the particular case. If the personal data being hashed is something simple like a name, a phone number or an IP address and the hashing function is a simple one (not a salted/peppered hash function) the hash is unlikely to be sufficiently anonymous. However, if the hash is such that there are no means reasonably likely to be used by anyone to identify the individual, then there are good arguments that the hash itself should not be regarded as personal data. This view is supported by a number of commentators including the German Blockchain Federation (Blockchain Bundesverband), which argues that the deletion of all off-chain data linking a hash to a data subject renders the hash anonymous,¹⁵ and the UK Anonymisation Network, which argues anonymous data is not personal data if all reference data that would enable one to identify a data subject using the anonymised data is destroyed - i.e., irreversible anonymisation.¹⁶

5.2 How to meet the GDPR challenge, part 2: establish a robust contractual governance framework

There are several key obligations under the GDPR which mean that any deployment of a commercial blockchain network will require a governance framework that is contractually binding on all participants. For the purposes of this paper, we consider those key GDPR obligations to be:

- 1 detailed data processing agreements as between controllers and processors;
- 2 clear and transparent agreements as between joint data controllers (where relevant);
- 3 restrictions on transfers of personal data out of the EEA; and
- 4 the provision of fair processing information (i.e. privacy notices).

However, as a pre-requisite to any governance framework, it will be necessary to implement GDPR-compliant blockchain solutions on a private, permissioned network (as opposed to a public, permissionless network).



The principal point of a public, permissionless network is that any person in any location can become a participant in that blockchain, without registration or restriction, simply by installing the relevant software and downloading a full copy of the blockchain. Generally, all participants on a public permissionless blockchain can see all the data on the blockchain ledger.

By contrast, to join, view data on or interact with a private permissioned blockchain network, participants must first obtain authorisation. Private permissioned blockchain networks employ various processes to approve new participants and part of this process can be to ensure all new participants subscribe to a set of rules or terms and conditions that govern their use of the network. Because anyone can join a public permissionless blockchain network, it is not possible to ensure participants agree to contractual terms and conditions before joining, nor is it possible to know the geographic location of members, assess their safekeeping of data or their compliance with the GDPR and other applicable regulations. For this reason, compliance with the GDPR mandates use of a private permissioned blockchain.

Public vs. private? Permissioned vs. permissionless?

The public vs. private and permissioned vs. permissionless distinctions dictate who can access and add data to a blockchain network. The public vs. private distinction refers to who can access the blockchain in any capacity, as public blockchains are open to all while private blockchains are open only to pre-approved members. The permissioned vs. permissionless distinction refers to who can add data (commonly in the form of submitting transactions and executing smart contracts) to the blockchain, as permissioned blockchains restrict this right to approved members while permissionless blockchains allow all members to add data.

A Four reasons why the GDPR makes a contractual governance framework necessary

1 - Data processing agreements

As mentioned in Section 4.4, the decentralised nature of blockchain makes the controller/processor analysis in a blockchain network relatively complex. While it is obvious that network members who actively upload personal data to a network are data controllers, there is much debate about whether members who merely operate nodes processing data on behalf of other participants in the network should be considered data processors or data controllers.¹⁷ One argument is that these members are data processors because they do not determine the means of processing, they only passively provide computational power needed to process the data.¹⁸ Conversely, it is argued that these members are data controllers because they actively choose to download and run the software used to process the personal data, thereby contributing to the decision of how the data is processed.¹⁹ We do not pass judgment on which of these arguments is better, we merely note:

- the decentralised nature of blockchain makes distinguishing between who is a data controller and who is a data processor difficult; and
- it is important to determine whether a member is a data controller or a data processor, as the GDPR imposes different responsibilities on each of them.

Both the French data protection regulator (**CNIL**), and the European Union Blockchain Observatory and Forum, recommend identifying data controllers as soon as possible when creating a blockchain network.²⁰ Blockchain network members can heed this advice by creating and agreeing to a contractually binding governance framework at the time of creation of a blockchain network. This governance framework would clearly delineate the roles of all network members, including members that join after the blockchain network is established. Such a governance framework should clearly identify which members will be uploading data onto the network, and which members only passively participate in the network. In this way, the governance framework can provide more clarity about which network members are data controllers, and which are data processors.

If the network includes data processors, then this contractually binding governance framework must also include the provisions contained in Article 28 of the GDPR, which require data processors and data controllers to document the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects implicated by the data processor's processing.²¹ Additionally, the Article 28 provisions require data processors to agree that, among other things, they will only process personal data on documented instructions from a data controller and will preserve the confidentiality of the data.



2 - Joint data controller agreements

The responsibilities of data controllers in situations where two or more data controllers jointly determine the purposes and means of processing are outlined in Article 26 of the GDPR. When data controllers act as joint data controllers, they must transparently determine how they will ensure GDPR-compliant treatment of data subjects' personal data, and what each data controller's relationship will be with data subjects.²² The joint data controllers must then make the essence of their arrangement available to data subjects.²³

Members of a blockchain network would most likely be joint data controllers, as most solutions will involve members jointly determining the purposes and means of processing data on the network to which they belong.

Creating a transparent and robust governance framework will compel joint data controllers to determine their respective responsibilities for compliance and their relationships with the data subjects. Further, the governance framework can either be made available to data subjects or can require the creation of a publicly-available, high-level summary of the joint data controllers' arrangement. By requiring the network members to publish at least a summary of their arrangement, a governance framework can enable compliance with the Article 26 requirements.

“Joint data controllers must make the essence of their arrangement available to data subjects.”

