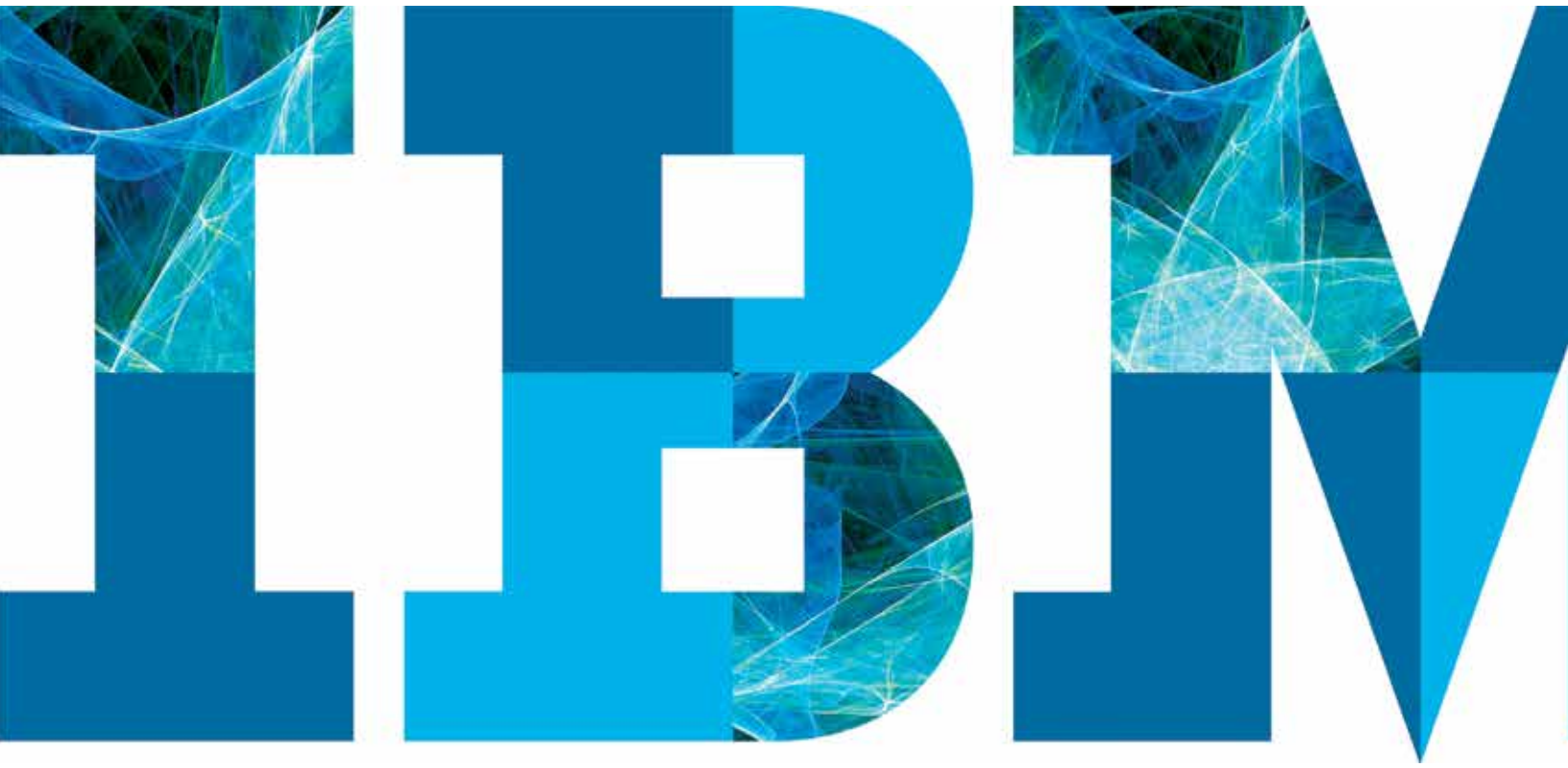
Blockchain and GDPR

How blockchain could address five areas associated with GDPR compliance



IBM

Introduction

Based on recent events, individuals are becoming more aware of the threats of data breaches and the use of their personal data for commercial purposes. The GDPR (General Data Protection Regulation) seeks to create a harmonized data protection law across the European Union and aims to give back the control of one's personal data. With GDPR, even organizations without a physical market presence in the EU may still be required to comply with the GDPR if the organization offers paid or unpaid goods or services to individuals located in the EU or if the organization is monitoring the behavior of individuals within the EU.

