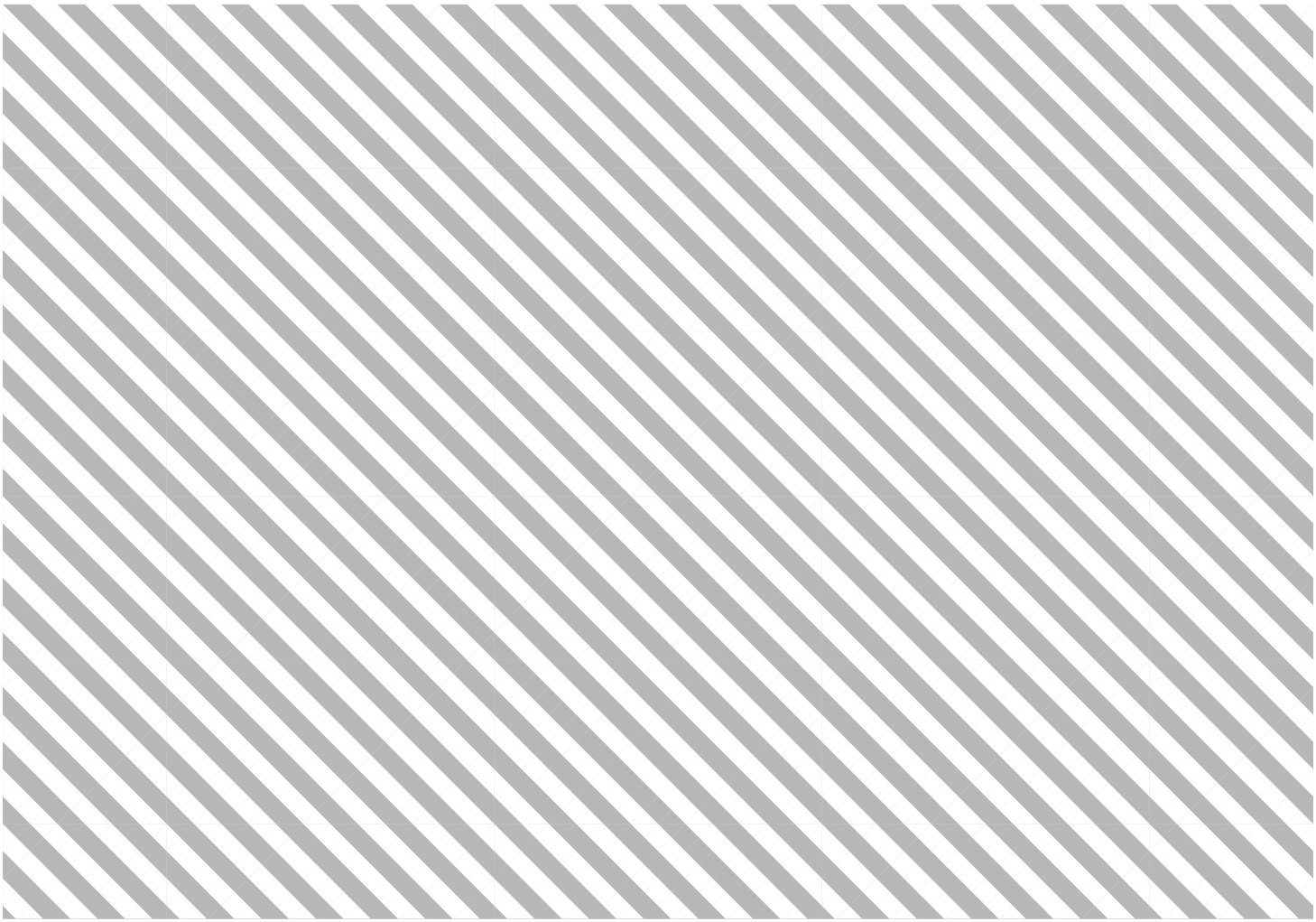
WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

White Paper

Inclusive Deployment of Blockchain for Supply Chains:
Part 4 – Protecting Your Data

September 2019



World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

Contents

Preface

Anne Josephine Flanagan, Project Lead, Data Policy, World Economic Forum

Nadia Hewett, Project Lead, Blockchain and Distributed Ledger Technology, World Economic Forum

The deployment of blockchain and other distributed ledger technologies in supply chains offers considerable advantages. Nevertheless, their deployment and implementation can raise concerns about how best to both meet data protection laws and protect commercially sensitive data.[1] Supply chain actors may be unwilling to take on what they perceive as additional legal risk, especially if data protection obligations become, or are seen to become, unduly burdensome. The European Union's General Data Protection Regulation, for example, is at the forefront of a new wave of data protection legislation globally, and brings with it important practical and regulatory obligations, with the potential for significant fines in cases of non-compliance.

With respect to safeguarding commercially sensitive data in supply chain transactions, the deployment of blockchain may lead to a perceived loss of control, raising questions about security, access rights and how to structure blockchain solutions: e.g. whether only some subsets of data should be shared on the blockchain and/or whether data sharing should be limited to only those parties involved in the transaction.

Within this context, this paper provides practical introductory guidance to supply chain actors who seek greater confidence as they navigate the implications for the protection of data when deploying blockchain solutions.

This is the fourth white paper in a series and part of a broader project focused on the co-creation of new tools and frameworks to shape the deployment of distributed ledger technology in supply chains towards interoperability, integrity and inclusivity. The World Economic Forum's Centre for the Fourth Industrial Revolution is working with a multistakeholder group to produce a project that includes:

– A series of white papers published in 2019. Collectively and individually, these papers will offer insights and investigations into specific considerations for decision-makers to harness blockchain technology responsibly.[2]

– A concise, easy-to-use toolkit to be released at the beginning of 2020 covering important topics for supply chain decision-makers to consider for responsible blockchain deployment, including a section on data protection to meet commercial and compliance considerations.

A blockchain and distributed ledger technology primer is available in Part 1 of this white paper series, *Inclusive Deployment of Blockchain for Supply Chains: Part 1 – Introduction* (April 2019),[3] which readers may find useful to read in conjunction.

This paper builds on that work in order to articulate, in simple terms, important blockchain and distributed ledger technology concepts as they relate to data protection compliance and commercial data confidentiality considerations.

1. Deploying blockchain technology: the need for data protection and practical efficiencies

The great value proposition of deploying blockchain and other distributed ledger technologies (herein referred to as "blockchain") in supply chains is that they may enable collaborative commerce without the need for a (potentially costly) third-party intermediary operating between parties that may not know or trust each other. The distributed nature and other features of these technologies can allow for greater transparency, identification of stakeholders, transfer of assets, new financial opportunities and increased accuracy in forecasting and planning, leading to more efficient and profitable operations in supply chains. While most companies and government entities want to realize these goals, there are countervailing concerns regarding data protection, privacy and the confidentiality of certain information.

In the course of selecting and deploying a blockchain solution, a supply chain operator should understand how blockchain protocols address both their data protection and privacy concerns[4] and those of other supply chain partners (including any concerns about potentially revealing commercially sensitive data) early in the process so as to ensure that such concerns can be adequately met for all supply chain partners. However, in Deloitte's 2019 Global Blockchain Survey, half of respondents cited privacy-related regulations as a matter of concern – markedly more than any other choice of blockchain regulatory issue.[5]

In many cases, data protection and privacy are enforced by legislation, e.g. the GDPR, or by commercial or supplier/client contract (covering client or commercial confidentiality), but blockchain technology affects how we address these protected rights and legitimate commercial concerns and can require complicated analysis.[6] This paper aims to provide an overview of the most common concerns regarding (a) data protection regulation; and (b) commercial confidentiality as raised by supply chain actors when considering blockchain solutions.

The paper does not examine the multitude of technical layers, complexities, hypotheticals and exceptions that exist within blockchain and distributed ledger technology, though the authors recognize their existence and importance. Specifically, this paper:

- Highlights important considerations in respect of (a) commercially sensitive data; and (b) data protection regulatory compliance (page 7 to 15)
- Examines the most accessible blockchain solutions available to overcome these data protection and privacy needs (page 16)
- Identifies some basic trade-offs in deciding which of these blockchain solutions represent the best fit (page 22)

The paper will make several important assumptions to guide a more robust analysis of these issues:

Given the international nature of supply chains, we will use the GDPR as a proxy for regulatory compliance obligations. The GDPR's standards are some of the most rigorous in the world and this lens of analysis will allow us to focus on the substance of the data protection principles at play. Compliance with regulations is jurisdiction- and use case-specific, however, and supply chain actors should obtain specialist advice on their individual jurisdictional requirements. This white paper does not discuss data access or localization laws, which may apply to data beyond personal information, but it is important to note that these restrictions may also have implications for any blockchain-enabled solution. In addition, the EU's ePrivacy Directive[7] is closely related to the GDPR and imposes legal obligations ensuring the privacy of electronic communications and data in transmission. An examination of the blockchain implications of the ePrivacy Directive is also beyond the scope of this white paper.

Similarly, there is no such thing as a typical supply chain or a typical blockchain-centric solution when applied holistically – users of this toolkit should adapt the recommendations and analysis to their own specific supply chain context, use case and blockchain design.

Supply chain-specific industry standards, customs and border protection, or sustainable or environmental requirements that require the collection and verification of certain supply chain data will also not be discussed in this paper.

2. Reality check: obligations in relation to data

Data confidentiality on the blockchain roughly bifurcates into issues of (a) commercially sensitive data; and (b) data that must be protected for regulatory compliance reasons. Many use cases will touch upon both sets of issues, but it is important to think of them as separate concepts since they are motivated by entirely different concerns and have differing implications.

