frontiers in Blockchain

HYPOTHESIS AND THEORY
published: 04 August 2020
doi: 10.3389/fbloc.2020.00036

# What Happens in Blockchain Stays in Blockchain. A Legal Solution to Conflicts Between Digital Ledgers and Privacy Rights

*Gianluigi Maria Riva**

*School of Information and Communication Studies, TEAM-ITN Project at Inisight Centre for Data Analytics, University College Dublin, Dublin, Ireland*

Blockchain is a disruptive technology presented in 2008 that allows both scarcity and timestamps to be introduced to the digital world. Whereas many technological applications may benefit from this architecture, it involves direct conflict with both Privacy rights and Data Protection rules, as introduced by the General Data Protection Regulation (GDPR). This study first provides an overview of what blockchain is, how it works, and how it can affect privacy. It describes how this technology functions, thanks to binary ledgers distributed amongst the system nodes, and what role they play in validating the succession of blocks. The work then analyses how blockchain can be applied to innovative fields and investigates related Privacy issues. Indeed, the chain can certify the time, the parties and the object included in a "block" but cannot guarantee the legal validity, the veracity or correctness of the content. Furthermore, its immutability is in direct conflict with the right to be forgotten. In addition, due to the distributed nature of the system, it does not allow identification of data controllers and, consequentially, the liable (accountable) subject for the personal data processed within the digital ledger. The study is intended for both legal and non-legal audiences and provides a technical overview of the technological foundations behind blockchain to the legal audience, and the conceptual tools to understand the legal requirements that apply to the non-legal audience. The aim of the study is to highlight the characteristics of the proposed solution, i.e., supporting centralised governance of blockchain infrastructures to ensure control over the distrubuted nodes, as well as having the capability to intervene in modifying the chain when the law requires it. This set of interventions would also render publicly available the personal information within the blockchain with different levels of accessibility ("Privacy by Layers," PbL) and, therefore, provide log control that can ensure compliance with the Data Protection regulatory framework. To provide a complete analysis on the matter, the study also addresses how Intelligent Systems running on a blockchain-based infrastructure that holds pieces of personal information can clash with Article 22 of the GDPR on automated decisions when it affects the fundamental rights of individuals. Finally, the conclusions crystallise the legal remarks by stressing the essential elements of the analysis that emerged during the study and framing them within the bigger picture of how the Lawaddresses social or technological phenomena.

**Keywords: blockchain, privacy, data protection, right to be forgotten, GDPR, IoT, digital ledgers, automated decisions**

OPEN ACCESS

***Edited by:***
*Volker Skwarek, Hamburg University of Applied Sciences, Germany*

***Reviewed by:***
*James Burnie, Eversheds Sutherland (International) LLP, United Kingdom*
*Reshma Kamath, Blockchain Research Institute, Canada*

***Correspondence:**
*Gianluigi Maria Riva*
*gianluigi.riva@ucd.ie*

***Specialty section:***
*This article was submitted to Smart Contracts, a section of the journal Frontiers in Blockchain*

***Received:*** *20 April 2020*
***Accepted:*** *09 July 2020*
***Published:*** *04 August 2020*

***Citation:***
*Riva GM (2020) What Happens in Blockchain Stays in Blockchain. A Legal Solution to Conflicts Between Digital Ledgers and Privacy Rights. Front. Blockchain 3:36. doi: 10.3389/fbloc.2020.00036*

## INTRODUCTION

The period from 2003 to 2008 seems to represent the time the technological era of human history has assisted the start of the 4.0 revolution (Morrar et al., 2017). During this time, Facebook was invented,[1] YouTube was founded,[2] Gmail was announced,[3] the first modern smartphone was presented by Apple,[4] and Amazon webstore became a market leader and launched cloud storage services.[5] In this melting pot of technologies, an unknown yet enigmatic character simultaneously presented an article detailing two other revolutionary technologies: blockchain and Bitcoin (Nakamoto, 2008).

These technologies remained unnoticed for several years, whilst interest in them built slowly amongst tech insiders only. The novelty started to gain momentum in 2012, but the potential for blockchain applications was still far from being reached, and Bitcoin only achieved its hype in 2017, whilst blockchain had started to feed the discussion for alternative applications some years earlier (Chohan, 2017).[6]

Blockchain is founded on a digital system based on the concept of distributed technologies, which operates as a shared digital ledger for recording data and metadata in blocks of information and each of them represents a transaction. One of the novelties that this architecture introduced is that blockchain, unlike traditional archives, does not have central administration and control functions. This digital recording system, which is made up of a chain of blocks, represents a distributed database that aims to create an egalitarian organisation-model based on the peer-to-peer network (Galuba and Girdzijauskas, 2009). The latter involves the principle of direct reciprocity among the participants, which permits management and control functions to be performed within the system without the presence of trusted intermediaries or third-party entities. In the blockchain system, the transactions[7] are recorded by any of the network nodes within the blocks that form the chain and these data remain permanently in the blocks in order to be verifiable. Indeed, all the nodes participating in the network can (and should) record and check the transactions and access the information contained in the blocks and the chronology of the block sequence at the same time.

Furthermore, blockchain-based cryptocurrencies (Bitcoin in particular) introduced the concept of scarcity into the digital world. Nowadays, blockchain represents a secure database that can ensure digital signature, timestamping, and hashing. The system grants the security of recordings by using asymmetric complementary key encryption, which guarantees protection for the data entered in the chain (Diffie and Hellman, 1976; Rivest et al., 1978). The combination of public and private keys and the hash function enable the origin of a particular message to be secured by guaranteeing its secrecy, authenticity and integrity, which also extends to the metadata and data contained within the blocks. The system creates a hash footprint for the particular transaction, to which it assigns a non-modifiable timestamp. As a result, the data entered into the blockchain, once validated by the nodes, can no longer be modified or deleted. The data is recorded for an indefinite time, and it is not possible to delete this data.

These characteristics are in direct conflict with the Data Protection[8] regulatory framework (specifically with the right of erasure)[9] and there appears to be no workable legal solution to solve the issue at present[10] (Mantelero, 2016). It must also be taken into consideration that the foundation of the current European Privacy regulation was drafted between 2010 and 2014 — i.e., before the hype of these technologies — and consequently does not address these matters and their implications properly.[11] The Law also does not regulate new technologies such as the Internet of Things (IoT), e-Health, Artificial Intelligence (AI) or Smart Contracts, which all represent potential fields of application for running the blockchain system.

This study investigates the nature of blockchain (independently by its applications in specific cryptocurrencies or other log systems) in relation to Data Protection, and aims to propose a practical legal solution to the conflicts between the public and immutable features of the distributed blockchain and Privacy rights, such as the right to be forgotten. In the first part, the study addresses the technical characteristics of blockchain (as originally proposed in the Bitcoin protocol) and how it works. In the central part, the study focuses on the Privacy issues relating to the blockchain system, paying attention to the main characteristics of distribution, anonymity and transparency and what they imply in terms of imputability and accessibility. The study also provides an overview of the clash of blockchain-based Intelligent Systems with Article 22 of the GDPR on automated decisions, when the blockchain infrastructure holds personal data. In the final part, the study describes a potential solution for Privacy conflicts, based on the concept of centralised model of governance of the blockchain which can allow the appointment of an accountable entity (data controller), and, finally, draws conclusions.

## BACKGROUND: WHAT IS BLOCKCHAIN AND HOW DOES IT WORK

Many people today, especially in the field of Computer Science, claim that blockchain can be a solution for preserving privacy (security aspects specifically) (Seybou Sakho et al., 2019), for

[1] See: https://en.wikipedia.org/wiki/Facebook, last accessed 17.02.2020.

[2] See: https://en.wikipedia.org/wiki/YouTube, last accessed 17.02.2020.

[3] See: https://en.wikipedia.org/wiki/Gmail, last accessed 17.02.2020.

[4] See: https://en.wikipedia.org/wiki/History_of_iPhone, last accessed 17.02.2020.

[5] See: https://en.wikipedia.org/wiki/Amazon_(company), last accessed 17.02.2020.

[6] See also: https://en.wikipedia.org/wiki/Bitcoin#2011%E2%80%932012, last accessed 17.02.2020.

[7] Note that "transaction" can be any type of relationship between two parties, e.g., a financial transaction, a contract, a set of actions (for instance in e-Health systems) and so on.

[8] When Data Protection and Privacy are capitalised, they refer to the whole legal regime, or, for what concern the capitalisation of "Law," to the whole legal system.

[9] GDPR Article 17, which also includes the so-called "right to be forgotten."

[10] EPRS | European Parliamentary Research Service, Scientific Foresight Unit (STOA), STUDY Panel for the Future of Science and Technology, Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law? https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf, last accessed 17.02.2020.

[11] See GDPR first draught 2014: https://iapp.org/resources/article/draught-gdpr-adopted-by-eu-parliament/, last accessed 17.02.2020.

instance in payments, healthcare services and IoT infrastructures (Zyskind et al., 2015; Sutton and Samavi, 2017; Biswas et al., 2019). Although it may seem as though blockchain could plug many gaps in privacy protection,[12] this technology may instead pose a threat to both Privacy rights and Data Protection principles.[13] The concept of blockchain was invented by Satoshi Nakamoto[14] in a article that described a new form of digital currency for distributed peer-to-peer networks: the Bitcoin[15] (Nakamoto, 2008). Blockchain can be defined as the sequence of all verified "blocks" of transactions, chronologically recorded one after the other in a digital ledger (Cuccurru, 2017). In other words, blockchain is composed of a set of single-unit files which contain specific information (the blocks). They are linked to one another in chronological order (the chain). The chain of blocks is therefore distributed amongst terminals (nodes) that contain software to analyse the chain itself. This software must check that the occurred transactions correspond with the formal information of the preceding set of blocks. We can call this set of information the "block metadata," and it consists of (what appears to be[16]) the parties, the object of the transaction, the alleged content, and the time of transaction. Indeed, in order to modify the information contained in one block — and, therefore, validate the transaction -, the majority of the nodes must approve the proposed modification. The nodes approve the transaction if the metadata of the proposed modification are consistent with the metadata from the previous block. This means that the new block must share one of the parties with the old block (i.e., the party who transmits the block), the object and alleged content (e.g., Bitcoin and the quantity transferred), and match the chronological order of the previous block's timestamp, meaning that the new transaction's time cannot precede the previous block's timestamp. In other words, the nodes run the computational software on the chain to ensure both the coherent origin of the new blocks and their validity. The blockchain is therefore a record book of the sequence of the transactions. The system ensures the authenticity of the data contained in every block thanks to a hash function connected to end-to-end asymmetric cryptography.[17] As a result, when a block is modified, it occupies a new position in the chain, and the old block also remains to prove the chronology of the transactions. This chronological chain of the performed transactions, recorded in blocks, forms the precise blockchain architecture. Every node has the computational power to analyse the current status of the chain and the proposed amendment. Hence, if it verifies that the amendment is consistent with the previous blocks, it approves it (Zheng et al., 2017; **Figure 1**). The blockchain is said to be (practically) unmodifiable, due to its architecture. In fact, to falsify it, control of at least 50% +1 of the nodes would be required. There would also be a computational limit to falsifying it, due to the exponential increase in computational capacity needed to reverse modify the chain, from the last block to the first. Moreover, a "pure" blockchain[18] renders this option uneconomic (even if theoretically feasible), thanks to complex mechanisms for rewarding[19] the nodes[20] for their activity of block

[12]Specifically, in terms of security.