In addition, if an organization works with suppliers or partners that operate in the EU, they will expect the organization to comply with GDPR in order to limit their own risk. Simply put, GDPR compliance will soon be considered a requirement to conduct business with EU data subjects. With enforcement starting May 25, 2018, organizations need to consider the steps required for readiness across their organization, encompassing people, processes, data and technology.

Have you considered how blockchain might help you to address your GDPR challenges? This paper explores five areas associated with GDPR compliance and how blockchain might address each.

Blockchain is a shared, immutable ledger for recording the history of transactions. It fosters a new generation of transactional applications that help establish accountability and transparency. Blockchain provides an unmatched level of accountability for how data is managed based on its tamper-resistant data store and its consensus mechanism used to modify the data. Basically, blockchain data is protected by design. Blockchain is still in its infancy but has notable networks already providing value such as food safety and global trade.

While blockchain and GDPR started with very different goals—creating a currency independent of a central authority versus introducing data privacy laws—the two initiatives are aligned on the principles of secured and self-sovereign data (individuals in charge of their data). For example, the recently announced Decentralized Identity Foundation lays down the pillars for decentralized identities anchored by blockchain.

IBM highlights five main areas associated with GDPR readiness: Rights of EU Data Subjects, Security of Processing, Lawfulness and Consent, Accountability of Compliance, and Data Protection by Design and by Default. In this paper, for each of the areas, we provide a point of view on how blockchain applies, we describe project examples, and we explore challenges and opportunities.

1. Rights of EU Data Subjects

GDPR by design will give individuals better control over their personal data (any information relating to an identified or identifiable natural person) and establish one single data protection regulation across the EU: *easier access* to personal data, right to *rectification*, a clearer right to *erasure* ("right to be forgotten"), a new right to *data portability*, right to consent, and right to be informed about a breach of one's personal data when that breach has a potentially high impact to one's rights and freedoms. Having personal data in multiple places for the same purpose makes it difficult to enforce these rights. Solutions based on blockchain can help you simplify as you fulfill these rules.

The implementation of a shared Know Your Customer (KYC) blockchain helps companies as they satisfy the data portability requirement (allowing individuals to obtain and reuse their personal data for their own purposes across different services). For example, Crédit Mutuel Arkéa created an operational permissioned blockchain network that provides a view of customer identity to enable compliance with Know Your Customer (KYC) requirements. The pilot offers a complete view of customers' documents across the bank's distributed network.

According to International Airlines Group, travelers are only 50 percent accurate when filling out the information required to fly[1]. This can be remediated with processes at the airport, but these add time, complexity and friction, making for a poor travel experience. To address these challenges, VChain Tech developed a solution, which used blockchain to provide digital identity as a service to help airlines share data safely and securely when passengers board connecting flights. Blockchain would provide a digital verification of passenger data for airlines with no data exposure.

The above examples show the applicability of blockchain to support the GDPR rights of data subjects. Some caveats, however, should be applied when using blockchain. Blockchain is an "append only" system and immutability is a key and desired characteristic of the architecture. With that in mind, a company that needs to comply with GDPR's "right to erasure" can be challenged. To comply with the right to erasure, personal data should be kept private from the blockchain in an "off-chain" data store, with only its evidence (cryptographic hash) exposed to the chain. Using that technique, personal data can be deleted when needed without any further impact. Blockchain immutability can be used to help implement consent management and to demonstrate compliance with the company's defined process and help enforce the right to erasure. As always, be sure to check with your legal counsel!