Below, we work through various considerations in respect of each category of concern.

3. Protecting commercially sensitive data

No supply chain actor will share its commercially sensitive data (whether via blockchain or otherwise) with its supply chain partners unless it can maintain its current competitive and informational advantages. The following outlines the most common baseline requirements for sharing data. Each of the examples is a real use case, with names hidden to protect confidentiality.

Transactions in a supply chain ecosystem cannot be fully transparent

While supply chain actors are interested in using blockchain precisely because it allows for transparency and visibility across multiple tiers upstream and downstream, it is undesirable to reveal data to this extent.

First, many critical operational points in supply chains rely on a lack of transparency. One particular supply chain, for example, may legitimately try to enforce a lack of visibility about the identity of upstream suppliers, the prices paid by downstream suppliers, the true length of a cash-conversion cycle, the status of regulatory compliance, true levels of demand and available inventory, and details about the production process.

Secondly, if confidential information such as trade secrets needs to be revealed to regulatory bodies, for instance, customs and oversight agencies, they are revealed for compliance purposes only and in strictest confidence. This information cannot and should not be shared across the supply chain where it would be visible to other actors. Even if this data is aggregated without important identifiers, the possibility of analysing trends and patterns for economic advantage is too great for most supply chain partners to consider this level of openness.

Confidential information has to stay confidential

One may wonder why two supply chain partners transacting with one another would want to keep certain information from the other and yet log that information onto the blockchain. There are two reasons:

- They believe that there is value in having the blockchain serve as a single source of truth for authenticated supply chain data so that participants can extract the particular data they need, and
- The practical challenges of understanding what should be obfuscated and what can be revealed during a one-to-one integration process are too immense.

Example: Information is on blockchain but has to stay confidential

Let's take a look at an example: An electronics contract manufacturer (CM) provides vendor-managed inventory services to its buyer, a large electronics original equipment manufacturer (OEM). The CM has been bundling storage, insurance and financing costs into its ultimate price for the finished goods to the OEM. The CM would now like to obtain supply chain finance on the blockchain, which will entail revealing to the OEM what their current financing costs are without revealing the other costs, or their own financing arrangements with the Tier 2 supplier. The financier providing the capital will want to know all of this information and is willing to offer more competitive financing precisely because of this visibility. For a distributed ledger system to have real commercial value, the CM would need to be able to share information on a secure, need-to-know and one-to-many basis with any counterparty, but there is not a pre-blockchain solution that presents a practical way of doing so.

Companies want to use ecosystem data in forecasting and planning without revealing raw data

Collaborative planning across a supply chain based on the sharing of accurate demand forecasts, inventory levels on hand and production estimates has long been a goal for optimizing supply chain operations. In terms of logistics, ocean carriers need rolling forecasts from their customers while inland rail operators need to know the number of inbound containers from the ocean liner and port a few weeks in advance to plan a schedule and allot resources. These are just a few examples of how the increased flow of information across an ecosystem can lead to greater efficiency and on-time delivery. However, supply chains have been unable to achieve this because there has not been an incentive to share accurate forecast information with partners – and even if there was, there was no way to securely share such information across the supply chain in a coordinated and timely manner.

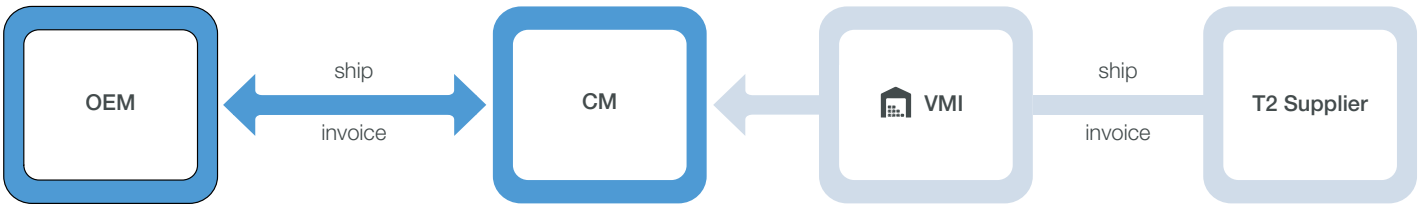
Consider the demand forecast example. A buyer is incentivized to either inflate a demand forecast to ensure supply or secure a volume discount. Anticipating that this is the case, a supplier will therefore underproduce. A supplier, on the other hand, will likely under-report the inventory on hand if it is trying to create scarcity or inflate it if it is trying to satisfy outsized demand. The buyer will therefore adjust its actual purchases accordingly. Lack of coordination within a supply chain frequently leads to shortages or excess inventory, and the cost of such inefficiency is high enough to drive the need for greater transparency and collaboration. The supply chain partners, then, have to thread the needle of sharing information without giving away their informational advantage or revealing sensitive information.

In addition, the lack of a mechanism by which data could be shared securely and authenticated to multiple networks of platforms at the same time means that faulty data abounds even when supply chains set out with the intention to openly share their information.

Companies need to hide even critical pieces of information in a transaction

In perhaps the keenest reminder of how valuable and important, and therefore sensitive, commercial information is in the supply chain, there are instances where value can be unlocked by hiding certain information from parties even when those parties need to use that information in a transaction (particularly in commodities). This is best illustrated with a use case. A commodities producer would like to get its inventory off its balance sheet as soon as possible and recognize revenue. It can sell this inventory to a trading company or third-party financier on the blockchain, who can then sell to the end buyer at the appropriate time. However, the sensitivity of commodities prices is such that, while all parties would benefit from this financing structure, it would be commercially unacceptable to the producers for the financier in the middle to know the actual price.

This use case is slightly different from the one in which parties acknowledge that information treated as confidential in the status quo must preserve the same level of confidentiality after a blockchain network is put in place. In this example, the information was not confidential when only two parties were involved. However, by bringing in a blockchain-based solution, that data must now stay hidden to participants on the blockchain, even where such information might be integral to the activities of the blockchain.



Bank currently knows this information for traditional supply chain finance.

Bank and OEM need to know this information for supply chain finance on the blockchain.

Companies can verify, but not see, information authenticated on the blockchain

This situation is similar to the one described above. Whereas that case can be solved with blockchain-enabled computation, this particular problem requires matching and verification of large volumes of data. Industries featuring complicated assembly processes and bills of material, such as aerospace and electronics, have to manage this issue across multiple supply chain partners. An aerospace manufacturer may have a joint venture, for example, to assemble an aircraft engine comprised of millions of parts. In order to coordinate procurement and assembly, the companies should share their individual part numbers so that parts can be reconciled. However, part numbers are sensitive proprietary data that cannot be shared.

The challenge, then, is to enable the matching and verification of the hidden information without ever revealing the information itself. Once hashed or encrypted, data has to remain in this state even when functions are performed on it.

4. Data protection compliance: GDPR as a lens

Data protection compliance requirements can dissuade the deployment of blockchain in supply chains if not properly understood, in part because the cost of non-compliance is so high, but also because such regulations are seldom made with blockchain in mind. While it is not possible to present a comprehensive treatment of all data protection regulations that might apply to an international blockchain solution, we use the GDPR as such regulations, due to its broad scope and the potential for significant penalties for non-compliance.[8]

GDPR meets blockchain technology

Although the GDPR is an EU regulation, its scope extends beyond the EU in specific circumstances (see Consideration 2: Territorial scope). As such, the GDPR has the potential, in certain circumstances, to touch all parts of an international supply chain, from source to end user.

Many blockchains, particularly public blockchains, have no single, centralized control function and thus reconciling them with the GDPR can be challenging. The European Blockchain Observatory and Forum, an initiative of the European Commission to accelerate blockchain innovation, has identified several specific challenges:[9]

(1) determining the legal basis upon which personal data is processed,[10] a core principle under the GDPR, is not straightforward on a blockchain due to the many blockchain actors and the fact that, in many cases, there will not be a direct relationship between those actors and the party whose data is being processed, and

(2) satisfying data subject rights under the GDPR, which include the right to access their data, have it rectified and deleted upon request, can be challenging on a technology that is generally designed to offer immutability: i.e. once data is written to the chain, it cannot be deleted.

Any blockchain deployment needs to address these.

Below, we explore questions that a supply chain actor needs to consider in order to move towards GDPR compliance for a blockchain solution.

Applicability of the GDPR

The first question a supply chain actor should ask in terms of obligations under the GDPR is whether or not the GDPR applies at all. The answer to that question rests on two main issues: (a) whether the data in the supply chain meets the definition of personal data under the GDPR; and (b) whether the territorial scope of the GDPR applies.

The GDPR applies only when both conditions are met. If the GDPR applies, then all collection, storage and processing of personal data must be done in accordance with the GDPR's requirements.

Consideration 1: Personal data

The GDPR treats the protection of personal data as a right. Personal data may include the name, an identification number, location data or an online identifier. There are therefore various data points within a supply chain that could be reasonably considered to meet the definition of personal data.[11] It is important to note that the GDPR's definition of personal data can also include anonymized data if such data can be de-anonymized, whether by cross-referencing it with other datasets or by other means.

