Blockchain and personal data

-

In search of digital identity management solution

Tommi Ojala
Advanced International Law and Technology
University of Turku Faculty of Law
26.03.2022

Tiivistelmäsivu

TURUN YLIOPISTO
Oikeustieteellinen tiedekunta
OJALA TOMMI: Blockchain and personal data – In search of digital identity management solution
Pro Gradu tutkielma, 58 s.
Oikeustiede
03/2022
Turun yliopiston laatujärjestelmän mukaisesti tämän julkaisun alkuperäisyys on tarkastettu Turnitin Originality Check -järjestelmällä.

Tutkielman aiheena ovat lohkoketjuteknologia, henkilötiedot ja sähköinen identiteetti. Tutkielman tavoitteena on löytää sellainen sähköisen identiteetin hallintaratkaisu, joka hyödyntää lohkoketjuteknologiaa henkilötietojen tallennuksessa ja on henkilötietojen käsittelyyn soveltuvan kansainvälisten sääntelyn mukainen. Tavoitteen saavuttamiseksi, tutkielma antaa vastauksen siihen, 1) voidaanko henkilötietoja tallentaa suoraan lohkoketjuun tai, 2) miten lohkoketjuteknologiaa voitaisiin muuten hyödyntää henkilötietojen säilyttämisessä, 3) mitkä ovat soveltuvat kansainväliset tietosuojalainsäädäntökehykset ja 4) mitä vaikutuksia soveltuvalla sääntelyllä on lohkoketjuteknologian ja henkilötietojen tallentamisen yhteensovittamisessa sähköisen identiteetin hallinnassa.

Tutkielman tutkimusmenetelmänä käytetään postposivistista lähestymistapaa, joten de lege lata -tietosuojalainsäädäntöä ei pidetä itsestäänselvyytenä ja sen sijaan lainsäädäntöä on pidettävä muuttavana ja suhteessa teknologiseen kehitykseen. Sisäisen kritiikin avulla pyritään purkamaan jännitettä kehittyvän teknologian ja tietosuojalainsäädännön välillä ja tunnistamaan lainsäädännölliset aukot ja ristiriidat. Tärkeimmät tutkimusaineistot ovat henkilötietoihin sovellettavat kansainväliset tietosuojakehykset sekä kehitteillä olevat kansainväliset identiteettiä koskevat lainsäädäntökehikot, ratkaisut, ohjeet ja teknologiset standardit.

Edistyksellisistä hajautusalgoritmeista huolimatta, lohkoketjuun tallennettuja henkilötietoja pidetään pseudoanonyymina tietona, ja lohkoketjuun tallennetut henkilötiedot kuuluvat kansainvälisen siten aina tietosuojalainsäädännön piiriin. Lisäksi, koska muuttumattomuus on erottamaton osa lohkoketjuteknologia, henkilötietoja ei voida tallentaa suoraan lohkoketjuun rikkomatta kansainvälisen tietosuojalainsäädännön periaatteita, joista keskeisimmät ovat oikeus tietojen oikaisemiseen ja poistamiseen ja oikeus tulla unohdetuksi. Yksityinen lohkoketju tarjoaa kuitenkin lohkoketjuun muutettavissa olevan lisäkerroksen, joka mahdollistaa lohkoketjuteknologian hyödyntämisen henkilötietojen tallentamisessa ja sähköisen identiteetin hallinnassa.

Kun kyvykkyydet ja esteet lohkoketjuteknologian soveltamiselle on tunnistettu, tutkielma analysoi itsehallittavan identiteetin hallintamallia, joka mahdollistaisi rekisteröidylle henkilölle sekä keinot luoda ja hallita sähköisen identiteetin muodostavia yksilöllisiä tunnisteita, että puitteet henkilötietojen tallentamiseen, aikaansaaden paradigman muutoksen.

Asiasanat

Henkilötiedot, kansainvälinen oikeus, lohkoketjuteknologia, pseudoanonyymi, rekisteröity henkilö, sähköinen identiteetti, tietosuoja.

TABLE OF CONTENTS

SOURCES

Literary Sources

Anisha Mirchandani, The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR, 29 Fordham Intell. Prop. Media & Ent. L.J. 1201 2019.

Capisizu, Larisa, Antonia, Digital Identity. Conf Int'l Dr 2020

CMS Legal Services, The tension between GDPR and the rise of blockchain technologies, January 2019.

Crawford James, Brownlie's Principles of Public International Law, 8th Edition. Oxford University Press 2012.

De Filippi, Primavera, Blockchain and the Law: The Rule of Code, Harvard University Press, 2018.

Gabrielle Patrick and Anurag Bana, Rule of Law Versus Rule of Code: A Blockchain-Driven Legal World, IBA Legal Policy & Research Unit Legal Paper 2017.

George Bouchagiar, 'Privacy and Web 3.0: Implementing Trust and Learning from Social Networks' 10 Rev Eur Stud 16 2018.

Hyland-Wood, David, and Shahan Khatchadourian, "A Future History of International Blockchain Standards." The Journal of The British Blockchain Association 2018.

IBA Legal Practice Division Working Group report, Digital Identity: Principles on collection and use of information 2016.

Klabbers, Jan, An Introduction to International Organizations Law, 3rd ed. Cambridge University Press 2015.

Klabbers Jan, International Law, 2nd ed. Cambridge University Press 2017.

McKay Cunningham, 'Complying with International Data Protection Law' 84 U Cin L Rev 2016.

Paul J Watanabe, 'An Ocean Apart: The Transatlantic Data Privacy Divide and the Right to Erasure' 90 S Cal L Rev 1111 2017.

Robert Herian, Blockchain, GDPR, and fantasies of data sovereignty, Law, Innovation and Technology, 12:1 2020.

Ross, Elisabeth Sara, Nobody Puts Blockchain in a Corner: The Disruptive Role of Blockchain Technology in the Financial Services Industry and Current Regulatory Issues, 25 Cath. U. J. L. & Tech 2017.

Steiner, Peter, Cartoon by Peter Steiner. New Yorker 5.6.1993 issue (Vol.69 (LXIX) no. 20)

Weiss, Martin A. and Archick Kristin, U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, CRS report R44257, 12 February 2016.

Official Sources

A Guide to UNCITRAL – Basic facts about the United Nations Commission on International Trade Law, UNITED NATIONS Vienna 2013.

Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, The right to privacy in the digital age A/HRC/27/37, 18 July 2014.

Article 29 Data Protection Working Party 14/EN WP 225 Guidelines on the implementations of the Court of Justice of the European Union judgement on Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" (C-131/12), exclusive summary.

APEC Privacy Framework 2015.

Blockchain applications in the United Nations system: towards a state of readiness Report of the Joint Inspection Unit JIU/REP/2020/7 Geneva 2020.

Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law? Panel for the Future of Science and Technology EPRS | European Parliamentary Research Service Scientific Foresight Unit (STOA) PE 634.445 – July 2019.

California Business and Professions Code 2015.

California Consumer Privacy Act of 2018.

Charter of Fundamental Rights of the European Union 2007/C 303/01.

CNIL Solutions for a responsible use of the blockchain in the context of personal data, September 2018.

Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers", OECD Digital Economy Papers, No. 186, OECD Publishing, Paris 2011.

European Parliamentary Research Service, Scientific Foresight Unit (STOA), Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law? PE 634.445 – July 2019.

EPRS study on technological innovation for humanitarian aid and assistance, (STOA) PE 634.411 May 2019.

General Data Protection Regulation (EU) 2016/679.

Harnessing blockchain for sustainable development: prospects and challenges Geneva, Switzerland 18-22 January 2020.

Identity in a Digital Age: Infrastructure for Inclusive Development, USAID September 2017.

International Covenant on Civil and Political Rights 1966.

Opinion 05/2014 on Anonymisation Techniques 0829/14/EN WP216.

Opinion of Advocate General Szpunar delivered on 10 January 2019, Case C-507/17

Prohibition on Release and Use of Certain Personal Information from State Motor Vehicle Records U.S. Code 2725.

Proposal for amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, 2021/0136 (COD), Brussels, 3 June 2021.

Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Report of the Joint Inspection Unit, Blockchain applications in the United Nations – system: towards a state of readiness, JIU/REP/2020/7, UN, Geneva, 2020.

Report of the United Nations High Commissioner for Human Rights, A/HRC/39/29, 3 August 2018.

Resolution adopted by the General Assembly on 25 September 2015 A/RES/70/1, 70/1. Transforming our world: the 2030 Agenda for Sustainable Development.

The Children's Online Privacy Act U.S. Code 6501.

The OECD Privacy Framework 2013.

UN Economic and Social Council Harnessing blockchain for sustainable development: prospects and challenge Distr. General 4 March 2021E/CN.16/2021/3.

UN High Commissioner for Refugees (UNHCR), Principles on Identification for Sustainable Development: Toward the Digital Age, February 2017.