Another topic that should be addressed is summarized by the question: who is the Data Protection Officer (DPO) of the personal data collected? In many circumstances, companies are creating consortia (a separate legal entity) to own and manage the blockchain solution. This topic should not be underestimated when setting up the agreement among different parties. And, as we will explain in section 2, no personal data should be stored on the blockchain itself.

2. Security of Processing

According to GDPR Article 32, data controllers and processors are required to implement "appropriate technical and organizational measures to ensure a level of security appropriate to the risk…." In particular, this article refers to the risk of harm to the data subject, along with a set of examples and guidelines for implementing security of personal data, such as pseudonymization and encryption, confidentiality, integrity, availability and resilience of systems and services. It goes on to state that accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access should also be considered when taking into account the appropriate level of security according to risk.

GDPR was designed to be technology agnostic and flexible enough to allow for innovations such as blockchain. We believe that many of the inherent capabilities in blockchain lend themselves well to supporting security of processing, covering the information security triad of Confidentiality, Integrity, and Availability (CIA). Blockchain uses cryptography to support transaction confidentiality along with access controls to prevent unauthorized use. In addition, since data is not stored centrally all in one place, we can mitigate the risk of having a central honeypot for attackers to target. Blockchain capabilities include audit trails and traceability, the use of consensus mechanisms to commit transactions, and transaction immutability. Similarly, blockchain can improve availability by eliminating single points of failure. The ledger and smart contract execution is distributed and if a node is not available, the network can continue to operate and the data is still accessible.

SecureKey leverages blockchain to implement an identity verification network in Canada. As a consumer, one can use the network to verify their identity when buying goods or services. One's identity attributes are distributed across the blockchain network instead of being all in one place. Confidentiality is supported by blockchain via "triple blind": the identity attribute provider doesn't know who they provide the attributes to; the consumer doesn't know who provided the attribute; and SecureKey doesn't know about the attribute exchange. Also, with this network, the consumer is in charge of their identity and decides what identity attributes they share, when they share them, and who they share them with. This is referred to as self-sovereign identity. We will talk more about consent in the next section.

B3i is a consortium dedicated to developing trading platforms across the whole insurance value chain using blockchain-based technologies. Each B3i member organization has a private ledger for storing its own insurance contract elements and data. Then, all organizations also participate in two shared ledgers: The shared master data ledger contains common and agreed master data including public company information and common contract clauses. The shared communication ledger is cryptographically secured and stores the communication used to provide consent on the state of the private organization ledgers. Only counterparties can see the content and destination of the communication.

Despite blockchain being immutable by design, there are still security risks even with private permissioned blockchain networks. For example, a vulnerable application connected with the network still has the potential for unauthorized access to the ledger, either directly to its disk or over the network. Therefore, organizations need to restrict and monitor network access and prevent unauthorized access. Encryption keys could also be tampered with or even lost or stolen, preventing access. Finally, the identity of blockchain participants must be verified to prevent threat actors from impersonating valid users. Using specific blockchain architectures such as Hyperledger and platforms such as the IBM® Blockchain Platform helps to mitigate the risks.

3. Lawfulness and Consent

Under the terms of the GDPR, processing of personal data is only allowed if there is a lawful basis for such processing. One such lawful basis is the consent of the data subject to such processing. Ensuring you have such consent of data subjects before processing their data will likely become much more difficult than it has been in the past. In order for consent to be considered valid, it must be freely given, specific, informed and unambiguous. In cases such as healthcare, where special categories of personal data are more likely to be handled, it must also be explicit. Complicating issues further, consent can be withdrawn by the data subject at any time.

Blockchain can be used to track and manage consent between data subjects, processors and controllers. Reproducibility, data sharing, personal data privacy concerns and patient enrollment in clinical trials are huge medical challenges for contemporary clinical research. APHP and Inserm explored how a blockchain-enabled consent workflow would allow for the collection of patients' informed consent in the context of clinical trials. They found that the technology ensures fine-grained control of the data, its security and its shareable parameters, for a single patient or group of patients or clinical trial stakeholders.