[13]In the European legal system, Privacy and Data Protection are two different aspects of the same domain and descend from two distinct fundamental rights, namely article 7 and 8 of the EU Charter of Fundamental Rights. Privacy affects "personhood rights" (such as honour, name, image and so on) and, as such, cannot be object of property rights (ownership) as in the United States legal conceptualisation. Therefore, personal data cannot be sold, but only be licenced by the data subject (the individual that holds the personhood rights) according to the limits and requirements provided by the Data Protection regulation. Data Protection, on the other hand, is a set of procedural rules that comprises data processing, data management, security, and so on, and determines how Privacy rights can be enforced.

[14]It might be a pseudonym that hides a group of people.

[15]In this study, the bitcoin blockchain protocol is considered to be the main and primary example of blockchain architecture and, therefore, as a term of comparison. The focus on bitcoin protocol is justified only in relation to the original architecture that inspired other blockchains and introduced the idea of distribution as a conceptual pillar. Here it is considered to be the "purest" example of distributed ledger because other distributed protocols are built by private, or centralised entities so that they maintain an element of control over the whole architecture. However, blockchain protocols other than Bitcoin exist.

[16]Meaning that the parties that appear in the block represent only the terminals that performed the transaction and may not correspond to two specific identities or real individuals. This concept will be clearer in paragraph . . . when the concept of the clock content will be addressed.

[17]The asymmetric cryptography system (in double-key) was invented by Withfield Diffie and Martin Hellman (Diffie and Hellman, 1976) and consists of sharing two cryptographic keys: private and public one. The private key consists of two larges prime factors of hundreds of digits each, and the public key consists of their product. Security is granted by the fact that it is impossible to trace the private key back from the public key, because no algorithm would be able to extract and track the factors. This is the reason the public key (the product) is known to third parties whilst the secret key (the factors) is kept secret by the private holder, i.e., the message sender. A message encrypted with the public key can only be decrypted with the private key, whilst a message encrypted with the private key can only be decrypted with the public key, so the message can only come from the owner of the corresponding key and the fact that it has not been altered can be verified.

[18]It must be considered that, theoretically, the only "pure" blockchain is the one that is able to ensure full anonymity, a completely shared, public, distributed set of nodes that cannot be controlled by anyone and in any case, a high level of computational complexity for modifying the blocks, with an incentive reward for the transactions verification (which is represented by the cryptocurrency). Thus, the miner who first solves the mathematical problem connected to the block (of transactions) is rewarded with a given quantity of Bitcoins (depending on the halving) and the majority of the nodes check this process and validate it. Consider that the blockchain-Bitcoin infrastructure is mathematically designed for scarcity and to increasingly reduce the issuing of Bitcoin, whilst simultaneously implementing the mathematical difficulty of the computational problems to be solved for mining. This mechanism should grant both scarcity, as well as the rewarding incentive (i.e., Bitcoin itself). In order to function correctly, the distributed blockchain architecture (i.e., the peer-to-peer transaction control from the crowd of nodes) should ensure a sufficient economic disincentive for trying to illicitly modify the blocks or control the majority of the nodes. Indeed, it is not convenient for a miner to trick the block information after solving it (for instance self-attributing more Bitcoins than those allowed), because the nodes would not approve the block and the miner would lose both the Bitcoins and the computational time/energy spent to solve the block. This rewarding mechanism relies on the Game Theory general principles Therefore, it can be argued that the only "pure" blockchain can be considered the Bitcoin architecture, as all the other blockchains are created by private entities that retain a certain degree of control (even with backdoors) of the nodes, as well as a commercial purpose (and so, a conflict of interest). Indeed, it should be noted that it is not the blockchain that serves the Bitcoin architecture but quite the opposite. The Bitcoin is an expedient that represents the reward to ensure economic incentives for the nodes and, therefore, to ensure the distributed nature of the blockchain infrastructure.

[19]According to Game Theory. See for instance, Toreto T., How Game Theory Helps Blockchain Tell The Truth About The World: https://hackerspace.kinja.com/how-game-theory-helpsblockchain-tell-the-truth-about-t-1820429325, last accessed 17.02.2020.

[20]More precisely: the miners, i.e., the pool of individuals' computational power that forms one node. Indeed, because of the computational complexity of the problems

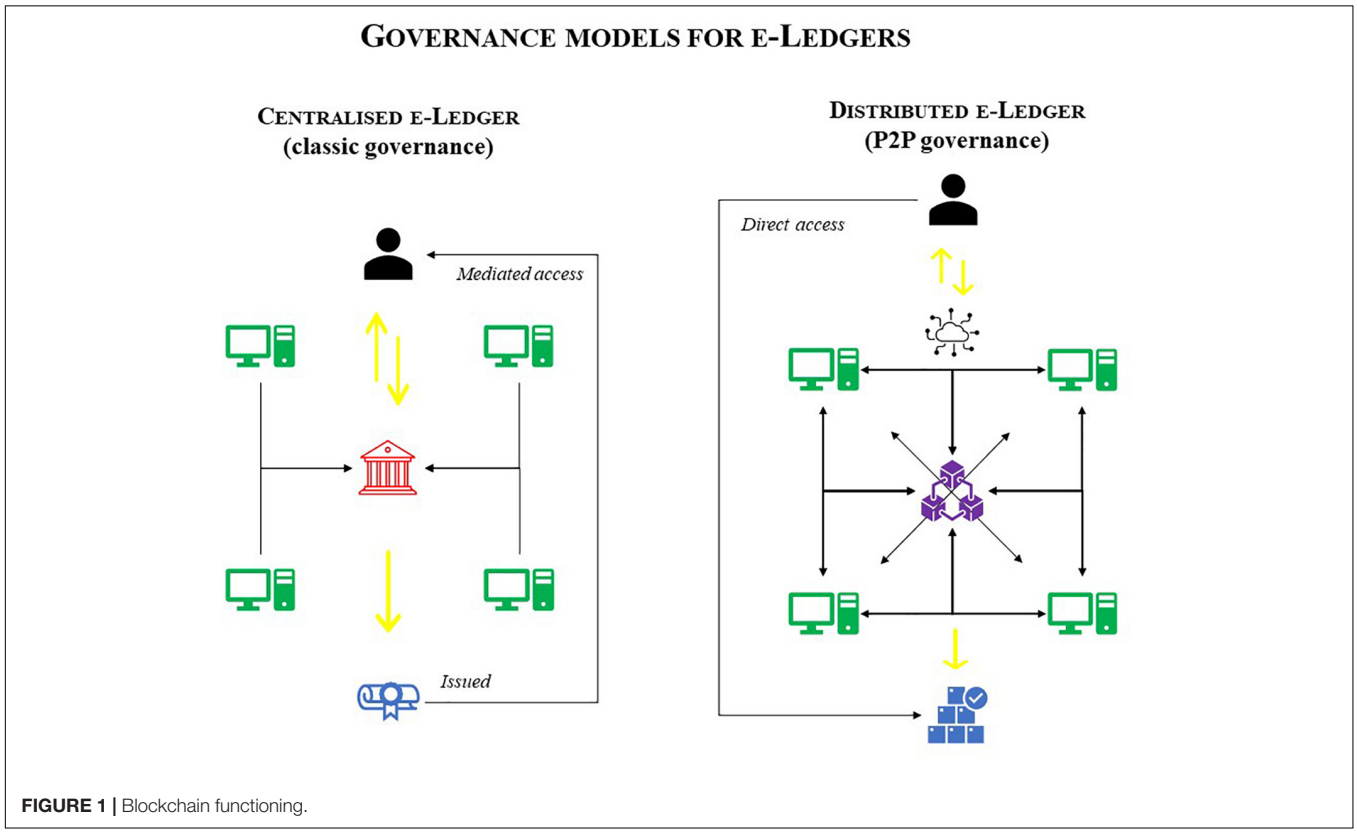


**FIGURE 1 |** Blockchain functioning.

processes control, i.e., so-called "mining".[21] This is the reason for the success of blockchain linked to Bitcoin, as well as for the existence of Bitcoin itself: namely Bitcoin plays the role of reward for the miners for their control of consistency and validity of each block, ensuring the stability and continuity of the blockchain[22] in its distributed nature. This is worth bearing in mind for the purposes of this study.

Therefore, aside from the specific symbiotic binomial blockchain/Bitcoin,[23] blockchain architecture alone functions as a distributed digital ledger[24] through the Net,[25] and it can be applied to a different range of phenomena, such as cryptocurrencies, system logs, micro-transactions, record systems and so on. The applications, indeed, are numerous, and with the advent of the IoT (Atlam et al., 2018), they will continue to increase (Fabiano, 2017).

## BLOCKCHAIN DISTRIBUTED E-LEDGERS AND PRIVACY ISSUES

### What Blockchain Entails in Terms of Data Processing

Blockchain architecture is precisely tailored to support all applications that involve micro-transactions or logging records. Some of its main applications include IoT-based technological solutions such as Smart Contracts (Cong and He, 2019) and e-Health (Mettler, 2016; Liu et al., 2017) for access control

to be solved to mine Bitcoin/verify the transactions, miners usually have to share and pool the computational capacity of their computers in order to solve these problems. This whole computational capacity is known as a node.

[21]To be precise, not every blockchain user plays an active role in the blockchain, as only the "miners" are able to authorise the transactions by allowing the blockchain to use their computational ability to solve complex mathematical operations (so-called "proof-of-work" problems). They are released in accordance with mathematical pre-defined terms contained in the blockchain architecture in order to be solved and so to unlock a block modification. As reward for their mining activity, the miners – often organised in "mining-pools" – receive newly created cryptocurrency, issued in a pre-defined amount by the algorithm (precisely, they assign themselves the pre-fixed amount and the network of nodes validates the whole operation). Also consider that new paradigms of blockchain for cryptocurrencies adopt the so-called "proof-of-stake" protocol, which aims to attain a qualified distributed consensus by requesting "validators" (no longer miners) to prove they hold a certain quantity of that cryptocurrency run in that particular blockchain system. This feature may be designed outside of cryptocurrency blockchains to request "validators" to prove certain qualities, such as identity or formal designation as data processors for instance (the latter example to comply with Data Protection requirements. See *infra* paragraph 4).

[22]See Sabin D., Everything You Need to Know About Cryptocurrency And Why It's The Future Of Money: https://futurism.com/cryptocurrency-future-money-bitcoin/, last accessed 17.02.2020.

[23]Which may be present in other cryptocurrencies or other blockchain protocols in different forms.

[24]Here the author proposes the term "e-Ledgers" for simplicity, hereinafter used to refer to distributed digital ledgers.

[25]Not necessarily the Internet. Indeed, developers might design a blockchain system to run in a private Intranet only. However, depending on the context, the Net can also represent the network of nodes, aside from the specific type of broadband network in which the blockchain runs.

in connected environments. These tools share the need to keep records of every online and offline "intervention" (log, transaction, and modification) performed by professionals (Ackerman Shrier et al., 2016) or parties. However, the range of applications is more extensive as these technologies also connect other domains and can interact with each other. For instance, e-Health blockchain solutions can also comprise both the field of medical "e-folders"[26] as well as all Speech Interface technologies (Daniels et al., 2018) such as Watson Health.[27,28] On the other hand, blockchain-based Smart Contracts can involve domains such as Robotic Process Automation (RPA) (Madakam et al., 2019) or Computational Law systems (CLS).[29] Blockchain architecture can even be implemented to ensure Intellectual Property Rights (IPR) in 3D printers (Holland et al., 2018). In general, in all these IoT environments, the blockchain can be used to ensure that all the processes are recorded, shared and tracked (Kshetri, 2017).

