# Security and privacy risks in the blockchain ecosystem

Received (in revised form): 31st October, 2019

**Ivana Bartoletti**

is head of privacy and data protection at Gemserv. Ivana's years of experience in the field span the public and private sectors, including senior roles in the NHS, Barclays and Sky. Ivana works across all sectors, from finance to AdTech, and within the energy market. She is passionate about new technology, big data, AI and blockchain and specialises in supporting clients with their digitalisation and innovation programmes. Ivana is an international public speaker and commentator on privacy, digital rights and data ethics and regularly features on the BBC, as well as writing for the *Guardian* and other outlets. She also leads the Women Leading in AI network, encouraging women to shape the debate around the use and norms of AI and big data. Ivana holds a Master's of Law degree (LLM) with distinction and a postgraduate management degree in European public affairs. Ivana was awarded Woman of the Year (2019) at the Cyber Security Awards in recognition of her growing reputation as an advocate of equality, privacy and ethics at the heart of tech and AI.

Gemserv, 8 Fenchurch Place, London, EC3M 4AJ, UK
E-mail: Ivana.bartoletti@gemserv.com

**Samuel Plantié**

is a principal data protection consultant in the data protection team at Gemserv. He has a PhD in Law (consumer law in the digital economy), is a data protection expert and an IP/IT lawyer, with over five years' experience in providing legal advice in intellectual property, information technology, contract drafting, commercial litigation and data protection. Samuel is a Certified Information Privacy Professional/Europe (CIPP/E) and has an excellent knowledge of the international digital market. His latest focus is on the use of blockchain technology with data protection requirements and the scrutiny of the AdTech industry by data protection authorities.

Gemserv, 8 Fenchurch Place, London, EC3M 4AJ, UK
E-mail: Samuel.Plantie@gemserv.com

**Arun Sambodaran**

leads the development and implementation of cyber security services for emerging platforms with a primary focus on connected devices (Internet of Things [IoT]) and emerging technology areas such as blockchain and machine learning. Arun holds an MSc in e-commerce within the business environment and has over a decade of experience within the private sector, architecting and managing enterprise solutions, operational technologies and cloud infrastructures. Arun also acts as a trusted advisor within the cyber security standards and regulatory space, helping businesses stay compliant against the changing threat and regulatory landscapes.

Gemserv, 8 Fenchurch Place, London, EC3M 4AJ, UK
E-mail: Arun.Sambodaran@gemserv.com

**Abstract** Over the last couple of years, we have seen much enthusiasm around blockchain and what it promises. While innovative applications are designed almost every day, blockchain comes with genuine concerns about its security and data protection. In this paper, we discuss the security risks specific to blockchain to take into consideration and how to mitigate them, the limits of using blockchain to record personal information in a stringent regulatory context, and the solutions offered to blockchain developers.

KEYWORDS: Blockchain, data protection, privacy, information security, GDPR, encryption, smart contracts, privacy by design

## INTRODUCTION

Blockchain is an example of a distributed peer-to-peer network, with the advantage that all transactions are encrypted, chained together and timestamped. This makes the network intrinsically secure and prevents any changes to already recorded transactions. From a cyber security perspective, users with malicious intent will find it impractical to circumvent this security design to falsify information on the network, thus adding a level of assurance to the integrity of data stored on it. Non-repudiation is supported as standard, as every transaction made on a public or private blockchain is digitally signed, timestamped and tied back to the public identity. The advantage of an immutable transaction history is that it provides additional reassurance that the data has not been tampered with and can be verified at any point in time. This feature increases its transparency to all the stakeholders involved in the transaction and beyond to audiences that need to verify the authenticity.

It is not surprising, therefore, that since the introduction and rise in popularity of Bitcoin, the industry has rushed to find use cases outside cryptocurrencies in areas[1] such as fintech, life sciences, logistics and health care. Fifty-three per cent of organisations surveyed by Deloitte[2] think the use of technology will be a strategic priority.

As the web gave us the ability to exchange information across digital geographies by creating an Internet of information, blockchain is now enabling a network for value exchange, effectively enabling an Internet of value.

Distributed ledger technology (DLT) systems can be structured as permission-less and permissioned (see Figure 1). These mainly determine the participation model of the network. In a permission-less network (or public blockchain), anyone can become a node (participant) to mine new blocks, verify transactions and support the governance[3] of the blockchain. In a permissioned network, however, node users must be identified and assigned a role before participation.

Examples of permissioned networks are Bitcoin and Ethereum, while examples of permission-less network platforms include Hyperledger from the Linux foundation and R3 Corda.

It is clear from the implementation models that enterprises and businesses will focus on solutions built specifically for them, such as the Enterprise grade permissioned private platforms.

