ISSN: 2409-6911
(CC-BY) 4.0 license
www.austrian-law-journal.at
DOI: 10.25364/01.8:2021.2.3

The Digital Avatar on a Blockchain: E-Identity, Anonymity and Human Dignity

Nora Schreier,* Graz

Robin Renwick,* Ireland

Tina Ehrke-Rabel,* Graz

Abstract: In order to comply with specific regulations (eIDAS, Payment Services Directive, Anti-Money Laundering Directive) and reduce risk profiles, financial service providers increasingly collect large amounts of information from their customers. The increasing opportunities and technical means for data collection afforded from digitalisation raise legal concerns related to proportionality, necessity, and data minimization. However, the concerns go beyond just GDPR compliance and legislative balance, as distinct architectures and technological deployments potentially impact rights, freedoms, and ethics. This paper will address the issue by examining aspects of digital identity, especially those that have proposed the use of a permissioned distributed ledger or blockchain as architecture for know your customer and onboarding evidential frameworks, using specific hashing schemes that derive unique identifiers from the combination of specific personal data points. Evidence is appended to a data structure, for the purpose of auditing and/or record keeping, potentially ensuring an immutable record of events is maintained. After elaborating on the notion of identity in the digital sphere and the applicability of the GDPR to such a data structure, the discussion will be developed to critically assess the current trend towards using the financial institutions' customers' mobile devices as interfaces to the distributed data structure and the legal and sociological implications of this technological development. The potential impact of the analysis goes beyond digital identity within the finance sector, positioning the discussion towards approaches for e-governance and the regulation of digital identity in a way that human dignity is

* Mag.ª Nora Schreier, Department of Tax and Fiscal Law, University of Graz.

* Dr. Robin Renwick, Trilateral Research Ireland.

* Univ.-Prof.in Dr.in Tina Ehrke-Rabel, Head of the Department of Tax and Fiscal Law, University of Graz.

This publication is based on research undertaken in the EU funded SOTER project which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833923. Although the publication was inspired by the underlying ideas and principles relating to the use case developed in the SOTER project, it does not reflect and does not intend to reflect the actual deployment of the project's use case.

Fundstelle: *Schreier/Renwick/Ehrke-Rabel,* The Digital Avatar on a Blockchain: E-Identity, Anonymity and Human Dignity, ALJ 2021, 202-218 (http://alj.uni-graz.at/index.php/alj/article/view/162).

preserved and the risks of creating a ubiquitous "digital avatar" are adequately addressed by the law.

***Keywords**: digital identity, mobile device, digital customer onboarding framework, financial services, distributed ledger technology, blockchain, privacy, fundamental rights, human dignity, surveillance, accountability, legal responsibility, personal data*

I. Introduction

> "WE CAN, I think, describe cases in which, though we know the answer to every other question, we have no idea how to answer a question about personal identity."[1]

The 21st century has brought with it a host of technologically leveraged socio-economic change. The omniscient internet, rooted in the ubiquitous nature of our relationship with the net-connected device, has altered the way in which the individual interfaces with reality; real, augmented, and virtual. *Floridi* professes that omnipotent information and communication technologies radically alter our sense of self, dispelling incumbent notions of individuality by dualistically evolving our understanding of both the public and the private sphere;[2] reshaping relationships with family, friends, individuals, entities, and government. Modern technologies surreptitiously move us closer to the centre of the 'infosphere', a world in which corporations gain considerable power and control over our digital lives, entrenching us in an explicit power imbalance as they mine the data we generate for behavioural insights,[3] predictive personalization,[4] and profit.[5] The existent incentives in play for digital traceability have focused efforts on digital identity as companies seek to attach unique, robust, and persistent identifiers to individuals as they traverse the open internet: browsing, shopping, and interacting with forums and applications. The trend towards mobile interfaced product and service provision has hastened the distinct need for an interoperable, secure, inclusive, and privacy-respecting system to be developed. Formal electronic identity (e-ID) systems have been deployed in jurisdictions within Europe (Estonia - e-ID) and further abroad (India - Aadhar), intended for use with both public and private sector services. However, considerable obstacles remain for digital identity-based technologies to achieve broad adoption, as ideological, technological, legal, and ethical questions have yet to be answered adequately.[6] While digital identity has potential to ease friction in the European Digital Single Market, there is no universally agreed method for achieving the aims of such a system, nor have the system

[1] *Parfit,* Personal Identity, 80 The Phil. Rev. 3, 3 (1971).

[2] *Floridi,* The Fourth Revolution: How the Infosphere is reshaping Human Reality (2014).

[3] E.g. *Alzubaidi/Kalita,* Authentication of Smartphone Users Using Behavioral Biometrics, IEEE Communications Surveys & Tutorials (2016) 1998; *Mahfouz et al.,* A Survey on Behavioral Biometric Authentication on Smartphones, J. of Info. Sec. & Applications (2017) 28.

[4] *Yeung,* Five Fears about Mass Predictive Personalization in an Age of Surveillance Capitalism, Int'l Data Priv. L. (2018) 258.

[5] See *Zuboff,* The Age of Surveillance Capitalism (2019) 27–198.

[6] See *Priv. International,* A Guide to Litigating Identity Systems https://privacyinternational.org/learning-resources/guide-litigating-identity-systems (last visited November 12, 2021).

requirements been adequately communicated across all sectors. Topics such as privacy, data protection, inclusivity, fundamental rights, and structural power imbalance continually surface as architectures are proposed.[7] At the forefront of this conversation is the financial services sector.[8] The emergence of the open-banking era has foregrounded the distinct need to provide a secure banking customer identification and authentication method, which can simultaneously provide for the needs of risk mitigation on behalf of the banks, whilst reducing onboarding costs. These efforts have been further buttressed by regulatory instruments such as the Anti-Money Laundering Directive, the Payment Services Directive and eIDAS regulation, as the Commission has sought to establish a technologically neutral legislative base for the deployment of cross-jurisdiction e-ID provision. This paper will provide an overview of digital identity and distributed ledger technology, providing insight into the nature of the current debate on the matter. Some of the key legal complexities at the heart of ongoing discussions will be detailed, shedding light on legal grey areas, whilst discussing potential ramifications and implications from legal, ethical, and privacy-orientated perspectives. While digital identity promises significant value, there are fundamental threats to existing European rights and freedoms should such systems be deployed. This is especially the case as financial service providers are closely related to state authorities, being highly involved in various crime detection schemes (in regard to money laundering, tax or payment fraud), either acting as agents of, or being (partially) publicly funded by, the state. Insight will also be provided into the nature of the interface – the mobile phone – in an attempt to understand how the device acts simultaneously as a gateway for digital identity, and the interface into our most personal and sensitive data-driven lives. Bridging the two brings with it enormous potential and substantial dangers – especially if the gateway is controlled and maintained by unscrupulous actors.