Of the data processed in a typical supply chain,[12] certain data, such as date/timestamps for loading and unloading of containers, would not be related to an identified or identifiable individual and therefore would not be considered to meet the definition of personal data. Other types of data – such as customs information, sensor/internet of things (IoT) data, beneficial cargo-owner information, identities of authorizing/confirming individuals for transactions, security and access-permission information – will probably include some aspect of personal data. Furthermore, these types of data will potentially contain what are known as special categories of personal data (such as data that would reveal a subject's racial origin, religious beliefs or sexual orientation), which are subject to greater protections under the GDPR.[13]

"When you look at the UN/CEFACT (United Nations Centre for Trade Facilitation and Electronic Business) multi-modal transport model, there are around 38 personal identifiers surrounding the data-led milestones within a container moving between two ports. This can range from an email address, signature, IP address all the way to a photo of a truck with license plate visible," advised Jody Cleworth, founder and CEO of Marine Transport International (MTI) after a thorough assessment of their solutions' compliance to GDPR.[14]

From a pragmatic and cost perspective, given the difficulty of extracting personal data from the overall dataset in the supply chain, the supply chain actor may wish to consider a one-size-fits-all approach: i.e. ensuring the entire dataset across the supply chain be treated as if it is personal data. This is the viewpoint taken in a recent report[15] based on the use case of MTI. It will be for the supply chain actor to decide whether it prefers to take a differentiated approach to treating personal data separately for compliance purposes or whether it prefers to treat the entire dataset as if it were personal data, bearing in mind that there are costs associated with both. For the purposes of this paper, we will assume the former option, but it is important to note that both approaches exist and that professional advice should be sought to determine the best fit.

Consideration 2: Territorial scope

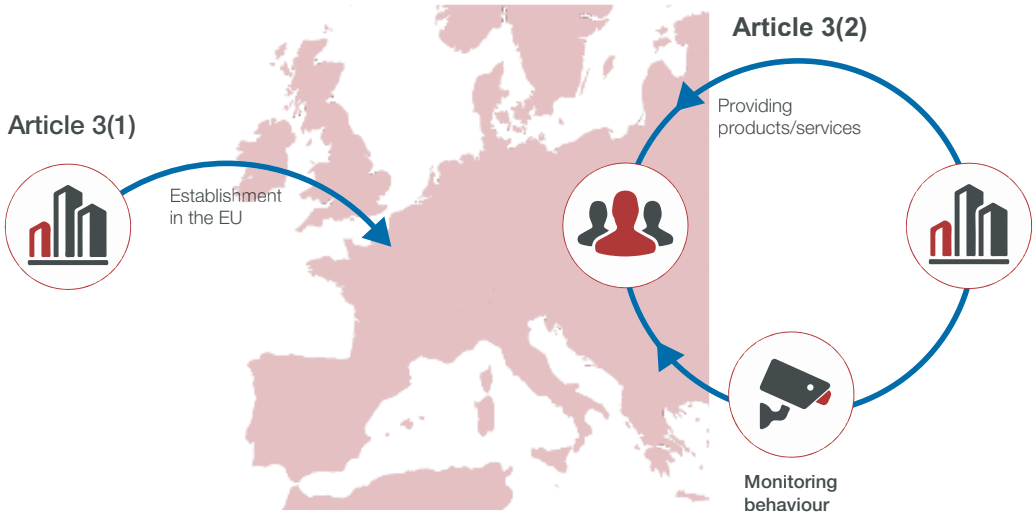
The question of territorial scope requires a consideration of (1) whether the controllers or processors are established within the EU (the "establishment test"); or (2) if the controller or processor is established outside the EU, whether it: (a) offers goods and services to data subjects in the EU (the "targeting test"); or (b) monitors the behaviour of data subjects in the EU, where that behaviour occurs in the EU (the "monitoring test").

Controller or processor?

The GDPR identifies two parties relevant to any processing of personal data: a "controller" and a "processor".[16] A controller is defined as "a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data". A processor is defined as "a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller".[17] In short, it is the controller who determines the legal basis on which the personal data is processed, and the processor is permitted to process the data only for purposes prescribed by the controller. This notwithstanding, the GDPR places direct obligations on both the controller and the processor, and both the controller and processor can be held directly liable for breaches of these obligations.

In the case of a supply chain, it is possible that the various actors could be either data controllers or data processors, or both (or even joint controllers). Identifying the controller, processor or joint controller in a complex processing environment needs to be considered carefully in terms of the specific facts and data being processed and is beyond the scope of this white paper. For the purposes of this paper, we have not distinguished between these parties on the basis that our main focus is on whether GDPR obligations apply generally irrespective of whether one is a controller, processor or joint controller.

Territorial applicability of the GDPR



There are two ways in which the processing activities of an entity fall within the GDPR's scope of regulation: (1) by being established in the EU (Article 3(1)); or (2) by providing products/services, or monitoring the behaviour of individuals in the EU.

Regarding Article 3(1), having or not having a legal entity in the EU is not decisive in terms of the establishment question. A controller/processor may still be "established" in the EU under the GDPR where there is an "effective and real exercise of activities through stable arrangements" (Recital 22). This threshold can be quite low, e.g. one employee or agent may trigger this threshold.

Regarding Article 3(2), the provision on providing products or services is engaged whether or not payment is required. If the processing activities of a non-EU entity are captured under Article 3(2), then that non-EU entity is required to designate a local representative inside the EU. This EU representative may be directly liable for the non-EU entity's breach of the GDPR.

Non-EU entities should be aware that it is not simply a matter of having a legal entity or a physical presence in the EU that settles this question: i.e. an organization can be "established" in the EU for the purposes of the GDPR even if it has no physical presence or legal entity registered in the EU.[18] The targeting and monitoring tests can also be complicated. Both require a holistic analysis of the relevant personal data-handling activities. For the targeting test, relevant factors might include (for example) using an EU top-level domain name, providing dedicated contact details to be used from an EU country or using a currency or language in an EU country. For the monitoring test, relevant activities that may meet the test threshold include behavioural advertising, online tracking through cookies, CCTV or geo-localization for marketing purposes. The correct application of these tests depends on the specific facts of the case, and professional legal advice is recommended. As the answer to this question is case-specific, it is recommended that legal advice be sought to determine the answer.

Supply chain actors usually operate in an international cross-border space and thus may find themselves being caught within the scope of the EU's GDPR. Some potential participants may also wish to consider entering data-sharing agreements (e.g. an agreement whereby the counterparties agree to abide by obligations mandated by the GDPR, such as upholding data subject rights, and apportioning any GDPR-related liability) to minimize liability across the supply chain.

Meeting GDPR obligations

If the GDPR applies, obligations on the processing of personal data and its six main principles (see below) will apply to processing operations. Achieving GDPR compliance is an ongoing process rather than a one-off exercise, and it requires effort beyond adding documentation. Ongoing employee training to handle personal data appropriately, and ongoing maintenance of the organization's security and data subject rights obligations, will need to be operationalized. These kinds of governance and policy/procedural exercises are often more time-consuming than technological fixes, and are arguably more difficult to implement, particularly if cultural change is needed within the organization in order to achieve effective compliance.

A first step will be to engage in a fact-finding exercise in relation to the organization's data profile: e.g. what personal data is collected; how is it processed and for what reasons; where is it processed; who is it provided to; who has access; how long is it retained etc. For further guidance on these and other questions, ample resources are available from the respective EU national data protection authorities' websites, offering practical considerations about moving towards compliance. The UK Information Commissioner's Office or the Irish Data Protection Commission provide some helpful English-language resources, which are pitched to be accessible even by non-specialists such as citizens and small business owners.

Because the GDPR is so broad in scope and the cost of non-compliance so high, it has become vital to conduct at least an initial analysis any time personal data is processed, however small, to ascertain whether the GDPR applies. This includes, for example, the requirement to respect data subject rights[19] or conduct data protection impact assessments (DPIAs).[20]

The GDPR contains many obligations, including the need to secure personal data against unauthorized processing (known as a data breach – this can include copying the data but also making the data unavailable, such as in a ransomware attack) and keeping an up-to-date record of all personal data processing. IT security is a matter of necessity for all companies, and blockchain security issues will be explored in a subsequent white paper in this series. Below, we look specifically at two of the main areas where blockchain and GDPR commonly interact and may create a legal liability for the supply chain actor; namely, determining the basis upon which personal data is processed and satisfying data subject rights.

Data processing

The GDPR brings to bear six principles[21] on personal data, which are that the data must be:

1. Processed fairly, lawfully and in a transparent manner (e.g. being clear about how the personal data is processed in a privacy policy and upholding data subject rights)

2. Adequate, relevant and limited to what is necessary (e.g. collecting only personal data that is necessary for the processing)

3. Collected for a specific, explicit and legitimate purpose and processed for that purpose only (e.g. processing the personal data only as set out in the privacy policy)

4. Accurate and up-to-date (e.g. updating the personal data so it is accurate on an ongoing basis)

5. Kept in a form that permits identification of data subjects for no longer than necessary (e.g. ensuring that retention periods for personal data are reasonable), and

6. Processed in a manner that ensures appropriate security of the personal data (e.g. keeping the personal data secure, accessible only to authorized individuals etc.).

All collection and processing of personal data must be aligned with these principles.

In addition, personal data is considered to be processed lawfully only when undertaken on one of the following lawful grounds described within the GDPR:[22]

1. Consent

2. Contractual necessity

3. Legal obligation

4. Protection of vital interests of a natural person

5. For a task undertaken under official authority or in the public interest, or

6. The legitimate interests of the data controller or a third party.[23]

Personal data on a blockchain can be problematic, in part, because it may be difficult to ensure that the parties accessing the personal data have a lawful basis on which to do so. It is also difficult to ensure that liability and recourse for any misuse of personal data is appropriately apportioned and enforceable (see *Controller or processor* box). In a non-blockchain context, the standard approach would be to execute a contract between parties sharing personal data to ensure that liability for compliance is properly accounted for. Where there is no relationship (contractual or otherwise) between such parties (as in some blockchains), it is difficult to ensure that GDPR requirements are met, such as upholding data subject rights.[24] In a private blockchain, a contractual relationship between the data processors/controllers of the network and the users offering their personal data usually exists. For public blockchains, contractual obligations are possible, but an organization have to think carefully about how to establish who can be held liable, both legally/contractually and practically, if something goes wrong.