Like any new technology, however, we must consider barriers to wider adoption

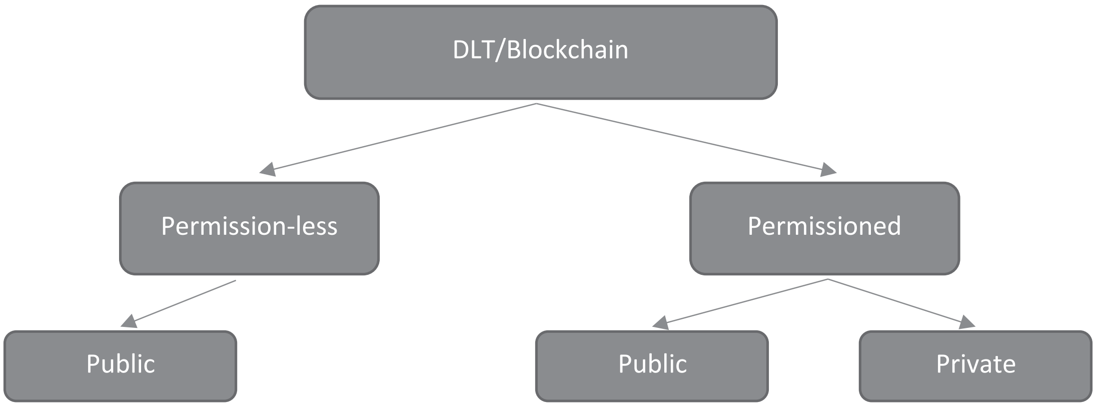


**Figure 1:** Structure of DLT systems
Source: Authors

that have emerged, with many institutions building proof-of-concepts. These real-world issues have been no different from those that plagued previous technologies: lack of mature security standards, interoperability issues from differing implementation types, complexity due to highly technical design, and vague or unassured total cost of ownership for stakeholders often in a collaborative network. In addition, a technology such as blockchain introduces an entirely new issue which goes against the principles of centralised control of systems: decentralised decision making and lack of single ownership of technology or data. Since not all blockchains are made equal due to their differing implementation techniques (cryptography constructs, distributed architecture of nodes and application contexts), a variety of attack vectors are introduced that can lead to exploitation of the blockchain network.[4]

## UNDERSTANDING THE BLOCKCHAIN STACK

To understand the various attack surfaces in a blockchain implementation, let us first look at what makes up the blockchain stack.[5]

Blockchain applications are fundamentally built on top of Internet protocols. There are four main layers: the hardware layer, the Internet layer, the blockchain layer (comprising both the data and consensus layers) and the application layer. Each layer of the stack inherits the protocols and rules of the layer below (see Figure 2).

### Hardware layer

This is the fundamental layer that provides the physical infrastructure to host and operate the nodes, either in physical or virtualised environments. The blockchain software is typically installed on these machines that count as individual nodes.