II. Digital Identity and Distributed Ledger Technology

The concept of digital identity emerged long before the creation, adoption and acceptance of distributed ledger technology. Identity has always been a cornerstone of society, a concept that binds one's understanding of the self, one's relationship with the external world, and perhaps most importantly the external world's relation to oneself. *Parfit* elucidates the notion of identity, framing it as a derivation of the nuanced relationship between mind and body – an extension of "Cogito, ergo sum" (I think therefore I am), the basis for Cartesian duality[9] – through a concept termed 'psychological continuity'.[10] *Parfit* outlines the notion of one's identity as being situated in psychology (the mind) more than physiology (the body). This territorialises identity further into realms of personality, amassed experience, memories (q-memory),[11] and the formation of 'the self'.

[7] See *Gstrein/Kochenov,* Digital Identity and Distributed Ledger Technology: Paving the Way to a Neo-Feudal Brave New World? Frontiers in Blockchain (2020) 1.

[8] See *Kaiser,* Privacy and Identity Issues in Financial Transactions: The Proportionality of the European Anti-Money Laundering Legislation (2018) (Ph.D. dissertation, University of Groningen) (on file with the University of Groningen Library).

[9] Cf. *Descartes,* A Discourse on the Method of Correctly Conducting One's Reason and Seeking Truth in the Sciences (Ian Maclean ed. & trans., Oxford World's Classics 2006) (1637) 28–34.

[10] *Parfit,* Personal Identity, 10.

[11] *Parfit,* Personal Identity, 14.

An OECD working paper recognises the dichotomy between self and identity through the concept of 'personhood', told through the lens of the information age.[12] The authors note:

"Law and technology must be crafted to respect certain 'Properties of Identity' in identity management (IDM) in order for the information society to be free and open. Respect for the Properties of Identity is necessary for data protection; data protection is necessary for accountability; and accountability is necessary for trust."[13]

Rundle et al foreground the philosophical roots of identity by conveying how and why trust, accountability, data protection, and user control are key to any successful, respectful, and human-centric IDM system.[14] By pointing to philosophers Locke and Hegel, the authors situate the conversation in concepts of 'the person' – framing the relationship between citizen and state through a formal legislative lens. More importantly, the authors acknowledge that IDM systems might potentially undermine notions of personhood, reminding us that fundamental rights are attributable to a person and not to any conveyance of digital identity (or the set of identifiers). This nuanced distinction opens up discussion surrounding the explicit need to protect and preserve the digital integrity of the individual[15] in order to safeguard, protect, and preserve the rights, freedoms, privacy and physical, legal, and ethical integrity of the person; especially pertinent as society ventures further into an information age, where one interacts as a digital agent as much (if not more than) as a physical agent – often engaging in augmented spaces where the lines between real and virtual begin to blur.[16] Indeed, the basic concept of legal subjectivity requires that individuals have rights and duties: They can be held accountable for their actions but at the same time are entitled to the protection of their fundamental rights, as only the guaranteed protection of fundamental rights allows for the free development of an individual's identity in the first place. The requirement for protection in this regard is further buttressed at the European level with initiatives to develop and implement a Declaration of Digital Principles,[17] an initiative that provides a pathway for the further protection of the individual and their digital interactions.

Mechanisms for identification and authentication have always been cornerstones of Identity Management systems. In a technologically interfaced world, robust methods for identifying and authenticating users are paramount, primarily to preserve both information security and authorised access.[18] The most common method for this has previously been username and

[12] See *Rundle et al.,* At a Crossroads: "Personhood" and Digital Identity in the Information Society (STI Working Paper No. 2007/7, 2008) https://www.oecd.org/sti/ieconomy/40204773.doc (last visited November 12, 2021).

[13] *Rundle et al.,* "Personhood" and Digital Identity, 4 https://www.oecd.org/sti/ieconomy/40204773.doc (last visited November 12, 2021).

[14] Cf. *Rundle et al.,* "Personhood" and Digital Identity, 6 https://www.oecd.org/sti/ieconomy/40204773.doc (last visited November 12, 2021).

[15] See *Guillaume/Mahon,* Le Droit à l'Intégrité numérique (2021); see *Rochel,* Connecting the Dots: Digital Integrity as a Human Right, Hum. Rts. L. Rev. (2021) 358.

[16] See *Baudrillard,* Simulacra and Simulation (Sheila Glaser trans., University of Michigan Press 1994) (1981) 121–128.

[17] *European Commission,* Declaration of Digital Principles – the 'European Way' for the digital society https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13017-Declaration-of-Digital-Principles-the-%E2%80%98European-way%E2%80%99-for-the-digital-society_en (last visited November 12, 2021).

[18] See *National Institute of Standards and Technology,* Digital Identity Guidelines: NIST Special Publication 800-63-3 (2017) 2 https://doi.org/10.6028/NIST.SP.800-63-3 (last visited November 12, 2021).

password combinations – the username acting as an identifier for a user, and the password as authentication method. The security of the process rests on the hypothesis that only the correct user (the identity holder) will know or have access to the password (the authentication method).