3 - Restrictions on transferring personal data out of the EEA

Additionally, the governance framework would need to facilitate GDPR compliant data transfers outside of the EEA. As discussed in Section 4.7, the GDPR restricts transfers of personal data out of the EEA. However, any global blockchain solution will likely involve the processing of data outside of the EEA (and outside of the countries currently the subject of an Adequacy Decision by the European Commission). To resolve this conflict, a governance framework could incorporate the European Commission's model international data transfer clauses. Since the governance framework will be agreed to by all members of a blockchain network, inclusion of these clauses into the governance framework will make the model clauses a multilateral agreement. The Article 29 Working Party previously endorsed the inclusion of data protection clauses into multilateral agreements as a means to comply with restrictions on international data transfers.²⁴

By incorporating the model international data transfer clauses into the overarching governance framework, network members necessarily agree to treat personal data in a way deemed sufficient by the European Commission, thereby enabling all network members to transfer personal data to other network members regardless of where the members are located.

4 - Fair processing notices

Lastly, the creation of a governance framework will enable network members to comply with Articles 13 and 14 of the GDPR, which oblige data controllers to provide data subjects with fair processing information (i.e. privacy notices). The obligation to provide fair processing information is triggered either when personal data is collected directly from the data subject, or indeed when personal data is obtained from someone other than the data subject.²⁵ In either case, the data controller must provide data subjects with certain categories of information, including the contact information of the data controller, the purposes for which the data are being processed, the recipients of the personal data, and the data controller's intent to transfer personal data to certain third countries.²⁶ Additionally, the data controllers must remind the data subjects of their rights under the GDPR, including their rights to request access to and rectification or erasure of personal data.²⁷

A clear governance framework would enable network members to operate the network in coordination while clarifying each member's role in the network. This framework provides the means for members to easily identify which of them must provide fair processing information and uphold other data subjects' rights. The framework solution allows members to create a cumulative document containing the information required by Articles 13 and 14 for each data controller. Lastly, the framework can obligate network members to make this information available to the public, either by requiring the members to create and maintain an easily accessible website disclosing the fair processing information, or by requiring the members to individually (or collectively) provide fair processing information to any data subjects whose data the members collect and obtain.

B Guiding the governance framework: key requirements

A complete catalogue of everything that should be addressed in a contractual governance framework for a blockchain network is beyond the scope of this paper. For example, a governance framework should also deal with various issues not related to data protection, such as rules around joining or exiting the network, audit requirements and practices, ownership of intellectual property and rights in blockchain data, permitted and prohibited conduct, remediation requirements when governance violations are identified, dispute resolution, and governing law and jurisdiction (to name but a few). From a data protection and privacy perspective, the governance framework should:

- be contractually binding on all participants in the blockchain network;
- implement the GDPR-required provisions for data processing, joint controllers, the model clauses for transferring personal data outside the EEA, and the making available of fair processing notices;
- establish a process for data subjects to exercise their rights under the GDPR, including a procedure to notify other data controllers to delete personal data when a request is received by one network member (see below); and
- provide mechanisms to achieve data minimisation, privacy by design, risk mitigation and permit the removal of personal data that is no longer required (see below).

5.3 Deleting personal data and upholding data subject rights

While a detailed contractual governance framework will go some way to addressing GDPR obligations and concerns, there are certain data protection problems which remain unsolved. In particular, these problems stem from a data subject's rights to request that: (1) their personal data be deleted; and (2) their personal data be corrected wherever it is inaccurate.

A The right to be forgotten and the obligation to delete data

1 - The challenge

For its part, one of the most valuable properties of blockchain technology is its immutable nature. This ensures the permanence (and, therefore, reliability) of the data on the blockchain. That being said, the immutability of data on a blockchain is at odds with a right to erasure (the so-called 'right to be forgotten') or an obligation to delete data. This particular challenge is thus understandably one of the most widely discussed in the context of the GDPR and blockchain.

As discussed above, it will be difficult in most cases to be certain that no personal data is stored on the blockchain. Thus, blockchain solutions must confront the need to manage personal information in compliance with the GDPR. This includes abiding by the data minimisation obligation discussed in Section 4.3, and the right to erasure discussed in Section 4.6 (A).

The data minimisation obligation will be satisfied so long as the data are limited to what is necessary for the purpose for which they are processed. Thus, if the

personal data stored on the blockchain remain necessary for the purpose for which they are processed, retention of the data on the blockchain does not violate the data minimisation obligation. Similarly, the qualified right to erasure does not require blockchain members to delete personal data if a valid purpose still exists to process that data. As discussed above, one such valid purpose is where the processing of said data is required by EU or EU Member State law.

In almost all cases, however, after a sufficient period of time, personal data will no longer need to be retained to fulfil the purposes for which it was collected. At this point, the exception to the right of erasure will no longer apply and the personal data must be deleted upon a request by the relevant individual. Additionally, the obligation in Article 5 of the GDPR (to retain personal data for only so long as is necessary for the purpose for which it is processed), requires data controllers to delete personal data once they are no longer needed, even absent a request from the individual. Almost any means used to store personal data in a business context must, therefore, enable deletion of that personal data.

2 - Potential solution: Blockchain "pruning"

If the personal data on a particular blockchain network must be retained for a certain number of years to satisfy a particular legal or regulatory obligation, one option may be to "prune" the blockchain. Pruning is the process of deleting historical blocks on the blockchain that pre-date a certain point in time. For example, if regulation requires data to be stored for seven years, the blockchain governance framework could require that all participants in the blockchain network delete all blocks of data that are greater than seven years old.