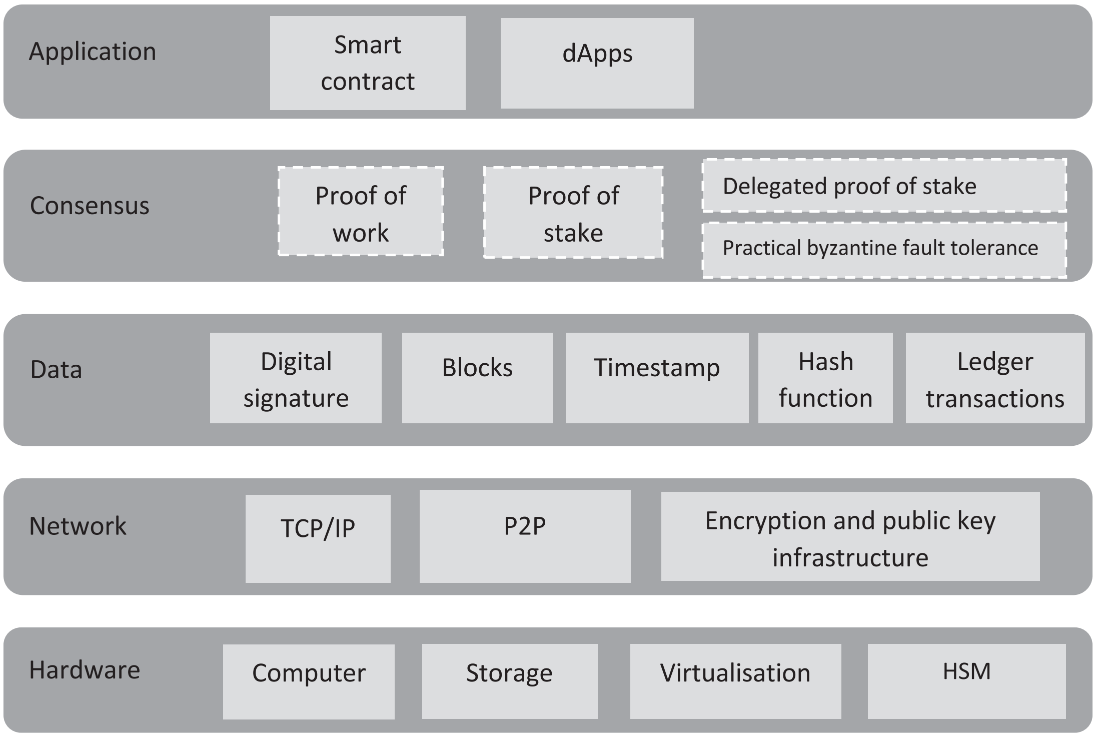


**Figure 2:** Layers of a blockchain technology stack
Source: Authors

Original equipment manufacturers (OEMs) and vendors such as Microsoft and Mediatek have already incorporated security in their hardware to provide a trusted execution environment.

### Network layer

Blockchain networks cannot operate without an Internet connection. Public and private blockchains rely on transmission control protocol/Internet protocol (TCP/IP) that route data packets between other blockchain nodes connected to the public wide area network (WAN). Therefore, it becomes critical for decentralised peer-to-peer networks to have unfettered access to data flows through the Internet for the proper functioning and integrity of the network. Unplanned interruptions such as unavailability of network routes or power outages and malicious attacks caused by denial of service (DoS) attacks on the nodes and Internet gateways can have an impact on communications and cause bottlenecks.

### Blockchain layer

Gluing together the distinctive features of the data layer and the consensus layer differentiates blockchain applications from traditional web applications. This layer unequivocally enhances the security of blockchain applications by hashing blocks and cryptographically chaining them together to create a secure thread of transaction history, one that is immutable and impractical to modify. A blockchain network can implement its own protocols, consensus algorithms and forking principles.

There are many consensus mechanisms existing today and new ones are taking shape. Some consensus mechanisms have gained more traction that others due to their differing properties. The two most popular mechanisms used by far are proof of work (POW) and proof of stake (POS).

### Application layer

It is well understood that Bitcoin has been the first pioneering application purpose built using the blockchain stack. Ethereum led to the innovation of distributed applications (dApps) and smart contracts led to the explosion of application use cases. dApps and blockchain applications are very similar to the web applications today using the similar underlying hardware requirements and the familiar network technologies of TCP/IP.

To manage digital identity, a special application called the wallet is required. In a permission-less blockchain application, this is hosted by entities such as exchanges, and in a permissioned blockchain is held in hardware on premise or using the cloud. Exchanges have been prone to distributed denial of service (DDoS) attacks. Malware Infections in their infrastructures, phishing attacks and wallet code vulnerabilities have been the main contributing reasons leading to such breaches. dApps also rely on third-party libraries or proxy contracts (which is a smart contract delegating calls to other smart contracts). References to third-party code are widely adopted and pose the risk of inheriting vulnerabilities, therefore these must be sanitised to prevent malicious code execution risks.

## SEPARATING SECURITY OF THE BLOCKCHAIN AND SECURITY IN THE BLOCKCHAIN

As the security in blockchain protocols is inherent in design, the security of the blockchain solution becomes a potential attack surface due to the involvement of collaborators in the form of distributed nodes. Malicious actors can employ traditional security hacking techniques, such as conducting network scanning and reconnaissance, to discover and exploit vulnerabilities and launch zero-day attacks on the node machines and its hosted infrastructure. Speed-to-market and competition pressures can force businesses to deploy applications with known vulnerabilities that can affect the distributed chain of actors who previously had siloed security perimeters.

## CRYPTOGRAPHY

Blockchain relies on the use of asymmetric cryptography[6] to endorse messages and data is encrypted with a private/public key pair. As with all cryptography implementations, it becomes important to consider key sizes and encryption suite versions. In an enterprise environment, key management and secure key storage is necessary to ensure identity theft is prevented. Enterprise grade crypto-processors can be used that can securely generate, protect and store keys in a hardware security module (HSM) that makes it impossible for unauthorised users to extract.

## NEW KIND OF DATA

Computing and decision making in a distributed fashion gives rise to the concepts of 'off-chain' and 'on-chain' data. Often the actual data (off-chain) is held outside the blockchain in traditional databases or distributed databases such as the interplanetary file system (IPFS) and need to be referenced by the application. On-chain data, however, usually stores metadata on the node database and points to the off-chain data. This can also be transactional data generated during the blockchain operation and serves as a transaction history. As blockchain databases do not allow for edits, it becomes especially important to maintain the integrity of input data, as once incorrect or malicious data is entered, it cannot be changed.