Alongside the apparent loss of permeability and traceability afforded by the increasing interweavement of physicality and digitality, there is a push for greater digital accountability and traceability – as sectors seek to robustly tie individuals to their digital transactions and interactions. This desire is most present in the financial services sector, where legal obligations exist regarding money laundering and terrorist financing. The requirement to maintain evidential registries of customers, to thwart illegal activity, leads us to distributed ledger technology. DLT, initially envisioned as a tool to subvert the existing financial system; a vehicle for the ideological libertarian to disintermediate their existence,[19] has been adopted by mainstream private sector entities (as well as the public sector). Entities seek to implement the data structure in a host of use cases: supply chain management, capital acquisition processes, land registries, etc. One of the potentially most lucrative use cases is identity management – as distributed ledger technology provides a sound technical architecture through which identities and related attributes or credentials may be stored, shared, and verified.

DLT allows for the recording and storing of information (such as personal data of customers relevant for complying with existing Anti Money Laundering provisions) in a transparent, tamper-resistant,[20] resilient, and decentralised way.[21] New information is included within a 'block', which is then appended to the chain after having been validated by the network.[22] Due to the fact that replications of the data stored on the blockchain can be found on computers all over the world,[23] the data structure is highly resilient. Moreover, ex-post changes in the data structure are hard to achieve, as blocks are linked together through the inclusion of the hash of the previous block in the following block's header, rendering the structure tamper-resistant.[24]

The concept of Self-Sovereign Identity (SSI) (seen as one of the cornerstone concepts of modern digital identity architectures) emerged adjacent to the initial forming of DLT technology, as the Web-of Trust[25] initiative forged ahead with methods to link distributed technologies with existing methods for identification and authentication. The concept has since evolved, through the development of a principles-based ideology.[26] At the root of the

[19] See *De Filippi,* Bitcoin: A Regulatory Nightmare to a Libertarian Dream, Internet Pol'y Rev. (2014) 1; *Karlstrøm,* Do Libertarians dream of Electronic Coins? Scandinavian J. of Soc. Theory (2014) 23.

[20] See *Bacon et al.,* Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralized Ledgers, 25 Richmond J. of L. & Tech. 1, 10 (2018) (discussing the properties of distributed ledger technology); see *Low/Mik,* Pause the Blockchain Legal Revolution, 69 Int'l & Compar. L. Q. (2020) 135, 137 (discussing the properties of blockchain technology).

[21] Cf. *Bacon et al.,* Blockchain Demystified 5–6; see *Bechtolf/Vogt,* Datenschutz in der Blockchain: Eine Frage der Technik, ZD 2018, 66 (67); see *Zetzsche et al.,* The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain, U. Ill. L. Rev. 1361, 1371 (discussing the properties of distributed ledger technology).

[22] E.g. *Zachariadis et al.,* Governance and Control in Distributed Ledgers: Understanding the Challenges facing Blockchain Technology in Financial Services, 29 Info. & Org. (2019) 105, 109 (discussing the process of validating new information in a block which is then appended to the previously validated block).

[23] E.g. *De Filippi/Wright,* Blockchain and the Law: The Rule of Code (2018) 34.

[24] *Filippi/Wright,* Blockchain and the Law 22, 36; see *Steinbrück,* Identitätsverwaltung über die Blockchain? Rechtliche Betrachtung am Beispiel des Internets der Dinge, in *Schweighofer et al.* (eds.), Internet of Things (2019) 283 (283–84).

[25] Web of Trust https://github.com/WebOfTrustInfo (last visited November 12, 2021).

[26] *Sovrin,* Principles of SSI https://sovrin.org/principles-of-ssi/ (last visited November 12, 2021).

ideology is the desire to pursue identity systems based on decentralised ideals, moving away from formal top-down, centralised identification mechanisms. The risks in centralised Identity Management Systems originate from vulnerabilities concerning the integrity and availability of personal data, as well as the possibility to link multiple identity attributes together by a single authority or enterprise, providing channels for extremely personalised and valuable insights regarding interactions and behaviour to be drawn.[27] Distributed Ledger Technology has been proposed to overcome this centralised approach,[28] as the data structure, in principle, does not contain a single point of failure.[29]

Although Distributed Ledger Technology has characteristics deemed suitable for a robust and secure identity management system, challenges remain – especially those that impact on specific rights and freedoms of individuals.[30] These challenges are even more pronounced if systems are proposed in a top-down fashion – tools for monitoring identity formation and identity evolution of individuals. DLT provides a structure from which records, entries, and transactions can be trivially linked together or further coupled with associated data sets either explicitly (time stamping and signing), or due to the meta-data leakages from the system (transaction propagation information, transaction hashes, IP address leaks, etc). In this instance, core properties of DLT based identity management systems may become operands of harm, outweighing any presupposed benefits, by altering the balance of power between the formal identity provider (the state) and the identity holder (the person), akin to prefigurative post-political strategy.[31] Moreover, the gateway to the distributed ledger – the wallet holding the user's credentials related to the user's private key – creates a link between the user's "analogue" identity and his "digital" identity – either represented by the hash value of their credentials stored on the blockchain for evidential purposes, or the address for their Decentralised Identifier[32] (DID), which in turn contains information regarding ownership, use, and interactions concerning identity credentials. Additionally, a digital identity wallet stores the credentials which contain both sensitive and non-sensitive personal data, thus security and fraud mitigation measures are required to be implemented to prevent unauthorised access. These mitigation measures often comprise far-reaching device data analysis methods as will be discussed in the following.

[27] Referred to as „Enterprise-Centric-Identity" in *Zanol et al.,* Self-Sovereign Identity und Blockchain, in *Schweighofer et al.* (eds.), Data Protection / Legal Tech (2018) 235 (235).

[28] See *Zwitter et al.,* Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual, Frontiers in Blockchain (2020) 1 (2–10).

[29] *Bacon et al.,* Blockchain Demystified 22; cf. *Zetzsche et al.,* Distributed Liability of Distributed Ledgers 1374.

[30] See *Goodell/Aste,* A Decentralized Digital Identity Architecture, Frontiers in Blockchain (2019) 1.

[31] See *Husain et al.,* Prefigurative Post-Politics as Strategy: The Case of Government-Led Blockchain Projects, The J. of the Brit. Blockchain Ass'n (2019) 1.