Given that both the IoT ecosystem in general and e-Health environments, more specifically, involve processing of sensitive personal data, such as health conditions, as well as biometric and genetic data, it is evident that blockchain applied to these kinds of ecosystem must be fully compliant with the GDPR and the specific provisions for these kinds of data.[30] Consider, for instance, that almost every set of personal data collected through wearable devices (heartbeat, gyroscope, movements, blood pressure and so on) can easily fall under both the definition of health data and dynamic biometric data (Riva 2018).[31]

## Modifying Blocks and Privacy Implications

One of the first issues concerning privacy can be related to the necessity to amend incorrect personal data (i.e., the right to rectification).[32] Technically speaking, in blockchain architecture, this is feasible only by modifying the latest block that contains the mistake. However, this procedure does not change the previous blocks, meaning that the incorrect information remains in the set of old blocks of the chain without the option to delete or amend this information. In order to amend all of the blocks in the chain that contain a piece of incorrect information, full control of the majority of the nodes that make up the blockchain infrastructure would be required, together with the related computational capacity for amending all the blocks. Therefore, if the blockchain follows the typical distributed architecture, this is not practically feasible or economically viable. This shows both the strength and weakness of blockchain, as it ensures both a permanent non-modifiable record and a resilient method of updating information contained in the blocks at the same time.

The main issue that arises is that the diffuse nature of the e-Ledger allows every node[33] to access the content of each block (meaning full transparency of private information). This is linked to another dichotomic aspect of the blockchain: if the architecture is designed to ensure anonymity of the parties, it is legally unreliable;[34] by contrast, if it ensures identification and transparency over personal information, it clashes with Privacy rights.

Assuming that blockchain systems such as those mentioned above must identify the parties, this raises many privacy issues, especially in IoT or e-Health environments[35] or in any situation in which blockchain architecture collects and records personal data.[36] Indeed, from a legal perspective, blockchain essentially functions as a public commercial register (Pollicino and De Gregorio, 2017) and anyone is able to anonymously access the information stored in the blocks. This uncontrolled and anonymous accessibility poses one of the main threats to individual privacy because it leads to a piece of information being disseminated publicly.[37] Undeniably, if the publicly distributed e-Ledger allows the "crowd" (of nodes) to control the validity of every amendment to the blocks, it also causes a broad, public "data breach"[38] without any control or record of when, where and by whom the information was accessed and for what purpose. On the contrary, a "private"[39] blockchain can theoretically ensure centralised control but, in turn, involves an ethical concern relating to the power of control of the majority of the nodes, and so the ability to perform illegitimate or unlawful modifications.[40]

[26] See Borras J., Webber D., Mattocks C., Kielland H.A.A. (2013), e-Health. The future service model for home and community Health Care: https://www.oasis-open.org/committees/download.php/48970/eHealth%20Future%20Care%20Model%20draft%202013-03-19.pdf, last accessed 17.02.2020.

[27] See https://www.ibm.com/blogs/blockchain/category/blockchain-in-healthcare/, last accessed 17.02.2020.

[28] See also https://www-03.ibm.com/press/us/en/pressrelease/51394.wss on the "Collaboration to Study the Use of Blockchain Technology for Secure Exchange of Healthcare Data" by IBM Watson Health, last accessed 17.02.2020.

[29] Cf. Genesereth M (2017). The Cop in the Backseat. Embedding Law in Everyday Life, http://complaw.stanford.edu/readings/cop.pdf, last accessed 17.02.2020.

[30] Article 9 on "particular categories of personal data," i.e., the so-called "sensitive data." Note that the GDPR updates the previous list, adding biometric and genetic data, amongst other things.

[31] Riva G.M., Metadata (2018), Semantic data and their protection: legal nature and issues under the GDPR and the E — Privacy draught Regulation. Amsterdam Privacy Conference (APC 2018).

[32] GDPR article 16.

[33] And, thus, everyone who has access to it.

[34] The Law requires the parties to be identified (or in some case at least identifiable) because of imputability, and therefore, accountability of actions. In turn, this is connected to the general aim of the legal system to provide stability to social, economic and legal relationships, as well as certainty and foreseeability of the effects of a legal situation.

[35] Office of the National Coordinator for Health Information Technology U.S. Department of Health and Human Services, Blockchain and Health IT: Algorithms, Privacy, and Data. White Paper 2016.

[36] According to GDPR article 4(1) 1, "personal data" means any information relating to an identified or identifiable natural person ("data subject"); 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."

[37] For Data Protection, the difference between communication and diffusion is that the first involves sharing the information with specific, identified people or entities, while the second involves sharing the information with unidentified and unquantified people, i.e., the public.

[38] GDPR Article 33.

[39] In the sense of non-distributed blockchain architecture.

[40] The difference between illegitimate and unlawful is that the first consists of a lawful activity (not forbidden by the law) performed by someone who is not entitled to do so, whilst the second is an illicit activity (contrary to the law) even if it is performed by someone entitled to do so. For instance, in private law, only

### Events Chain vs. Content Blocks

Blockchain only ensures transmission, but it is not capable of guaranteeing the content of the block, aside from the block's metadata.[41] This means that whereas the nodes track and validate every single modification in the chain in accordance with the information that the block conveys in a particular moment, the content itself is not ensured. Indeed, if incorrect or false personal information is input into a block, the chain is not able to certify the validity of the content itself and its correspondence with the truth, i.e., that the piece of personal information is real. The mismatch between content information and metadata information is clearer in Smart Contract applications (Raskin, 2017). The parties, the object of the transaction (e.g., supply of products versus payment of a sum) and the timeframe of the relationship represent the metadata, which appear in the block.

However, the contractual conditions, description of the products, terms of supply and payment represent the content, which does not appear in the block, or where it does appear, it cannot be validated by the nodes as true, real, valid, lawful or legitimate. Therefore, blockchain can validate that a particular transaction occurred at a particular time, between specific parties, for a particular object[42] and with certain conditions; however, it is not able to guarantee that the price that appears in the transaction was the real price paid,[43] that the description of the goods was accurate, correct or incorrect, or that the conditions agreed between the parties were respected. When this content includes personal data, this could create significant problems, as the GDPR also protects false or inaccurate personal data. Therefore, an individual whose personal information appears incorrectly in the blockchain is able to enforce all the data protection remedies that are actionable (Bolognini et al., 2016).

The distributed nature of the "classical" blockchain, however, does not permit any data subject[44] to enforce their rights, as there is no data controller[45] to whom any privacy request could be sent, i.e., there is no representative to whom a request can be addressed as the distributed blockchain is publicly available (but not public in the legal sense)[46] and is without any owner or entity that formally controls it. Other studies have already highlighted the need for a legal entity to determine who is responsible for a particular blockchain network (Henderson and Burnie, 2018).

This means that any blockchain infrastructure that contains personal data would need a trusted third party to assume the position of data controller (which would imply governance of the infrastructure). This data controller would then certify, or be accountable for the validity of the personal information introduced into the system, in order to render the blockchain itself compliant with the GDPR provisions. In addition, a publicly accessible distributed blockchain involves that none of the GDPR rules concerning accountability can be applied[47] due to the diffuse nature of the e-Ledger and its anonymous accessibility (Buocz et al., 2019). In turn, that there is no way to apply any liability rule and therefore none of the players in the chain would be legally protected against any unfortunate occurrence. On the contrary, even if the nodes were not anonymous, the subjects that manage them (or are part of them), i.e., every single miner, would all have to be unrealistically[48] nominated as data processors, but yet there would be no data controller.[49] This would appear as a Data Protection short-circuit, as the data controller is the one that appoints the data processors. Therefore, if no data controller exists, the miners cannot be appointed as data processor, even if their would have been identified. These issues are the reason why the European legislator should consider regulating the so-called "sidechain"[50] qua required third-party entities who are able to close this legal loophole, i.e., can assume the role of data controllers.

## The Distribution Dogma and the Misunderstanding About Anonymity

The idea of the distributed architecture of the blockchain traces back to Nakamoto's article, in which they precisely state that their double-payment system (Bitcoin) must be based on "a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions." This architecture has a very precise scope for Nakamoto, namely, to avoid the need for a "trusted third party" to manage the system at any stage. In essence, the blockchain system was created to bypass the intermediation of any entity in the exchange of goods, which is the case for electronic payment (**Figure 2**). This idea is firmly linked to the current payment system in which central banks act as a trusted intermediary to allow the exchange of money, payments and general transactions. Even

the owner can destroy his/her own property, i.e., a legitimate action, but the owner cannot, for instance, burn his/her own house to destroy it because it is against the law, i.e., an unlawful action. Legal actions can be legitimate and lawful; illegitimate and lawful; legitimate and unlawful or both illegitimate and unlawful.

[41] See for instance Varsheney N., Bitcoin's blockchain is full of content that can land you in jail: https://thenextweb.com/hardfork/2018/03/21/bitcoins-blockchain-content-land-in-jail/, last accessed 17.02.2020.

[42] As per the legal meaning of object, i.e., the contractual object, or, broadly speaking, the object of the transaction (meaning both material or immaterial goods).

[43] Or the actual value of the good.

[44] The GDPR does not define the concept of "data subject," which however, represents any physical person whose personal data are processed by a third party.

[45] Defined by GDPR Article 4(7) as "the 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."

[46] Indeed, public goods or public entities fall into specific legal regimes that govern the relationships occurring between them and private or other public parties. Here, perhaps the only plausible parallel that can be drawn with the distributed blockchain is the "market," although the latter is a more ethereal concept, while blockchain relies on specific material infrastructures and is governed by a pre-determined mathematical architecture.

[47] GDPR articles 25 and 5.

[48] As they remain anonymous, at least in a "classically" distributed architecture.

[49] According to GDPR article 4 (7), the data controller is someone who "determines the purposes and means of the processing of personal data." Thus, as nodes administrators do not decide the purpose of the blockchain data processing, nor do they do it collectively with miners, they cannot legally be assigned as data controllers. Nevertheless, they should be appointed as data processors because they collect, access, manage and process personal data. However, paradoxically, they could not be appointed by anyone as such, as data processors are nominated by data controllers and this role is missing in the distributed blockchain.

[50] Meaning a sort of private blockchain. See https://www.quora.com/What-are-sidechains, amongst many others. Last accessed 17.02.2020.