Data subject rights

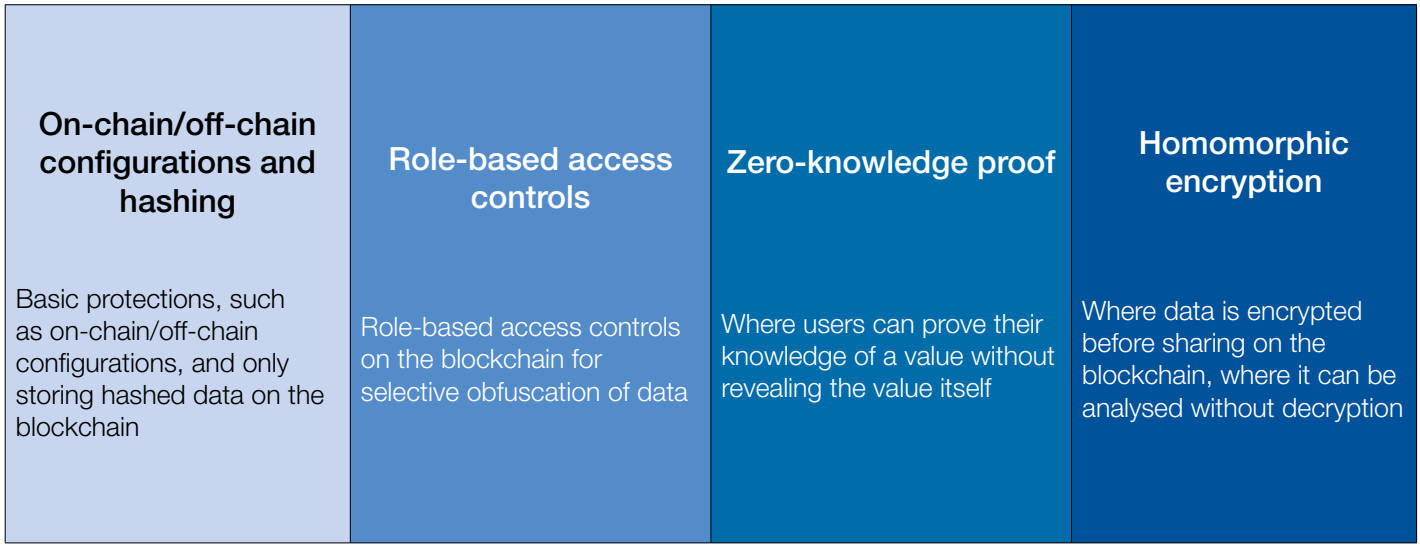
A data subject is an individual whose personal data is at issue. The GDPR ascribes a number of rights to data subjects, including the right to information and transparency, rectification, erasure, restriction of processing, data portability and the right to object to profiling.

These rights must be respected/enforced by the relevant controller. Any relevant processors should also be subject to contractual obligations to the controller to assist the controller in upholding such rights. Processors will also have some direct obligations under the GDPR (e.g. maintaining appropriate security measures), but in either case, both controllers and processors are subject to enforcement by data protection regulators.

It is important to note that these rights can be exercised at any time by a data subject. For example, a data subject can expect to have clear and easy-to-understand information on how their personal data is collected and processed and, for whatever reasons, demand that erroneous personal data be corrected, demand that any personal data no longer necessary for the purposes collected be deleted, restrict the processing of their personal data, demand access to their personal data in a commonly used and machine-readable format, and object to processing of their personal data for profiling or automated decision-making purposes.

It is recommended that such data subject rights be taken into account in the design of the blockchain solution when that data is subject to the GDPR.

5. Blockchain solutions for commercially sensitive data and data protection compliance



Early public blockchain protocols, such as Bitcoin, made their transactions completely transparent to others in the network and, due to their nature as public blockchains, to the general public as well. Each transaction could be identified by the public keys of the sender and recipient of cryptocurrency, the date and time, the amounts transacted and various data related to the hash of the transaction. While the pseudonymity of the system is difficult to crack, a vigilant party, such as a government agency, could trace a history of transactions.

Since then, blockchain protocols, frameworks or platforms such as Hyperledger, Corda and Quorum (a private fork of Ethereum) have greatly improved the ability to implement data privacy and confidentiality. These protocols vary in the degree of decentralization in their data management and transaction validation, but they allow identity management, can deploy product features across the ecosystem and establish a set of policies for governance and control of the network. Importantly, these protocols are rarely deployed without middleware or an application layer sitting on top of them, each of which will likely have their own data-privacy functionality. The solutions explored in this white paper treat the full technology stack, from blockchain to application, as an integrated solution. To the extent that the paper speaks about public and private blockchains independent of the applications built on top of them, the intention is to highlight certain properties that are also likely to be mirrored on the application layer, given the choice of blockchain protocol.

There is no single blockchain solution or set of solutions to solve the issues described above. The solutions adopted depend on the technological capability of a particular blockchain platform and the specific privacy and performance factors that a supply chain is attempting to optimize, as well as any contractual relationships that may exist between the blockchain users or node operators. The following are the most accessible technologies that may be used to meet certain requirements when handling personal and commercially sensitive data while enabling the desired functionality.

Basic protections, such as on-chain/off-chain configurations and only storing hashed data on the blockchain

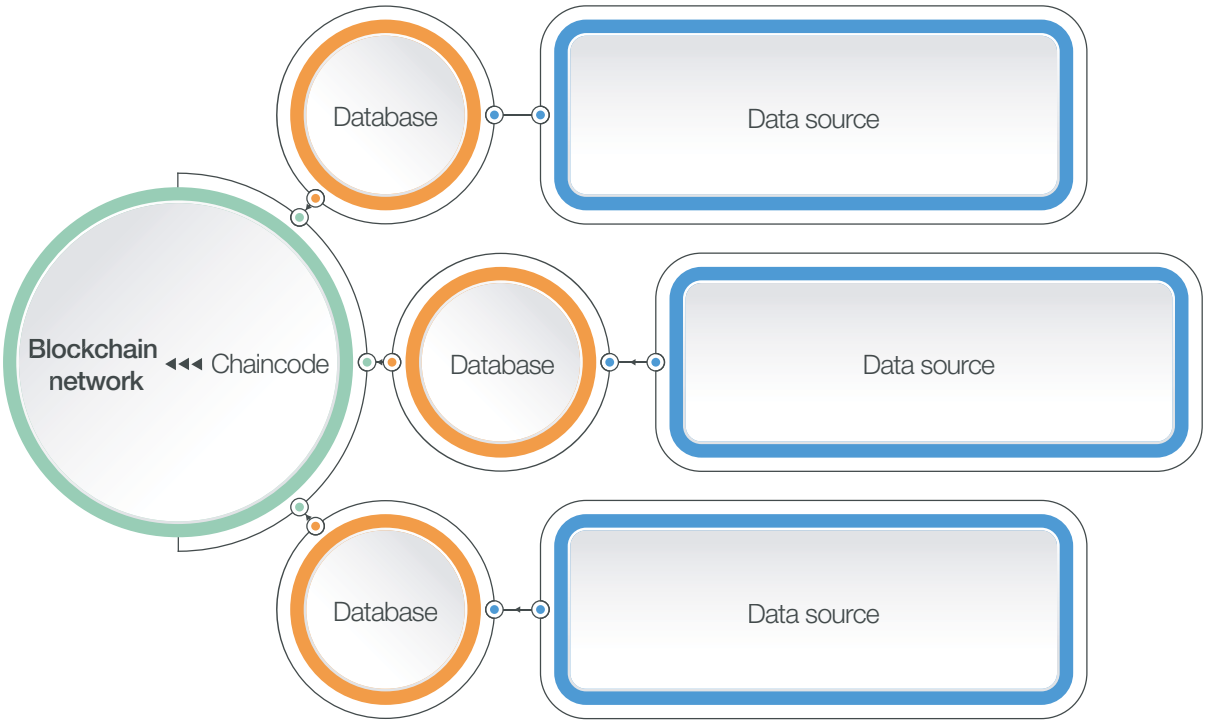
The simplest way to prevent data from being shared on the blockchain is to never log it there to begin with. One common misconception is that if a supply chain ecosystem goes “on the blockchain”, then any and all supply chain data will be shared by all parties; practically speaking, not *all* data needs to be on the blockchain. The truth is that the selective placement of data on the blockchain, typically from an enterprise resource planning (ERP) system, is one of the most important and time-intensive steps of using a blockchain system. An enterprise can choose to store information off-chain in its own centralized databases, or even in a database provided by the blockchain system that is one layer removed from the blockchain itself. Only information that needs to be shared with others will go on to the blockchain.

For example, a logistics provider at origin must share the purchase order numbers with the origin consolidation facility for a given consignment or shipment. However, the carrier does not wish to share other purchase order information, such as end-customer details. In this case, the purchase order number will go “on-chain” but other details attached to the purchase order will be kept “off-chain” and therefore will not be visible to the origin consolidation facility.