[32] *W3C,* Decentralized Identifiers (DIDs) v1.0 https://www.w3.org/TR/did-core/ (last visited November 15, 2021).

III. Legal challenges to using distributed ledger technology as onboarding evidential framework

Although distributed ledger technology promises to constitute a fertile technical environment for concepts of digital identity, the societal implications of implementing the technology should be carefully considered, as deployment of a mandatory digital identity architecture may cement existing power structures and imbalances in power.[33] Concurrently, the use of a permissioned blockchain network as an evidential framework for customer onboarding in the finance sector also poses specific legal challenges. In order to fully acknowledge the legal implications of such an identity management system, the means of storing the identity related data and the means of accessing this data from the user's perspective have to be considered: In the context of digital identity provision, the peer-to-peer characteristics of the distributed ledger technology deployed are relativized by the fact that bank customers do not themselves operate a node within the blockchain network, but rather demonstrate ownership over their hashed credentials stored on the blockchain via digital identity wallets.[34] Thus, the inherent properties of distributed ledger technology and the fact that service providers in the sector collect vast amounts of sensitive personal data of their customers using wallets stored on their mobile phones as a gateway to the ledger are prone to interfere with the concept of human dignity if not properly framed.

A. Legal Challenges arising from the Deployment of Distributed Ledger Technology

While some scholars initially deemed distributed ledger technology disruptive in the context of regulation, due to its revolutionary peer-to-peer characteristics,[35] the law is not yet overturned by distributed structures for identity management.[36] Some specific questions relating to the deployment of DLT as evidential framework for onboarding customers will be discussed in the following sections.

1. Personal data or non-personal data?

If a distributed ledger structure is used by players in the finance sector to record specific information (as evidence) about individuals, the legal qualification of the data processed becomes foregrounded. There are specific legal requirements within the finance sector, especially if the data structure is intended for use as a decentralised evidential registry for customers who have passed an identification verification process.[37] The data recorded on-ledger is derived from an onboarding setting (identity verification) and relates to a natural person – for example name, date, place of birth, information about purpose and intended nature of the business relationship with an individual, and biometric data which are required according to Anti-Money-Laundering provisions[38] – therefore, the information processed in

[33] See *Gstrein/Kochenov,* Digital Identity and Distributed Ledger Technology 5.

[34] Cf. *Zwitter et al.,* Digital Identity and the Blockchain 11.

[35] Cf. *Dimitropoulos,* The Law of Blockchain, 95 Wash. L. Rev. (2020) 1117, 1122 (discussing the possibilities offered by blockchain technology); *Svikhart,* Blockchain's Big Hurdle, 70 Stanford L. Rev. Online (2017) 100, 101.

[36] See *De Filippi/Wright,* Blo2ckchain and the Law 174–175, 179.

[37] E.g. *Moyano/Ross,* KYC Optimization Using Distributed Ledger Technology, Bus. & Info. Sys. Eng'g (2017) 411.

[38] Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for purposes of money laundering or terrorist financing, as last amended by Directive 2018/843, art. 13 para. 1 lit. a and c, 2018, O.J. (L 156) 43, 56 (EU).

the blockchain qualifies as personal data.[39] The data relates directly to an identifiable person, even if the source personal data (represented through a credential or series of credentials) has been hashed prior to being stored. Knowledge of the customer data which functioned as input data for the hash value allows for the hash on the blockchain to be at least theoretically related to an individual, as it is used as verifiable proof that a distinct individual has passed an identity verification process, even though it may be practically unfeasible to reverse-engineer the hash value to determine the input data from the hash value alone.

The hashing of the input data unambiguously constitutes processing of personal data in the sense of Article 4 paragraph 2 GDPR. Whether hash values derived from personal data qualify as pseudonymised or anonymised data depends on various elements, such as the algorithm used for computing the hash, the entropy of the input data, or the extent of pre-processing of the input data.[40] Contrary to anonymised data, pseudonymised data allows the identification of a person and thus qualifies as personal data. According to the case law of the CJEU an identifiable person is a person who can be identified, directly or indirectly.[41] "Indirectly" means that it is not necessary that the information alone allows the data subject to be identified.[42] As long as a data point is directly linked to the hash value stored on the ledger and technically related to the digital wallet of the customer, the hash value is personal data. A direct link between the DID and the private key that controls the DID ensures that the person may be identified. In this respect it is necessary to establish whether data can qualify as personal data from the perspective of one person and non-personal data from the perspective of another person. According to the *Breyer* decision by the CJEU (with regard to dynamic IP-addresses), "it is not required that all the information enabling the identification of the data subject must be in the hands of one person".[43] However, the Court further states that pseudonymised data can only qualify as personal data, if the possibility to combine the pseudonymised data with the additional data held by another person constitutes "a means likely reasonably to be used to identify the data subject."[44] This shall not be the case if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires disproportionate effort in terms of time, cost and man-power, so that the risk of identification in reality appears to be insignificant.[45]

Consequently, depending on the architecture of the blockchain and the legal and factual relationship between the nodes running the blockchain and the wallet providers storing the hash-related personal data off-chain on the one side, and on the operator using the hash

[39] Cf. *Bacon et al.,* Blockchain Demystified 61, 63.

[40] *Agencia Española Protección Datos & Eur. Data Prot. Supervisor,* Introduction to the Hash Function as a Personal Data Pseudonymisation Technique (2019) 21 https://edps.europa.eu/sites/default/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf (last visited November 15, 2021); see *Finck/Pallas,* They who must not be identified – distinguishing personal from non-personal data under the GDPR, 10 Int'l. Data Priv. L. (2020) 11, 25 (elaborating on hash-based ID replacement and the qualification of the hash value as personal data).

[41] See EugH 19.10.2016, C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, ECLI:EU:C:2016:779, 40.

[42] EugH 19.10.2016, C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, ECLI:EU:C:2016:779, 41.

[43] EugH 19.10.2016, C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, ECLI:EU:C:2016:779, 43.

[44] EugH 19.10.2016, C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, ECLI:EU:C:2016:779, 45.