UN Office of information and communication technology, Blockchain – What does it mean for the UN, Emerging technologies whitepaper series: Blockchain and distributed ledgers, June 2018.

UNCTAD Data protection regulations and international data flows: Implications for trade and development, New York and Geneva, 2016.

UNHCR, Principles on Identification for Sustainable Development: Toward the Digital Age, February 2017.

United Nations, Universal Declaration of Human Rights 1948.

WAPIS Best Practice Guide on Personal Data Protection, June 2020.

Legal Decisions

Commission implementing decision (EU) 2016/1250

Google Spain v Agencia Española de Protección de Datos and Mario Costeja González, ECLI:EU:C:2014:317.

Google v CNIL C-507.

Internet sources

BBC: Facebook emotion experiment sparks criticism, 30 June 2014 https://www.bbc.com/news/technology-28051930.

Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf.

Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers, OECD Digital Economy Papers, No. 186, OECD Publishing, Paris. http://dx.doi.org/10.1787/5kg1zqsm3pns-en.

EU Blockchain Forum https://www.eublockchainforum.eu/about.

EU Blockchain Observatory and Forum https://www.eublockchainforum.eu/about.

Harnessing blockchain for sustainable development: prospects and challenges Geneva, Switzerland 18-22 January 2020 https://unctad.org/system/files/non-official-document/CSTD_2020-21_c30_B_Thailand_en.pdf .

ICO guideline to Right to erasure https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/.

ID2020 Alliance https://id2020.org/alliance.

OECD Global Blockchain Policy Forum 2021 https://www.oecd.org/finance/oecd-blockchain-policy-forum.htm.

Privacy Shield Program Overview available at https://www.privacyshield.gov/Program-Overview.

PWC Time for trust report, October 2020 https://www.pwc.com/hu/en/kiadvanyok/assets/pdf/Time_for_Trust_The%20trillion-dollar_reasons_to_rethink_blockchain.pdf.

Royal Bank of Scotland launched the banking app in May 2011 https://www.natwestgroup.com/heritage/history-100/objects-by-theme/going-the-extra-mile/banking-app-2011.html.

The Guardian: “I Made Steve Bannon's Psychological Warfare Tool”: meet the data war whistleblower 18 March 2018 https://perma.cc/HK5S-VS5C.

UN Office of information and communication technology, Blockchain – What does it mean for the UN, June 2018 Emerging technologies whitepaper series: Blockchain and distributed ledgers https://unite.un.org/sites/unite.un.org/files/emerging-tech-series-blockchain.pdf.

UN Principles on Identification for Sustainable Development: Toward the Digital Age p.1 https://www.osce.org/files/Identification%20Principles%20FINAL_0.pdf .

UN Sustainable Development https://sdgs.un.org/goals.

ABBREVIATIONS

Abbreviation	Definition
APEC	Asia-Pacific Economic Cooperation
CCPR	Covenant on Civil and Political Rights
CNIL	Commission nationale de l'informatique et des libertés (the Frecnh data protection authority)
DID	decentralised indentifier
ECHR	European Court of Human Rights
eID	European Digital Identity
ECOWAS	Economic Community of West African States
EIDAS	Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market
GDP	Gross domestic product
GDPR	General Data Protection Regulation (2016/679)
IGO	Intergovernmental organisation
ISO	International Organization for Standardization
ITU	International Telecommunication Union
JIU	The Joint Inspection Unit
OECD	Organisation for Economic Co-operation and Development
PwC	PricewaterhouseCoopers LLP
SSI	Self Sovereign Identity
UDHR	Universal Declaration of Human Rights
UNICITRAL	United Nations Commission On International Trade Law
WAPIS	West African Police Information System

1 INTRODUCTION

1.1 Background

Privacy issues regarding online identities remain unsolved, even though the problem has been identified for a long time. However, it is no longer true that "On the Internet, nobody knows you are a dog" as the quote says in the famous cartoon from issue in 1993 New Yorker.[1] The hiding of identity is not too easy anymore but rather, the hiding of identity online is near impossible. Although there are multiple ways to create trusted and verifiable digital identities in order to protect personal data, it is easier than ever to identify online users, as was highlighted by the court in the case Google Spain (2014) establishing the right to be forgotten.[2] However, the right to be forgotten is applicable only after one's identity have been exposed and this raises a question, if there is a way to protect one's identity beforehand? Companies gather people's data and can build a profile of a person based solely on the different facts found all over the internet. In many cases, although a person's real identity may not immediately be revealed, it can be exposed by someone with enough access to either their data or their attributes (e.g., social media connections, location data, online behaviour).

By following the trace of information that a person leaves behind while surfing on the internet, one is able discover who that person is, but because of new ways of business transactions and

[1] Steiner, Peter, Cartoon by Peter Steiner. New Yorker 5.6.1993 issue (Vol.69 (LXIX) no. 20) p. 61.

[2] Google Spain is mainly known for the application of right to be forgotten, but the case also highlights that search engines gather personal information and are able to build a profile of a person based solely on the different facts found all over the internet. See more Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014) ECLI:EU:C:2014:317 para 37.

personal and professional purposes, the information reveals even more than just the identity.[3] The information is not only personal data, but it goes beyond that to inform how a person behaves, where that person is located, what that person enjoys etc. All this information has marketing value, and businesses are profiting from this information using data mining.[4] This would suggest that identity needs to be understood in broader sense online than offline.

Certainly, most people have come across a situation where they have visited a particular online shopping site and immediately after visiting, the ads start displaying the products of that site. This is an example of how companies take advantage of the digital identity. Every site a person uses and every transaction they make will create a digital record.[5] The problem is that this phenomenon is global, and people cannot choose alternative ways of using the internet and not to expose their digital identities. In 2014 Facebook conducted a test on their users where their data scientist would analyse the users' reactions to a manipulated news feed.[6] Even though there was no unnecessary collection of data there was no consent either and the experiment went beyond product testing. The issue is global and therefore need a global approach. Otherwise, interpretations and applications in specific jurisdictions will differ significantly and these differences will increasingly affect negatively on privacy rights of individuals.

---

[3] IBA Legal Practice Division Working Group report, Digital Identity: Principles on collection and use of information, 2016, p.5.

[4] Data mining means the use of data analysis tools to discover previously unknown, valid patterns and relationships in large data sets. See more, Seifert, Jeffrey W. Data Mining: An Overview, CRS Report for Congress, 2004.

[5] IBA Legal Practice Division Working Group on Digital Identity, 2016, p.6.

[6] BBC: Facebook emotion experiment sparks criticism, 30 June 2014, https://www.bbc.com/news/technology-28051930 visited 9.3.2021.

Imagine a person is sitting on their living room couch, sipping their favourite spirit, and watching their favourite TV series while wearing the comfy activewear that they received in the mail earlier that day. Now imagine while doing this, there would be a stranger, probably sponsored by a giant technology company, watching them behind the window with a notepad in hand and writing down all of the observations about the label of the person's spirit, the name of the TV series and the brand of the clothes. The previous scenario seems outrageous. However, there is always someone tracking what any person watches or does online and storing every piece of information they drop while surfing on websites. The relevancy of this study is highlighted by the abovementioned scenario when considering technology can provide us the tools to shift the management of our digital identities from the organisations to people, the identity holders — meaning there would be no more virtual strangers spying behind virtual windows.

Privacy issues still exist online despite the effort of multiple international privacy frameworks in protecting the individuals. I have identified blockchain technology as a technological solution to tackle the privacy issues online. The primary considerations on blockchain-based solutions are on 1) blockchain's design, 2) applicable international privacy legislation 3) coordination of protection of personal data and blockchain and 3) the identification of potential solution. There are multiple international privacy frameworks that the solution needs to be in compliance with. The reason why blockchain could potentially be ground-breaking in solving the privacy issues online is that it possesses the technical capabilities to manage individuals' digital identities. However, the legislation produces difficulties in coordinating personal data and blockchain technology and this is mainly because the technology clashing with the exercising key data subject rights. What is more, the privacy frameworks and the technology are both relatively new which results in the lack of case law, standards, and guidance. Nevertheless, this study will seek solutions that reconcile the international privacy frameworks and technical solutions, which essentially have the same goal: to promote natural person's data protection. Trust services are currently in high demand and international organisations are searching for solutions to build trust online. Blockchain-based solution could

potentially result in paradigm shift in the way the digital identities, are managed. In this study, I will attempt to identify this solution.

1.2 Research questions and limitation of the study

This study seeks to find a blockchain-based digital identity management solution that is in compliance with the international privacy legislation. My main research question is if the digital identities can be managed by a solution that utilises blockchain technology in storing of personal data and is in compliance with international privacy frameworks regulating the procession of personal data. To answer this question, I need to study 1) if personal data can be directly stored on blockchain, and if not, 2) how could blockchain technology be otherwise utilised in storing of personal data, 3) what the applicable international privacy frameworks are and 4) how the applicable international privacy frameworks affect the coordination of blockchain technology and personal data in the management of digital identity. Finally, I will present a potential solution to the main research question based on the results of sub-research questions.