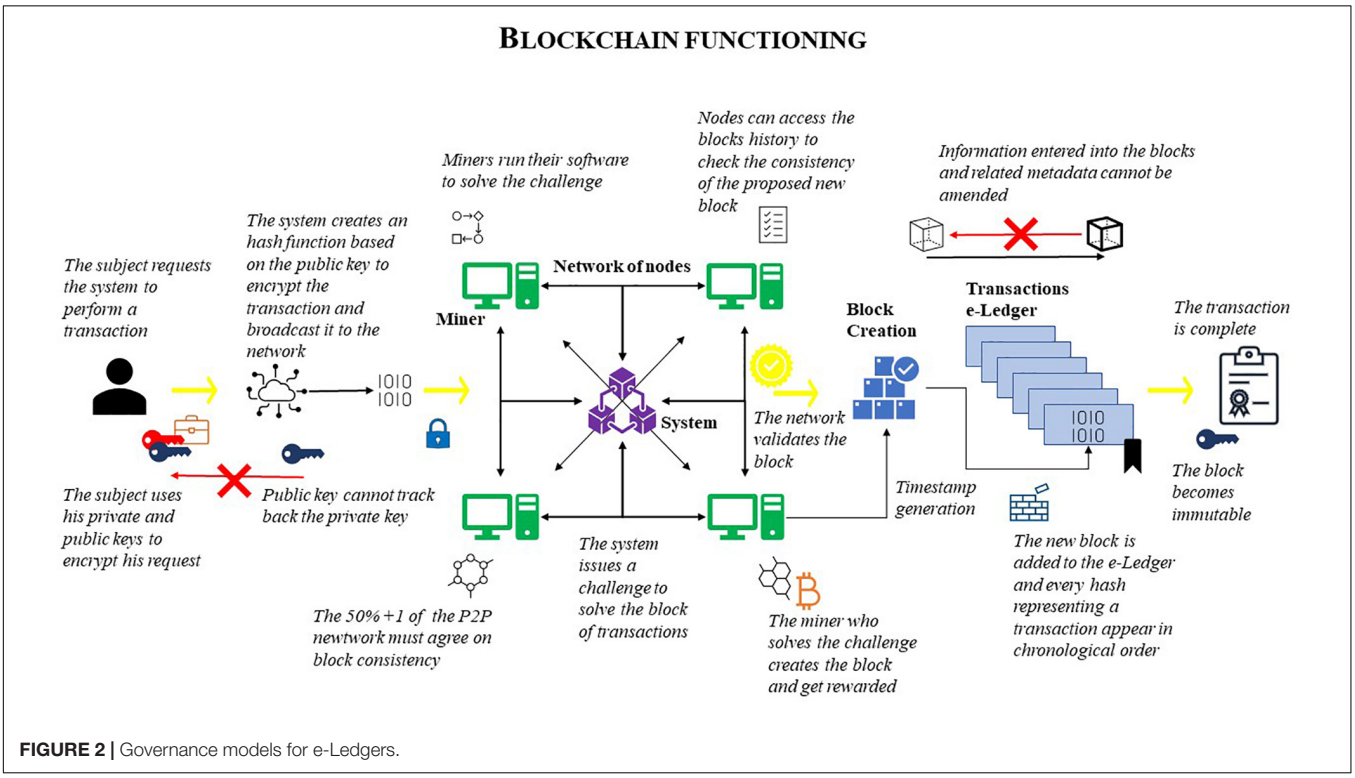


**FIGURE 2 |** Governance models for e-Ledgers.

PayPal, which was founded with the same intentions as Bitcoin, had to (and still does) adhere to the global payment regulatory system and therefore is connected to the banking system to process payments made through its service platform. Another example is (Facebook) Libra, which although in its infancy and may never see the light of day represents an alleged blockchain system for payments, which works in precisely the same way as PayPal, and thus relies on – and complies with – the central banking system.[51] The need for a central system of reference, and for a trusted third party as a representative, is based on the social necessity for stability and the related legal need for accountability and enforceability, which thus allows for that precise stability mentioned above.

## P2P "Democratisation" Utopia

The idea of a peer-to-peer system with distributed nodes (namely that cannot be controlled by a single entity) can be traced back to the earliest concept of the Internet, which was designed as a "free land"[52] in which everyone could have enough space for whatever purpose they wished. This kind of idealistic free and accessible space seems connected to an utopic concept of democracy, which would ensure an high level of transparency in order to match information accessibility for the public. However, the utopia of a free and democratic Internet has been already criticised as a sort of "hippie" illusion that has been completely reversed by the capitalistic model of disintermediation (Rampini, 2015; Rheingold, 1993) and that has eventually ended in "multi-monopolistic" models (Riva and Barry, 2019).

Nevertheless, the original idea of peer-to-peer blockchain/Bitcoin is similar to offline cash payment methods, in which private entities exchange goods for money (cash), without the direct intervention of any intermediary. Therefore, the idea of removing the intermediary from payments in peer-to-peer relationships was not new at all and yet was only an attempt (that has been successful so far) to reproduce this mechanism in online relationships. Note that this was only made possible by introducing the concept of scarcity on the Net, as well as by introducing the actual possibility for it, which has been a technological revolution.

Cash and Bitcoin,[53] however, share another crucial common feature, which also informs the respective systems behind said currencies,[54] i.e., financial standards and blockchain architecture respectively. Indeed, a "sovereign" entity allows both systems to function. The State grants that the currency that people use as cash for their payment was issued; had a stable and exchangeable value; was accepted among parties in a specific territory; was limited and governed by rules; and had a fixed scarcity. Even if it does not appear as such, the Bitcoin/blockchain system works in the same way and the sovereign entity is Nakamoto itself,[55] or at least, the architecture that they designed,

[51] White Paper: An Introduction to Libra. https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US.pdf, last accessed 17.02.2020.

[52] With no owner, nor ruler.

[53] As mentioned, Bitcoin is taken as example of cryptocurrency based on blockchain, and the discourse can be extended to other protocols.

[54] More precisely: the payment systems.

[55] Which still holds the "keys" of the blockchain/Bitcoin system, together with thousands of actual Bitcoins (which, however, the community have identified and can track, and that seem have remained untouched since 2008).

which ensures the same elements as described above for regular offline currencies.[56] According to this perspective, Nakamoto undemocratically have decided how to ensure the scarcity and according to which pre-determined parameters, how to design the architecture of the nodes and the percentage required for validity (50% +1), the (mathematical) rules to mine the to create both "forks"[57] and "halvings",[58] and the borders of the territory for the exchange (i.e., the jurisdiction), which is the Internet in this case.[59] It can even be argued that both systems ensure the record of transactions as much as anonymity. It is indeed fact that offline transactions (payments for goods) are recorded for tax purposes by sellers, but this does not involve the payer being identified.

## Anonymity and the Difference Between Identification and Recognisability

Anonymity appears to be another pivotal paradigm of the classical blockchain/Bitcoin architecture. Nakamoto built Bitcoin on the concept of anonymity to grant that nobody controlled the peer-to-peer transactions performed throughout the blockchain, even ex-post. However, the Bitcoin blockchain infrastructure has already proven that it cannot ensure full anonymity (Juhász et al., 2018), as well as some studies having shown how to ensure "access privacy" without anonymity (Henry et al., 2018). Nevertheless, the concept of anonymity must not be confused with the concept of potential identifiability (i.e., recognisability). From both a purely legal and a Data Protection viewpoint, there is a grey area between the status of being anonymous and the status of being identified and this is the status of being unidentified but still identifiable. This is exemplified precisely by the aforementioned example of ordinary cash payers in offline transactions. One can remain unidentified but still identifiable, meaning that an individual can be anonymous (in practise) until the identification occurs. This is an ordinary feature of everyday life for citizens, in which the system requires everyone to be recognisable.[60] The element of recognisability[61] allows people to perform their activities in an unidentified manner, but it ensures that the system is able to trace identities back under particular circumstances, usually regulated by the law. This concept is evident for images representing individuals: anonymised images do not show any personal feature (eyes, mouth, nose, hairs, tattoos and so on) and therefore they compromise identification (and re-identification[62]). However, a plain image of an individual does not render him/her identified but only recognisable. This is the normal way for Legal Systems (national States) to ensure the stability of socio-legal relationships and the enforcement of and punishment for criminal actions and civil liabilities. The difference between anonymity and recognisability[63] is that the former ensures that no one can ever trace a specific activity back to anyone and relate it to a specific individual (imputability), whilst the latter allows the individual to remain unidentified if there is no need to connect a specific action to a specific individual for particular socio-legal reasons. The concept of imputability is indeed the element that connects identity and accountability, and therefore stands in between anonymity and identification. In any system, the ability to identify (a unit, an individual, an element) allows the system itself to impute (ascribe) a situation (an action, a deed or occurrence) to that single subject. This, in turn, enables the system to make that subject responsible for their behaviour and the related cause-effect events. Essentially, imputability means the ability to differentiate[64] between different individuals to establish who did what and, if the event caused damages, whom to hold accountable for these outcomes.

Given this analysis, it can be argued empirically that most of the current blockchain designers adopt both the "distributed nodes" and "anonymity" paradigms as unsurpassable dogma (Baldwin, 2018). It can be speculated that these two dogmatic features can work with the functioning mechanisms of particular online payments and cryptocurrencies. Nevertheless, this does not need to be valid for other different blockchain applications. In fact, if programmers are able to overcome the cultural/psychological limits of the distribution paradigm and the anonymity feature, the blockchain architecture can easily be implemented to be compliant with legal requirements for accountability (Henderson and Burnie, 2018) and to work accordingly.

## Transparency Misconception and Its Difference From Accessibility

The idea of distribution can also be based on the democratic concept of transparency. Literally speaking, transparency means "entirely visible to anyone"[65] and, therefore, the concept is often used in the architecture design of "open access" services. This kind of conceptualisation, however, relies on both an ontological and epistemological misjudgement on the qualitative nature of transparency. Something is transparent if it can be seen by those for whom it is intended, meaning they have the tools (even technical) that enable them to access it. For instance, an open access code is considered transparent but, actually, it is accessible

[56] This can be extended to other cryptocurrencies, which are bound to the parameters, protocols and architectures arbitrarily decided by their creators.

[57] A fork is a change in protocols of the blockchain infrastructure, often driven by software upgrade that brings new technical features to the blockchain system, which then diverges into two potentially different systems. Because different parties need to use common rules to maintain the history of the blockchain, forks occur when these parties are not in agreement with these rules.

[58] In cryptocurrencies, halving refers to a process that reduces the issuance rate of new coins that can be mined. It represents the periodic reduction of the block subsidy provided to miners, which is pre-determined by the system architecture. The scope of halvings is to ensure that a particular crypto-asset will follow a steady issuance rate until its maximum supply is eventually reached.

[59] The Internet as governed by the ICAAN. The bitcoin blockchain does not run in IoT infrastructure, for instance.

[60] i.e., to reveal those traits that allow the State to identify the individual, such as their face. This is why covering faces, even for religious purposes, is not permitted in many countries, except for specific circumstances such as carnivals (or now for COVID-related reasons).

[61] Meaning the ability to attribute an identity.

[62] i.e., the ability to reverse the anonymisation process and trace back the identity. In the image example, this would mean the ability to reconvert an anonymised picture (which, for instance, covers the eyes) into the full original image.

[63] i.e., the status of remaining unidentified but still identifiable.

[64] In the broader sense and not as per the negative connotation of the term, with which is used commonly.

[65] See https://www.lexico.com/en/definition/transparent. Last accessed 17.02.2020.

only to those who know that particular coding language and have the technical tools (laptop, broadband, and coding software) to read the code. For anyone without access to these tools, it is no more transparent than an encrypted code and they essentially have to trust those who can read it (who spontaneously emerge as trusted third parties) and blindly rely on their judgement.

Indeed, transparency should be distinguished from accessibility and in terms of Law this is evident. Accessibility differs from transparency because it is the ability to obtain information (generally to enter a particular "legal" space) regardless of mediating tools and regardless of the features of the repository, i.e., hidden or transparent. For instance, it is possible that documents related to activities performed by public institutions are not published (transparent) but they can still be accessed on request. Legally speaking, transparency may even damage public interests or private rights as well as accessibility being designed to grant access "in layers" only under specific circumstances recognised by the law.[66] For example, in a public competition[67] based on written exams for a job position issued by a public institution, the final scores may be transparent, whilst the individual written examinations of the participants remain unpublished, but would be accessible to those with a legitimate interest in accessing the documents. As a result, the privacy of participants would be upheld, as would the general interest in being able to access all the written examinations under specific circumstances. This would be the case for one of the participants should he/she wish to check the validity of the evaluation procedure (legitimate interest).

However, even if transparency differs from accessibility, this does not mean that the concept itself is not important. It only means that these two concepts should remain differentiated and treated accordingly when designing the architecture of a system infrastructure. This is important, especially given that transparency may infringe on individual privacy rights or interests, and that accessibility requires elements in addition to mere visibility to be properly implemented.

## Privacy Dilemmas Concerning Information Immutability, Storage, and Availability

Blockchain should not be only be intended for cryptocurrency, as is often the case, especially in non-technical contexts. It can actually reach its full potential in many other and diverse applications, ranging from commercial to public aspects of society. In order to do so, blockchain systems must, however, be able to surpass the legal "stress-test" of accountability, which, in Privacy domains, can be a difficult challenge.