[45] EugH 19.10.2016, C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, ECLI:EU:C:2016:779, 46.

value on the other, the hash value can either qualify as non-personal or personal data. From the perspective of the nodes, it qualifies as non-personal data if the technology that connects the information contained in the off-chain wallet to the hash value cannot be accessed by nodes in the network, and if the nodes and the wallet are not operated by the same persons. Furthermore, it must be ascertained whether source data is stored separately after the hashing, and whether future developments in specific technologies and computing power may permit the re-identification of hashed personal data, even if the hash function was deemed secure at the time of hashing.[46] This is especially relevant given the fact that data stored on a distributed ledger is difficult to amend[47] and, if new possibilities to relate hash values to individuals evolve, the data has already been distributed to as many entities as there are validating nodes in the network.[48] The hash value could thus over time transform from non-personal data to personal data.

For the wallet provider in charge of facilitating the cryptographic proof that the hash value relates to a specific set of personal data, the hash value will always qualify as personal data. The link between the hash value and the input data can furthermore be established by the relying party receiving the credential for purposes of verification and by the issuing party which is also aware of this link. Consequently, except for the blockchain running nodes under specific circumstances, even if following the relative criterion of the possibility of re-identification the ECJ seems to establish through the *Breyer* judgment,[49] a hash value representing personal data has to be deemed pseudonymous, rather than anonymous,[50] especially as persistent identifiers linked to individuals' data or public keys are used to determine an individual's identity in order to comply with existing KYC and AML requirements.

2. Allocation of Legal Responsibility in Distributed Ledgers

It has been demonstrated that the hashing constitutes processing of personal data and that the hash value itself qualifies as personal data if linked to the underlying personal data. It has also been elaborated that only under certain (technical) prerogatives the hash value qualifies as non-personal data. In order to comply with GDPR requirements and to be able to have legal assurance that a specific technical set up does not allow the indirect identification of a natural person, legal responsibility needs to be analysed.

Within GDPR, the key figure for enabling compliance and the protection of the data subjects' rights is the data controller.[51] In so far as wallet providers act off-chain they qualify as data controllers with regard to the processing of personal data contained in the wallet and with regard to the link that is created to the hash value on the blockchain. As for the hash value stored on the distributed ledger, legal responsibility is not certain. Although the GDPR has

[46] E.g. *Zanol et al.,* Self-Sovereign Identity und Blockchain 240.

[47] E.g. *Finck,* Blockchains and Data Protection in the European Union, 4 Eur. Data Prot. L. Rev. (2018) 17, 19 (characteristics of blockchains functioning as data storage).

[48] E.g. *Zanol et al.,* Self-Sovereign Identity und Blockchain 240.

[49] EugH 19.10.2016, C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, ECLI:EU:C:2016:779, 45, 48–49.

[50] E.g. *Dimitropoulos,* The Law of Blockchain 1128; *Finck,* Blockchains and Data Protection 17, 22–23; *Martini/Weinzierl,* Die Blockchain-Technology und das Recht auf Vergessenwerden, in NVwZ 2017, 1251 (1257).

[51] E.g. *Buocz et al.,* Bitcoin and the GDPR: Allocating Responsibility in Distributed Networks, 35 Comput. L. & Sec. Rev. (2019) 182, 183 (discussing the addressees of duties according to GDPR).

been drafted to be technology agnostic,[52] the question of who ultimately retains control over personal data on a distributed ledger is unclear. Naturally, the issue has been deemed especially delicate regarding permissionless blockchains,[53] but even in a permissioned distributed ledger, the allocation of legal responsibility is complex, as copies of the ledger are held by multiple nodes.

When interpreting the existing rules on the definition of the data controller, there is no definite answer as to who retains the control over the processing, as the result relies on the fact that network nodes may be seen as both controllers and as processors, depending on the perspective.[54] Alternatively, the whole distributed ledger could be deemed a joint venture.[55] A yet further possibility would be to deem the party controller which has control over granting access to the blockchain network.[56] Despite possible interpretative solutions, legal uncertainty remains for both the (potential) controllers and the data subjects.

Within a permissioned system all node operators subscribe to pre-determined system and governance rules, and in doing so trust is established.[57] While establishing a contractual relationship between system operators, nodes and other participants may turn out to be practical in some cases,[58] the law should protect the customer by providing a "default"-option if there is no such contract. This implies a need for legal rules and, hence, supervision by the state as a "last resort". On a permissioned blockchain, this could be achieved by holding systems operators and wallet providers who operate as newly established intermediaries responsible.[59] However, regarding the principle that one can only be held responsible for what he has the power to control, due regard must be given to these intermediaries' power to exercise control over the distributed ledger.

Codes of Conduct (CoC) have been proposed to aid proper functioning of certain technology dependent sectors. In the context of digital identity, the latest proposed eIDAS amendment places specific emphasis on how a proposed European wide digital identity ecosystem will rely on Member States adopting a specifically tailored CoC to ensure that rights, freedoms and specific security requirements are adhered to[60] while other jurisdictions have proposed

[52] See Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the free Movement of such Data (General Data Protection Regulation), at 4, COM (2012) 11 final.

[53] See *Buocz et al.,* Bitcoin and the GDPR 197; see *Moerel,* Blockchain and Data Protection, in *DiMatteo et al.* (eds.), The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms (2019) 213 (215–216).

[54] *Bacon et al.,* Blockchain Demystified 66–67.

[55] *Zetzsche et al.,* The Distributed Liability of Distributed Ledgers 1390, mentioning that this could be an especially viable interpretation, if the distributed ledger is set up by a core group which uses the ledger for their purposes.

[56] *Piska/Wagner,* Zukunftstechnologie Blockchain und wie man den Stolperstein DSGVO vermeiden, ZTR 2018, 195 (199).

[57] See *Low/Mik,* Pause the Blockchain Legal Revolution 140.

[58] *See Bacon et al.,* Blockchain Demystified 74.

[59] *Dimitropoulos,* The Law of Blockchain 1190; *Moerel,* Blockchain and Data Protection 216.