My study aims to find out the positive and negative legal and technical implications of the use of blockchain technology in storing of personal data and managing digital identity. Mainly, there seems to be tension between the fundamental design of the blockchain technology and fulfilling the key data subject rights. Blockchain technology and digital identity are also complicated to start with, and therefore this study aims to explain the concepts comprehensibly. However, I will not deep dive into the encryption methods of blockchain technology or try to identify alternative techniques that could secure data subjects' data online. I acknowledge and agree that there is ambiguity on how to enforce the data subject rights if blockchain technology is utilised, but I am leaving the question of who would be the controller

of blockchain-based digital identity management solution out of scope of this study.[7] What is more, I acknowledge that companies and international organisations may also have their own digital identities, but I will restrict this study to the point of view of natural persons.

International organisations have a significant impact on international custom and a great deal of international law is created by or within international organisations.[8] The international organisations are built around functions and can therefore act more efficiently globally, whereas states are bound on the territory. There are multiple definitions for international organisations and none of them is comprehensive.[9] However, in the meaning of this thesis, the international organisation has the meaning of intergovernmental organisations (IGOs), mainly focusing on the ones that have produced data privacy regulations, guidelines or policies or blockchain related opinions. The reason for choosing this definition is due to the IGOs' capability of dealing with global data protection matters and emerging technology with a meaningful impact.

1.3 Research methodology

I use a post-positivist approach in my study. Thus, I do not take the de lege lata data privacy legislation for granted, especially in relation to emerging technology. Instead, I consider the legislation to be transformative and relative to current technological developments. One may not be familiar with blockchain technology and digital identity because the defiance and usage

---

[7] According to EU's General Data Protection Regulation Article 4(7), the controller means 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.

[8] Klabbers, Jan, International Law (2nd ed.) 2017, p.91.

[9] Klabbers, Jan, An Introduction to International Organizations Law (3rd ed.) 2015, p. 6.

of the terms have only become relevant as the technology has provided us the means and methods to potentially govern our digital identities. The blockchain-based digital identity solutions have made the digital identity more tangible, and it can finally be conceptualised to the full extent.

Hence, the international privacy frameworks have to be reviewed due to the emergence of blockchain technology. The blockchain-based digital identity, and privacy threats it faces, have to be dealt with at the international level because identity is protected in human rights legislation. Furthermore, the nature of the internet makes the issue automatically global because data knows no territorial boundaries. To add with, the legislation concerning technology must always be preserved emphatically unstable and constantly changing. With the help of internal critique, I am looking to expose controversy between emerging technologies and privacy legislation and identify the gaps and conflicts.

The main sources for this study are international privacy frameworks applicable to personal data as well as emerging international legislation concerning digital identity. Additionally, international guidelines, principles and studies published by international organisations regarding data protection and privacy as well as identification are used as relevant sources. In addition, several academic articles from various authors and scholars are studied.

1.4 Structure of the study

This thesis is divided into 5 chapters, beginning with the introduction of the topic to give a brief background to the studied subject and the methodology used in the thesis. In the second chapter, blockchain technology is explained and relevant its characteristics are identified. In the third chapter, I will map out the relevant international privacy frameworks applicable for the purpose of this study and identify the key data subject rights that may have implications on utlising blockchain in storing of personal data. The fourth chapter focuses on digital identity and the application of blockchain technology to digital identity management based on previous

findings. The final chapter includes the concluding remarks and summarises the outcome of the study.

2 BLOCKCHAIN TECHNOLOGY

2.1 Blockchain technology explained

In this chapter 2, I will explain the main characteristics of blockchain technology in order to present why the blockchain technology could be advantageous in storing of personal data. Blockchain technology is an infrastructure that functions as data storage and management for software applications.[10] The innovation is significant, but its outputs are invisible for end-users.[11] The blockchain and databases it may side-line are the foundation for all applications, and online service platforms. To this day databases have been upheld and controlled by centralised service providers. This power dynamic may change by courtesy of blockchain technology and creating a paradigm shift in the way digital identity is managed.

In 2008 Satoshi Nakamoto[12] introduced the public with a blockchain model, which is a combination of public-private key cryptography, digital signatures and peer-to-peer

[10] De Filippi, Primavera, Blockchain and the Law: The Rule of Code, 2018, p.33.

[11] For example, in Finland this technology has already found its way to banking and real estate business in the form of DIAS which is a platform for digital trading of shares of stock in a housing company. The platform connects comprehensive real estate business players such as banks, real estate agents and property developers. See more https://www.unlock-bc.com/news/2020-03-16/finlands-housing-market-now-securely-on-the-blockchain/ visited 6.3.2022.

[12] Satoshi, whose true identity is unknown, is the author of Bitcoin whitepaper, see more Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf visited 6.3.2022.

technologies, and created the most famous decentralised digital currency, Bitcoin.[13] Even though the blockchain technology have been published already in 2008, only recently it has been realised that the blockchain technology, where Bitcoin operates, can be used to revolutionise the way individuals disclose information online while creating transparency and trust.[14] Blockchain technology was not standardised until 2016 by the International Standards Organization (ISO) and ISO TC 307 remains to be the only backwards looking standardisation effort so far as many believe the standardisation for rapidly evolving blockchain technology are premature.[15] The ISO TC 307 mainly provides standards for blockchain architecture, taxonomy and ontology as well as blockchain-related vocabulary.[16]

Blockchain enables secure electronic transactions of data through cryptography to validate transactions before recording them on a decentralised public or private ledger in which all network transactions are displayed.[17]

---

[13] De Filippi, Blockchain and the Law 2018, p. 20

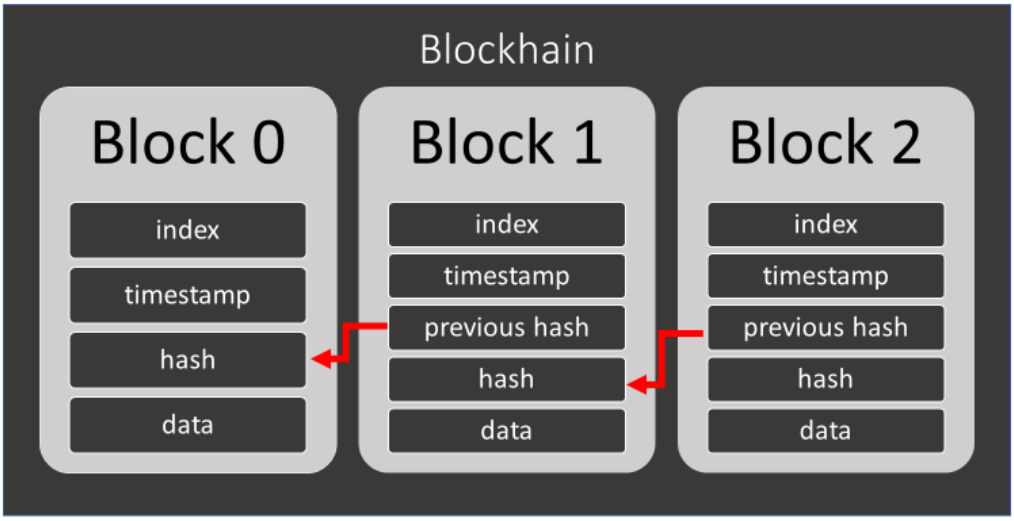
[14] The blockchain is specifically a subcategory of distributed ledger technology.

[15] Hyland-Wood, David, and Shahan Khatchadourian, "A Future History of International Blockchain Standards." The Journal of The British Blockchain Association, 2018, p. 27.

[16] Ibid.

[17] Ross, Elisabeth Sara, Nobody Puts Blockchain in a Corner: The Disruptive Role of Blockchain Technology in the Financial Services Industry and Current Regulatory Issues, 25 Cath. U. J. L. & Tech 2017, p. 360-361.

Figure 1 Blockchain



To put it simply, a blockchain is a database where data can be stored online in storage named blocks (see above figure 1). Once the data is transferred to the block, the block is then encrypted by using a hash which is a unique sequence of letters and numbers. The hash is established by a secret encryption key so that only those who know the key can access the data. The linking blocks create a chain, hence the name blockchain. In a public blockchain, the chain is formed by multiple different computers of the public that store the local copy of the blockchain. The generic term of the computers creating the public network relating to a blockchain is nodes.[18] Every block in the chain holds the hash of the previous block in addition to a timestamp. In this way, the blocks are creating a decentralised peer-to-peer network.

[18] In private entities that control the access to blockchain are the nodes. This means there is less nodes in private blockchain and the trust is based on the credibility of the nodes/entities. In public blockchain where every user (or rather their computer) is a node, the trust is based on the large number of nodes.