## RISK AND COMPLIANCE CONSIDERATIONS

There are several factors that increase the risk of blockchain implementations. The number of system actors that take part in a blockchain network varies, but can include users, node owners, developers, administrators, platform operators, governance institutions and even auditors. In certain use cases such as in public blockchains, further stakeholders may also get involved such as wallet providers and dApp operators. This varied set of actors will require appropriate compliance checks and ongoing monitoring. The corporate risk management framework will need to be inclusive of the current and future risks this can bring and adjust their policies and procedures to meet obligations and mitigate any significant risks.

## IDENTITY MANAGEMENT AND KYC (KNOW YOUR CUSTOMER)

Each of the previously mentioned actors will need to have their roles and responsibilities defined before they can participate in enterprise blockchain implementations. In some cases, entities can have multiple roles or identities, and this can require segregation of duties.

To prevent operational inconsistencies, decisions need to be made at the outset, such as who has authority to grant permissions in a permissioned system, how the system can assure the identify of validators and how collusion can be prevented by parties with majority stakes.

In permissioned blockchain solutions, typically the identities of participants in the network are relatively well known through a know your customer (KYC) process and the consensus mechanism allows for enterprises to leverage the existing identity of users and systems.[7] The concept of zero-knowledge-proof identity protocols such as zero-knowledge succinct non-interactive argument of knowledge (zk-SNARK) proposes a radical change in proving identities without revealing personal data about parties. Enterprise-ready blockchain platforms such as Microsoft's Blockchain as a Service (BaaS) and Hyperledger are bridging the gap between traditional identity systems and the blockchain.

## SMART CONTRACTS

Smart contracts introduced the ability to codify complex logic and promised to simplify autonomous transition processing by removing intermediaries. In theory, this opens many use cases where it is highly desirable to automate processes, such as peer-to-peer (P2P) energy trading or allowing access to assets based on access rules. Smart contracts are application coded, however, and all the pitfalls with software development apply here. The infamous decentralised autonomous organisation (DAO) hack[8] in 2016 proved this when 3.6m ether (Ethereum token) was stolen by a hacker using a loophole in the code. Several attacks such as 're-entrancy' and 'overflow/underflow' attacks have taken place since then, which have led to financial loss.

Smart contracts can be audited through manual and automatic code analysis using penetration testing tools to ensure code is free of bugs or vulnerabilities and securing it from zero-day attacks.

## SOFT AND HARD FORKS

Changes to blockchain protocol implementations are sometimes needed to address a critical issue with their deployment and these are called forks, observed mostly in permission-less networks.

Soft forks allow nodes in the network to operate without updating proposed changes such as a change in block size. Hard forks often become necessary when updates to protocols are required to close security vulnerabilities. For example, if a security flaw is discovered in its underlying algorithm or the smart contract, participating nodes will be expected to accept the updated version that fixes the bugs. In permissioned systems, forking rules and platform maintenance can be agreed prior through a governance mechanism and in such cases hard forks may be prevented.

Legal reasons may also prompt hard forks if, for example, sensitive information need to be removed from the network.

## ORACLES

Oracles are external information sources whose function is to supply and correlate data to enable smart contracts to validate its logic. These could be online sources or data collected from connected hardware sources such as radio frequency identification (RFID) tags. As data from oracles is implicitly trusted, it is vital for the source to be accurate and not tampered with. Falsifying data will result in permanently executing incorrect transactions in the blockchain, with consequential effects across the network. Therefore, organisations will need to consider multiple oracles and put additional controls in place to secure the integrity of these information sources.

## DENIAL OF SERVICE

Blockchain networks avoid single point of failure due to their distributed nature and promote a self-healing network. Private blockchain networks with insufficient node redundancy across multiple regions may not be resilient, however, and can cause disruption to the continuous operation during a natural disaster or a coordinated attack.

## MALICIOUS USERS

As blockchain implementations go mainstream, it is inevitable that hackers will develop more knowledge about blockchain networks and their vulnerabilities. In permission-less deployments, identity of users is pseudonymous at best. This could mask the operations of malicious entities and cause longer-term damage if they take over the network using techniques such as the 51 per cent attack, where most of the network's hashing power is controlled by the rogue entity.

Administrators of the hosted infrastructure for permissioned blockchain implementation may also misuse access rights. Rogue employees may be able to disrupt node operations, power supply or hosted network operations to affect participation.