[60] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity [hereinafter Proposal for a Regulation establishing a Framework for a European Digital Identity], art. 12b, at 28–29, COM (2021) 281 final.

the use of a 'Trust Framework',[61] but it is not yet clear how these will be adopted or mandated sector-wide, let alone regulated across jurisdictions. Open identity initiatives such as Sovrin[62] and Trust-over-IP[63] have proposed similar, intimating that machine-readable governance mechanisms and regulated trust registries may be the most effective method to solve complex regulatory issues. However, concerns remain that these mechanisms, and CoCs will be self-regulatory instruments, as opposed to tools for greater legal and judicial oversight. These concerns are specifically important where fundamental rights of natural persons are endangered. In order to effectively regulate the legal responsibility for the data flows in a permissioned blockchain, further regulatory effort is required in order to ensure that effective protection is granted to data subjects.[64]

The allocation of legal responsibility is not only relevant for GDPR, but also in regard to other regulations, such as Anti-Money Laundering provisions. As every bank or financial institution is by itself liable for implementing know-your-customer measures, the mere fact that a bank receives verifiable credentials of an onboarded customer does not free it from the responsibility of collecting the necessary personal data.[65] Moreover, current Anti-Money Laundering Law requires every financial institution to retain certain documents relating to their customers, preventing an entirely decentralised solution.[66] In regard to the provisions of the Directive on the Security of Network and Information systems,[67] challenges also arise concerning the allocation of legal accountability for complying with security and incident notification requirements.[68]

B. The Interface for Accessing the Distributed Ledger – The Customer´s Digital Identity Wallet

On the surface, it seems appealing that the data owner is the only individual who holds the means to access and manage their identity credentials, but the technical management of the user's private key is often left to wallet providers, storing the private keys off-chain, but not offline.[69] Even if the hash values might appear as anonymous to an individual looking at the public blockchain without any additional information, they relate to a natural person's real identity by means of the wallet holding the credentials which functioned as an input for the hash values stored on the ledger. Moreover, through the wallet, the user's credentials can be shared or exported off-chain.[70] The wallet provider thus functions as a central threat

[61] *UK Government,* The UK Digital Identity and Attributes Trust Framework https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework#rules-for-all-trust-framework-participants (last visited November 15, 2021).

[62] *Sovrin,* Sovrin Governance Framework https://sovrin.org/library/sovrin-governance-framework/ (last visited November 15, 2021).

[63] *Trust Over IP Foundation,* Governance Stack https://trustoverip.org/working-groups/governance-stack/ (last visited November 15, 2021).

[64] Cf. *Finck,* Blockchains and Data Protection 35; *Stadler/Bichler,* Die Blockchain-Technologie im Lichte der DSGVO, ZIIR 2019, 382 (393).

[65] Directive 2015/849 of the European Parliament and of the Council, art. 25, 2015 O.J. (L 141) 73, 95 (EU).

[66] Directive 2015/849 of the European Parliament and of the Council, art. 40, 2015 O.J. (L 141) 73, 95 (EU), as last amended by Council Directive 2018/843, 2018 O.J. (L 156) 43, 65 (EU).

[67] Directive 2016/1148 of the European Parliament and of the Council, 2016 O.J. (L 194) 1 (EU).

[68] Directive 2016/1148 of the European Parliament and of the Council, art. 14, 2016 O.J. (L 194) 1, 20 (EU).

[69] See *Low/Mik,* Pause the Blockchain Legal Revolution 158.

[70] Where the hashes of the credentials are stored on the blockchain, as described in the "Claim Registry Model", the identity claims may be stored off-chain, for example in the wallet, see *Mühle et al.,* A Survey on Essential Components of a Self-

surface,[71] exposing the vulnerability of the whole system and the personal data processed within it,[72] and thus requiring appropriate regulation in order to protect individuals' rights. Not only is the wallet provider a central conduit for access to the network, phone operating systems act as gateways to the digital domain – with the privacy preferences of platform providers baselining the privacy affordances of application developers.[73] This raises privacy concerns as wallet providers exercise the technical safeguard for the private key of the customer which is crucial to maintain control over the customer's identity credentials. Additionally, the wallet provider potentially has access to the hashed credentials stored on the blockchain, including the customer's biometric data, and is thus in fact in control over the identity of the data subject even beyond the digital sphere, as the digital identity becomes a crucial part of real-life access to financial services. Although the privacy issues related to wallet providers being newly created intermediaries seem to have been acknowledged by the European Commission's proposal for an amendment of eIDAS regulation,[74] future developments will show whether the issuance of a digital identity wallet by the Member States,[75] under a mandate from the Member States or recognised by the Member States will solve the privacy concerns or reinforce them.

In a digital wallet ecosystem, the digital identity wallet stored on the mobile phone allows customers to access and exercise control over their credentials. However, the customers' mobile phones are simultaneously used by financial service providers for fraud mitigation purposes. Fraud mitigation depends on proper safeguarding of the device, the access it affords, and the information contained on it. It is crucial to detect and prevent unauthorized use, whether through access to the user's personal data directly, or fraud attempts that use the bank customer's identity credentials.[76] The information collected from a bank customer's mobile device is moving towards increasingly privacy-invasive methods such as message analysis, network log analysis, social network analysis, interaction pattern analysis, and behavioural biometrics.[77] If linked to financial information related to an individual, a nearly completely accurate picture of the customer can be created, building a "digital avatar" of that individual.

Sovereign Identity, 30 Comput. Sci. Rev. (2018) 80, 81 (discussing different variations of self-sovereign identity architectures); and the corresponding private key proves custody and ownership of the claims in that specific wallet, see *Wang/De Filippi,* Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion, Frontiers in Blockchain (2020) 1, 3.

[71] See *Wang/De Filippi,* Self-Sovereign Identity in a Globalized World 6–7.

[72] See *Low/Mik,* Pause the Blockchain Legal Revolution 164; *Morrison,* Biometric Data Matching Risks and the Rise of Self-Sovereign Identity, in *Aggarwal et al.* (eds.), Autonomous Systems and the Law (2019) 99, 101; *Zetzsche et al.,* The Distributed Liability of Distributed Ledgers 1369, 1376–1377.