Blockchain has the ability to build trust in online services by applying the existing service as a layer on top of the technology. The main benefits of blockchain technology are consensus, immutability and decentralisation.[19] All in all, the important practical consequence of blockchain for end-users is that for the first time, one individual can present or transfer a unique piece of digital information to another individual online in a way that the transfer is guaranteed to be safe and secure leaving no doubt for the transfer to be not have taken place. By utilising hashing and encryption, the data can be protected very well on the blockchain.[20] In a public blockchain like Bitcoin, anyone can become a node by downloading and using the relevant software and storing data on the blockchain. In a private blockchain, only trusted nodes can store the copy of the blockchain. Blockchain technology provides an opportunity to reduce the dependence on centralised control and increase data protection for data subjects.[21]

2.2 Public blockchain

Public blockchains are transparent and offer completely peer-to-peer transactions and they can be viewed by anyone at any time, because the ledger is located all over the network and not a single institution is charged with auditing transactions or keeping records.[22]. In all blockchains, the blocks are connected to the chain by being attached to the previous block and so on creating the secure structure of the blockchains. Once the block containing data is added

---

[19] Anisha, Mirchandani, The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR, 29 Fordham Intell. Prop. Media & Ent. L.J. 1201 2019, p. 1213.

[20] Hash is a mathematical function which cannot be reverse-engineered since hash functions are a one way street. Hashing in the context of blockchain means having an input item which reflects to an output item. Encryption is used when normal text is processed to random sequence of bits.

[21] De Filippi, Blockchain and the Law (2018), p.33.

[22] Robert Herian, Blockchain, GDPR, and fantasies of data sovereignty, Law, Innovation and Technology, 12:1, 156-174, DOI: 10.1080/17579961.2020.1727094, 2020, p. 163.

to the blockchain and attached to another block the blocks cannot be altered and therefore making the entire chain secure.[23] The blocks are added to a public blockchain through a mining process by complex process that put consist of proof of work and verification.[24] Consensus is critical on a public blockchain since there is no central operator all users have to concur the validity of the block prior its addition to the chain. Immutability is a key part of public blockchain due to its permanency. As a result of the mining process the public blockchain is genuinely decentralised and completely immutable data storage.[25] However, the fact that the block cannot be by any means erased, deleted, or otherwise amended and the lack of central operator seem to make storing of personal data in public blockchain incompatible with all current privacy legislations.

At least for now, despite possessing the true innovation and decentralised nature, public blockchain cannot be utilised in storing of personal data and therefore digital identity management solution cannot be based on public blockchain. However, a different kind of blockchain could offer all the positives of blockchain technology and still be in compliance with privacy demands.

---

[23] Anisha, GDPR-Blockchain Paradox 2019, p. 1207.

[24] Ibid., p. 1210.

[25] Ibid.

2.3 Private blockchain

Private blockchain operates similarly to public blockchain with a distinction that an additional layer is added on the blockchain in a form hash function and private key.[26]

Figure 2 Transition from public to private key

On private blockchain, access is restricted and not open to the public. In addition, there is a central operator or network of operators that control the participation, access rights to the data and validation of data added to blocks. The central operator may hand out read access to others, but this kind of access needs to be managed with caution when it comes to personal data. There is difference in opinion among experts if private blockchain respects the core characteristics of traditional blockchain i.e., public blockchain in the sense of decentralisation and mutual validation.[27]

Private blockchains operate in closed private systems and they offer transparency and peer-to-peer transactions and are deployed within closed networks like an intranet or back-office system.[28] This means that the ledger, where the data is stored, is accessible to only those who have been granted prior access. In private blockchains the function of the additional layer is to

---

[26] Anisha, GDPR-Blockchain Paradox 2019, p. 1211.

[27] CNIL Solutions for a responsible use of the blockchain in the context of personal data, 2018 https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf.

[28] Herian, Robert, GDPR, and fantasies of data sovereignty 2020, p. 162.

enable the ability for parties to restrict access.[29] The information on private blockchain and the verification of the transactions/blocks is controlled by a central organisation.[30] It follows, that private and public blockchain are fundamentally different when it comes to consensus of the validity of transactions and blocks. This gives more control to companies over the data and makes it less of a problem from a data protection point of view.[31] This is why the main advantage of private blockchain is achieving compliance. The ability to see and track the entire chain of transactions without risking data breach or data alternation, results to efficient and reliable audit which in turn results to better compliance.[32] Private blockchain could also be used effectively for record-keeping for centralised entities like credit institutions or government offices that are found trustworthy to store personal data.[33] However, most notably digital identity management solutions can be built on private blockchain. Due to the immutability of the private blockchain, it can only be accessed by the centralised operators and to whom they have granted access creating a situation where the base of trust isn't in the entities ability to protect from e.g., hackers but in the blockchain technology itself. Moreover, an advanced blockchain technology should prevent hackers from altering data subjects' information because the blocks could not be altered, only viewed.

However, it is important to note that because private blockchains lack the genuine decentralised system that is characteristic for public blockchains, data subjects still need to be able to trust the central operator as they possess the technical capabilities to behave

---

[29] Anisha, GDPR-Blockchain Paradox 2019, p. 1211.

[30] Ibid., p. 1212.

[31] CMS Legal Services, The tension between GDPR and the rise of blockchain technologies 2019, p. 3

[32] Anisha, GDPR-Blockchain Paradox (2019), p. 1214.

[33] Ibid.

fraudulently towards data subject's personal data or alter the data.[34] Still in my mind, personal data would be more secure when stored on blockchain than traditional database and due to direct benefits for entities processing personal data, blockchain technology is superior to traditional databases.

Conclusively, private blockchain appear to be more suitable solution should be favoured over public blockchain. However, anonymity of hashes and encryption technologies is another important feature involving blockchain's design that needs legal assessment in order to analyse the compliancy of digital identity management solution build on blockchain technology with privacy legislations.

2.4 Anonymisation and blockchain

Public keys are blockchain user's pseudonymous identifiers which can be hashed and encrypted and therefore the identity of the user is protected and not revealed.[35] This unique feature enables parties to interact with each other without revealing their identities because they can trust the underlying technical design of the blockchain. However, especially the General Data Protection Regulation (GDPR) sets a high threshold for data until it can be considered completely anonymised. If the keys can be traced back to the data subject it is considered personal data according to the GDPR.[36] This is important because the European Data Protection Board has stated that complete anonymisation of personal data in a way that

[34] Anisha, GDPR-Blockchain Paradox (2019), p. 1214.

[35] CMS Legal Services, The tension between GDPR and the rise of blockchain technologies 2019, p. 4.

[36] Patrick Breyer v Bundesrepublik Deutschland, C-582/14 §42, 43, 45 EU:C:2016:779, Ruling 1

the personal data can no longer be identified is out of the scope of the GDPR.[37] However, hashed personal data is still personal data and the threshold which the GDPR sets for anonymisation is high but it could be achieved, in principle, by the means and techniques which results to complete irreversibility of identification.[38] The European Data Protection Board has stated that hashing is considered pseudonymisation technique, because hash keys can be inserted all over again through the hash function so that the correct value for each record is discovered.[39] Therefore, it is necessary to look into the difference between pseudonymised and anonymised data.

In accordance with the GDPR, pseudonymisation is the processing of personal data so that it can no longer be used to identify a data subject without the use of additional information.[40] The legal issue to be solved is if the encryption techniques used in hash function result in personal data being anonymous or pseudonymous. According to Opinion 05/2014 of article 29 working party (Data Protection Board) anonymisation results only from processing personal data in a way that it irreversibly prevents identification.[41] The working party states that no matter how advanced the encryption used in blockchain is, it does not result in anonymisation if the key or the original data are available.[42] Because encryptions can always be decrypted when the accurate key is discovered, the encryption can never be considered completely

---

[37] Opinion 05/2014, p. 3.

[38] CMS Legal Services, The tension between GDPR and the rise of blockchain technologies 2019, p. 4.

[39] Opinion 05/2014 p. 20.

[40] GDPR Article 4(5).

[41] Article 29 Data Protection Working Party (replaced by European Data Protection Board) Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN WP216, 10 April 2014, p. 3.

[42] Hashing considerably increases the protection on personal data but it will not provide for irreversibly anonymous data, see Opinion 05/2014 p. 29.

irreversible. Thus, no matter how advanced the hash function would be the hashed data will always be pseudonymous data. However, some weight should be given to the advanced hashing techniques which is discussed more closely in chapter 3.2.2. The situation does not change even if trusted third-party service provider.[43] So it seems that hashing does not solve the issue, even though it is undeniably desired feature of blockchain and makes data more secure, blockchain still falls under the scope of privacy frameworks regardless of the chosen hash function.

In determination whether the person is identifiable after anonymisation technique used, all means reasonably like to be used shall be taken in account.[44] When assessing reasonable means, focus should be on factors of cost and amount of time required on identification and taking in account available technology. One may argue that using supercomputers to re-engineer hashes to identify a person should not be regarded as reasonable when taking into account cost, and in the case of advanced hash function, the amount of time needed to decrypt the hashing function. However, this conversation has been ignored possible due to the reason of high threshold of protection granted for personal data and the ongoing rapid development of computing power.[45]

According to the French data protection authority (CNIL), hashing by using secret key as an additional input may result in anonymisation of data.[46] This is dependent on whether it is still reasonably likely to decrypt the blockchain and reveal the data subject's identity regardless of

---

[43] Hashing considerably increases the protection on personal data but it will not provide for irreversibly anonymous data, see Opinion 05/2014 p. 29.