One product that focuses specifically on providing on-chain/off-chain organization is the Blockchain Integration Hub™, deployed by EVRYTHNG. Once data is on the EVRYTHING platform, it can be selectively propagated to a number of blockchain networks of which the customer is a member. While the full data in clear text can be propagated to the blockchains, it is more common for a hash of the transactions to be propagated or for the transactions to be encrypted using private/public key pairs prior to propagating them on a supported blockchain or DLT.

In any event, the best technique for storing authenticated data on the blockchain is to simply store the hash of data on the blockchain, while the data itself stays in a database off-chain. This is a popular solution for documents, which are data-intensive files. In addition to increased data privacy, this structure helps with the throughput rate of the blockchain. The less data there is on the blockchain, the less time it takes to run a query on it so that the data can be processed.

For industry consortia that have come together to form blockchain networks, on top of which industry-specific applications will be built, on-chain/off-chain management of data is the easiest way to provide greater transparency and availability of data to the whole ecosystem without compromising proprietary or confidential information. For example, maritime trade community members or industry players are sometimes competitors and sometimes partners, and if they are using one blockchain network, such as TradeLens or the Global Business Shipping Network, special care will need to be taken to protect the data and to give blockchain network members access only to relevant information as carefully determined within the context of the blockchain's objective.



On-chain Off-chain

On-chain/off-chain, obfuscating personal data and GDPR compliance

For GDPR, the immutability of data added to a blockchain naturally prompts consideration of off-chain arrangements, particularly for personal data. Under the GDPR, personal data must only be kept for as long as is necessary to achieve the aims for which it was collected. Being unable to delete or effectively delete such personal data from a blockchain could constitute a breach of the GDPR because the "data controller" (the effective owner or controller of personal data) would be unable to protect the data subject's right to erasure/to be forgotten. Currently, certain supply chain actors, such as European beneficial cargo owners, are known to decline the disclosure of information that contains personal data to data-sharing schemes to avoid falling foul of GDPR rules.[25]

Avoiding the gathering of personal data in supply chain transactions altogether is not possible. Personal data is included in supply chain-related transactional data for many reasons, and is typically needed as required (a) by law; (b) for increased value; or (c) because it makes business sense. For instance, direct-to-customer shipments or last-mile shipments very likely include end customers' personal information. Or, the data elements that the United States Customs and Border Protection require as part of importer security filing (or more commonly called 10+2) also include personal data such as (a) the manufacturer's (or supplier's) name and address; (b) the seller's (or owner's) name and address; and (c) the buyer's (or owner's) name and address (if such information relates to a data subject and not a company).

Where personal data must be incorporated into a blockchain supply chain application, a potential solution would be to store only a hash of the relevant personal data on the blockchain. This keeps the control and security of the original personal data maintained by the data controller, and allows the data controller to continue to protect and fulfil any data subject rights (e.g. if the data subject were to request erasure of their personal data, the data controller would be able to make such deletion), but still permits a hash to be added to the immutable blockchain to serve as a substitute for the personal data. We used the term "original personal data" advisedly, as it is not necessarily true that all hashed data is not personal data. If a hash can be combined with other accessible information to produce data on an identified or identifiable individual, then the hash also qualifies as personal data under the GDPR.

This solution also presumes that (a) the hash makes the original personal data inaccessible – e.g. the hash cannot be somehow processed to reveal the original personal data; (b) deleting the original personal data is not enough to render the hash meaningless even when combined with any other information – e.g. any relevant keys, information stored on other parts of the distributed ledger;[26] and (c) that the regulators are satisfied that this effective deletion – though not an actual deletion – is enough to satisfy this data subject right.[27]

Still, this approach would permit meaningful analysis to be conducted (on usage patterns, for example), but it has the potential to achieve GDPR compliance by avoiding the need to control access to personal data on the blockchain (among other issues) if applied comprehensively across the entire blockchain – and the presumptions in (a), (b) and (c) are true.

Role-based access controls on the blockchain for selective obfuscation of data

Prior to a world in which zero-knowledge proof and fully homomorphic encryption (described in more detail below) entail little to no latency, the best solution is to place information on the blockchain and reap the benefits of authenticated data while exploiting familiar security tools. One effective combination of these methods is to implement access controls directly on the blockchain. In private blockchains, this is achieved in its simplest way by opening up private channels between nodes so that their transactions remain confidential and hidden from the rest of the blockchain network, or networks, of which they are a part. The equivalent in public blockchains is some variation of sidechains.

A more sophisticated method is to implement access controls in chaincode or a system of smart contracts, which are a layer of logic that governs a business user's interface with blockchains. Public and private keys native to the blockchain systems are generated for individual users and can be integrated with an enterprise's existing identity-management system. The public keys of individual users will let the system know whether this user has read/write access to certain information on the blockchain, and only those users will be able to decrypt the information as a result. The key to making this system as fine-grained as possible, so that supply chain actors can precisely specify what data can be seen and by whom, is a blockchain data structure that corresponds to access controls. That way, user privileges go all the way down to a particular data field. This could mean that even within, say, a spreadsheet, certain rows and columns are hidden for specific users.

Taking advantage of data architecture

Any supply chain operator deploying a blockchain solution should be aware of how that solution, its data architecture and its incorporation of personal data fits in with the supply chain operator's existing GDPR-compliance systems and procedures. Understanding where and how personal data is collected and stored in a blockchain solution can assist in demonstrating compliance for the collection, use and security of that data as well as satisfying data subject rights, such as data subject access requests.

Chaincode and smart contracts can also be programmed to trigger operations off of data that is either still hidden or revealed. Therefore, a computation can be run on obfuscated data queried from the blockchain, but the user will be able to see the decrypted result only, not the underlying data itself. This solution does not necessarily have the ironclad security of bleeding-edge cryptography behind it, but it is sufficient to satisfy the supply chain confidentiality needs discussed above while the more advanced methods improve their performance.

Role-based access controls and GDPR compliance

From a GDPR perspective, role-based access controls may be an effective tool to address compliance challenges.

As discussed above, one of the basic assumptions in the GDPR is that all relationships in a personal data context take place among three participants: a data subject, a controller and, in some cases, a processor. Ultimately, the GDPR obligations largely apply to the treatment of the personal data regardless of whether the data handler is defined as a controller or processor. In the GDPR framework, the controller in a blockchain is anyone who writes or adds personal data to the blockchain in a professional/commercial capacity, and a processor is anyone who processes that personal data on the controller's behalf. Notably, someone who merely accesses the blockchain to read that personal data is not a processor unless they are doing it on behalf of a controller; if they are a controller, they need to ensure that they have a lawful basis on which to process the data they access. In a blockchain, this lawful basis is unlikely to exist without some sort of contractual relationship between the blockchain actors.

An open-access blockchain solution without role-based access controls or other access restrictions (such as a public blockchain) does not fit neatly into this concept, primarily because it is difficult to identify any one entity who can be held liable, or be compelled to uphold data protection regulations that would apply to the personal data on that public blockchain solution. While it may be clear who the controller is before the personal data is uploaded to the blockchain, it is less clear what happens after upload. On upload, the controller would then be granting access to the personal data to all participants in the blockchain but, in a public blockchain, there would be no contractual relationship between the controller and any blockchain recipient. In this example, if the blockchain participant is a processor for the original controller, then the problem is determining how the original controller can compel the processor to help them meet the GDPR requirements (such as enforcing data subject rights) and abide by the original terms of disclosure from the data subject to the controller.

If the blockchain participant is a new controller, they have no defined relationship with the data subject, so it is unclear on what legal basis they process that personal data. It is clear, then, that the disclosure of personal data to the blockchain would present significant GDPR compliance problems for the original controller and create an enforcement nightmare for the data subject.