One of the main privacy issues with blockchain is the immutability of personal information entered into the chain, mainly once a node introduces new data. This activity is in direct conflict with the principle of the right to be forgotten (Di Ciommo, 2017; Pizzetti, 2017),[68,69] as well as with the right of opposition and rectification.[70] Legal literature has already explored this type of clash, but no practical solutions have been found so far to overcome the conflicting situations. According to the literature, blockchain clashes with privacy in three main aspects:

- Data cannot be modified once entered into a block (clash with the right to erasure/opposition/rectification);
- Data are publicly available to every blockchain participant (clash with the principles of confidentiality, accountability and the duty of appointing data controllers and possibly data processors);

[66] See note 21 for a parallel with "proof-at-stake" protocols for blockchain.

[67] E.g., for job positions related to public institutions in which applicants must match formal requirements (for instance holding a master's degree) and take written examinations.

[68] GDPR article 17: Right to erasure ("right to be forgotten"):

(1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) The data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
(c) The data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
(d) The personal data have been unlawfully processed;
(e) The personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
(f) The personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

(2) Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

(3) Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) For exercising the right of freedom of expression and information;
(b) For compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(c) For reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
(d) For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
(e) For the establishment, exercise or defence of legal claims."

[69] See also: The European Union blockchain observatory & forum, Blockchain and the GDPR (2018). Whitepaper, Consensys, 25.

[70] GDPR articles 16, 17, and 18.

- Data are kept (stored) forever (clash with the principles of purpose, necessity, and minimisation).

## To Centralise or Not to Centralise?

These issues involve at least two other crucial aspects to consider: without centralisation, there is no possibility to appoint any data controller (i.e., a legal entity, Henderson and Burnie, 2018) and at the same time, no one performs the duty of informing data subjects[71] and neither defines the purposes for data processing, nor the consequent legal basis on which to base the processing, and the related Data Protection Impact Assessment[72] (DPIA). Moreover, the distributed nature of the ledger implies distributed storage, which not only undermines the security of personal data but also implies that the provisions for data transfer outside the EU can be completely bypassed.

The lack of a trusted third party to validate personal data in the blockchain as real, true or exact, can therefore reflect on the usability of personal information in e-Ledgers. Without this kind of external certification, non-verified personal information entered into the chain may even be the subject of illicit usage or even a tool for manipulation purposes.[73] The problem of the lack of data controllers to validate personal information affects the practical management of the blockchain system in many aspects that should not be underestimated, especially concerning the fines provided by the GDPR for unlawful data processing.[74]

The issue has been addressed at system architecture level, and with a US privacy conceptualisation[75] by designing alternative architectures for privacy self-management (Zyskind et al., 2015). Although these solutions could work in practical terms, they may not be sufficient to ensure that the GDPR provisions and, in general, the legal requirements are adequately respected. Indeed, the fact that the GDPR is not a standalone regulation, but instead must be read in relation to the whole legal system and the principles that inform it must always be taken into account. In general, addressing the issue of blockchain incompatibility with the right to be forgotten (erasure), the classical solution that the literature proposes, relies only on pseudonymisation and encryption.

## The Need for an Accountable Entity (Data Controller)

Although pseudonymisation and encryption appear to be workable solutions, they actually avoid addressing the elephant in the room, which is the lack in the distributed ledger of any subject able to perform, or accountable for performing the encryption. In fact, in order to work in this sense, the encryption must dictate the architecture of the blockchain system, which comes back to the subject that designs it and its "sovereignty",[76] i.e., the data controller. Furthermore, even if the encryption mechanism were embedded in the system by default, it would still be necessary to have an appointed entity to manage encryption and decryption when needed. This legal entity must be appointed or identified in some way for the sake of allocating responsibility, and correspond precisely to what the GDPR defines as a data controller.[77]

Hence, if there is no data controller, no action can take place to ensure the privacy rights of data subjects and data protection compliance. These rights would be undermined even before addressing the right of erasure/rectification issue. Indeed, if an entity inputs the data subject's personal data into the chain, they collected these data somehow, somewhere, which already implies data processing.[78] As a result, they should have informed[79] the data subjects in accordance with articles 13 or 14 of the GDPR.[80] Moreover, in relation to the right to erasure or rectification, and admitting that the blockchain could be theoretically entirely modified,[81] in order to eliminate every trace of incorrect personal data, they would need the data subject's consent (or at least his/her knowledge) to amend their personal data. However, this is an external input not taken into consideration in a blockchain system (Fabiano, 2017).

## The Clash of the Titans: Anonymous Nodes vs. Accountability

The distributed chain implies a distributed storage system, which, in turn, involves a serious concern about the application of accountability principle and rules,[82] as it is practically impossible (especially for data subjects) to identify/locate all the nodes, their managers or pool participants, and thus to enforce Data Protection rights. Besides, the distributed nature of the e-Ledger

[71] As per GDPR articles 13 and 14.

[72] GDPR article 35 et seq.

[73] European Data Protection Supervisor EDPS Opinion No. 3/2018 on online manipulation and personal data.

[74] GDPR article 83.

[75] Which relies on the Common Law system, while the GDPR refers to Civil Law tradition, and the two work according to different legal paradigms and principles. Indeed, the US Privacy approach is based on the proprietary paradigm of personal data (ownership), which can be sold by accepting terms and conditions (the so-called "third party doctrine"). However, using this Common Law legal background to understand and decipher the GDPR provisions (designed according to Civil Law) is incorrect, as it works according to a different legal paradigm. For the European conceptualisation of Privacy rights, privacy belongs to the personhood right (such as dignity, name, image, self-determination and so on) and it descends directly from fundamental rights, as accorded by article 7 and 8 of the European Charter of Fundamental Human Rights. Therefore, under the European Civil Law privacy conceptualisation, data subjects can dispose of their privacy rights by licencing their use to data controllers under the conditions that the GDPR provides. Hence, in Europe, data subjects do not own their data and cannot sell them and, accordingly, every translation of GDPR provisions in this light is legally incorrect. It follows that many US-oriented Privacy and Security approaches to solve privacy issues can turn out to be legally incorrect, or perhaps just insufficient, to tackle the legal problems related to Privacy rights, as fundamental human rights.

[76] Held by what Henderson and Burnies defines as a "community leader" (Henderson and Burnie, 2018) p. 5.

[77] GDPR article 4(7).

[78] GDPR article 4(1,2) "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

[79] More precisely, they should have informed the data subject prior to collection, aside from the case of data processing performed on the legitimate interest legal basis ex GDPR Article 6(1)(f).

[80] Article 13 or 14 applies depending on how the data controller obtained the data.

[81] This occurrence would imply both the control of the majority of the nodes and a massive computational capacity that ordinary CPUs – even in pools – do not afford.

[82] GDPR article 5(2) and Section "Blockchain Distributed e-Ledgers and Privacy Issues."

can be exploited for unlawful profiling purposes on the personal data contained in the system, as both the content and metadata of the block may be tracked and exploited to micro-target the data subjects (Riva and Barry, 2019).[83,84] This fact also has a legal basis in the rule provided by article 9(2)(e) of the GDPR in which publicly disclosed personal data could be used without the consent of the data subject.[85] In light of this, the unfortunate wording of article 9(2)(e) creates a loophole that exposes data subjects to any uncontrolled data exploitation for personal information that appears to be publicly disclosed. The only barrier to this kind of exploitation is that the rule demands that the information is manifestly made public by the data subject, but it appears to be an insignificant requirement. Indeed, regarding publicly disclosed information, it may be argued that if one finds personal information related to someone else in a public register,[86] this may be sufficient to presume that the information is compliant with the requirements of article 9(2)(e).

On the one hand, neither pseudonymisation (D'Acquisto and Naldi, 2017) nor encryption[87] seem to solve the problem (Daoui, 2019), as it has already been proven that it is possible to reconstruct the user's identity with semantic analysis of the metadata generated by the blockchain (Ron and Shamir, 2013). Furthermore, anonymous transactions undermine the primary element of stability, trust, and accountability of any socio-legal relationship, namely the imputability of actions to a specific subject. Indeed, complete anonymisation, even if it was possible through a high level of encryption, creates an obstacle for the usability and service trust of the blockchain itself. This is especially true in economic, IoT and e-Health environments, which require a high degree of transparency, accessibility, and accountability. Indeed, we must bear in mind that applied e-Ledgers must serve the primary purpose to certify the continuity and validity of transactions (or actions) in the system, to create a stable and reliable record system. No system is stable or reliable if there is no accountability and in turn, accountability cannot exist without identification, for imputability purposes, as seen above.

This is a simple legal equation and cannot be solved using encryption or avoiding addressing the key point of the lack of data controllers. Thus, it seems that the already mentioned "Privacy dilemma" that exists between ledger distribution and anonymisation may be unsolvable unless a different kind of solution is proposed.

## Black Box Issues for Intelligent System Analyses Performed on the Blockchain

Blockchain can be used to run Intelligent Systems (IS) such as Computational Law systems or Smart Speaker interfaces[88] in order to manage the information contained in the blockchain itself. When this information involves personal data management, Data Protection applies.

Any decision that is made on the analysis of meaningful information requires a certain level of abstraction, which, in turn, implies interpreting ability. In legal situations (social relationships with legal effects), every legal interpretation, as well as the reasoning linked to it, must be justifiable. Particularly when it comes to legal decisions made by judges, the motivation for the practical application of a specific interpretation is what ensures the Rule of Law. Indeed, the legal decision cannot be arbitrary and must follow the mandatory legal canons provided by the legal system. The decision must therefore be coherent, logical, adhere to the legal provisions, and be justifiable in every step of the reasoning. These safeguards help to ensure the accountability of the decision itself. The benefit of this approach is evident when interpreters make bad (judicial) decisions, because it enables the system to observe patterns of behaviour, to provide alternative remedies for reviewing the decision, and to ensure the correct application of the law. The "appeal" stage of a trial plays this role, and it can be seen as a method to address the bugs of the system and to grant an acceptable error-rate outcome.

Blockchain technology could serve as a potential solution to part of this problem. As a reasoning- log tool, a blockchain framework could be used to ensure that an analytical IS run on the chain to elaborate data can be explained in every step of the analytical process (right to explanation).[89] According to this perspective, a blockchain black-box log system[90] developed to respond to the need of explainable IS decision process, should mimic all the passages that the computational algorithm performs in its legal analysis, by issuing a block in the chain for each step. This procedure should ensure that the legal reasoning can be retreaced, i.e., each consequential logical step can be traced backwards. Also, this blockchain mirror system would require a permanent (and separate) register for the whole Intelligent System activity in order to allow an ex-post reconstruction of its analyses and performances. We could refer to it as a "twin e-ledger." Although this may seem too demanding in terms of infrastructure, architecture and complexity, the necessity of providing a piece of evidence for both reasoning or practical effects (such as in a Smart Contract) would implicitly and mandatorily require a blockchain log register to be maintained,

[83] Even Satoshi Nakamoto worried about it, *ibid*. (n 7): She/he (they!) argues (argue) that "privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous." However, the author also states that "the risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner."

[84] Cf. also Ron and Shamir (2013) in which how it is possible to presume users' characteristics by simply looking at the network of transactions undertaken by any account is empirically demonstrated.

[85] Moreover, Article 95 states that "This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connexion with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC."

[86] Here public means that the register is intended for public needs, such as the commercial register in Chambers of Commerce, or Tax registers in some countries, for instance.

[87] CNIL, Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, 06 November 2018, available at https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data, last accessed 17.02.2020.

[88] Also known as Speech Interfaces, Conversational Agents, and Digital or Virtual Assistants.

[89] As derived from Article 22 of the GDPR.

[90] i.e., a parallel log record ledger for the principal Blockchain, which aims to ensure the traceability of the activities performed on the chain.

which could also serve this same need for explainability in Internet of Things ecosystems. In turn, these legal solutions would require an accountable entity to manage the system.