[44] GDPR recital 26.

[45] In Breyer v Bundesrepublik Deutschland, 2016, CJEU stated the anonymisation of personal data would only be considered if it would be practically impossible to identify the data subject.

[46] CMS Legal Services, The tension between GDPR and the rise of blockchain technologies 2019, p. 5

secret key added to the hash.[47] Secret key could be for example dialogue from Lord of the Rings movies. Why this could potentially work is, that when the secret key (or the chosen line of dialogue) is deleted, the data been hashed cannot longer be verified and therefore there is no danger for identification.[48] The deletion must extend to all systems where the information of secret key is stored. Thus, hashed personal data may not conclusively result in pseudonymous data and some protection techniques may leave it out of scope of the GDPR, but this remains to be decided. So even though the use of hash function does not result in transforming personal data into anonymous data, multiple data protection legislations recommend the use of pseudonymisation techniques.[49]

The GDPR and the Organisation for Economic Co-operation and Development (OECD) principles are technology-neutral, and they view the compliance of the chosen technology not by categorising certain techniques as compliant or not but in what way the certain technique potentially achieves compliance from the data subject's point of view.[50] However, the lack of categorising of compliant blockchain technologies have caused the guidance to be out-dated as new solutions are arising rapidly. Because the compliancy with the GDPR is analysed case by case, the burden to clarify the key points of ambiguities is on the regulators and the pace of which they have acted have left more to be desired.

After all, anonymisation probably is not even something that legislators prefer to be sought after, as it would make authorities supervision much harder and therefore technologies using full anonymisation techniques could induce criminal activity. To conclude with, hashed

---

[47] CMS Legal Services, The tension between GDPR and the rise of blockchain technologies 2019, p. 5

[48] Ibid.

[49] Anisha, GDPR-Blockchain Paradox 2019, p. 1220.

[50] GDPR Recital 15, OECD Privacy Framework p. 66.

personal data will be considered pseudonymous data. After the anonymisation question is settled, I will look into applicable international privacy legislations and perhaps the most cumbersome issue related to blockchain technology: the exercising of key data subject rights.

3 PERSONAL DATA AND BLOCKCHAIN

3.1 International privacy framework for personal data

In this chapter 3, I will identify what current international privacy legislations are applicable to storing of personal data and to be considered when searching for digital identity management solution. The international framework for regulating the processing of personal data consist of many basic principles and policies. The current framework needs to be evaluated in relation to blockchain technology to recognise possible gaps in regulation and to provide adequate protection for individuals. If left explicitly unregulated, the blockchain technology could cause implications for rights of individuals.

To begin with, I will look into the fundamental starting point that ensure the fundamental regulatory and legal safeguards globally for protection of personal data. The principle of privacy is established in the international human rights law and according to Article 17 of International Covenant on Civil and Political Rights (CCPR) one's privacy is protected of interference.[51] The European Convention on Human Rights (ECHR) article 17 and Universal Declaration of Human Rights (UDHR) article 12 equally protects private and family life, home and correspondence.[52] Both articles are applied broadly, and privacy has long been

[51] International Covenant on Civil and Political Rights, Article 17.

[52] ECHR Article 17, UDHR Article 12.

considered a fundamental human right.[53] The right to privacy is to be considered as a "private sphere" where individuals have the area to determine and develop their own identity, interaction, choices etc.[54] Online this translates to informational privacy which covers all information that already exists or can be derived about an individual, including personal data.[55] What is more, the information extends to metadata if it is analysed in a way of attempting to learn about the individual's behaviour, identity and this implication is particularly true when technology companies such as Facebook collect and analyse social media of the individuals.[56] Indeed, Facebook is particularly good example as the sheer existence of secret surveillance equals interviewing with the right to privacy.[57] Companies' reliance on personal data is increasing simultaneously with the growing digital footprint of individuals.[58] Companies have been caught collecting the data without knowledge or purposeful consent of the individual leading to a situation where there is no genuine possibility for individuals to actually control or track the use of their data.[59] There is growing desire and

---

[53] see for example Article 12 UN Declaration of Human Rights and Article 17 International Convenant on Civil and Political Rights.

[54] Report of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age. A/HRC/39/29, 3 August 2018 para 5.

[55] A/HRC/39/29, para 6.

[56] Ibid.

[57] Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, The right to privacy in the digital age A/HRC/27/37, 18 July 2014, para. 20.

[58]A/HRC/39/29, para 12.

[59] Most notably, Cambridge Analytica was caught harvesting millions of Facebook profiles in order to politically influence the users during the 2016 US presidential campaign. See the Guardian: "I Made Steve Bannon's Psychological Warfare Tool": meet the data war whistleblower, 18.12.2018 https://perma.cc/HK5S-VS5C visited. 6.3.2022.

support for the shift of control where individuals would no longer be mere users of social networks but actual subjects and beneficiaries of the big data they produce together.[60]

However, no international processes exist that would bind private businesses to protect human rights.[61] There is ongoing debate concerning horisontal effect of international human rights law and if human rights should extend to private action regardless of institutional stance on the matter.[62] Blockchain technology could, by design, protect the privacy, and personal data of individuals without any institutional expression. However, rule of the code would go only as far as the states take action on the matter.

The primary source for international privacy principles is the OECD privacy framework. According to the OECD privacy framework's data quality principle 8, personal data should be accurate and complete and kept up to date.[63] This would entail that at least control would be required over the information stored on blockchain. What is more, in accordance with another relevant principle regarding blockchain technology, the individual participation principle 13, the individuals should be able to challenge the data and have it erased, rectified, completed, or amended.[64] To comply with this principle, public blockchain can be ruled out since the public blockchain is immutable without exception. Other principles do not cause conflict with

---

[60] Also known as phenomenon "Web 3.0.", see more George Bouchagiar, Privacy and Web 3.0: Implementing Trust and Learning from Social Networks, 2018.

[61] Brownlie's Principles of Public International Law (9th Revised edition), p. 656.

[62] Ibid. p. 655.

[63] The OECD Privacy Framework 2013, Principles 8.

[64] The OECD Privacy Framework 2013, Principle 13.

blockchain technology, quite the opposite, blockchain technology fulfils for example security safeguards principle by default.[65]

In Asia, the continent's most profound privacy framework is the Asia-Pacific Economic Cooperation (APEC) Privacy Framework first published on 2005 and updated on 2015.[66] The framework is consistent with the core values of OECD Privacy Framework. However, the focus of APEC privacy framework is on potential harm on individuals rather as opposed to OECD Privacy Frameworks individuals' rights -approach. What is more, APEC privacy framework does not impose treaty obligations whereas OECD privacy Principles have the support of states' legal regimes.

In Europe, the GDPR came into effect on 2018 with an objective to protect personal data and regulate the way it is collected and shared in the EU. This was significant change to previous legislation which allowed companies to process personal data almost as they wished. The previous data protection legislation was also a directive which meant that the EU member states were inconsistent with the implementation. The GDPR applies to the processing activities related to offering goods or services to such data subjects regardless of remunerativeness.[67] The principles of the GDPR apply to all data related to an identified or identifiable natural person ("personal data").[68] What is more, pseudonymous personal data is still on the scope of the GDPR which is highly relevant as blockchain uses various hashing

---

[65] The OECD Privacy Framework 2013, Principle 5: "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.".

[66] The APEC is a forum for trade and economic growth. Foreword, APEC Privacy Framework 2015.

[67] GDPR Recital 23.

[68] GDPR Recital 26.

and encryption techniques to make the data on the blockchain secure and users of blockchain have already undergone pseudonymisation.

In Africa, the most advanced privacy policy is the West African Police Information System (WAPIS) which concerns total of 15 member states of Economic Community of West African States (ECOWAS). The WAPIS Best Practice Guide on Data Protection (WAPIS Guide) was funded by EU and unsurprisingly the policy includes many principals similar to the GDPR e.g., right to access and right to rectification and it uses the same terminology.[69] The Australian data protection regulation is also largely consistent with the GDPR apart from application to small companies, but the Australian law haven't yet received adequacy status by the EU.[70]

According to the GDPR and OECD Privacy Framework, personal data means any information relating to an identified or identifiable natural person ("data subject").[71] From here onwards, for the purpose of this study, I will use data subject as universal term regardless of what regulation or guideline is in question, as a majority of international organisations seem to have adopted this term. The international privacy frameworks seem to generally agree on how personal data should be processed. Firstly, all privacy frameworks above give the same requirements on data quality. According to WAPIS Guide, personal data should be accurate and kept up-to-date and all reasonable steps should be taken to ensure that personal data that

[69] See more WAPIS Best Practice Guide on Personal Data, 2020.