## EVOLVING ENTERPRISE SECURITY IN THE FUTURE

Use of blockchain technologies from a business perspective opens a new frontier for chief information officers (CIOs) and chief information security officers (CISOs), who are already juggling to keep their organisations safe from growing cyberattacks and system failures. At the same time, they are expected to embrace the Fourth Industrial Revolution by integrating emerging technologies such as artificial intelligence (AI), advanced robotics, IoT, additive manufacturing and augmented reality (AR).

For many of these application use cases, blockchain can serve as the backbone to bring them all together. Over time, blockchain implementations will introduce new participants and new processes and will have an influential impact on the enterprise architecture.

Leaders and security champions must stay ahead of the curve, starting with developing necessary skills, talent and relationships to bring about these pivotal changes, helping to achieve changing business goals. They must also do this while continuing to align with security best practices[9] and conforming to the compliance posture necessary for the organisation within the industry in which they operate.

As the technical standards mature and software development principles evolve, blockchain developers will play a critical role in establishing secure engineering practices that support security by design at the Implementation layer. Infrastructure engineers will need to upskill and work in tandem with security DevOps to foster a secure application environment.

Underpinning the strength of blockchain as a revolutionary technology is its built-in cryptography. With advancement in quantum computing,[10] the possibility to weaken current encryption or take control of the network through the speed of processing may be achieved.

Google and IBM have already built qubit processors that are capable of processing at quantum speeds and the research continues to mature on such systems. Our public key cryptography and symmetric key cryptography infrastructure at large will need to be updated to stay ahead of this.

Finally, a continuous monitoring approach through ongoing audits, code analysis and penetration testing will have to be extended to blockchain implementations, networks and governance actors to ensure risks are mitigated.

## THE PRIVACY CHALLENGES OF BLOCKCHAIN

If blockchain technologies raise security concerns, there are also numerous privacy challenges. Many public regulators and institutions have produced reports in the last year on the compatibility of blockchain technologies and the European General Data Protection Regulation (GDPR).[11]

Whereas blockchain is a technology that can be used for a processing activity (as in recording and securing data or authenticating transactions), it is not a processing activity in itself and remains only a technology to store data.[12]

Although initially blockchain has been designed to capture the least amount of personal data possible as an anonymous way of authenticating transactions without disclosing a party's identity or using a trusted intermediary, new blockchain usages are invented every day, some of which involve the recording of personal data directly in the chain, thereby raising data protection challenges.

To understand the full data protection implications, a quick review of the roles in the blockchain is necessary.

All blockchain technologies are based on three different roles: the readers — people who can access, read and obtain a copy of the chain (right to read); the participants — people who can create a transaction and submit this transaction for approval to the miners (right to write); and the miners — people who can approve a transaction and add a block to the chain. In theory, miners are only involved from a technical perspective.

Additionally, we mentioned earlier the three different types of blockchain. Figure 3 shows their different implications from a data protection point of view.

## THE ISSUES OF RECORDING PERSONAL DATA IN BLOCKCHAIN

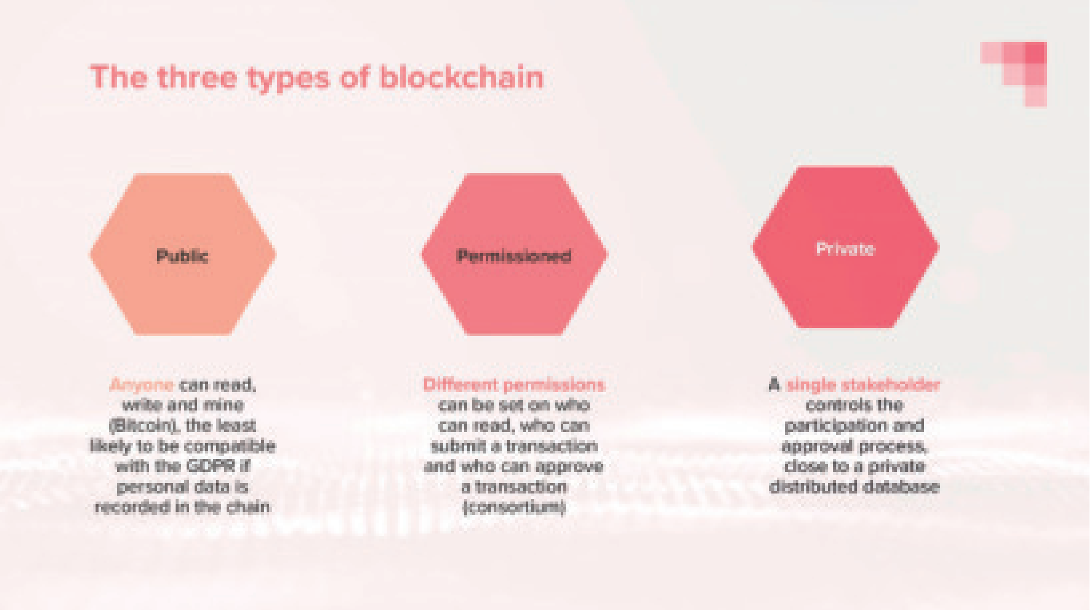
When envisaging to record personal information in blockchain, several issues arise. These include determining controllership and processing roles, identifying the controller(s) and the processors, honouring the rights of data subjects (access, rectification, erasure, automated decision) and international transfers (as blockchain is more susceptible to be spread across the world by essence).[13]