[73] *Greene/Shilton,* Platform privacies, New Media & Soc'y (2018) 1640.

[74] Proposal for a Regulation establishing a Framework for a European Digital Identity, 8, and art. 6a 7., 24–25.

[75] Proposal for a Regulation establishing a Framework for a European Digital Identity, art. 6a 2., 23.

[76] See *Zetzsche et al.,* The Distributed Liability of Distributed Ledgers 1376–7.

[77] *Rivner,* Identity Crisis: Detecting Account Opening Fraud in the Age of Identity Commoditisation, Cyber Security: A Peer-Reviewed Journal (2018) 316.

IV. The General Data Protection Regulation, Fundamental Rights and the State´s Obligation to Protect Human Dignity

While mentioned legal unclarities persist, the increasingly excessive collection of customers' device data requires close attention as it is prone to infringe on fundamental rights. This is even more concerning where legal responsibilities are unclear, muddying data safeguarding guarantees. This sentiment has been echoed by the European Data Protection Supervisor in their recent communication on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, published on 7 May 2020.[78]

While the General Data Protection Regulation provides a specific framework for the protection of the fundamental right to data protection, its scope in fact extends to the protection of other related fundamental rights such as the fundamental right to privacy or freedom of expression,[79] rendering its provisions especially important in relation to private actors, such as financial institutions. From a fundamental rights perspective and in accordance with the underlying principles of the General Data Protection Regulation, the protection of personal data is especially crucial in relation to private entities that are closely related to the public sector, either because they are partially owned or funded by the state or because they fulfil tasks in the public interest, thus acting on behalf of the state.[80] The recent proposal of the Regulation on Privacy and Electronic Communications acknowledges that the interception of data created by terminal equipment creates delicate privacy issues which is a good initial starting point, particularly as websites visited, timing, and interaction with others[81] map individuals' behaviour and reveal delicate aspects of their lives to data controllers and processors. However, the data subjects' consent remains a vulnerable link within the process of massive data collection activities conducted by financial institutions – especially if such a power imbalance between data subject and data controller exists as undoubtedly does between banks and their customers.

A parallel can be drawn between existing practices to present opaque terms of consent in regard to the processing of vast amounts of device data and secret surveillance by technical means. While the secret gathering of metadata concerning individuals by technical means has been held lawful in some cases,[82] the existing court decisions take account of various factors. In contrast to the facts of the case P.G. and J.H. v. the United Kingdom, device data collection is conducted by financial service providers who are not state authorities. However, financial institutions function as agents of the state under certain circumstances and the

[78] See Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing, 2020 O.J. (C 164) 21; European Data Protection Supervisor Press Release EDPS/2020/09, Data Protection requirements must go hand in hand with the prevention of money laundering and terrorism financing (2020).

[79] Cf. *Seubert/Becker,* The Democratic Impact of Strengthening European Fundamental Rights in the Digital Age: The Example of Privacy Protection, German Law Journal 2021, 31 (43) (describing the relationship between privacy, democracy, freedom of communication and freedom of expression).

[80] E.g. for purposes of anti-money laundering measures, see *Heiden,* Banken als Erfüllungsgehilfen staatlicher Politik (2013) 137.

[81] Cf. *General Secretariat of the Council,* Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Mandate for negotiations with EP, No. 6087/21 of 10 February 2021, recital 15.

[82] See P.G. and J.H. v. The United Kingdom, 2001 Eur. Ct. H. R 42–51.

same might be the case in regard to identity wallet providers if issued by the state as suggested in the recent proposal for an amendment of the eIDAS regulation.[83] In regard to what data are potentially collected by financial service providers, the means of data collection are more invasive nowadays than in the aforementioned case brought before the ECHR. The data collected do not only comprise metadata but contain information about every potential aspect of individuals' lives. Proportionality is moreover questionable as in the case of financial service providers collecting device data, the aim of this infringement of fundamental rights is not to protect life and limb, but rather – apart from preventing the financing of terrorism – to protect either the banks' financial interests or as a consumer protection measure – as opposed to a measure necessary to maintain the financial system as a whole. The ECHR has stressed that the measure restricting the fundamental right to privacy must be foreseeable and lack arbitrariness. In the case where the data processing is based on consent, foreseeability of the data processing often is in fact not given, especially if the ability to deny consent under one's own free will is compromised by the fact that financial services are essential in daily life and that there is a considerable imbalance of bargaining power between financial institutions and their customers.[84] In order to prevent violations of fundamental rights, it is the state's duty to not infringe fundamental rights when acting vis-à-vis its citizens on one hand, and also to prevent private entities from infringing its citizens' fundamental rights on the other.

V. De lege ferenda approaches to mitigating fundamental rights concerns

The state's obligation to protect its citizens from infringements of their fundamental rights requires legal action on different levels: Appropriate regulation has to be passed in order to effectively protect citizens from infringements of their fundamental rights by private actors by laying down clear rules stipulating legal responsibility. In regard to digital identity management systems, it has to be accounted for that there exist obligations for financial institutions to guarantee data protection and data security, especially if specific technical implementations are not only essential for achieving the required level of data security, but determine whether, and from whose perspective, the data processed within the distributed ledger are relatable to a natural person and thus qualify as personal data. Where personal data are stored immutably within a distributed data structure, clear legal responsibility has to be stipulated, and provisions have to clarify why certain data subject rights (such as the right to erasure) may not be able to be exercised due to technological limitations.

Furthermore, the law has to set limits of self-determination in order to protect data subjects from consenting to extensive processing that reaches a level of non-transparency which may constitute de facto secret monitoring, which has been deemed lawful only under certain

[83] Proposal for a Regulation establishing a Framework for a European Digital Identity, art. 6a 2., 23.