[70] UNCTAD Data protection regulations and international data flows: Implications for trade and development p. 43.

[71] GDPR Article 4(1), OECD Privacy Framework, Part one, definitions 1(c), see also WAPIS Best Practice Guide on data protection, Chapter 1.4 General terminology which defines Data subject as "an individual who is the subject of personal data processing".

are inaccurate, incomplete or not up-to-date are not transmitted, shared or made available.[72] OECD Privacy Framework correspondingly demand data to be accurate, complete and kept up-to-date.[73] Similarly, the APEC Privacy framework demand integrity of personal information and personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.[74] In addition, the GDPR provides the same threshold for data quality and accuracy, or even higher, as protection of personal data is considered a fundamental right according to EU Charter.[75] According to the GDPR principles relating to processing of personal data, the personal data shall be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay".[76] What is more, the data minimisation principle according to which the data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" is relevant when considering the storing of personal data on blockchain.[77] Secondly, all international privacy frameworks grant multiple rights for data subjects in order to protect their personal data which is in high relevance when it comes to utilising blockchain technology, or any new technology, in storing of personal data. The GDPR and WAPIS Guide provide right to rectification and erasure of personal data if conditions apply as well as strong

[72] WAPIS Guide 2020, Chapter V, DATA QUALITY

[73] OECD Privacy Framework, Data Quality Principle.

[74] APEC Privacy Framework, VI. Integrity of Personal Information.

[75] EU Charter of Fundamental Rights Article 8 – Protection of personal data.

[76] GDPR Article 5(d).

[77] GDPR Article 5(c).

access rights for data subject.[78] APEC and OECD privacy frameworks provide similar access rights for data subjects as well and the right is in principle two-fold: the data subject have 1) the right to obtain the information if the controller has data related to them and 2) the right to have the related data communicated to them.[79] Additionally, in accordance with OECD and APEC privacy frameworks, the data subject should have the right to challenge the data related to them and have the data erased/deleted, rectified, completed or amended accordingly.[80]

On the contrary to previous, there are few jurisdictions that have taken more lenient regulative stance on data protection, the US being the foremost. The US privacy laws are best described as patchwork as there is no one comprehensive data privacy legislation. The organisations storing and processing personal data need to consider collection of different rules and restrictions making the US privacy regulation one of the most complex in the world.[81] The US privacy legislation consists of confusing mixture of state and local laws, federal legislation and self-regulation.[82] This naturally causes compliance issues among companies and for this reason only, blockchain technology could provide additional and much needed protection by design for data subjects. As opposed to Europe, the US legislation does not consider right to privacy a fundamental right and, as matter of fact, the US Constitution of rights does not

[78] see GDPR Section 3 Rectification and erasure and Article 15 Right of access by the data subject and WAPIS Guide, guidelines Chapter IX – Data subject rights (Right to access and right to rectification or erasure).

[79] OECD Privacy framework, Individual Participation Principles a) and b) and APEC Privacy Framework, principle VIII. Access and Correction 23.a).

[80] OECD Privacy framework, Individual Participation Principle c) and APEC Privacy Framework, principle VIII. Access and Correction 23.c).

[81] McKay Cunningham, Complying with International Data Protection Law, 2016, p. 421.

[82] Ibid.

explicitly grant right to privacy.[83] Perhaps the strongest data protection legislation belongs to state of California, although it still offers much weaker rights than the GDPR. According to 2015 California statute, minors have the right to forgotten and the right can be referred to when demanding the websites to delete posted content regarding 18 or younger persons.[84] In addition, California Consumer Privacy Act grants right to know, right to delete personal information, right to opt-out of the sale of their personal information being the landmark law in US.[85]

However, even though lacking in domestic privacy legislation, the US reacted to EU's privacy legislations in 2000s (previous to the GDPR) with a Safe Harbor Privacy Principles issued by United States Department of Commerce. The Safe Harbor was intended to work as a self-certifying legal framework which allowed US companies to comply with EU's data protection legislation and consequently permit the legal transfer of personal data between the EU and the US.[86] In 2015, the CJEU rendered the Safe Harbor Agreement null and void because it was essentially failing to meet the EU data protection standards.[87] It followed that the Safe Harbor Agreement was updated to the EU-US Privacy Shield Framework in order to repair the mechanism that would be able to restore US companies' compliance with EU's regulation on

[83] McKay Cunningham, Complying with International Data Protection Law, 2016, p. p.422.

[84] California Business and Professions Code 2015, 22580-81.

[85] California Consumer Privacy Act 2018, 1798.100 - 1798.199.100.

[86] Weiss, Martin A. and Archick Kristin, U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, February 12 2016, CRS REPORT R44257, Summary.

[87] Ibid.

transfer of personal data.[88] However, in 2020 the CJEU invalidated the Privacy Shield Framework, in its entirety, due to it being incompatible with GDPR Article 45 according to which a transfer of personal data to a third country may take place only if an adequate level of protection is ensured.[89]

The previous examples highlight how poorly the personal data have been protected in the US. The reason for poor data protection in the US is because the prioritisation of freedom of expression over privacy.[90] Another reason for lack of federal data protection legislation is because the US rely heavily on self-regulation and overregulation is seen as a threat to growing market and data-driven US companies, which constitute significant part of the market sector.[91] It appears that the US is not going to, at least in near future, put much weight on data protection and therefore blockchain based solutions could be highly effective way of managing digital identity and governing personal data of data subject. Therefore, innovations like self-sovereign identity, which will be introduced later, could level the playing field in US, while being in line with the stance on favouring self-regulation.

I have drawn the conclusion that even though both, the existing data protection frameworks and blockchain technology, are designed to protect personal data and improve data management, there is clear tension between the underlying design and fundamental characteristics of blockchain technology and the fulfilling of data subject rights laid down in

---

[88] Privacy Shield Program Overview available at https://ww.privacyshield.gov/Program-Overview visited 6.3.2022.

[89] Commission Implementing Decision (EU) 2016/1250, para 199-201.

[90] Paul J Watanabe, An Ocean Apart: The Transatlantic Data Privacy Divide and the Right to Erasure, 2017, p. 1116.

[91] Paul J Watanabe, An Ocean Apart: The Transatlantic Data Privacy Divide and the Right to Erasure, 2017, p. 1123.

the frameworks mainly due the immutability of blockchain technology. International privacy frameworks are drafted to apply systems in which centralised actors control personal data.[92] Blockchain functions different in a way that could result in shifting of power from the centralised actors to the identity holders.

Next, I will study how to coordinate blockchain technology and key data subject rights and if personal data can be stored on blockchain.

3.2 Compliance and blockchain

3.2.1 Key data subject rights

To coordinate blockchain technology and key data subject rights, it is necessary to revisit the main characteristics of blockchain. The fundamental feature creating tension between blockchain technology and current international privacy frameworks is the immutability of data on the blockchain. Otherwise, the characteristics of blockchain technology promote the fulfilment of data subject rights such as right to access and security safeguards.

The GDPR, OECD Privacy Framework, APEC Privacy framework and WAPIS Guide all grant the data subjects rights that seem to conflict with blockchain technology. The immutability causes tension between the blockchain technology and international privacy frameworks because it is impossible to amend or delete the data on blockchain creating a bit of a paradox since the immutability stemming from decentralisation is an integral part of blockchain technology that makes it so revolutionary. There are of course data subject rights

[92] CMS Legal Services, The tension between GDPR and the rise of blockchain technologies, 2019 p. 3.

that can be applied within blockchain environment such as right to access which is underlined in the blockchains design. Additionally, principles and articles regarding data security are covered by blockchain's design. In addition to immutability, the lack a central operator in the public blockchain makes the right to transfer data or data portability hard to enforce, but with private blockchain this issue can be potentially surpassed.[93] I am leaving the identification of data controllers out of scope of this study even though it remains an issue to be solved.

All the relevant international privacy frameworks grant data subjects rights, that when executed, require some sort of data alteration. These rights include GDPR's and WAPIS Guide's right to erasure and rectification and OECD Privacy Frameworks individual participation principle and APEC Privacy Frameworks access and correction principle that could all result in the data being erased/deleted, rectified, completed, or amended.[94] Because of the non-detachable nature of data on blockchain, the previous rights cannot be fulfilled if personal data is stored in public blockchain. According to the GDPR, right to rectification means that the data subject can demand the inaccurate data to be completed or corrected.[95] In addition, there needs to be a mechanism in place in order to implement this right.[96] Therefore, to comply with current international privacy frameworks, the underlying blockchain of digital identity management solution shall be alterable.

According to the GDPR, the data subject has the right to have their data erased where there is no legal ground for the processing, the data have not been processed lawfully or the data

---

[93] GDPR Article 20.

[94] GDPR Article 16, OECD Privacy Framework principle 7, APEC Privacy Framework principle VIII.23, WAPIS Guide Chapter 9.2.