### Controllership on a blockchain

The first thing to consider when determining the controllership of the data is that participants should be considered as the controllers, because they determine the purpose and the means of the processing for the purposes of data protection laws when deciding to create and submit a transaction for approval.

The second thing is that as long as a single miner (or a homogeneous group of miners) does not contribute to more than 49 per cent of the approval process, they remain a simple processor and are not considered as having controllership on the data.

Finally, all participants would be deemed joint controllers if they do not organise themselves differently in a contract.



The three types of blockchain

Public

Permissioned

Private

Anyone can read, write and mine (Bitcoin), the least likely to be compatible with the GDPR if personal data is recorded in the chain

Different permissions can be set on who can read, who can submit a transaction and who can approve a transaction (consortium)

A single stakeholder controls the participation and approval process, close to a private distributed database

**Figure 3:** The three types of blockchain
Source: Authors

### The rights of data subjects

One of the most delicate challenges faced is respecting the rights of individuals when recording their personal information in the blockchain.

As a preliminary thought, we should note that blockchain may not be relevant for a processing activity involving personal data. Privacy by design obligations require that a controller balances the benefits and disadvantages of the technology before its use, and a data protection impact assessment should assess the relevancy of using such technology against other solutions and identify possible mitigation.

While the right of access should not be an issue, once a block is added to the chain it cannot be altered or deleted. As a result, complying with a request of rectification or erasure is impossible when personal data is directly recorded in the chain.

Another interesting consideration when dealing with a smart contract is the right to object to an automated decision. When designing a blockchain for performing smart contracts, the controller must implement mechanisms to allow an individual to obtain human intervention and contest a decision when a smart contract is executed.

### International transfers of data

GDPR restricts transfers outside of the European Economic Area (EEA) if they do not have proper safeguarding mechanisms. These can include signing a contract including mandatory clauses and conducting careful due diligence with the recipient prior to the transfer.

It is worth noting that in the case of a public blockchain, there is no possible technical solution to properly safeguard international transfers of data. The recipients will be unknown by definition, making it impossible to identify them and, even less, implement the relevant safeguards prior to the transfer.

There is more room for compliance when involved in a permissioned blockchain. Solutions such as standards contractual clauses, binding corporate rules and codes of conduct or certifications are more plausible when transferring data abroad.

## DATA MINIMISATION AND STORAGE LIMITATION

Data minimisation refers to the requirement to collect and process as little personal information as possible, while storage limitation mandates retention of collected information only as long as it is necessary.

Participants' and miners' details (such as their public key) are intrinsically part of the blockchain technology and could not be further minimised.

The general advice, however, is to not record personal data in plain text in the chain. Instead, organisations should use a cryptographic hash function on personal data sets stored off-chain, or encryption to store the data directly in the chain if the latter is not feasible.

These cryptographic solutions have the massive advantage of giving a workaround for the rectification and erasure problem: deleting the cryptographic key could be considered equivalent to deleting the data, as the encrypted data would no longer be readable.

## THE ADVERSE IMPACTS OF BLOCKCHAIN FROM A PRIVACY AND DATA ETHICS POINT OF VIEW

The use of blockchain raises many issues when processing personal data is involved. A prime example could be the permanent inscription of negative social impacts in an immutable database — such as personal debts or discriminatory practices.[14]

Blockchain also raises questions around regulation and the place of private actors when it comes to services substituting the roles historically invested in the intervention of the states, such as controlling the monetary system or officialising some legal operations. Like any new technology, blockchain raises philosophical and political questions for the society. Its environmental impacts should also not be overlooked, as substantial computational power is required when a blockchain solution is scaling up.

More practically, the reliance on private keys intrinsic to blockchain increases the risk of a permanent loss of information. The misadventures of QuadrigaCX's investors earlier in 2019 — the largest Canadian cryptocurrency exchange, of which CA$190m in cryptocurrency were lost after the founder died — are an acute example.