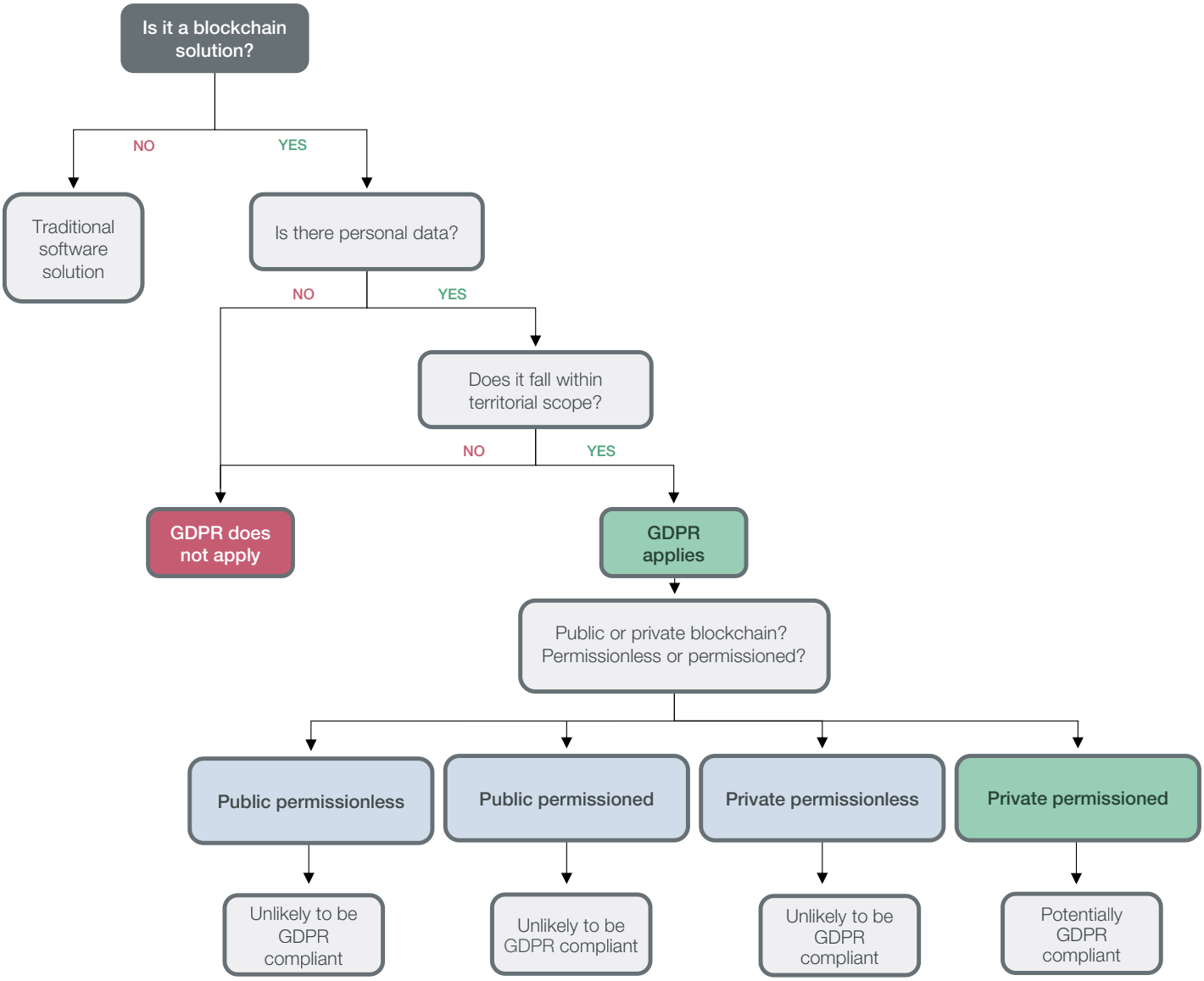
It may be possible to address this problem architecturally by designing a private permissioned blockchain solution, whereby all participants must agree to abide by certain GDPR-compliant terms as a condition to being granted permission: e.g. permitted uses, rules on retention periods, deletion, security and data export to foreign jurisdictions. No public or unauthorized access to the blockchain data would be permitted. However, it is unlikely that this would address concerns regarding how liability for errors would be apportioned (if at all).

Also, while blockchain maintains good security over data tampering once that data has been added, any solution will still have to deal with the problem of faulty or fraudulent data being added in the first place. A possible countermeasure may be to cut off a "bad" participant who consistently shares faulty or fraudulent data. However, where such errors have financial consequences, the matter of enforcement (such as data types and format) among the blockchain participants (e.g. who can bring a claim; what would be the quantum of such a claim; how will liability be apportioned) becomes important and should be considered at the blockchain-solution design stage.

Other approaches to GDPR compliance

Storing personal data off-chain with an on-chain hash and adopting role-based access controls are two of the most commonly used approaches to strive for in order to achieve GDPR compliance in a blockchain deployment. However, it is important to note that other approaches also exist. Although less common, editable blockchains permit data subject rights to be respected by allowing a private permissioned blockchain administrator to delete and edit incorrect or outdated information, the trade-off is that it also sacrifices the immutable nature of blockchain. Other solutions allow for deletion by encryption, whereby a blockchain administrator makes certain data inaccessible by increasing the permission needed to access a preexisting block on the blockchain. It is currently unclear whether or not this solution would be considered GDPR-compliant by data protection regulators.

The following decision tree provides a simplified summary of common approaches to achieving GDPR compliance in a blockchain context.



Because of the great variety of blockchain solutions and configurations, each needs to be analysed on its own distinct merits. A solution unlikely to be GDPR compliant (as per the decision tree above) requires further evaluation and a data protection impact assessment.

Zero-knowledge proof

Zero-knowledge proof is a well-established concept in cryptography that allows one party to assert the validity of a statement without revealing the underlying facts that make the statement true or false. The algorithm that accomplishes this runs a statement through a true/false test repeatedly until the probability that that statement is false becomes incredibly low. At this point, one is able to confidently assert that the statement is true.

For example, a bank would like to lend money to a supplier. Before it does, the bank would like to verify that the supplier has confirmation from a credit insurance company for the buyer's risk. A zero-knowledge proof will allow the bank to verify that fact without learning the exact amount of the limit on the credit insurance policy. Now consider this outside of the two parties to the transaction. Suppose an auditor needs to audit the validity of this transaction, but they cannot know that the bank or the supplier were involved, nor the amount. With zero-knowledge proof, an auditor can run an algorithm that returns that verification.

One of the key advancements in zero-knowledge proof is zk-SNARKs.[28] The name is short for zero-knowledge succinct non-interactive argument of knowledge. This technology significantly reduces the time it takes a zero-knowledge proof algorithm to return a result. It also makes the process much more secure by minimizing the opportunity to "fake" a proof through traditional interactive algorithms. Both of these improvements allowed zero-knowledge proof to have much more traction in real-world use cases.

Even with zk-SNARKs, however, zero-knowledge proof solutions have high latency. When added to the inherent latency of both public and private blockchains, the throughput rate can be too low for real-world operations. JP Morgan, for instance, implemented zero knowledge proof in its financial audit of blockchains. The processing time for each individual transaction exceeded 40 seconds. Given that this is one of the most powerful and promising features of blockchain, research is being undertaken by the wider blockchain community to bring down the time it takes for a proof to complete its work. For supply chain transactions that are lower volume, and for which this level of data privacy is important, it can nevertheless make sense to adopt this technology in its current state.

Fully homomorphic encryption

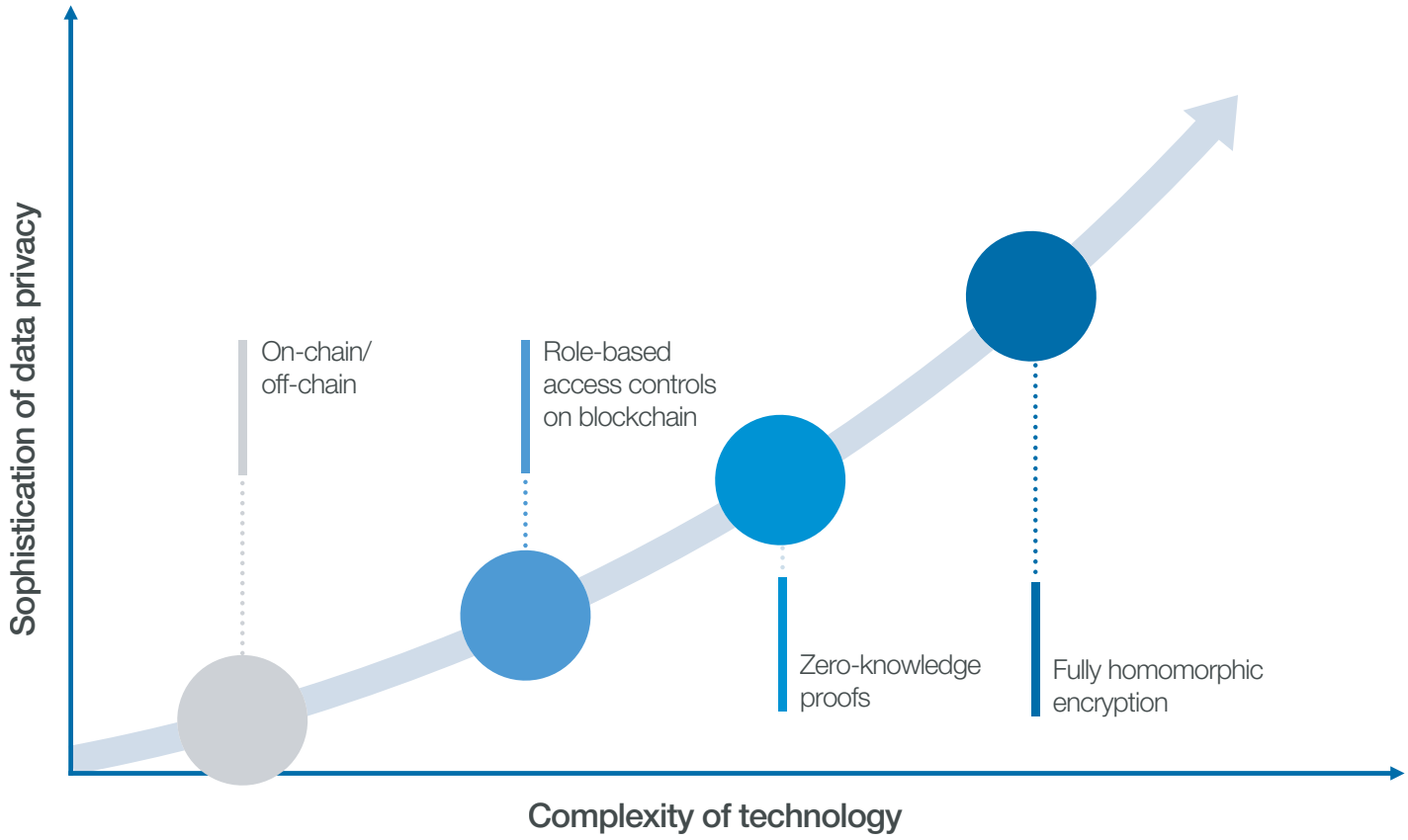
Fully homomorphic encryption (FHE) is a way by which mathematical calculations can be performed on encrypted data and return an encrypted result. However, the latency of a system that uses this method of computation is even slower than one that uses zero-knowledge proof. FHE was first conceptualized as the most secure way to perform multiparty computations, in which parties jointly agree to a protocol for analysis without revealing any of their private data. A decade ago, using FHE could increase the time it takes for a computer to run a calculation by a magnitude of 10 to 12. Four years ago, researchers reduced this magnitude down a magnitiude of six to seven, and the efforts continue in earnest to minimize the difference between real-time computation in a native environment using unencrypted data and FHE.