[95] GDPR Article 16.

[96] GDPR Article 16.

subject withdraws consent for the processing of data.[97] Similarly, WAPIS Guide and OECD Privacy Framework contain the right to erasure and APEC Privacy Frameworks uses the wording "deleted".[98] In addition to erasure, the GDPR grants data subjects the right to be forgotten. Right to be forgotten and right to erasure ought not to be confused with each other as the former is an extension to the latter[99]. The main difference with the rights is that when it comes to the right to be forgotten, the information in itself is not false. The right to erasure can be demanded only after the information is made public in which case the right to be forgotten extends to private information as well. In the case of the right to erasure, the information is incorrect or untruthful. The right to be forgotten is an authorisation for a data subject to request blocking of data or deletion of data that is published lawfully. It is notable that compared to the right to erasure, the right to be forgotten is satisfied when all links to the data are erased meaning, that the data itself need not be deleted/destroyed which could be interpreted from the right to erasure. The same is implied in the Google Spain (2014) case.[100]

The Court of Justice of the European Union (CJEU) stated that the right to erasure only affects the search results that come up when searched by the data subject's name and what is more, the search engine is not required to delete the original source of information meaning that the information can still be accessed directly from the original source or it can come up with different search results.[101] In the same case, the CJEU ruled that the deletion of links have to

---

[97] GDPR Article 17.

[98] According to APEC Privacy Framework principle VIII.23(c), Individuals should be able to "have the information rectified, completed, amended or deleted."

[99] GDPR Recital 66.

[100] Google Spain v APED and Mario Costeja González C-131/12, 2014, para 81.

[101] Data Protection Board Guidelines in the implementation of the CJEU judgement on Google Spain v APED and Mario Costeja González (2014) exclusive summary, para 4.

be up to the limit the data subject's data cannot be accessed in EU domains but also in "relevant domains", including .com, in order to satisfy the effective exercise of the right to erasure.[102] The British data protection authority, Information Commissioner's Office (ICO), has also weighed in on to which extend the right to erasure shall be exercised. According to the ICO, the right is efficiently implemented if the data cannot be deleted which is the priority, the data can be put "beyond use".[103] What is more, the WAPIS Guide recognises the restriction of processing but only when there is uncertainty over the accuracy of the personal data, or the personal data must be maintained for evidentiary purposes.[104] This nevertheless entails that there should be technical means in place to restrict the procession of data. My interpretation of the meaning of "beyond use" would be that the data is not required necessarily to be destroyed, but the access to it have to be irretrievably blocked. Nevertheless, more case law is needed, or regulatory guidance is required, to solve the ambiguity upon erasure.

In accordance with the GDPR, it is the data controller's obligation to implement the data subjects' rights and the CJEU tackled this issue by naming the search engines controllers.[105] CJEU also held that the right to be forgotten could not be applied outside the EU.[106] This means that domains are only blocked on European territory which is not an efficient way of exercising the right to be forgotten since EU citizens or residents can still access the

---

[102] Data Protection Board Guidelines in the implementation of the CJEU judgement on Google Spain v APED and Mario Costeja González (2014) exclusive summary, para 7.

[103] ICO guideline to Right to erasure https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/ visited 24.10.2021.

[104] WAPIS Guide 2020 9.2.6.

[105] Google Spain v APED and Mario Costeja González C-131/12 (2014), para 27, 28 and 33.

[106] Search engine operators are not obligated to remove links on all the version of its search engine globally according to EU law, Google v CNIL C-507/17, para 65.

information, even though Google uses geo-blocking, by asking the information from someone outside the EU or simply using VPN. One may think, how would this affect data subjects in general, as the right to be forgotten is usually linked to articles that cover sensitive information about high profile persons. However, almost certainly, if one uses social media and googles their name, some of the person's profiles would come up as search results (unless the name in question is generic and will lead to thousands of search results). With a digital identity management solution built on blockchain technology, search results could potentially be managed by restricting the information provided to each social media service provider.

Even after considering the ruling of Google v CNIL, the EU seems reluctant to accept that the GDPR is only applying inside EU borders. According to the Opinion of the Advocate General of the EU, the operator of a search engine should delete all links that come up in the search result of the data subject's name regardless of the place from which the search is carried out.[107] The Opinion of the Advocate General upholds the confusion surrounding the question of territory and undermining the clarity that the court ruling could have provided.

Because data flows know no borders, and most data is processed by multinational companies, an international stance in some form is needed to clarify the transnational level of data protection. However, I shall note that in addition to the GDPR, the other international privacy frameworks provide extensive data subject rights on all continents apart from the US.[108] Right to be forgotten remains the odd one out and the CJEU seem to have thrown the ball in EU legislators' hands as it reasoned that the right to be forgotten could not have been applied outside the EU's borders because, according to Article 17 GDPR, the right does not extend

[107] Opinion of Advocate General Szpunar delivered on 10 January 2019, Case C-507/17, para 79(1).

[108] However, neither OECD Privacy Framework nor the APEC Privacy Framework are legally binding.

beyond Member State territory.[109] This could be interpreted in a way that if extraterritorial clause is added to the GDPR, the right would accordingly apply extraterritorially. To this day, the scope of the right is still unclear, and the digital identity management solution has the ability to fill this gap.

To clarify, I am not researching the legal grounds for the right to erasure of right to be forgotten, but I acknowledge their existence and study the implications they may have on blockchain-based digital identity management solution. For example, the territory question highlights the demand for global short term and long-term solutions for managing digital identity i.e., managing data subject's data that may include personal data. However, erasing and altering data from the blockchain have proven to be difficult because of the technical design. Moreover, immutability is the cornerstone of blockchain technology, and it is purposefully designed that way in order to uphold trust in the network.[110] To comply with the right to erasure, creative technological innovations need to be implemented. What is more, clarity on international level is needed for the definition of the term erasure as there seems to be no clear definition for the technical implementation of erasure.[111] However, because blockchain technology provides privacy by design, it solves many issues that are resulting from the uncertainty of the interpretation of privacy rules.

After interpretation of current international privacy framework, the personal data cannot be stored on blockchain, because it would be incompliance with right to rectification, erasure and right to be forgotten. Rights protecting personal data are so strong that privacy legislations

---

[109] Google v CNIL, para. 62.

[110] Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law? Panel for the Future of Science and Technology, European Parliamentary Research Service Scientific Foresight Unit (STOA) PE 634.445 – July 2019 p. 75.

[111] ibid.

would not allow keeping up immutable records. Nevertheless, public blockchain could have very productive use cases, such as storing financial transactions, if it can be ensured that no personal data is processed on the blockchain. However, there are ways to utilise private blockchain in storing of personal data while benefitting of blockchain technology's attributes without storing personal data on blockchain.

3.2.2 Potential solutions for ensuring compliance

Immutability and decentralisation are integral parts of the public blockchain. However, with private blockchains it could be possible to exercise the key data subject by deployment of an additional layer of creative solution that could offer compliance.

One of the most feasible solutions to ensure compliance with the right to rectification and right to be forgotten among other rights is off-chain storing of personal data. What is more, off-chain storing complies with the data minimisation principle of the GDPR as well.[112] However, this technique does not quite accomplish the full potential of blockchain as the personal data is in fact stored off-chain and not on the blockchain. In off-chain solutions, the personal data is stored on separate off-chain storage and only the hashes of personal data are stored on the blockchain.[113] In compliance point of view, this is extremely useful as the personal data is no longer immutable due to it being stored on a traditional database. In order to exercise the data subject rights that could result in amending or erasure of data, personal data can be simply deleted from the traditional database. In this way, the hash function on a blockchain does no longer link to personal data and therefore making the blockchain unusable for identification

[112] GDPR Article 5.

[113] Anisha, GDPR-Blockchain Paradox, 2019, p. 1229.

attempts.[114] Along the same lines, the right to rectification can also be fulfilled as the personal data off-chain can be altered with ease. Notwithstanding, off-chain solution is not compatible with a public blockchain since the public keys cannot, for fundamental reasons, be stored off-chain. In my view, an off-chain solution could be a promising solution for digital identity management as it seems to be already compliant with current international privacy frameworks and it is superior to traditional storing from a security perspective as well.

Apart from off-chain solutions, a few state-of-the-art technologies have been developed to tackle compliance issues. Ring signature, which is a cryptographic technique, allows multiple parties to agree on a contract without revealing the parties' identity by creating a ring of trusted parties to validate various data e.g., transactions.[115] This, however, does not apply to the ongoing processing of personal data as the users in a ring signature-solution are using public keys. Other potentially feasible technique is one called zero-knowledge proof that could be beneficial for adopting blockchain use when personal data is in question. The way this technique works is that it enables users to authenticate and verify blocks of a blockchain without learning the information of the blocks.[116] Zero-knowledge proofs can provide a true or false type of signal without compromising access to data and would keep it secure.[117] This would be especially useful regarding identification. To emphasise, this could for example be utilised in a situation where an individual must prove that they are over 18 in order to have an online credit card application approved. By utilising zero-proof technique, the individual is able to simply provide an answer that they are over 18 and the data provided from the

---

[114] Anisha, GDPR-Blockchain Paradox, 2019, p. 1229.