Operationally, however, pruning may prove to be an unattractive option for many blockchain solutions. Many blockchain solutions use the blockchain to record a base state and subsequent transactions. The only way to ascertain the current world state from the blockchain is to start with the base state and track through every subsequent transaction. If a blockchain like this were to be pruned, it would be necessary for the participants on the network to formulate and agree, and to record in a similarly immutable and decentralised way to the original blockchain, a new base state that will replace the original base state and all transactions up to the most recent block that has been pruned. There are technical means available to help achieve this, but the blockchain technology employed by the solution will inevitably be somewhat more complex.

Additionally, while pruning would assist compliance with the obligation to delete data after it is no longer required for the purpose for which it was collected, it is usually not a viable means of complying with ad hoc requests from data subjects for personal data about them to be erased or rectified.

3 - Potential solution: Deletion by way of encryption

Alternatively, it may be possible to delete personal data stored on the blockchain by irreversibly encrypting the data. Under this approach, the encrypted data containing the personal data would remain permanently on the blockchain, but the personal data would be "deleted" from the blockchain by deleting all keys that enable decryption of the encrypted data. This method appears to be a natural extension of the view held by the German Blockchain Federation (Blockchain Bundesverband) and the UK Anonymisation Network that data is no longer personal data if it has been irreversibly anonymised.

However, the Article 29 Data Protection Working Party previously classified encryption as pseudonymisation, not anonymisation.²⁸ One pseudonymisation technique mentioned in the Article 29 Data Protection Working Party opinion included using a keyed-hash function to produce a hash and then deleting the key.²⁹ The opinion did note that employing this technique would make it "computationally hard for an attacker to decrypt or replay the function, as it would imply testing every possible key, given that the key is not available."³⁰

Nonetheless, it remains unclear whether the Working Party opinion considers personal data that is irreversibly encrypted and keyless to be anonymised for the purposes of the GDPR and thus theoretically deleted from a blockchain network.

It is for this reason that we are calling on the European Data Protection Board and national data protection authorities to settle this point and set standards for encryption and key deletion that can achieve an adequate level of anonymisation.

If deletion by encryption is a feasible solution, then any blockchain network employing deletion by encryption will need to ensure its governance framework obligates its members to delete keys in response to a data subject's request for erasure. If any member does not delete its key, then the data would not be considered anonymised under the Article 29 Working Party's definition of anonymised data, which holds that data are only considered to be anonymised when no person can re-identify them.³¹



An added benefit of deletion by encryption is that it preserves the immutable nature of the blockchain, as the data on the blockchain itself is not altered. Additionally, it offers another way to achieve “pruning” of a blockchain (as discussed above). Every block added to the chain could be encrypted with a key and, after the specified time, every participant on the network could be required to delete the keys to blocks older than that a particular age.

4 - Potential solution: Editable blockchains

Editable blockchains are a new solution that enable the deletion and rectification of data on the blockchain. They are divisive (in certain areas of the blockchain community) because they are not immutable, which is seen by some to undermine one of the fundamental premises of blockchain technology. That being said, we believe it is important at this stage to strike a pragmatic balance between the ideological purity of a blockchain solution and the commercial need for privacy compliance.

As described in a recently granted U.S. patent, editable blockchains function in a manner which allows certain permissioned members to be able to apply hash functions to existing blocks, to substitute or remove the data contained in the blocks.³² The hash functions used to edit the blockchain can be programmed to leave a “scar” on the edited blocks, enabling all network members to identify which blocks have been edited.³³

If an editable blockchain solution is adopted, then members must implement well-defined governance rules that control who can edit the blocks and what situations allow or require editing of the blockchain. To enable GDPR compliance, the governance rules should mandate the editing of blocks that contain personal data when the data are no longer necessary for the purpose for which they are processed or when data subjects exercise their rights to erasure and rectification.

5 - Potential solution: Deletion by “forking” the blockchain

As a last resort, it is possible to “fork” a blockchain to remove personal data. To perform a fork of the blockchain, a majority of nodes on a pre-existing blockchain must agree to a new set of initial rules, and then update the software used to run the blockchain so that a majority of nodes on a blockchain network agree to the new ledger. As part of these initial conditions, network members can agree to remove the blocks in the blockchain that contain personal data. However, this technique requires re-running the hashes for every subsequent block that built upon any removed blocks.

It is important to note that network members should set out what events merit performing a fork of the blockchain within their governance regime. Further, that governance regime should also obligate network members to update the blockchain’s software when a fork is conducted, thereby avoiding contentious forking situations that could lead to different groups of network members claiming different branches of a blockchain are the one true branch. By inserting these requirements into the governance framework, members can control when and how the drastic step of forking the blockchain occurs.

That being said, as a practical matter, forking is a very costly technique that will also be operationally disruptive. What is more, the GDPR requires deletion of personal data within a maximum of three months from a valid request, meaning that a forking exercise would be required multiple times each year. Given the costs and time involved in such an exercise, it is difficult to conclude that forking is an adequate data deletion solution. These negative aspects of forking are further evidence of the need for up-to-date, pragmatic regulatory intervention in this space to enable reliance on innovative but effective forms of data deletion.

B The right of rectification

1 - The challenge

A second major challenge posed by the GDPR relates to the right of rectification. This can be thought of as two distinct rights: (a) the right to rectification of inaccurate personal data; and (b) the right to complete incomplete personal data. As explained in Section 4.6(B) this right is unqualified. Therefore, none of the exceptions that apply to the right of erasure (such as the right of the data controller to retain data for the establishment, exercise or defence of legal claims) apply to the right of rectification. If a data subject with inaccurate or incomplete personal data on a blockchain asks the data controllers to rectify the information, the data controllers must do so.