Similarly, IBM Watson Health has signed a research initiative with the Food and Drug Administration (FDA) aimed at defining a secure, efficient and scalable exchange of health data using blockchain technology. IBM and the FDA are exploring the exchange of owner-mediated data from several sources, such as electronic medical records (EMRs), clinical trials, genomic data, and health data from mobile devices, wearables and the Internet of Things. By keeping an audit trail of all transactions on an unalterable distributed ledger, blockchain technology will establish accountability and transparency in the data exchange process.

As mentioned in section 1, no personal data should be stored on the blockchain.

4. Accountability of Compliance

As a controller or processor of data, an organization must be able to demonstrate compliance with GDPR obligations—or at least document how it is progressing toward compliance. Steps toward achieving compliance may include risk assessments, data protection impact assessments, the establishment of a governance model and an enterprise-wide code of conduct, and the design and implementation of a system of record keeping that formalizes and documents implemented data protection measures and audit trails.

With traditional record keeping, information can be siloed, not verifiable, and quickly outdated. These characteristics make the data untrustworthy and clearly not insightful. Using blockchain offers the opportunity to raise the level of accountability and insight in the data and to help a company prove compliance against specific regulations.

Blockchain has been put to work to enable data provenance capabilities such as food safety. Tracking provenance is possible because blockchain not only keeps track of the current state of the data ("world state") but also of all of the changes that have ever been made to the ledger (the chain of blocks). Moreover, thanks to blockchain's consensus mechanism, data on the blockchain can only be altered when key participants with a stake in the data reach consensus.

Unsurprisingly, industry regulators have a keen interest in blockchain, as is apparent in the financial services sector. For example, in capital markets, Northern Trust has used blockchain to digitize the traditionally manual and paper-heavy world of private equity fund management. The UK-based Guernsey Financial Services Commission was one of the participants in the Minimal Viable Product (MVP) build. Instead of relying on paper reports, blockchain gave them direct and near real time access to the ledger data they needed to see.

When being faced with potentially thousands of regulations and millions of records to keep in accordance with the GDPR, automation is critical. This is where the smart contracts capabilities of blockchain can help. For example, Everledger Ltd. uses blockchain to track the provenance of high-value goods such as diamonds. In this demo (start at 1:25:45), we enhanced the IBM Regulatory Compliance Analytics solution with blockchain.

Specifically, we took the diamond trade obligations from the United Nation's Kimberley Process and codified them as blockchain smart contracts. This solution allows for diamonds managed on the blockchain to be automatically checked for compliance—and to trigger alerts or workflows as a result of a non-compliance event. For GDPR, a similar concept could be used to manage controller/processor agreements with a documented chain of contract terms.

In this section, we used blockchain project examples to show how blockchain applies to GDPR's accountability towards compliance. Specifically, we made the following three assertions: Blockchain's provenance and consensus characteristics help establish accountability and immutability. Blockchain helps to improve transparency. Blockchain smart contracts help companies as they automate compliance checks.

5. Data Protection by Design and by Default

GDPR requires data protection to be designed into the development of business processes for products and services. Specifically, privacy settings must be set at a high level by default and the controller should have technical, procedural, and organizational measures in place in order to demonstrate compliance with the GDPR regulation. Controllers should also implement mechanisms to ensure that personal data is only processed when necessary for each specific purpose.

Pseudonymization and encryption of personal data are key technologies identified in the regulation to assist in achieving this goal. Being based on advanced encryption technologies, blockchain can help in the implementation of GDPR-compliant solutions.

Estonian eHealth Foundation revolutionized the healthcare system with innovative solutions: patients, doctors, hospitals and the government benefit from the convenient access and savings these services have delivered. Each person in Estonia who has visited a doctor has an online e-health record that can be tracked. In order to keep health information completely secure and at the same time accessible to authorized individuals, the electronic ID card system uses blockchain technology provided by Guardtime to ensure data integrity and mitigate internal threats to the data.