Given the privacy this technology affords, the question becomes: Why is blockchain relevant in this particular context? Without the ability to independently verify the encrypted data that is being processed through FHE, it becomes that much more important for the data to be of good quality to begin with. Blockchain is able to authenticate that data in a supply chain in a trustless manner, ensuring that the inputs to FHE are themselves reliable.

The benefits for supply chain data obfuscation are clear. Supply chain partners would be able to run data analytics on AI algorithms on fully encrypted data, and only those who should have access to the result would be provided with a key to decrypt it. The slowness of FHE, however, means that it is generally not worth the undertaking unless a supply chain has a computation for which it does not need real-time, or close to real-time, transmission. Skuchain, a blockchain company, uses role-based access controls and smart contracts for collaborative planning applications across the supply chain to coordinate procurement, management, production and delivery, but it is starting to use FHE for sensitive data and more complex algorithms that require an extra layer of security.[29]

This paper mentions FHE to highlight what is becoming one of the most powerful and useful encryption technologies for blockchain and supply chains, but other technologies may currently be better equipped to provide value.

6. Reconciling blockchain and data confidentiality



Blockchain never requires a company to reveal more data than it is comfortable with. In fact, the cutting-edge obfuscation techniques that blockchain offers can unlock new possibilities in supply chain operations and finance that were not previously possible. Technologies will be chosen depending upon the degree of confidentiality and functionality required. The figure below offers a simple illustration of how these technologies compare today, both in terms of complexity (ease of adopting the technology) and sophistication (the ability to perform data analysis and enable more flexible and open sharing of data stakeholders).

The more complex the technology becomes, the more trade-offs are experienced, including:

- Limited transaction speed[30]
- Limited payload size
- Higher transaction costs (in terms of computing power), and
- Risk of irrelevant data being included in the payload.

To see how technologies may be adopted on a curve or combined to achieve optimal results, Appendix 1 walks through a use case in collaborative planning, one of the most fertile grounds for efficiency gains in supply chain and one of the hardest to achieve for privacy reasons.

Conclusion

Data is a precious commodity in the supply chain, but exploiting its value with blockchain raises commercial and compliance issues that have the potential to significantly hinder blockchain adoption if left unaddressed.

Whether a supply chain operator is concerned about commercial data sensitivities or data protection compliance risks (or, more likely, both), technology solutions exist to meet these challenges. Supply chain partners using blockchain need to have conversations with counterparties about how to balance the need to maintain data confidentiality with the benefits of sharing it in order to increase the mutual effectiveness of their operations. In addition to reaching a purely commercial agreement among themselves, supply chain ecosystems must also comply with legal requirements such as GDPR, customs regulations, product safety regulations and other laws, none of which (to date) explicitly addresses the sharing of data via technology such as blockchain. Enterprises with extensive supply chains should therefore: (1) continue to be active participants in industry consortia to ensure that solutions under development meet industry-specific requirements; and (2) engage with regulators and stakeholders to set appropriate and practical standards and effective methodologies. These efforts should yield new ways of doing business in supply chains, increasing value based on authenticated information and improving collaboration between supply chain partners. Blockchain can be used as a tool within a broader data-privacy context to solve real-world concerns about transparency, but also to enable previously impossible business opportunities.

Appendix 1

Use case: blockchain technologies for commercially sensitive needs

To see how technologies may be adopted on a curve or combined to achieve optimal results, this section presents a use case in collaborative planning, one of the most fertile grounds for efficiency gains in supply chain, and one of the hardest to achieve for privacy reasons.

A major heavy manufacturing company has historically overstated its forecast to its plastics supplier to account for potential emergency orders. The supplier has become aware of this practice after years of building up excess inventory because the manufacturing company ultimately does not buy anywhere near the levels of its forecast.

One year, the supplier decides to significantly cut the procurement of resin from its supplier, a Tier 2 supplier to the manufacturing company. The supplier cuts too much, however, and can not meet demand for the manufacturing company that year.

In an effort to avoid supply outages, the manufacturing company would like to access data about the inventory and production rate of the plastic supplier, and even that of the the resin supplier, on a more frequent basis. The plastic supplier would like to know the manufacturing company's inventory level, consumption rate and demand forecast as often as possible. None of the parties has any incentive to share this information with one another given how it will affect pricing and negotiation leverage. The question therefore arises of what can be done.

If the manufacturing company simply knew the schedule of delivery, in real time, of resin to the plastic supplier and of the plastic supplier to them, there could be an incremental improvement in planning. Perhaps the resin supplier is not ready to share other information at this time, though, so the logistics information goes on to the blockchain, while other data stays off chain.

On the other hand, another solution may be one in which all parties are comfortable placing just-in-time (JIT) inventory data on the blockchain, but only their immediate counterparty has access to the information. In addition, the counterparty may have access for purposes of executing smart contracts or algorithms with the data, but the counterparty may not see the underlying data itself. With role-based access controls on the blockchain, the parties are able to accomplish this. They can then engage in collaborative planning with data that is obfuscated but usable for valuable data analysis.

With both of these technologies, sensitive data can stay hidden, but it is not exactly encrypted. If the companies are unsatisfied with that level of encryption but still want to use the encrypted data, then more sophisticated means will have to come into play. If the manufacturing company wants to control the level of resin inventory at the plastic supplier, then, when the level falls below 5,000 litres, the manufacturing company will ask the plastic supplier to order more. A zero-knowledge proof can certify to the manufacturing company that this threshold has indeed been crossed without revealing exactly how much resin remains at the plastic supplier.

Finally, FHE allows all parties to place their data on the blockchain, keep it encrypted and simply run any planning algorithms on the encrypted data. While latency for these kinds of transactions is decreasing with new advancements in the technology, this is still the slowest method of preserving data privacy.

Glossary

Chaincode: Software code executing business logic that helps the underlying blockchain network communicate with the application functionality that a typical business user would see.

Commercially sensitive data: Data of a commercial nature or origin that, if known to parties other than the owner of the data, can result in adverse business consequences. Examples of such data include pricing, identity of subcontractors, true cost of goods and identity of end buyers downstream in a supply chain.

Controller: Under the GDPR (Article 4), the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by European Union or EU member state law, the controller or the specific criteria for its nomination may be provided for by those laws.

Cryptocurrency: The generic term for any digital asset or "token" that can be mined, purchased or transacted within a blockchain or distributed ledger network. The most famous cryptocurrency is bitcoin and others, of which there are over 1,000, include ether, Litecoin and NEO.

Cryptographic techniques/Cryptography: Disciplines or techniques that embody principles, means and mechanisms for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use [ISO/IEC 74498-2: 1989, ISO/IEC SD6].

Data protection impact assessment: An assessment of the impact of processing operations on the protection of personal data that is mandated in certain cases by the GDPR (Article 35).

Data subject: As defined in the GDPR (Article 4), an identified or identifiable natural person where an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

General Data Protection Regulation 2018 (GDPR): Regulation number 2016/679 entitled Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Regulation (EU) 2016/679).

Immutability: Inability to be changed. Data stored in a blockchain is very hard to change, even by administrators. However, absolute immutability does not exist.

Internet of things (IoT): A network of real-world objects that: (1) have a digital identity; (2) are connected to the internet (directly or via a gateway); (3) have sensing and or actuation capabilities.

JIT inventory: JIT, or just-in-time, inventory is a supply chain management technique whereby inventory is procured and transported to the point of need only when that inventory will be used imminently for production or the fulfilment of orders. Using this technique, supply chain managers can avoid holding excess inventory.

Network nodes: Nodes that represent network agents or participants, such as banks, government agencies, individuals, manufacturers and securities firms within a distributed network. Depending on the permissions set in the network, they may be able to approve/validate, send or receive transactions and data. They may validate transactions through a consensus protocol before committing them to a shared ledger (though not all nodes perform validations depending on the system, architecture etc).

Personal data: As defined in the GDPR (Article 4), personal data means any information relating to a data subject. It is important to note that information that relates to a data subject, even without a name, can qualify as personal data under the GDPR.

Processing: As defined in the GDPR (Article 4), any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor: As defined in the GDPR (Article 4), a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.

Smart contract: Blockchains can be programmed to automate business processes (e.g. making payments) in different entities. A smart contract is a computerized transaction protocol that automatically executes (whether by all or a large number of network nodes) the terms of a contract upon a blockchain once predefined conditions are met.

Contributors

The World Economic Forum's Centre for the Fourth Industrial Revolution Blockchain for Supply Chain project is a global, multi-industry, multistakeholder endeavour aimed at co-designing and co-creating frameworks to encourage responsible deployment. The project engages stakeholders across multiple industries and governments from around the world. This report is based on numerous discussions, workshops and research and the combined effort of all involved; the opinions expressed herein may not necessary correspond with each one involved with the project.

Sincere thanks are extended to those who contributed their unique insights to this report. We are also very grateful for the generous commitment and support of the fellows at the Centre dedicated to the project: **Soichi Furuya** from Hitachi and **Francis Jee** from Deloitte.