Similar to the right to erasure, the immutable nature of blockchain technology is seemingly at odds with the right to rectification, especially the right to rectify inaccurate personal data.

2 - Potential solution: Rectification by a supplementary notice

The GDPR is clear that it is possible to rectify incomplete personal data about a data subject by supplementing that data with a clarificatory statement. That being said, there are obvious difficulties for blockchain solutions in rectifying incomplete personal data set out in historical blocks on the chain. This stems from the fact that, as discussed above, alteration to historical blocks will impact the entirety of the blockchain as it then exists.

While the rectification of incomplete personal data may be feasible by way of a clarificatory statement, it is not clear whether the same is true for the rectification of inaccurate personal data under the GDPR. The fact that a supplementary statement is specifically mentioned in the context of the right to rectify incomplete personal data, and not in the case of the right to rectify inaccurate personal data, suggests it is not a sufficient means of rectifying inaccurate personal data.

This would mean that to comply with the right to rectification of inaccurate personal data, the earlier incorrect information would need to be erased and replaced with the corrected information. This of course makes sense in many instances – it will usually be more appropriate to remove a statement about someone that is plainly incorrect than to simply supplement it with a correction.



For example, suppose the statement: “Ms X has entered internationally sanctioned Country Y on a business visa” is recorded in your database. If this statement about Ms X is incorrect and Ms X and her business are, in fact, prohibited under international sanctions from conducting business in Country Y, Ms X might reasonably submit a request to you that the incorrect statement be corrected. It is by no means certain that a regulator or a court would regard it as a sufficient rectification if you were simply to update your database to say: “Ms X did not enter Country Y on a business visa. This statement is actually incorrect; Ms X has not done business in a country subject to international sanctions.” Indeed, Ms X may well not be satisfied with this and demand that all evidence of the initial statement to be deleted and replaced with a correct statement.

By contrast, however, there may be cases where it is not appropriate to erase personal data, even if incorrect, in order to replace it with correct information. One example is data that serves an evidential purpose, such as a signed contract. It may not be appropriate to modify a signed contract to, for example, correct a mistake in the job title of an individual named in the contract. It may be preferable to attach a clarificatory statement to the contract, so that the contract can still serve as evidence of the exact, unaltered terms of the agreement the parties to the contract reached.

It is unclear whether a regulator or a court would ever regard a supplementary statement as sufficient to comply with the Article 16 GDPR right to rectification of inaccurate personal data. Unfortunately this is an area where there is no reliable guidance from regulators, making it a further issue on which we would urge the relevant regulatory bodies to provide clear guidance on.

3 - Potential solution: Rectification by deletion

To the extent it is not possible to comply with the obligation to rectify incorrect personal data by a supplementary statement, it would be necessary to look to the methods outlined above to enable deletion of incorrect personal data (for example, deletion by encryption) followed by addition of the correct personal data to the blockchain. Because a data subject might request that incorrect personal data about them of any age be rectified, pruning of the blockchain may not offer an effective solution.

Pending guidance from a data protection regulator that in certain circumstances a supplementary statement might be sufficient, it is prudent to ensure any GDPR-governed blockchain solution facilitates the effective deletion of incorrect personal data and permits correct personal data to be substituted in its place.

Our call for regulatory intervention

The European Data Protection Supervisor announced in January 2019 its intention to increase efforts to monitor the evolution of blockchain technology in order to “adequately advise the EU legislator on the possible risks and safeguards involved”³⁴ However, in addition to this, greater action is required by both data protection authorities and law-makers in relation to the interplay between blockchain and data protection. More specifically, we are calling for:

1. Regulatory intervention, particularly in relation to:
 - a whether (and how) innovative forms of data deletion (such as deletion by way of encryption) can function in such a way that robustly upholds individuals' rights to have their own personal information deleted by data controllers in line with Article 17 of the GDPR; and
 - b whether a corrective supplementary statement can function as a suitable means of rectifying inaccurate personal data in line with Article 16 of the GDPR.
2. Greater engagement by, and co-operation between, regulators, law-makers and blockchain technology developers such that legal and regulatory obstacles might be overcome in a manner that facilitates the continued growth and exploitation of blockchain as a technology of currently indefinable potential.



6

Application to MTI's Solution

6.1 Current problems in the shipping industry

For the first time in fifteen years, global GDP growth outpaced container shipping growth in 2016.³⁵ One way to reverse this trend is to address the numerous inefficiencies plaguing the shipping industry. Many inefficiencies stem from the shipping industry's outdated treatment of data.³⁶ While some ports share real-time shipping information in connected ecosystems, data silos throughout the shipping chain prevent easy upstream and downstream data transfers.³⁷ Instead, piecemeal information is passed along the chain of participants as the shipping process takes place. This disjointed flow of information makes it difficult for anyone at a given stage of the chain to obtain complete, real-time information regarding other stages.³⁸ Further, because global trade participants use idiosyncratic databases developed separately over decades to conduct their business, there has been a general inability to agree on the use of any centralised aggregator of information in the shipping industry.³⁹ These inefficiencies are believed to cost the global shipping industry approximately 10% of global shipping costs each year.⁴⁰

See diagram on page 40.

6.2 Blockchain helps to alleviate shipping industry issues

A blockchain-based solution gives all players in the end-to-end shipping chain access to the same information in real-time. This enables participants to communicate with each other based on a single shared view of applicable data. Information can be shared in a trusted and consistent way that is auditable and without the need for any centralised aggregator. The shipping blockchain offers a single source of truth without a single point of failure.

See diagram on page 41.