## Blockchain-Based Smart Contracts and Data Protection

Smart contracts are one of the many blockchain-based applications for the Law,[91] and they could meet the requirements of those business fields in which standard transactions can be automated. This technology allows computer-coded transactions to automatically execute all or parts of an agreement that underpins a relationship between different parties (Cuccurru, 2017). Practically speaking, this allows an industrial supply relationship to be automated in a way that manages payments when and as certain events occur in the supply chain.

The benefit of this system is evident in industrial and business applications and may be applied to IoT smart environments as well, despite the risks that it still faces (See Kolluri et al., 2018). Nevertheless, it should be remembered that smart contracts actually represent only a technological upgrade to the technical infrastructure underpinning these relationships.

Legally speaking, smart contracts have some practical limitations because their effects in some cases bypass and therefore conflict with some general legal principles, regulations, and contract law provisions.[92] Indeed, one general provision that might clash with smart contract's self-enforcement rules is the "*ne cives ad arma ruant*",[93] which informs the whole Rule of Law of Civil Law systems. This principle must be read in combination with many contract law principles, which are aimed at ensuring symmetrical positions,[94] fairness,[95] and avoiding *contra legem*[96] dispositions in private agreements. For instance, in the supply agreement example, if the goods supplied are damaged, the counterparty may want to suspend the payment but would be prevented by the automated execution of the smart contract. Thus, the party affected by the damaged goods would either be required to pay the sum, or it could try to block the payment (which is increasingly difficult when the process is automated) and suspend any further supply. In both scenarios, the party suffers damages. These scenarios become more dangerous if provisions in a smart contract directly contravene a law or suggest that no law applies inside of a smart contract. However, these issues could be overpassed if an accountable entity manages the system that runs the smart contracts, as this entity could intervene upon request of the parties to suspend the automation. This accountable entity would also play the role of data controller for the personal data entered, or however processed, within the system in general and the smart contract in particular.

Indeed, blockchain-based smart contracts involving personal data could, however, be beneficial for ensuring both effective protection for the data subject, and the data controller's compliance with the GDPR informed consent requirements. Smart contracts could also be adopted for creating smart consent forms, in which both data subjects and controllers could keep track of the real-time data processing and related compliance when performed by an Intelligent System using blockchain technology. In this way, data subjects (consumers, in general) could even be aware of when their personal data is the subject of a smart transaction between third parties and this would improve the data subject's control over their data and privacy.

## Blockchain-Based Automated Decision and the Human-in-the-Loop Incongruity

When blockchain-based IS performs any interpretative activity which may involve the concept of decision based on personal information, it affects the Data Protection regime for automated decisions. In order to apply to this situation, Article 22 of the GDPR requires that the decision based on automated processing or profiling must have legal or significant effects on the data subject. This can be the case in IS decisions performed in blockchain-based systems for smart contracts, e-Health or IoT services when they involve personal data processing.

Automation is a key concept in the GDPR, as it is strictly linked to the notion of data processing and it is referred to in a wide variety of specific provisions in the regulation itself.[97] In addition, the GDPR addresses automation relating to both the measures that a data controller must implement to protect data subjects' rights and personal data. Indeed, the Regulation even seems to implicitly encourage the adoption of those "appropriate technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance"[98] with the law. Other provisions appear to indirectly refer to the same concept, for instance in relation to Data Protection Impact Assessment[99] (DPIA), data processing ledger[100] and coordination with the Data Protection Authority[101] (DPA). Many managing

[91] A smart contract is an automated tool to govern legal relationships. The term is used to describe computer code that automatically executes all or parts of an agreement. The system relies on a blockchain-based platform, and the code can either totally rule the agreement between the parties or integrate it to execute particular provisions of an ordinary text-based contract. The terms of the agreement are codified as structured data into the code, which in turn is embedded into the chain and distributed across multiple nodes. The smart contract begins its execution when the parameters determined by the parties in the agreements occur. When it is executed, new blocks are added to the chain, rendering the transaction permanent and immutable. Smart contracts are not necessary to run a CL system, this is merely one of their applications (See Kolluri et al., 2018; Levi and Lipton, 2018).

[92] At least for what concerns Civil Law systems and connected international transactions.

[93] Literally means "in order to prevent citizens to fight (with weapons)" and refers to the general need for a Legal System to avoid, thanks to the legislative action, people fighting (which may be violent) each other directly to protect arbitrarily their own interests. The principle aims to ensure peaceful coexistence in which all disagreements between parties are decided by an impartial third-party (the judge) with judicial power to decide in a binding manner according to the law.

[94] Prevention of abuse of a dominant position [See Council Regulation (EC), 2002].

[95] Which may be interpreted as comprehending "good faith," which is a principle that applies automatically to contractual relationships in Civil Law systems, even if the parties exclude it contractually.

[96] Literally means "against the law" and refers to all those clauses or agreements that are directly contrary to some positive legal provision or to some principle and, therefore, not only these contractual clauses are not enforceable but they can also be null and invalidate the whole contract relationship.

[97] GDPR Articles 2, 4, 15, 21, 22, 35, 47 and Recitals 15, 63, 67, 68, 71, and 105.

[98] GDPR Article 24.

[99] GDPR Article 35 and cf. Article 32.

[100] GDPR Article 30.

[101] GDPR Articles 31, 33, 36.

softwares are already in place to help entities and professionals keep track of their data processing and manage the correct features in compliance with the regulation. In this sense, a blockchain-based IS could support these management tools into the performance of dynamic processes with a real-time compliance check analysis, ensuring log recording and dynamic processing ledgers (the abovementioned "twin e-ledger"). Again, the appointment of a data controller is a pivotal requirement to ensure that the system complies with the GDPR and that these features can be adopted correctly.

On the other hand, the GDPR addresses the concept of automatisation in reference to the potential threats for data subjects' fundamental rights, created by the invasive power of profiling techniques and related technologies that exploit automated decision processes. With the advent of blockchain-based technologies, RPA, Smart Contracts and Computational Law system for the self-management of user privacy (and more generally, for all those interactive AI interfaces, such as smart speakers), Article 22 of the GDPR related to automated individual decision-making[102] may represent a factual barrier. Indeed, said provision requires the so-called human-in-the-loop for the automated data processing that produces legal effects concerning data subjects, especially when it comes to automated e-Ledgers. The provision refers to "decisions," "legal effects" or just significant implications that concern the data subjects.

Many of the implications come from the taxonomy of "decision." In general, "automated decision-making" is defined as "the ability to make decisions [solely] by technological means without human involvement".[103] However, neither the WP29 guidelines in notes, nor other official opinions[104] on the related matters provide a specific definition of what must be considered to be a decision. Given the general definition of "decision" as the conclusion or resolution reached after consideration,[105] it is unclear whether automated data processing management through blockchain-based systems fall into the GDPR regime or not. D The dividing line between one solution or the other depends on the semantics of the term "consideration." Indeed, if we refer to it as the activity to comprehend both the situation and the impact of a decision, a machine system definitely does not fall under that definition, as this is a typically human interpretative process. Instead, if we refer merely to the process of analysing a pattern and deriving the logical consequences in relation to the set of pre-defined parameters, we can certainly consider it to be a decision.

This point is crucial to understand whether Article 22 disciplines blockchain-based systems, which appears likely. In this scenario, this would create an incongruity, as blockchain-based Intelligent Systems created to empower data subjects with real control over their personal data and related records could not function unless mediated each time by a human who ratifies it.[106]

The solution may be to allow the data subject itself to make the decision in real-time, but this would undermine the benefits of automating the whole set of data processing through an intelligent e-ledger system. In this sense, the only extensive normative interpretation that would preserve the automation feature would be to consider the data subject's choices for set-up options for the blockchain architecture configuration as the "human intervention" required by the law (but this activity should be performed in advance). However, even this approach may clash with the general interpretation, as the human intervention must occur at the end of the process and cannot be general and preventive. This shows that despite the novelty of the GDPR, some parts of it represent a regulation which is neither up to date nor able to correctly tackle current socio-technological needs.

## CENTRALISED SIDECHAIN ENTRUSTED TO ACCOUNTABLE ENTITIES AND "PRIVACY BY LAYERS" AS POTENTIAL SOLUTIONS

From the analysis performed, two pivotal related aspects emerged concerning the conflicting relationship between blockchain and Privacy. First, the distributed nature of e-Ledgers makes it impossible to appoint a data controller, which undermines accountability and, in a cascade effect, all consequential Data Protection requirements for a data processing relationship,[107] i.e., legal basis, data subject's information, purpose definition, data processing framework definition, DPIA, appointment of data processors, and security duties. Secondly, a conflict emerges with

[102] GDPR Article 22 "Automated individual decision-making, including profiling:

(1) The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

(2) Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or:
(c) is based on the data subject's explicit consent.

(3) In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

(4) Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place."

[103] WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP251rev.01.

[104] European Data Protection Supervisor opinion on online manipulation and personal data, Opinion 3/2018.

[105] Decision, Merriam-Webster dictionary, https://www.merriam-webster.com/dictionary/decision (last visited November 25, 2019).

[106] However, the WP29 guidelines underline that this should not be the case and, instead, the human intervention in the decision-making process should be substantial.

[107] The data processing relationship is the relationship established between a data controller and a data subject whenever personal data processing occurs.

the anonymity paradigm, which does not solve the real issues concerning Privacy Law and Data Protection and complicates the legal need for imputability of actions in legal relationships.

The legal solution to the equation can be both simple and quick to implement and consist merely of abandoning the distribution dogma of blockchain and surpassing both the mere security conceptualisation of Privacy and related anonymity aspects. As noted, sidechains differ from blockchain because they rely on centralised architectures and this can be the key to addressing all the issues described above (**Figure 3**). From a legal perspective, blockchain has existed offline for centuries and it is a basic way of keeping track of situations over time that are relevant for society in some specific domain. Logbooks solved the need for recording transactions and their timestamp for a long time. When the ledger has to serve as proof for public trust, the validity of the transaction and the certainty of the timestamp is certified by a trusted entity. Notaries play this role in Civil Law systems and they must be trained experts in Private Law to ensure their high level of competence,[108] as well as belonging to a professional guild with deontological codes to ensure they carry out their duties ethically and fairly, aside for their personal liability.

In terms of blockchain-based e-Ledgers, States may appoint a trusted private party[109] for control – and subsequent accountability – in the chain, as well as the ability to validate the legality of the content and to modify the entire chronology of the chain or metadata related to the blocks, if required. This may be the case for thorough application of the right to be forgotten but may also allow only erasure of the latest block content, preserving the record of the previous ones. This is precisely what happens with offline commercial registers for the Chamber of Commerce (Pollicino and De Gregorio, 2017). Indeed, the old-fashioned legal solution of creating an institutional legal body,[110] may be the perfect approach to solve the issue even for this highly technological phenomenon. This solution can also identify a precise data controller that can be accountable for any illicit or unlawful data processing. In this sense, the way to ensure both the functioning of the blockchain system and compliance with Data Protection regulatory framework is to provide clear procedures and rules for this kind of certification activity, as is the case with notaries, for instance.

The need for a transparent blockchain and the opposing need to ensure the privacy rights of the individual can be solved with what can be called a "Privacy by Layers" approach, in which the data controller maintains the overall transparent chain and publicly releases a pseudonymised chain or a minimised personal data chain. External individuals can then access this e-Ledger using log systems and based on legitimate interest or by declaring their purpose, as is the case for administrative data access in many jurisdictions.[111] This resilience can be ensured with tokens or dual authentication security accesses and controlled access.[112] If someone wishes to access specific block content, they may make a request for said access by providing reasons and legitimate interest. This solution also ensures the abovementioned concept

[108] Which is furthermore assessed through examinations performed as public competitions.

[109] More precisely: an identified legal body.

[110] Such as notaries, Chambers of Commerce or recognised professional organisations.