Finally, no encryption solution is 100 per cent reliable and can be broken given enough time. Could a robust solution today still be reliable in 10 years? Records that may currently be acceptably safe in the chain could become suddenly visible to anyone. When processing personal data, this could seriously harm the privacy of individuals.[15]

## BLOCKCHAIN AS A TOOL TO IMPLEMENT PRIVACY

Many things can be read about blockchain and GDPR, the most common assumption being that blockchain is not compliant with GDPR. There are certainly numerous demonstratable challenges associated with GDPR compliance.

It is not that simple, however. If using blockchain technology directly on personal data in plain text is highly likely to be incompatible with the GDPR, due to the intangibility of the record, blockchain can also be a powerful tool to implement GDPR compliance.

Here are three examples where blockchain technology can be used to support privacy by design in an organisation.

### Decision traceability

The accountability principle, one of the major changes associated with GDPR, requires an organisation to demonstrate its actions or decisions on daily data protection activities. At any time, an organisation must be able to demonstrate and explain why it has taken a specific decision regarding its use of personal data. It must also record and document every action or decision taken in respect of its data protection governance.

This is where blockchain could find an application. Blockchain can be used internally to record and demonstrate that the relevant stakeholders have been involved at the right time, and to record the decision-making process.

### Consent recording

A further challenge associated with GDPR is that of affirmative consent. The requirement to seek consent has been strengthened, and an organisation needs to be able to record and demonstrate it has captured valid consent.

This can be delicate for many reasons. One example would be that systems or databases may not be designed to fulfil the obligation. Another associated challenge is capturing and recording consent over a phone call. For the latter, blockchain will not be helpful, unless implementing solutions that would be even more challenging in terms of compliance, such as recording the relevant piece of the phone conversation in the chain.

For a situation where capturing consent is required, especially online, blockchain could be very useful for demonstrating valid consent. The purpose would be to assign a random identifier to an individual and record in the chain that this identifier has provided valid consent at a specific timestamp. This would also allow records of when consent is withdrawn.

This solution may not be convenient for all situations; despite it being a useful tool, its use may not be appropriate as a default. Blockchain is not always a relevant or proportionate technology to implement; however, when dealing with special categories of data (data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, sex life or sexual orientation), and where the only legal basis for processing such data is explicit consent, the use of blockchain may provide a powerful tool for keeping robust and verifiable records of its collection.

### Action recording

The last use of blockchain — and maybe the most interesting — is the ability to record any action made on a personal data asset in the chain, especially when acting upon a data subject's request.

This is not only useful to keep track of any event happening on a data asset, as any good old logging system would do, but it can be used to demonstrate that the right actions have been taken in the right timing by the right person.

This can become handy for businesses receiving a high volume of subject access requests — for example, a credit reference agency that receives many subject access requests with a high probability of getting claims to a supervisory authority. The integral ability to record, and demonstrate with unforgeable certainty, that appropriate actions have been taken would be a highly valuable asset.

If a blockchain audit trail could, however, actually show that permissioned data ownership and processing had been adhered to throughout the lifetime of a record, implementing such solution without actually disclosing any information protected into the chain or without compromising the security of the permissions themselves could be a challenge. Developing such system would need extreme and careful engineering to not inadvertently jeopardise the initial purpose.

These examples help to portray a different perspective on blockchain. Application of this technology, with some careful and creative thinking, can provide integral and reliable ways to achieve compliance with the requirements and obligations of GDPR.

## SOME INTERESTING APPLICATIONS OF BLOCKCHAIN

Blockchain does not only come with adverse effects and challenges in terms of data protection and privacy — several extremely exciting applications have already been designed.

Blockchain could substantially help to expand an individual's access to certain services, either by automating their provision (which is the purpose of smart contracts) or by immediately identifying citizens entitled to social benefits.[16] It could also help prevent human trafficking by providing a digital identity in order to protect vulnerable persons such as asylum seekers, or improve medical research and healthcare by providing an empowered, personalised sharing solution for medical data to health professionals.

While we acknowledge that blockchain can present challenges when dealing with personal data, there are certainly situations where such information should naturally be public. This is the case when recording public transactions, and blockchain technologies become extremely attractive when considering land registers, court decisions or companies registers.

## CONCLUSION

The debate on the future of blockchain is open, and only time will tell whether it will fulfil the promise some think this technology holds. It is certain that blockchain poses questions from both a regulatory and a privacy standpoint and will challenge current systems and legislation. It is our opinion, however, that although not a panacea, use of this technology is promising, especially where immutability of data is an important factor.

Blockchain could assist with the accountability and transparency of automated decision-making systems where issues around liability and the necessity to explain these decisions — explainability — require the traceability of all actions taken.