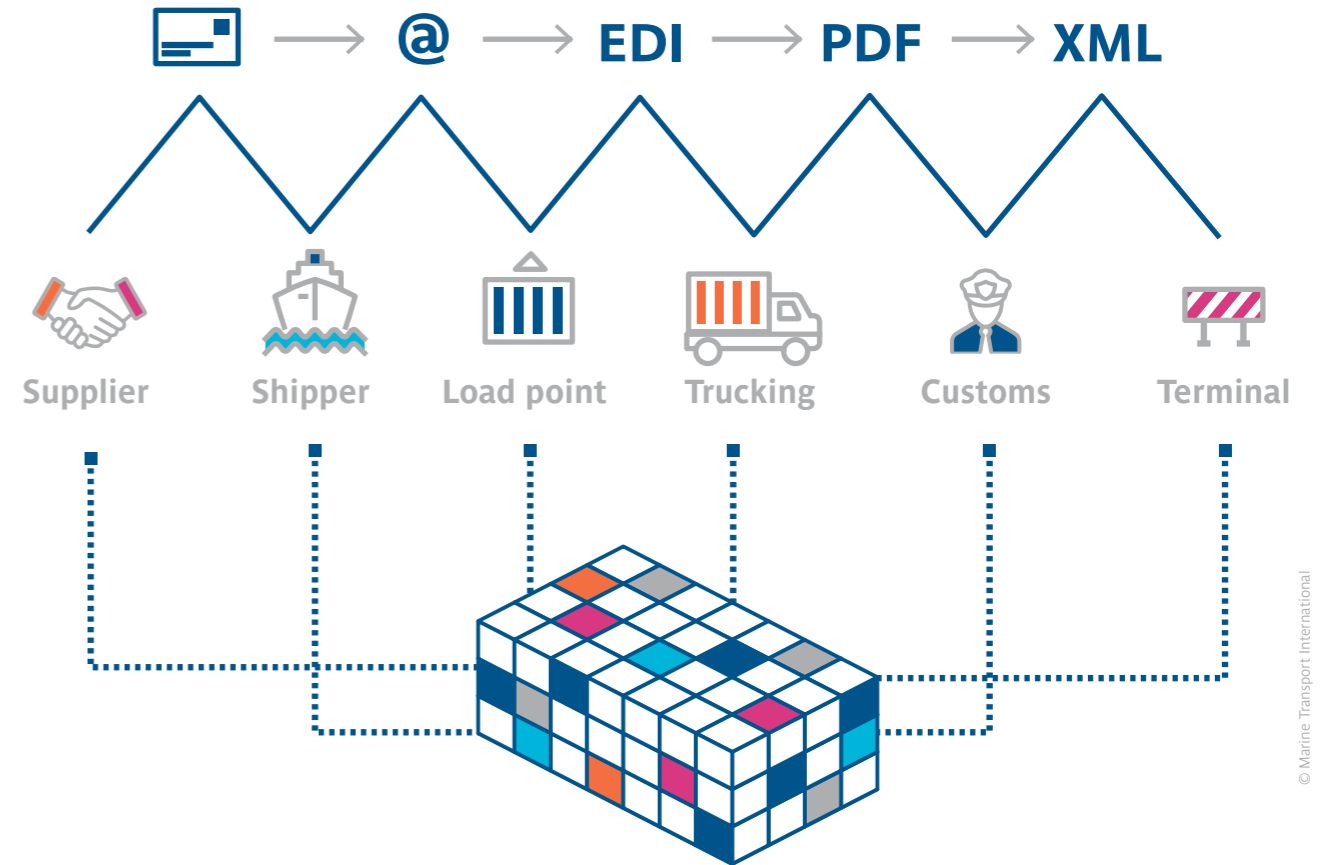
Current process



© Marine Transport International

Problems: sequential, data silos, work intensive, must trust data intermediaries

New process



© Marine Transport International

Solutions: automation, visibility, streaming the information flow, low price, encrypted data

6.3 Outline of MTI's solution

The crux of MTI's solution is MTI's adapter, a middleware application for interfacing with certain blockchain networks. MTI's adapter is suited for use in a wide variety of supply chains, including in international freight and shipping. It enables systems currently in use in the shipping industry to interface with one or more blockchain networks. Each network can be run by different industry players and can use different underlying blockchain technologies (such as IBM's Hyperledger Fabric, Activedger, Corda, Quorum etc.). There is thus no need for every player in the industry to use one particular network, as multiple networks can operate in parallel. Each shipping industry player can aggregate their multiple networks and existing shipping industry systems in a single place using MTI's adapter.

To drive commercial adoption of its adapter, MTI plans to establish, together with a consortium of industry players, one such blockchain network for use in international shipping. This network will likely be built on Hyperledger Fabric and will be a private, permissioned network.

In line with the GDPR principle of data minimisation, the network will store on the blockchain (on-chain) only information that everyone on the network has the right to view. Where a transaction involves information that only some participants have a right to see, that private information will be hashed and the hash will be added to the blockchain. The underlying private information will then be sent, via a side channel peer-to-peer network, to those participants with a right to see the

information. This focus on privacy by design means that information that should not be visible to everyone is kept off the blockchain (off-chain) and is only stored locally by those participants with a right to access the information. Any person who has a copy of the off-chain private information can run the hashing algorithm over it and compare the result to the hash stored on-chain to verify that it has a true copy of the private information associated with the transaction recorded on the ledger. This also ensures all information associated with transactions on the network are fully auditable.

6.4 What personal data may be processed?

The personal data likely to be involved in MTI's solution are not likely to be particularly sensitive. They would likely be limited to:

- names of people signing certain shipping documents;
- business contact details of certain people involved in the shipping process, such as phone numbers or email addresses; and
- photos of shipping cargo that may incidentally include recognisable individuals or other personal data.