[84] Cf. *Clifford et al.,* Pre-formulated Declarations of Data Subject Consent – Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections, German Law Journal 2019, 679 (680) (discussing similarities between data subjects and consumers vis-à-vis data controllers and businesses).

circumstances.[85] Account has to be taken for situations typically involving an imbalance of power, such as for example between a consumer and a provider of essential services. The very subtle and nearly unnoticed collection of device data not only affects certain fundamental rights such as the right to privacy, freedom of speech, the right to data protection, or the right to effective remedy, it might even threaten the whole notion of human dignity constituting the philosophical and ethical maxim and the foundation of fundamental rights' protection.[86] One regulatory approach to protecting data subjects could be to prohibit certain contents of declarations of consent or to declare consent invalid if given under specific circumstances. In practice, however, these (or similar) legislative approaches have to be effectively enforced. This can only be achieved, and an effective protection of fundamental rights properly afforded to individuals, if the existing fundamental rights – and also the notion of consent according to GDPR – are interpreted by the courts of law in a dynamic way, considering the basic principles of human dignity and the potential impacts of ever-changing technologies and the evolving process of digitalisation.

VI. Outlook

In distributed architectures for digital identity, personal data may be processed by multiple parties: Aside from entities such as credential issuers, and relying parties (those that verify credentials against the evidential record maintained on-ledger), new kinds of intermediaries have evolved. Digital identity wallet providers and the parties or entities responsible for permitting new nodes to the permissioned network have emerged – each bringing with them a suite of legal complexities. These legal nuances, in combination with the additional technical possibilities of the mobile device functioning as a gateway to the identity management system create delicate privacy issues: The mobile phone might provide the technical possibility to function as a surveillance tool for either financial institutions individually, or jointly with other actors such as wallet providers and state authorities. Legal responsibility within the distributed ledger, as well as the duties and obligations of digital identity wallet providers, are yet to be regulated – and perhaps require further restrictions regarding data harvesting practices. This is even more concerning in scenarios where personal data is immutably stored in a distributed manner, posing risks to specific fundamental data protection rights, as well as the fundamental right to privacy.

The judiciary will be confronted with the question as to what extent data processing by private actors for security reasons, or even commercial purposes, shall be allowed and whether there exists a limit to what is still compatible with the notion of the self-determined, free and sovereign individual – based on scrolling down and ticking a box saying "I consent". Only a strict interpretation of consent in the light of fundamental rights against the backdrop of digitalization can ensure data subjects' informational self-determination, especially in situations of power imbalance such as the case of financial service providers and their customers. This interpretation will have to consider the following circumstances: Firstly, financial services are inevitable in modern-day society and private service providers such as

[85] See EuGH 6.10.2020, C-623/17, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others, ECLI:EU:C:2020:790, 80–81; see P.G. and J.H. v. The United Kingdom 42–51.

[86] *Ulgen,* AI and the Crisis of the Self: Protecting Human Dignity as Status and Respectful Treatment, in On the Frontline of AI Ethics: Machines like us? In *DeFalco/Hampton* (eds.), forthcoming 2020 (manuscript at 7–8).

banks form part of critical infrastructure, which are highly supervised by state authorities, publicly funded and partially act in fulfilment of tasks in the public interest. Secondly, individuals' mobile devices enable the collection of vast amounts of data, possibly including information about the most personal aspects of humans' lives. And thirdly, ubiquitously storing data points on distributed ledgers as persistent identifiers constitutes a high privacy risk – even more so if digital identity architectures are broadly applied in areas related to the sovereign functions of the state such as taxation and democratic participation.[87] This conversation is brought further into focus as credential-based architectures are being proposed as the backbone for proof of COVID-19 vaccination status;[88] technology purported as being integral to a safe and secure post-covid environment, even though criticisms have been forthcoming from technical,[89] ethics,[90] and legal[91] researchers.

Whether these issues can be solved by interpreting the General Data Protection Regulation and the fundamental rights to privacy and data protection in a way that is aware of the implications of current and future technological data processing possibilities, and whether current legislative approaches in regulating wallets for digital identity provision[92] are enough, is questionable. The ethical concept of human dignity, enshrined in the European concept of fundamental rights, does not only imply reactive protection of fundamental rights, but also requires proactive steps to be taken by legislators.[93] This has been previously demonstrated by legislation and legal practice in the protection of physical integrity which is ensured by criminal law provisions which exclude the possibility to agree to major physical injury with the effect that the perpetrator cannot be prosecuted. The underlying value might be transposed to the protection of the integrity of the identity in the digital realm which is becoming more and more important in our daily lives. Thus, technical and legal innovation will have to go hand in hand, especially when it comes to (partly) automated processing of data such as in a distributed ledger. The need for clear regulation of responsibility and interpretation of the law by the judiciary which properly and adequately considers privacy implications in a dynamic manner is essential, especially considering cross-sector approaches to digital identity that not only determine the way we define identity in the 21st century but also impact on our understanding of democracy,[94] responsibility, fundamental rights and society as a

[87] Like the digital identity framework proposed by the OECD, aiming to render taxation a more seamless experience by collecting massive amounts of data about taxpayers and combining them, see *OECD,* Tax Administration 3.0: The Digital Transformation of Tax Administration (2020) 24, https://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/tax-administration-3-0-the-digital-transformation-of-tax-administration.pdf (last visited November 17, 2021).

[88] *European Commission,* EU Digital COVID Certificate https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en (last visited November 17, 2021).

[89] See *Halpin,* A Critique of Immunity Passports and W3C Decentralized Identifiers, in Int'l Conf. on Rsch. in Sec. Standardisation (2020) 148.

[90] See *Renieris,* The Dangers of Blockchain-Enabled "Immunity Passports" for COVID-19, Medium (2020) https://medium.com/berkman-klein-center/the-dangers-of-blockchain-enabled-immunity-passports-for-covid-19-5ff84cacb290 (last visited November 17, 2021).

[91] See *Paris,* Applying the Proportionality Principle to COVID-19 Certificates, Eur. J. of Risk Regul. (2021) 1.

[92] See Proposal for a Regulation establishing a Framework for a European Digital Identity, art. 6a 23–25.

[93] See *Suzor,* Lawless. The Secret Rules that Govern our Digital Lives (2019) 118.

[94] See *Seubert/Becker,* Democratic Impact of Strengthening European Fundamental Rights in the Digital Age 40–41.

whole. Debates at the core of the issue will have to go beyond technical and legal reasoning, exploring comprehensive ethical and political approaches.