Lead authors

Anne Josephine Flanagan, Project Lead Data Policy, World Economic Forum, USA
Fiona Maclean, Technology Transactions Group, Latham & Watkins, UK
Mark Sun, Technology Transactions Group, Latham & Watkins, UK
Nadia Hewett, Project Lead Blockchain and DLT, World Economic Forum, USA
Rebecca Liao, Executive Vice-President, Skuchain, USA

Contributors

Andrew Ballinger, Project Specialist, World Economic Forum, USA
Ashley Lannquist, Project Lead, World Economic Forum, USA
Austin Hunter, Project Specialist, World Economic Forum, USA
Connor Keenan, Co-Founder and Engineer, Treum, USA
David Kappos, Partner, Cravath, Swaine & Moore, USA
David Treat, Global Blockchain Lead, Accenture, USA
Dominique Guinard, Co-Founder and Chief Technology Officer, EVRYTHNG, Switzerland
Francis Jee, Deloitte Consulting (and World Economic Forum Fellow), USA
Gabriela Zanfir-Fortuna, Senior Counsel, Future of Privacy Forum, USA
Hanns-Christian Hanebeck, Founder & Chief Executive Officer, Truckl.io, USA
Henrik Hvid Jensen, Senior Blockchain Adviser, Trustworks, Denmark
Homan Farahmand, Digital Identity and Blockchain Technology Adviser, Canada
Madhav Durbha, Group Vice-President, Industry Strategy, LLamasoft, USA
Markus Kaulartz, Lawyer, CMS, Germany
Michael Klein, Associate Director – Blockchain Technology, Accenture, USA
Michele Nati, Tech Analyst, IOTA Foundation, Germany
Moritz Petersen, Senior Researcher, Kühne Logistics University, Germany
Partha Das Chowdhury, Head, Blockchain CoE, VARA Technology, India
Peder Muller, Blockchain Solutions Architect, Deloitte, USA
Ryan Wichtowski, Law Clerk, Cravath, Swaine & Moore, USA
Soichi Furuya, Senior Researcher, Hitachi (and World Economic Forum Fellow), USA
Sumedha Deshmukh, Project Specialist, World Economic Forum, USA
Wolfgang Lehmacher, Senior Supply Chain Executive, Hong Kong
Yingli Wang, Cardiff University, UK

Commentators

Gadi Benmoshe, Chief Information Officer, Israel Ports Development & Assets Company, Israel
Joachim Moller Andersen, Chief Legal Counsel, Head of IT and Digital Law, A.P. Moller – Maersk, Denmark
John Monarch, Chief Executive Officer, ShipChain, USA
Jong Choi, Chief Executive Officer, MarkAny, Republic of Korea
Neepa Patel, Chief Compliance Officer, r3, USA
Richard Morton, Secretary General, International Port Community Systems Association (IPCSA), UK
Robert Maslamoney, Managing Director, A.P. Moller – Maersk, Angola
Sean Cocks, ISC Improvement Analyst, Kmart International, Australia
Simon Kiilerich Vedel, Senior Product Manager, A.P. Moller – Maersk, Denmark
Shawn Muma, Technology Research Leader, The Center for Global Enterprise, USA

Endnotes

1. In this white paper, we use the term "commercially sensitive data" to refer to data that may hold commercial value (whether via analysis, for competitive advantage or otherwise) for a supply chain participant.
2. As of June 2019, two white papers in the series have been published:
   - *Inclusive Deployment of Blockchain for Supply Chains: Part 1 – Introduction* (April 2019) https://www.weforum.org/whitepapers/inclusive-deployment-of-blockchain-for-supply-chains-part-1-introduction
   - *Inclusive Deployment of Blockchain for Supply Chains: Part 2 – Trustworthy verification of digital identities* (April 2019) https://www.weforum.org/whitepapers/inclusive-deployment-of-blockchain-for-supply-chains-part-2-trustworthy-verification-of-digital-identities (links as of 24/7/19).
3. See endnote 2.
4. "Data protection" and "data privacy" are terms that are sometimes used interchangeably and generally refer to the regulation of personal data. In this white paper, we use the term "data protection" to refer to the regulation of personal data and the term "privacy" to refer more generally to the commercial and practical considerations surrounding use of data, generally (not just personal data).
5. Deloitte, 2019, https://www2.deloitte.com/content/dam/insights/us/articles/2019-global-blockchain-survey/DI_2019-global-blockchain-survey.pdf (link as of 24/7/19).
6. United Nations Economic and Social Council, *Blockchain in Trade Facilitation: Sectoral Challenges and Examples*, March 2019.
7. Also formally known as the Privacy and Electronic Communications Directive 2002/58/EC (as amended by Directive 2009/136/EC). A proposal, in the form of a draft e-privacy regulation, to overhaul and better harmonize EU law in this area is currently in the EU legislative process and is intended to eventually replace the current e-Privacy Directive.
8. Pursuant to Article 83 of the GDPR, regulators may impose administrative fines up to the greater of €20 million or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year for infringements of the GDPR.
9. *Blockchain and the GDPR, A Thematic Report prepared by the European Union Blockchain Observatory and Forum*, October 2018. This paper was produced as part of a series of thematic papers published by the European Union Blockchain Observatory and Forum, a European Commission initiative to accelerate blockchain innovation and development.
10. All processing of personal data must have a lawful basis under Article 6 of the GDPR. The lawfulness of processing must be underpinned by one of the following: (1) the data subject has consented to the processing of his or her personal data; (2) processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps prior to entering into a contract; (3) processing is necessary for compliance with a legal obligation to which the controller is subject; (4) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (5) processing is necessary for the performance of a task in the public interest or in the exercise of official authority vested in the controller; or (6) processing is necessary for the purposes of legitimate interests pursued by the controller except where such interests are overridden by the interests or fundamental rights of the data subject.
11. Information that relates to a legal entity (e.g. a company), such as stock information or number of employees, is not considered personal data and is not protected under the GDPR. If no personal data is being collected or processed, then the GDPR can be eliminated as a potential concern; however, in reality the likelihood of a supply chain containing no personal data whatsoever is slim.
12. For example, identity of the goods in transit, health and safety data relating to such goods, date/time of loading and departure, customs information, insurance details, contractual terms of carriage, sensor/internet of things device data, logistics provider data, transport provider data, source data, destination data, beneficial cargo owner data.
13. Article 9 GDPR.
14. The Center for Global Enterprise, Cravath, Swaine & Moore, DSCI and Slaughter and May, 2019, "The Right to be Forgotten Meets the Immutable", https://www.cravath.com/files/Uploads/Documents/Publications/3898415_1.pdf (link as of 13/8/19).

15. *March of the Blocks: GDPR and the Blockchain* 2019.
16. Article 4 GDPR.
17. ibid.
18. Further to Recital 22 of the GDPR, an "establishment" is created by an "effective and real exercise of activity through stable arrangements" (Recital 22 GDPR). A supply chain operator with no legal entities in the EU may still be caught by the establishment test if it operates a branch office or representative office in an EU territory, for example. In this case, the GDPR would apply to personal data processed "in the context of the activities of" (Article 3 GDPR) the relevant establishment (wherever it might take place). It is important to note that interpretation of this test, including the vital phrase "in the context of the activities of" is, to date, yet to be settled. Recent draft guidance issued by the European Data Protection Board (EDPB) indicates that the establishment test may still be met even if the relevant establishment does not conduct the processing itself if the facts of the case show that there is an "inextricable link" (Guideline 3/2018 on the territorial scope of the GDPR (Article 3) – version for public consultation – between the EU establishment's activities and the processing (wherever and by whomever it takes place). How an inextricable link is established is not completely clear, but raising revenue locally that is inextricably linked to the processing outside the EU will be processing carried out in the context of the activities of the EU establishment. This is still a fluid area of law where the facts can quickly change the legal position.
19. See Chapter 3 (Articles 12–23) GDPR.
20. See Article 35 GDPR. The results of that initial analysis may require further action under the GDPR, including Data Protection Impact Assessments required for "high-risk" processing and/or ongoing training activities for employees, for example.
21. Article 5 GDPR.
22. Article 6 GDPR.
23. Separate, more stringent grounds are required for special categories of personal data, e.g. explicit and separate consent must be provided for processing of special categories of personal data. See Article 9 GDPR.
24. Article 26 requires joint controllers to determine their respective GDPR compliance duties and provide this information, along with their contact information, to the data subjects whose data they are processing. As such, it may be difficult to comply with the requirements set forth in Article 26 of the GDPR in a blockchain/supply chain context primarily because any joint controllers here may not be aware of who the other joint controllers are and who holds what responsibilities.
25. (This was in the context of a non-blockchain-enabled data-sharing scheme, but the concerns would be the same for blockchain-enabled solutions.)
26. It is important to note that the GDPR's definition of personal data (Article 4(1) GDPR) can include "anonymous" data if it can be de-anonymized by cross-linking it with other personal datasets.
27. Data protection regulators are still in an early stage of examining the regulatory implications of blockchain technology. The French data protection authority (known as the CNIL for Commission Nationale de l'Informatique et des Libertés) has recently published a blog post and accompanying paper on the matter (see https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data; https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf; links as of 24/7/19).
28. Bitansky, Nir, Canetti, Ran, Chiesa Alessandro and Tromer, Eran, "Recursive composition and bootstrapping for SNARKS and proof-carrying data", *Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing*, 2013.
29. Rebecca Liao, a co-author of this paper, is executive vice-president at Skuchain.
30. United Nations Economic and Social Council, *Blockchain in Trade Facilitation: Sectoral Challenges and Examples*, March 2019

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org