MTI's solution intends to use the side-channel model described above for all information that should not be freely visible to every participant on the network, which will include all personal data. This includes using the side-channel model to restrict the visibility of free form comments. There will, of course, always be the risk that some personal data is not properly confined to the side channels and finds its way on to the network, and we therefore consider how MTI may ensure GDPR compliance given this possibility.

To minimise the risk of personal data finding its way onto the network, MTI will implement technological solutions to identify personal data submitted to the network and prevent such data from entering the network. These solutions could range from restricted data fields that do not accept data formats containing personal data, to artificial intelligence solutions that screen all submitted data for personal data and either flag suspected personal data for review, thereby preventing submissions containing personal data from entering the network, or redact personal data from otherwise compliant data submissions. The artificial intelligence screening described above has the added benefit of reduced business impact, as data entries could still be submitted to the network with no interruption and only personal data inadvertently included in a data submission would be impacted.

These techniques could help reduce MTI's GDPR-related compliance burden by limiting the opportunities for personal data to enter the network. Instead of having to ensure GDPR-compliant treatment of vast amounts of personal data intentionally entered onto the network, MTI would be left with only personal data inadvertently entered into the network that had evaded the front-end screening mechanisms described above. The effort by MTI to implement privacy by design and make use of data minimisation techniques demonstrates a genuine attempt at compliance with data protection and privacy legislation. While there may be a risk of non-compliance with the GDPR in this solution, the concerted efforts at compliance undoubtedly act as mitigants of that risk.

6.5 Who will be data controllers and who will be data processors?


Given that each participant who is transmitting personal data across the network (including via any specifically designed off-chain side channel) will likely be determining the purposes and means of processing in relation to any personal data, it would seem logical to conclude that these participants are data controllers. The same holds true for participants that store personal data in their own right, whether or not that personal data was received via a side channel or extracted from personal data that has inadvertently entered the blockchain.


To the extent that there are participants in the network who are simply operating a node which processed personal data on behalf of other participants, these participants would likely be data processors. However, it should be noted that a participant involved in creating the architecture of the system could be deemed as acting as a data controller in determining the purposes and means of processing.





6.6 Measures to help achieve GDPR compliance

In summary, MTI can substantially achieve a GDPR-compliant blockchain solution by following the below steps.

 1. Keep personal data off-chain to the maximum extent possible. To keep personal data off-chain, MTI should only allow corporations (not natural persons) to be participants on the blockchain network. By preventing natural persons from joining the blockchain network, MTI can prevent network participant identifiers from being considered personal data. Additionally, MTI should have all network participants agree in the network governance document that they will not upload personal data to the blockchain. Lastly, MTI may consider using technological solutions such as restricted data entry fields and artificial intelligence to prevent personal data submitted to the network from being uploaded to the blockchain.

 2. Use a private, permissioned blockchain. This will allow MTI (or whatever group or entity is specified in the network's governance document) to control who is able to join the blockchain network (which is needed to prevent natural persons from joining as network participants) and who is able to upload data to the blockchain (which is needed to ensure only those who have agreed to the limitations on uploading personal data contained in the network governance document are permitted to actually upload data).

 3. Employ privacy by design when creating its blockchain network. This includes designing the network to only collect and store data that are adequate, relevant and limited to what is necessary for the purpose for which they are processed, and to comply with data subjects' rights (particularly the rights to rectification and erasure).

 4. Document all of these obligations and more in a transparent and robust governance framework. This governance framework should contain terms and conditions to which all network participants must agree before being permitted to join MTI's blockchain solution. Among other things, the terms and conditions should:

- prohibit network participants from uploading personal data to the blockchain;
- incorporate the data processing clauses required by Article 28 and oblige all network participants that are data processors to abide by those clauses;
- incorporate the European Commission's model international data transfer clauses; and
- establish the processes by which the network participants will enable data subjects to exercise their rights.

By taking the above steps, MTI can create a substantially GDPR-compliant blockchain solution.



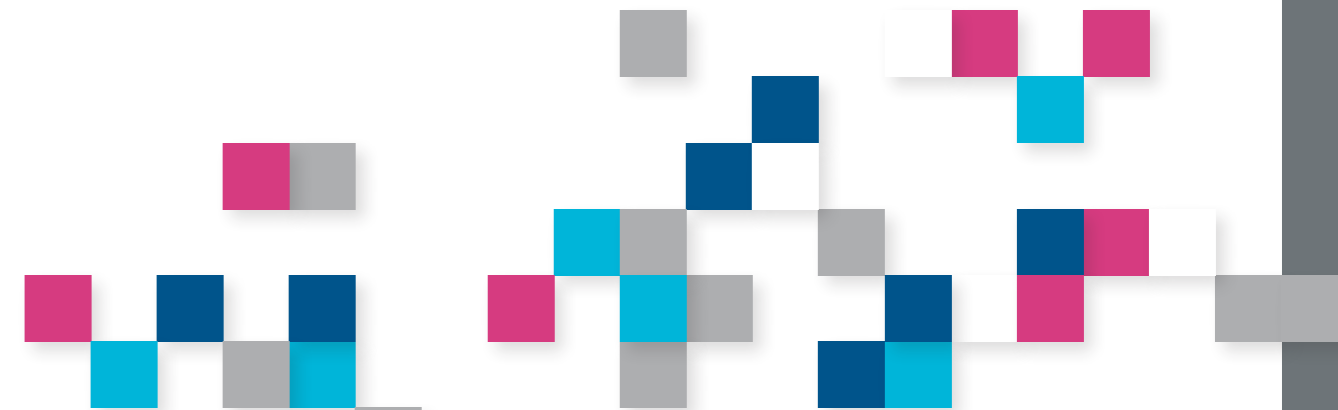
6.7 Regulatory engagement with open issues