Every stored data record comes with independent proof that the data is in its original state and has not been manipulated, so it becomes possible to provide an independent forensic-quality audit trail for the lifecycle of the patient records. We believe that this provides increased security in a country under fierce pressure from cyber-attacks, an ask for transparency, auditability, and the need to govern for electronic systems and lifecycle management of over one million patient records.

Stampery acts as a digital notary, binding and guaranteeing business contracts, wills and intellectual property. Stampery leverages blockchain technology to ensure the existence, integrity and attribution of communications, processes and data. Its blockchain-based data certification solutions generate an immutable record of all the activity in document management systems through which audit, accounting or law firms' depositions, affidavits or oaths can be certified automatically. Raw data or plain text are never published to a public blockchain, but rather only unique cryptographic identifiers (hashes) in order not to reveal the original data. Since hashes are one-way cryptographic algorithms, it is possible to prove that a determinate hash relates to some data, but nobody will ever be able to obtain the data by only having its hash.

This solution is implemented in public blockchains accessible by anyone in the world at zero cost. Everything is transparent and extremely easy to verify while maintaining absolute privacy. The generated cryptographic proofs are everything anyone needs to prove or verify that a given dataset existed at a certain point in time. Furthermore, the verification of the cryptographic proofs can be done in an automatic way, enabling secure machine-to-machine transactions.

As GDPR places emphasis on demonstrating compliance, the latter example demonstrates that blockchain's built-in "audit trail" can help organizations prove who has accessed personal data, where, and when.

Conclusion

In the last two years, blockchain has emerged and generated value in areas such as supply chain, provenance, compliance, food safety and digital identity. Blockchain adds accountability and transparency for the participants involved in the value chain, while preserving privacy and confidentiality. More importantly, blockchain can help to remove the friction points that existed in traditional business processes. In this paper, we have described example blockchain projects in the context of GDPR themes and obligations, illustrating the opportunities and challenges for applying blockchain to your GDPR efforts. Blockchain is not a solution to all GDPR challenges, but blockchain can be considered as a mechanism to help control the use of personal data. One thing is for sure: when it comes to GDPR and blockchain, the time to get started is now!

For more information

To learn about ways IBM can help you address your GDPR obligations, please visit the following websites:

For more information on GDPR, see **ibm.com**/gdpr

For more information on blockchain, see **ibm.com**/blockchain

To learn how IBM Security can help support your GDPR journey, see ibm.biz/PrepareForGDPR

To assess the progress of your GDPR journey, see ibm.biz/GDPR-Ready

Acknowledgements

The authors would like to thank Salman Baset, Joseph Douglas, Kevin Gill, Krishna Ratakonda, Bob Yelland, and other IBM colleagues for their contributions.

About the Authors

Cindy Compert (@CCBigData), CIPT/CIPM, is the IBM CTO for Data Security & Privacy and the IBM CTO for US Public Sector Market in IBM Security. In her role, Cindy helps clients address the GDPR regulation and leads the IBM Security GDPR solution strategy.

Maurizio Luinetti (@MauLui) is an Executive Architect proposing, designing and implementing innovative solutions addressing IBM client business goals by linking IBM capabilities and client strategic initiatives.

Bertrand Portier (@lebertrand) is an IBM Distinguished Engineer in IBM's Financial Services Sector. In his role, Bertrand works with IBM clients to help them to evaluate and adopt blockchain in the context of their business environment.

[1] http://www.iairgroup.com/phoenix.zhtml?c=240949&p=irolnewsArticle&id=2263872

IBM Security
75 Binney Street
Cambridge MA 02142

Produced in the United States of America
March 2018

Learn more about IBM's own GDPR readiness journey and our GDPR capabilities and offerings to support your compliance journey here.

Please Recycle

61014461-USEN-00