[111] Consider, for instance, the Italian FoIA (Freedom of Information Act), Legislative Decree 97/2016.

[112] For both the miners as well as for general public outside of the chain.

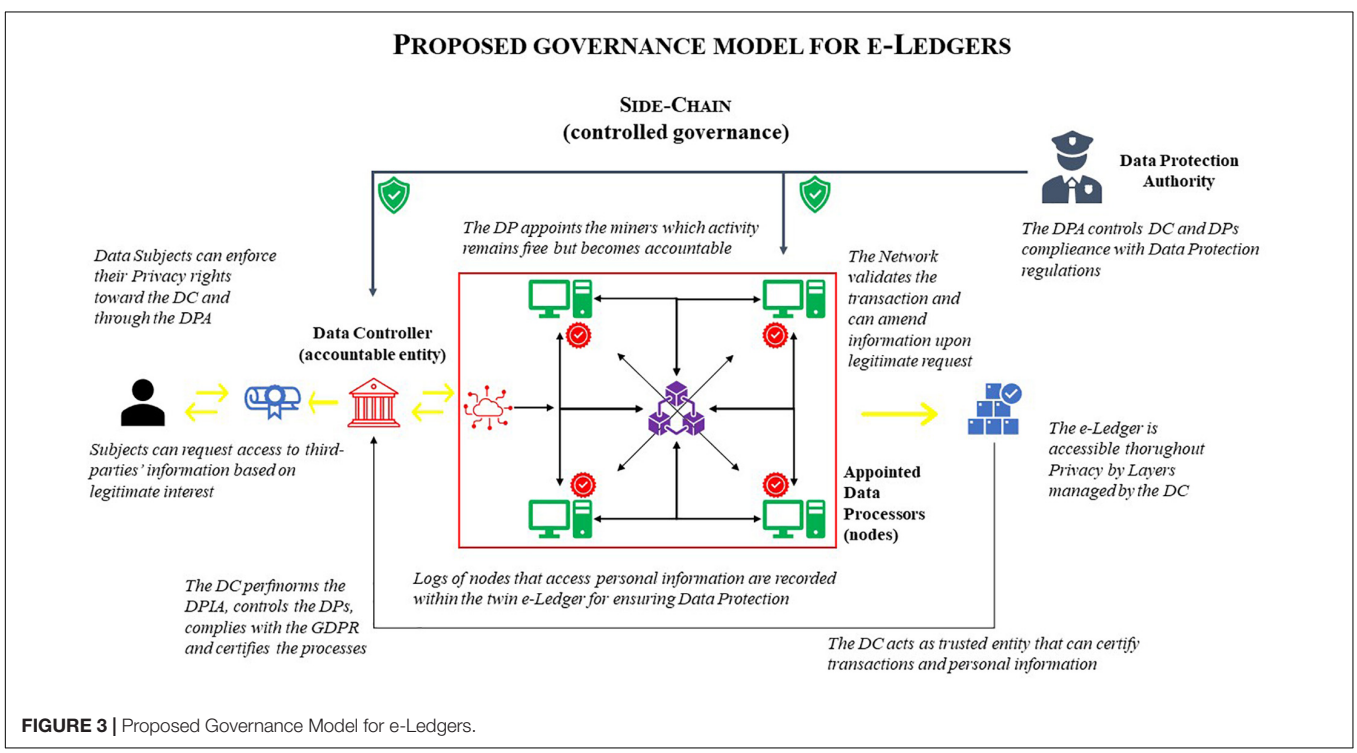


**FIGURE 3 |** Proposed Governance Model for e-Ledgers.

of public accessibility. Furthermore, this solution would also work to check the internal logs to personal information as performed by the nodes, that would be appointed by the data controller as data processors. It must be noted that a centralised blockchain does not imply that the nodes or storage cannot be designed using distributed architecture. The element that must be centralised is controlling and managing the complete functioning of the blockchain. This means that what should be centralised is the governance of the blockchain. When this condition is met, the nodes can still be distributed amongst trusted professionals that are appointed as data processors by the e-Ledger central manager, who acts as a data controller. Accordingly, the data controller can manage distributed storage amongst nodes or other third parties appointed as data processors, granting all the security requirements of the GDPR on the basis of DPIA auditing activities. Furthermore, the reward for the nodes can still be granted. Indeed, instead of issuing cryptocurrency for rewarding the miners (data processors), the data controller can pay them actual fees. In turn, the data controller collects the payment for the logging/recording services from both those individuals that perform transactions in the chain and those that request to access the content. This is no different from what happens for offline public registers. Finally, the data controller would inform the data subjects about these aspects in accordance with GDPR provisions.

In other words, this potential solution relies on centralising the control exercised by the legal entity that manages the blockchain architecture and which functions as the data controller. It then can grant a certain degree of accessibility (PbL) to block information to those external parties that demonstrate a legitimate interest and keep record of these accesses.

Other solutions have been proposed or debated by the literature (Berberich and Steiner, 2016; Frosio, 2017; Herian, 2018; Biswas et al., 2019) but they differ from what is proposed here as they rely mainly on technological aspects (anonymisation, pseudonymisation, encryption and system security) rather than on legal aspects, or only partially address the connected issues that this study discusses as a unique phenomenon. Others adopt a reverse approach and describe the blockchain as a solution to foster GDPR compliance (Geelkerken and Konings, 2017; Truong et al., 2019). Furthermore, although the CNIL[113] addressed it,[114] only a few studies have specifically addressed the issue of the data controller and data processor appointment regarding the key privacy problem of the distributed e-Ledgers (Wirth and Michael, 2018). No real practical solution has been proposed in these studies to address the issues as a whole and to combine both technical and legal sides. The solution proposed in this study offers a potential method of solving this problem in a simple factual way[115] and concretely addressing both the need for accessibility and to preserve privacy.

[113] i.e., the French DPA.

[114] See note 79.

[115] i.e., by exploiting a classical legal solution for offline registers based on the "legal analogy," with no need to "reinvent the wheel." The legal analogy is a classical method that legal systems adopt to address and regulate a new phenomenon using a legal regime already in place for another existing phenomenon with which there are common features. For instance, when aviation was invented it was regulated adopting the norms already in place for navigation.

## Blockchain's Data Controllers, Privacy by Layers and the GDPR

The need to appoint a data controller for data processing is a crucial aspect for the GDPR regime.[116] Indeed, all the core elements required by the Regulation[117] to ensure both privacy rights and the principles of data protection are respected call for an accountable entity that can put them into place. For instance, no right of access or portability can be granted to data subjects if they cannot forward this request to a precise and identified entity that has both the legal duty (which implies accountability) and power to perform the actions required to ensure that the legitimate requests are fulfilled. Data controllers are also those legal entities that define the purpose(s) of the data processing. This is another pivotal aspect for complying with the GDPR and encompasses the blockchain entirely. Indeed, any personal data processed, collected, stored or however present in the chain must adhere to a pre-determined purpose set out by the data controller. In turn, the data controller has also the duty to inform data subjects in advance about data processing, as per articles 13 and 14.

It is evident that blockchain architecture in which nodes are anonymous and distributed cannot ensure that any accountable legal entity can be identified and appointed as a data controller. Therefore, designing an architecture in which (at least) one accountable entity is legally responsible for ensuring the GDPR provisions are respected, and aside from any other legal requirement that may apply, is pivotal for ensuring privacy compliance in blockchain protocols. This, however, cannot be done in a "pure"distributed ledger in which nodes are unidentified and there is no central control of the protocol processes.

In this regard, it is worth underlining the conceptual difference between security solutions and Data Protection solutions. Whilst the former addresses the "what," the latter addresses the "how" of data processing. In other words, security ensures that only one particular type of data is processed (anonymous, pseudonymised or encrypted) and focuses on what the data is, and what the architecture is. Data Protection instead focuses on who processes the data and how they are processed. Essentially, within the scope of the GDPR, every kind of data can be processed as long as it is processed according to the principles and provisions provided by the Regulation and within the limits set out by it. Essentially, Data Protection encompasses security, which is only one of the many aspects that compose the whole spectrum of the legal requirements for the protection of personal data.

Privacy by Layers responds precisely to the challenge of how personal data are processed, meaning, in this case, how they are accessed by third parties. Indeed, no personal information is secret merely because it is personal. The GDPR defines it clearly in its scope in Article 1, in which it states that it protects three legal goods: "natural persons with regard to the processing of personal data and rules relating to the free movement of

[116] GDPR articles 24, 26 and 28.

[117] GDPR from article 5 to 22.

personal data," as well as "fundamental freedoms" that stand above the first two. Personal data and the so-called "data flow" can be in direct contrast when representing opposite subjective interests of two or more parties. Therefore, the Regulation and its actors (data controllers, DPA, national legislators, judges and interpreters) must balance the individual privacy rights with the counter interests of the free movement of data on a case by case basis.

This means that depending on the type of service for which the data controller designs the specific blockchain architecture, the legitimate criteria that justify accessibility (PbL) to personal information in the blocks for reasons of public interest or interests relating to the free movement of data (for instance in financial transactions) can be determined.[118] In this case, particular attention shall be paid to the legal status of those requesting access, in order to determine their legitimate interest for accessing personal information. As already mentioned, a key aspect of this is the need to keep a log record of such access, which must contain the identity of the applicant as well as the metadata for the access, in accordance with articles 25,[119] 30[120], and 32.[121]

These provisions, however, should be integrated into both the regulation and ethical code of conduct for the use of personal data in blockchain systems, in order to work properly. These coding solutions should then follow the relevant EU Court decisions regarding the right to be forgotten and other rights protected by the GDPR. Nevertheless, in order for the solution proposed with this study to work, the EU legislator should establish the technical standardisation for blockchain applications. Furthermore, the current European legal framework for private law, competition law and consumer law should be harmonised with the GDPR provisions and the relevant forthcoming regulations.[122]

## CONCLUSION

Blockchain architecture represents an invention that disrupted the previous technological environment by introducing the concept of scarcity online. Its capacity to mimic a timestamp ledger in online relationships allows it to be applied to a wide variety of situations, connected environments, or tools, such as the IoT ecosystem, e-Health applications, RPA solutions and smart contracts. Although blockchain is valued as an excellent tool to implement privacy solutions, with a focus on security aspects, it may actually cause a breach of Data Protection rights, such as the right to be forgotten. These conflicting relationships show how the GDPR loopholes may be exploited for opaque data processing, especially when processing sensitive and publicly manifested data, which do not involve data subject's consent. Nevertheless, if the "public" and distributed architecture of this e-Ledger moves to a centralised and "privately managed" one, these issues can be easily resolved. Indeed, it is possible to allow distributed and recorded access to a block's information (both metadata and content) based on legitimate interest, by granting the control and management of the sidechain architecture to a certified and trusted third-party, ensuring the third parties have recorded Privacy by Layers accessibility when supported by legitimate interest. The latter solution can preserve the essential nature and usefulness of the blockchain and, at the same time avoid the clashes with privacy rights and Data Protection provisions. On the contrary, the solution proposed by this study can precisely respect the promise to enhance privacy rights thanks to blockchain applications (included smart contracts, RPA and Intelligent Systems services) and guarantee both compliance with the GDPR requirements and data subjects' rights. Thus, in order to implement this proposed solution, both the EU and national legislators should define precise technological standards for sidechains as well as the formal and substantial characteristics required for third-party entities to be considered trusted and accountable.