In addition to our calls for specific guidance from European data protection authorities in certain areas, there may also prove to be value in actively engaging with regulators to elicit suggestions to further aid compliance. Since the GDPR is a new regulation, there is much uncertainty about how regulators will enforce its provisions. As of May 2018 (the month the GDPR came into effect), seventeen of twenty-four EU member state authorities said they were unable to fulfil the obligations the GDPR placed on them.⁴¹

As recently as November 2018, the European Parliament Committee on Civil Liberties, Justice and Home Affairs called for additional research into blockchain technology to determine how the technology may clash with

the GDPR.⁴² In light of this uncertainty, there are likely to be benefits from developing strong relationships with regulators to ensure up-to-date information around regulatory views on specific areas of GDPR compliance.

One way to develop relationships could be to enter into programs such as the UK Information Commissioner's Office (ICO) regulatory sandbox, which will aim to provide a safe space where organisations can develop innovative products and services using personal data while engaging with the ICO on ways to comply with the GDPR. Entities inside the sandbox will not be exempt from the GDPR's obligations, but will benefit from close interaction with the ICO about what is required for GDPR compliance. Through participation in programs such as the ICO's regulatory sandbox, implementers and regulators can become aware of and champion new blockchain technology that provides creative approaches to the regulatory challenges posed by the immutable nature of blockchain.





7 Conclusion and Key Takeaways

Through this publication we have identified that, while it may not yet be possible to definitively solve all of the challenges posed by the GDPR and other privacy regimes to the implementation of blockchain solutions, progress can be made if the interested parties work together openly and pragmatically.

Blockchain and the GDPR can co-exist

We do not feel that, by definition, blockchain technology and data protection and privacy are inherently contradictory. Quite the opposite. Indeed, we believe that a blockchain solution that respects the fundamental principles of data protection and privacy is achievable, and the four key elements necessary to achieve that aim, as identified in this publication are:


- 1 Use of a private, permissioned blockchain.
- 2 Avoiding, if possible, the storing of personal data on the blockchain, eliminating/minimising freeform data fields.
- 3 Implementing a detailed governance framework.
- 4 Employing innovative solutions to traditional data protection problems even if untested.

A Call for Guidance

We will conclude by repeating our call on regulatory authorities to take the steps necessary to address the outstanding privacy challenges posed by blockchain technology, most importantly, in relation to

- 1 the use of encryption as a means of anonymisation and deletion of personal data; and
- 2 the use of supplementary statements as a means of complying with obligations to correct inaccurate personal data. Regulatory intervention is necessary here because innovative solutions to traditional data protection challenges will only succeed with the understanding and support of regulators and lawmakers.

There is a risk that, if steps are not taken by regulators and lawmakers to bridge the gap between data protection law and blockchain technology, we will witness a slowing in (or even end to) advancements in blockchain solutions. Such an outcome would ultimately be detrimental to technological developments that may have the capacity to deliver substantial benefits to the world as a whole.