Some GDPR requirements may be currently difficult to reconcile. The text is thought for a centralised digital ecosystem — to address the substantial concentration of power in the hands of large American companies. In the world of the GDPR, there are centralised actors or organisations, such as Google, Apple, Facebook, Amazon and Microsoft, clearly identified as data controllers. Blockchain technology is a complete change of paradigm with such vision of the world. In an age of data sovereignty, evidenced by the introduction of privacy regulations globally similar to the GDPR, is focusing on an inherently decentralised technology even relevant?

It is indeed patent that open blockchain used to record personal information will never be compatible with any data protection requirement. The immutability of data, the absence of control on any international transfer, the impossibility to comply with basic individuals' rights in respect of their data is making blockchain a rather unfit technology to process personal data.

Solutions or applications safeguarding privacy in the context of blockchain are emerging, however — and many are yet to be invented. Some applications could even become a tool to empower individuals by giving them control over their own information.

Ultimately, the GDPR is a living document operating in wider context. It will certainly be interesting to see how regulators and authorities deal with the challenges associated with the evolving concept of privacy and the involvement of emerging technologies.

## References

1. Ogée, A. and Guinard, D. (August 2019), 'Blockchain is not a magic bullet for security. Can it be trusted?', available at https://www.weforum.org/agenda/2019/08/blockchain-security-trust/ (accessed 4th November, 2019).
2. Deloitte (2019), '2019 Global Survey', available at https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf (accessed 4th November, 2019).
3. ISO (Draft 25th June, 2019), 'Governance of blockchain and distributed ledger technology systems', available at https://isotc.iso.org/livelink/livelink?func=ll&objId=20097186&objAction=Open&nexturl=%2Flivelink%2Flivelink%3Ffunc%3Dll%26objId%3D20098174%26objAction%3Dbrowse%26viewType%3D1 (accessed 28th November, 2019).
4. Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D. and Mohaisen, A. (April 2019), 'Exploring the Attack Surface of Blockchain: A Systematic Overview', available at https://arxiv.org/pdf/1904.03487.pdf (accessed 4th November, 2019).
5. Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C. and Rimba, P. (April 2019), 'A Taxonomy of Blockchain-Based Systems for Architecture Design', 2017 IEEE International Conference on Software Architecture, pp. 243–252.
6. Yaga, D., Mell, P., Roby, N. and Scarfone, K. (October 2018), 'Blockchain Technology Overview', NIST, available at https://doi.org/10.6028/NIST.IR.8202 (accessed 4th November, 2019).
7. Born, C. (August 2018), 'Ethereum Proof-of-Authority on Azure', Microsoft Azure, available at https://azure.microsoft.com/en-us/blog/ethereum-proof-of-authority-on-azure/ (accessed 4th November, 2019).
8. Orcutt, M. (April 2018), 'How secure is blockchain really?', MIT Technology Review, available at https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/ (accessed 4th November, 2019).
9. European Union Agency for Cybersecurity (ENISA) (January 2017), 'Distributed Ledger Technology & Cybersecurity: Improving information security in the financial sector', available at https://www.enisa.europa.eu/publications/blockchain-security (accessed 4th November, 2019).
10. Chen, L., Jordan, S., Liu, Y-K., Moody, D., Smith-Tone, D., Peralta, R. and Perlner, R. (April 2016), 'Report on Post-Quantum cryptography', NIST, available at http://dx.doi.org/10.6028/NIST.IR.8105 (accessed 4th November, 2019).
11. European Parliament (July 2019), 'Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?', available at https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf (accessed 4th November, 2019).
12. Commission Nationale de l'Informatique et des Libertés (CNL) (November 2018), 'Solutions for a responsible use of the blockchain in the context of

personal data', available at https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf (accessed 4th November, 2019).

13. Finck, M. (February 2018), 'Blockchains and Data Protection in the European Union', Max Planck Institute for Innovation & Competition, University of Oxford, Research Paper No. 18-01, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080322 (accessed 4th November, 2019).
14. UNOPS (April 2018), 'The Legal Aspects of Blockchain', available at https://www.unops.org/news-and-stories/news/unops-partners-with-the-dutch-governments-blockchain-pilots-to-explore-legal-dimensions-of-distributed-ledger-technology (accessed 4th November, 2019).
15. PwC Switzerland (2019), 'Data protection within new technologies: Blockchain Is your personal data secure when processed on a blockchain?', available at https://www.pwc.ch/en/publications/2019/Data%20protection%20within%20new%20technologies_EN-web.pdf (accessed 4th November, 2019).
16. Allessie, D., Sobolewski, M., Vaccari, l. and Pignatelli, F. (ed.) (2019), 'Blockchain for digital government', European Commission, Joint Research Centre, Digital Economy Unit (JRC/B6), available at https://joinup.ec.europa.eu/sites/default/files/document/2019-04/JRC115049%20blockchain%20for%20digital%20government.pdf (accessed 4th November, 2019).