In a digital era in which everything seems to have to be automated, democratised or disintermediated, old solutions can still be valid and useful. In fact, it can be said that the modern need to regulate every stage of a given phenomenon, and to measure every performance, clashes with the original approach of the Law, which focuses on the effects. The Law implicitly recognises that human phenomena are too complicated, too heterogeneous and too expensive to be tracked in every single stage of their process. Thus, the Law adopts a general and abstract conceptualisation of social phenomena and focuses on the regulation of the outcomes that derive from these human interrelations, i.e., the apparent facts. The facts can, indeed, be measured and proven to be true or false, and when this is not possible, the Law uses presumptions and legal fictions to correct the uncertain reality. The same legal mechanisms can be still valid in digital phenomena, and yet this approach can give humans back their central role in managing the technology. Centralised blockchain systems, i.e., sidechains, can still be reliable because the centralisation of management and control is tempered by one of the most powerful technologies that human beings invented: the Law. The Law allows presumptive trust to be granted to those trusted entities that function as e-Ledger managers and provides the mechanisms to ensure that this trust has not been misplaced and remove it (with related punishments for accountable entities) should such an action be required.

Further investigations could focus on a complete analysis of the aspects arising from a centralised "sidechain" infrastructure, in relation to the practical elements that may be compromised to ensure governance and accountability. This kind of analysis can also look more closely at the impact on security aspects, and this may change the risk profile during auditing activities and DPIA procedures. The discussions that would emerge from

[118] In advance and in compliance with the GDPR principles of fairness and lawfulness.

[119] Data Protection by design and by default.

[120] Records of the processing activities.

[121] Security of the processing.

[122] European Commission. Draught Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). COM (2017) 10 final. 2017/0003 (COD).

deepening these analyses can even support the interdisciplinary study concerning the economic impact of specific blockchain infrastructures (cryptocurrency, smart contracts and e-Health systems) in terms of value, business models and contractual methods for lawful transactions.

## AUTHOR CONTRIBUTIONS

The author confirms being the sole contributor of this work and has approved it for publication.

## FUNDING

This research was funded under the EU Horizon 2020 scheme of Marie Skłodowska-Curie Action grant agreement No. 722561.

## ACKNOWLEDGMENTS

The author thanks Dr. Marguerite Barry for her helpful perspective and the invaluable opinions on how the shape the study, without any responsibility for the content.

## REFERENCES

Ackerman Shrier, A., Chang, A., Diakun-Thibault, N., Forni, L., Landa, F., Mayo, J., et al. (2016). *Blockchain and Health IT: Algorithms, Privacy, and Data, (White Paper, Project PharmOrchardTM of MIT's Experimental Learning "MIT Fintech: Future Commerce", 2016)*. Washington, D.C.: Office of the National Coordinator for Health Information Technology U.S. Department of Health and Human Services.

Atlam, H. F., Alenezi, A., Alassafi, M. O., and Wills, G. B. (2018). Blockchain with internet of things: benefits, challenges, and future directions. *Intell. Syst. Appl.* 6, 40–48. doi: 10.5815/ijisa.2018.06.05

Baldwin, J. (2018). In digital we trust: bitcoin discourse, digital currencies, and decentralized network fetishism. *Palgrave Commun.* 4:14. doi: 10.1057/s41599-018-0065-0

Berberich, M., and Steiner, M. (2016). Blockchain technology and the gdpr-how to reconcile privacy and distributed ledgers. *Eur. Data Prot. L Rev.* 2:422. doi: 10.21552/edpl/2016/3/21

Biswas, S., Kashif, S., Fan, L., Boubakr, N., and Yu, W. (2019). A scalable blockchain framework for secure transactions in IoT. *IEEE Internet Things J.* 6, 4650–4659. doi: 10.1109/jiot.2018.2874095

Bolognini, L., Pelino, E., and Bistolfi, C. (2016). *Il Regolamento Privacy europeo*. Milano: Giuffrè, 109.

Buocz, T., Ehrke-Rabel, T., Hödl, E., and Eisenberger, I. (2019). Bitcoin and the GDPR: allocating responsibility in distributed networks. *Comput. Law Secur. Rev.* 35, 182–198. doi: 10.1016/j.clsr.2018.12.003

Chohan, U. W. (2017). *A History of Bitcoin*. Available at: https://ssrn.com/abstract=3047875 (last visited April 1, 2020).

Cong, L. W., and He, Z. (2019). Blockchain disruption and smart contracts. *Rev. Financ. Stud.* 32, 1754–1797. doi: 10.1093/rfs/hhz007

Council Regulation (EC) (2002). *Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty (TFEU)*. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32003R0001 (accessed April 1, 2020).

Cuccurru, P. (2017). Beyond bitcoin: an early overview on smart contracts. *Int. J. Law Inform. Technol.* 25:182.

D'Acquisto, G., and Naldi, M. (2017). *In Big Data e Privacy by Design*, F. Pizzetti (eds). Torino: Giappichelli editore, 117.

Daniels, J., Sargolzaei, S., Sargolzaei, A., Ahram, T., Laplante, P. A., and Amaba, B. (2018). The internet of things, artificial intelligence, blockchain, and professionalism. *IT Profess.* 20, 15–19. doi: 10.1109/mitp.2018.2875770

Daoui, S. (2019). *GDPR, Blockchain and the French Data Protection Authority: Many Answers but Some Remaining Questions*. Available at: https://stanford-jblp.pubpub.org/pub/gdpr-blockchain-france (last visited April 1, 2020).

Di Ciommo, F. (2017). Privacy in europe after regulation (EU) No 2016/679: what will remain of the right to be forgotten? *Ital. Law J.* 03, 623–646.

Diffie, W., and Hellman, M. E. (1976). New directions in cryptography. *IEEE Trans. Inform. Theory* 22, 644–654.

Fabiano, N. (2017). "The internet of things ecosystem: the blockchain and privacy issues. The challenge for a global privacy standard," in *International Conference on Internet of Things for the Global Community – IoTGC 2017/2* (Madeira: University of Madeira).

Frosio, G. (2017). *Right to Be Forgotten: Much Ado About Nothing. SSRN Scholarly Paper*. Rochester, NY: Social Science Research Network, 31.

Galuba, W., and Girdzijauskas, S. (2009). "Peer-to-peer system," in *Encyclopedia of Database Systems*, eds L. Ling, and M. T. Özsu (New York, NY: Springer), 2081–2082.

Geelkerken, F. V. J. V., and Konings, K. (2017). "Using blockchain to strengthen the rights granted through the GDPR," in *Litteris et Artibus: мат epianu* ( Видавництво Львівської політехніки), 458–461.

Henderson, A., and Burnie, J. (2018). Putting names to things: reconciling cryptocurrency heterogeneity and regulatory continuity. *J. Int. Bank. Finan. Law* 33:4.

Henry, R., Herzberg, A., and Kate, A. (2018). Blockchain access privacy: challenges and directions. *IEEE Secur. Privacy Mag.* 16, 38–45. doi: 10.1109/MSP.2018.3111245

Herian, R. (2018). Outputs regulating disruption: blockchain, GDPR, and questions of data sovereignty journal item. *J. Int. Law* 22:1. doi: 10.1093/oso/9780198842187.003.0001

Holland, M., Stjepandić, J., and Nigischer, C. (2018). "Intellectual property protection of 3d print supply chain with blockchain technology," in *Proceedings of the 2018 IEEE International Conference on Engineering, Technology and Innovation* (Stuttgart: ICE/ITMC).

Juhász, P. L., Stéger, J., Kondor, D., and Vattay, G. (2018). A bayesian approach to identify bitcoin users. *PLoS ONE* 13:e0207000. doi: 10.1371/journal.pone.0207000

Kolluri, A., Nikolic, I., Sergey, I., Hobor, A., and Saxena, P. (2018). *Exploiting the Laws of Order in Smart Contracts*. Available at: https://arxiv.org/abs/1810.11605 (last visited April 1, 2020).

Kshetri, N. (2017). Blockchain's role in strengthening cybersecurity and protecting privacy. *Telecommun. Policy* 41:1030.

Levi, S. D., and Lipton, A. B. (2018). *An Introduction to Smart Contracts and Their Potential and Inherent Limitations. Skadden, Arps, Slate, Meagher & Flom LLP*. Available at: https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/ (last visited April 1, 2020).

Liu, W., Zhu, S. S., Mundie, T., and Krieger, U. (2017). "Advanced block-chain architecture for e-health systems," in *Proceedings of the 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)* (New York, NY: IEEE), 1–6.

Madakam, S., Holmukhe, R. M., and Jaiswal, D. K. (2019). The future digital work force: robotic process automation (RPA). *JISTEM – J. Inform. Syst. Technol. Manage.* 16, 1–18.

Mantelero, A. (2016). Right to be forgotten and public registers – A request to European Court of Justice for a preliminary Ruling *EDPL – Eur. Data Protect. Law Rev.* 2, 231–235. doi: 10.21552/edpl/2016/2/14

Mettler, M. (2016). "Blockchain technology in healthcare: the revolution starts here," in *Proceedings of the 2016 18th IEEE International Conference on e-health Networking, Applications and Services (HealthCom)* (New York, NY: IEEE).

Morrar, R., Arman, H., and Mousa, S. (2017). The fourth industrial revolution (Industry 4.0): a social innovation perspective. *Technol. Innovat. Manage. Rev.* 7:11.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-peer Electronic Cash System*. Available at: https://bitcoin.org/bitcoin.pdf (last visited April 1, 2020).

Pizzetti, F. (2017). *Intelligenza Artificiale, Protezione dei Dati Personale e Regolazione*. Torino: Giappichelli, 25.

Pollicino, O., and De Gregorio, G. (2017). Privacy or transparency? A new balancing of interests for the 'right to be forgotten' of personal data published in public registers. *Ital. Law J.* 03, 647–667.

Rampini, R. (2015). *Rete Padrona*. Milan: Feltrinelli.

Raskin, M. (2017). The law and legality of smart contracts. *Georgetown Law Technol. Rev.* 304:37.

Rheingold, H. (1993). *The Virtual Community. Homesteading on the Electronic Frontier*. Boston, MA: Addison-Wesley.

Riva, G. M., and Barry, M. (2019). Net Neutrality matters: privacy antibodies for information monopolies and mass profiling. *Publicum* 5:2.

Rivest, R., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* 21, 120–126. doi: 10.1145/359340.359342

Ron, D., and Shamir, A. (2013). "Quantitative analysis of the full bitcoin transaction graph," in *Financial Cryptography and Data Security*, ed. A.-R. Sadeghi (Berlin: Springer), 6. doi: 10.1007/978-3-642-39884-1_2

Seybou Sakho, S., Zhang, J., Mbyamm Kiki, M. J., Kouassi Bonzou, A., and Essaf, F. (2019). Privacy protection issues in blockchain technology. *Int. J. Comput. Sci. Inform. Secur. (IJCSIS)* 17:2.

Sutton, A., and Samavi, S. (2017). "Blockchain enabled privacy audit logs. international semantic web conference ISWC 2017: The Semantic Web," in *Proceedings of the 16th International Semantic Web Conference (ISWC)*, Vienna, 645–660. doi: 10.1007/978-3-319-68288-4_38

Truong, N. B., Kai, S., Gyu, M. L., and Yike, G. (2019). GDPR-compliant personal data management: a blockchain-based solution. *IEEE Trans. Inform. Foren. Secur.* 15, 1746–1761. doi: 10.1109/tifs.2019.2948287

Wirth, C., and Michael, K. (2018). "Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data," in *Proceedings of 1st ERCIM Blockchain Workshop 2018* (Siegen: European Society for Socially Embedded Technologies (EUSSET)), 2018.

Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H. (2017). "An overview of blockchain technology: architecture, consensus, and future trends," in *Proceedings of the 2017 IEEE 6th International Congress on Big Data*, Honolulu, HI.

Zyskind, G., Nathan, O., and Pentland, A. S. (2015). "Decentralising privacy: using blockchain to protect personal data," in *Proceedings of the 2015 IEEE Security and Privacy Workshops, 2015/05*, San Jose.

**Conflict of Interest:** The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.