Endnotes

- 1 “European Commission launches the EU Blockchain Observatory and Forum” European Commission press release (1 February 2018), available at: http://europa.eu/rapid/press-release_IP-18-521_en.htm.
- 2 “EU Blockchain Roundtable paves the way for Europe to lead in blockchain technologies” (20 November 2018), available at: <https://ec.europa.eu/digital-single-market/en/news/eu-blockchain-roundtable-paves-way-europe-lead-blockchain-technologies>
- 3 French National Commission on Informatics and Liberty (CNIL), “Blockchain and the GDPR: responsible solutions regarding the presence of personal data”, 24 September 2018, available at: <https://www.cnil.fr/en/node/24807>. German Blockchain Federation (Blockchain Bundesverband), “Blockchain, data protection and the GDPR”, 25 May 2018, available at: https://www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v1.0.pdf. EU Blockchain Observatory and Forum, “Blockchain and the GDPR”, 16 October 2018, available at: <https://www.eublockchainforum.eu/reports>.
- 4 Gabrielle Orum Hernández, Why Blockchain Poses an Unusual Challenge for GDPR Compliance, LAW.COM, 25 May 2018, available at: <https://www.law.com/2018/05/25/why-blockchain-poses-an-unusual-challenge-for-gdpr-compliance/?srlreturn=20181103145145>; Tom Cox and Andrew Solomon, Block chain: Is the GDPR out of date already?, Lexology, 30 August 2017, available at: <http://www.lexology.com/library/detail.aspx?g=d4c0481a-c678-4748-80cb-4ab91766207>.
- 5 EU Blockchain Roundtable paves the way for Europe to lead in blockchain technologies” (20 November 2018), available at: <https://ec.europa.eu/digital-single-market/en/news/eu-blockchain-roundtable-paves-way-europe-lead-blockchain-technologies>
- 6 EU Blockchain Observatory and Forum, “Blockchain and the GDPR”, 16 October 2018, available at: <https://www.eublockchainforum.eu/reports>.
- 7 Article 9 of the GDPR lists the following special categories of personal data: “data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation”.
- 8 GDPR Article 25.
- 9 GDPR Article 17(3)(b).
- 10 GDPR Article 17(3)(e).
- 11 The European Commission has to-date issued a finding of adequacy in respect of: Andorra, Argentina, Canada (partial), Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland and Uruguay. Adequacy talks are ongoing with South Korea.
- 12 The Article 29 Data Protection Working Party was established under Article 29 of the Data Protection Directive (Directive 95/46/EC), but has since been replaced by the European Data Protection Board under Article 68 of the GDPR.
- 13 Article 29 Data Protection Working Party, opinion 05/2014 on Anonymisation Techniques (adopted on 10 April 2014), available at: <https://www.pdpjournals.com/docs/88197.pdf>.
- 14 Endorsement 1/2018 of the European Data Protection Board dated 25 May 2018, available at: https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en.
- 15 German Blockchain Federation (Blockchain Bundesverband), “Blockchain, data protection and the GDPR”, 25 May 2018, available at: https://www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v1.0.pdf.
- 16 UK Anonymisation Network, The Anonymisation Decision-Making Framework, 2016, available at: <http://ukanon.net/wp-content/uploads/2015/05/The-Anonymisation-Decision-making-Framework.pdf>.
- 17 EU Blockchain Observatory and Forum, “Blockchain and the GDPR”, 16 October 2018, available at: <https://www.eublockchainforum.eu/reports>.
- 18 Id. This argument appears to be supported by the European Parliament’s Committee on Civil Liberties, Justice and Home Affairs, which distinguishes between data controllers and data processors in a blockchain setting on the basis of whether a network member uploads data onto the network. European Parliament Committee on Civil Liberties, Justice and Home Affairs, opinion 2018/2085(INI) on Blockchain: A Forward-Looking Trade Policy (adopted on 15 November 2018), available at: <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2018-0407&format=XML&language=EN#title3>.
- 19 EU Blockchain Observatory and Forum, “Blockchain and the GDPR”, 16 October 2018, available at: <https://www.eublockchainforum.eu/reports>.
- 20 CNIL, Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, 6 November 2018, available at: <https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data>. EU Blockchain Observatory and Forum, “Blockchain and the GDPR”, 16 October 2018, available at: <https://www.eublockchainforum.eu/reports>.
- 21 GDPR Article 28.
- 22 GDPR Article 26.
- 23 Id.
- 24 Article 29 Data Protection Working Party, 14 June 2017 Letter to ESMA, available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=45447.
- 25 GDPR Articles 13 and 14.
- 26 Id.
- 27 Id.
- 28 Article 29 Data Protection Working Party, opinion 05/2014 on Anonymisation Techniques (adopted on 10 April 2014), available at: <https://www.pdpjournals.com/docs/88197.pdf>.
- 29 Id.
- 30 Id.
- 31 Article 29 Data Protection Working Party, opinion 05/2014 on Anonymisation Techniques (adopted on 10 April 2014), available at: <https://www.pdpjournals.com/docs/88197.pdf>.

This view is not shared by the UK Anonymisation Network, which has adopted a relative view of anonymization—i.e., data can simultaneously be anonymous data to one data controller and personal data to another data controller depending on the individual data controller’s ability to identify the data. Regardless of whether characterization as anonymous data is a relative or absolute determination, the only way to ensure personal data becomes anonymous data for all members of a blockchain network under the deletion by encryption technique is to obligate all members to delete their keys. UK Anonymisation Network, The Anonymisation Decision-Making Framework, 2016, available at: <http://ukanon.net/wp-content/uploads/2015/05/The-Anonymisation-Decision-making-Framework.pdf>.

32 U.S. Patent No. 9,959,065 (filed Oct. 5, 2017). For more discussion on the patent and editable blockchains, please see: Accenture, Editing the Uneditable Blockchain, available at: https://www.accenture.com/t201609277033514Z_w_us-en/acmedia/PDF-33/Accenture-Editing-Uneditable-Blockchain.pdf#zoom=50.

33 Id.

34 European Data Protection Supervisor Newsletter No.66, January 2019, available at: https://edps.europa.eu/press-publications/publications/newsletters/newsletter-66_en.

35 Steve Saxox & Matt Stone, Container Shipping: The Next 50 Years, McKinsey & Company (October 2017). Available at: <https://www.mckinsey.com/~media/mckinsey/industries/travel%20transport%20and%20logistics/our%20insights/how%20container%20shipping%20could%20reinvent%20itself%20for%20the%20digital%20age/container-shipping-the-next-50-years-103017.ashx>.

36 Michael White, Digitizing Global Trade with Maersk and IBM, IBM (16 January 2018). Available at: <https://www.ibm.com/blogs/blockchain/2018/01/digitizing-global-trade-maersk-ibm/>.

37 Steve Saxox & Matt Stone, Container Shipping: The Next 50 Years, McKinsey & Company (October 2017). Available at: <https://www.mckinsey.com/~media/mckinsey/industries/travel%20transport%20and%20logistics/our%20insights/how%20container%20shipping%20could%20reinvent%20itself%20for%20the%20digital%20age/container-shipping-the-next-50-years-103017.ashx>.

38 Id.

39 Michael White, Digitizing Global Trade with Maersk and IBM, IBM (16 January 2018). Available at: <https://www.ibm.com/blogs/blockchain/2018/01/digitizing-global-trade-maersk-ibm/>.

40 Id.

41 Reuters, European Regulators: We’re Not Ready for New Privacy Law (8 May 2018), available at: <https://www.reuters.com/article/us-europe-privacy-analysis/european-regulators-were-not-ready-for-new-privacy-law-idUSKBN1I915X>.

42 European Parliament Committee on Civil Liberties, Justice and Home Affairs, opinion 2018/2085(INI) on Blockchain: A Forward-Looking Trade Policy (adopted on 15 November 2018), available at: <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2018-0407&format=XML&language=EN#title3>.