[115] De Reya, Mischon, GDPR Challenges for Blockchain Technology, Interactive Entertainment Law review vol 2 issue 1 June 2019, p. 16.

[116] Ibid.

[117] EPRS, Blockchain and the General Data Protection Regulation, 2019, p. 32.

blockchain would simply signal the service provider that this is "true", and the service provider would not learn the individual's actual age because the provider never received the data concerning the age of the individual. Utilising both, zero-knowledge proof and off-chain storing, could provide even more promising solution for digital identity management solution.

The CNIL states that using one-of-a-kind hashes with a secret key could guarantee the exercise of the data subject rights.[118] In this way, the secret key could be erased, and the data would be locked away forever. However, it does not result in erasure of the data, but the data could be considered anonymised and thus falling out of the scope of the international privacy frameworks. Similarly, the right to rectification can be guaranteed by adding a new block to the blockchain containing the rectified data but this does not result in deletion of the block containing wrongful data.[119] Therefore, guidance is needed to clarify if restricting access to data or supplementing data with additional block is sufficient enough, or should the data be de facto deleted from blockchain in order to achieve compliance. To this day, there have not been guidelines or court rulings if this is sufficient enough way to fulfil the right to rectification or erasure. Additionally, there is yet to be invented a cryptographically secure obfuscation method and it has been argued that there would never be one.[120] This would mean that hashing and encryption techniques would always result in pseudonymous information and therefore always end up in the scope of regulation. However, if the erasure or deletion of data would be interpreted loosely and if restriction of access to data would be sufficient, then storing of data on private blockchains could already be compliant with the right to rectification.

---

[118] CMS Legal Services, The tension between GDPR and the rise of blockchain technologies, 2019, p. 5.

[119] CMS Legal Services, The tension between GDPR and the rise of blockchain technologies (2019) p. 8.

[120] Ibid.

All the above-mentioned techniques either could solve the major issues of exercising data subject rights surrounding blockchain technology by adding a layer to alter or delete data or by leaving the storing of data out of the scope of regulation. At the very least, all solutions contribute to increasing data security and make it considerably harder for reasonably identify a natural person. In my opinion, the test of "all the means reasonably likely to be used", provided by the GDPR, creates a lot of ambiguity waiting to be clarified because as long as no additional guidance is provided, all obfuscation solutions have to unfortunately be deemed insufficient.[121] For practical reasons companies may steer away from blockchain-based solutions because of undesirable compliance risks created by legal ambiguity. It remains unclear if there ever will be an encryption or equivalent method that results in satisfactory data anonymisation. The shortcut for solving this problem by classifying hashed personal data as anonymised is undesired as well. It should be noted that in states such as the US, where data protection regimes are more lenient and individual freedoms are given priority, consent and contractual agreements could be sufficient enough to facilitate the storing of personal data on blockchain. However, this is not attainable solution on a global scale. Next, I will emphasise why the use of blockchain technology could have significant impact in the management of personal data by introducing digital identity.

4 DIGITAL IDENTITY AND BLOCKCHAIN

4.1 Digital identity

For the purpose of digital identity management, it was necessary to study the implications of international privacy frameworks on blockchain technology in order to reconcile processing of

[121] GDPR Recital 26.

personal data with blockchain technology. Governance of personal data and privacy are key parts of digital identity managements. Furthermore, digital identity management solution could have significant contribution to improved privacy by providing the data subject the means and methods to govern their own personal data online through digital identity. In this chapter, I will define the meaning of digital identity, study the relevant rules and regulations related to digital identity and demonstrate how personal data could be managed by providing a potential digital identity management that is in compliance with relevant international laws regulating personal data.

Everyone has the right to participate in society and economy.[122] This right cannot be fully exercised without proof of identity. Identity needs to be proven when opening a bank account, applying for education or more or less in any other situation when engaging in modern society. Management of identity in the real world supports the risk assessment related to human interactions and increases confidence between the parties and that is why identity is essential for economic and social interactions.[123] The same is true online, where the lack of a verifiable link between a physical person and a digital identity can create additional uncertainties that would not otherwise exist offline.

For this study I will define digital identity in accordance with the International Bar Association which defines digital identity as:

---

[122] UN High Commissioner for Refugees (UNHCR), Principles on Identification for Sustainable Development: Toward the Digital Age, February 2017, available at: https://www.refworld.org/docid/59db4aaa4.html. Visited 26.11.2020.

[123] "Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers", OECD Digital Economy Papers, No. 186, OECD Publishing, Paris. http://dx.doi.org/10.1787/5kg1zqsm3pns-en visited 9.3.2021.

1. “the collective aspect of the set of characteristics by which a thing is definitively recognisable or known”;

2. “the set of behavioural or personal characteristics by which an individual is recognisable as a member of a group”;

3. “the distinct personality of an individual regarded as a persisting entity; individuality”; and

4. “information, such as an identification number, used to establish or prove a person’s individuality”.[124]

The digital identity and the personal data are overlapping and therefore governance of personal data needs to be taken into high consideration when searching for digital identity management solution. The same characteristics that define digital identity can without doubt relate to identified or identifiable natural person and therefore the management of digital identity would constitute as processing of personal data as well.[125]

Digital identity that is not only covering the personal identity in the means of Article 8 of the European Court of Human Rights which the foundation of identity but additionally, the concept of digital identity extents the concept analogically to the digital environment and the definition is intended to cover the extensive characteristics associated with the digital environment, also referred to as online identity.[126] Under the right to privacy, individuals have the right to determine on what extent they share their private sphere. In short, privacy online concerns the identity and data ownership relevant to the identity. In addition, under ECHR Article 6, "everyone has the right to recognition everywhere as a person before the law” and

[124] IBA Legal Practice Division Working Group on Digital Identity, 2016, p. 11.

[125] Online-specific identifiers are for example internet cookies and IP addresses.

[126] ECHR Article 8.

digital identity could provide this for all, including refugees, in accordance with UN's Sustainable Development Goal 16.9.[127]

The blockchain can be virtually incorporated into the process of everything possible to identify digitally.[128] Consequently, blockchain technology enables the effective materialisation of digital identity. The way private blockchain will change and develop the services that manage personal data is by applying the existing service as a layer on top of the technology. Digital identity covers more information than offline identity due to digital environment and digital identity is essentially the combination of all the fragments of attributes that exist about the identity holder in the digital world. Moreover, digital identity is everchanging and it is constantly enriching itself with new information through each internet connection meaning that for example every time a person watches a video for a certain period of a time or like a post on social media site or search for certain clothes brand, they reveal a little more of themselves by leaving fragments of attributes.

The blockchain-based digital identity management enables trusted remote peer-to-peer and client-to-service provider interactions. Identity management and trust are highly important in the digital world, and it is critical that the legal issues and ambiguities, for example relating to data anonymisation techniques and what constitutes as erasure of data, relating to blockchain technology are clarified. Current developments are already foreseeable, and the legal issues related to the paradigm shift of digital identity are being solved proactively by enabling legal framework to facilitate cross-border recognition of digital identity credentials.[129] The

---

[127] ECHR Article 6 and UN Sustainable Development Goal 16.9 according to which by 2030 legal identity for all is provided.

[128] Ross, Nobody puts blockchain in a corner, 2017, p. 365.

[129] Gabrielle Patrick and Anurag Bana, Rule of Law Versus Rule of Code: A Blockchain-Driven Legal World, IBA Legal Policy & Research Unit Legal Paper, 2017, p. 35.

accounting and consulting PricewaterhouseCoopers LLP (PwC) have estimated that blockchain technology could boost global gross domestic product (GDP) by 1.76 trillion dollars amounting to 1.4% of global GDP by 2030.[130] PwC have identified the ability to create, store and share sensitive information online and protecting the personal identity as main benefits of blockchain technology.[131]

Current fragmented digital identity has many disadvantages, for instance users are expected to have different passwords for different accounts which can lead to forgetting the password and, on the other hand, if the user using same passwords causes a security risk.[132] Correspondingly, decentralised digital identity will create transparency and enable data subjects to keep track on their data by adding visibility. Most importantly, decentralised digital identity would make personal data more secure and add privacy over the data. The paradigm of digital identity today is considered centralised because the information of the user is on the servers of the entities issuing the information and that information is used solely on the purpose of the entities, for example banks require digital identity for logging into their applications.[133] With the utilisation of blockchain in digital identity management, it is possible to go through a paradigm by shifting from centralised digital identity to decentralised digital identity as

---

[130] PWC Time for trust report, October 2020 p. 4, https://www.pwc.com/hu/en/kiadvanyok/assets/pdf/Time_for_Trust_The%20trillion-dollar_reasons_to_rethink_blockchain.pdf visited 4.3.2022.

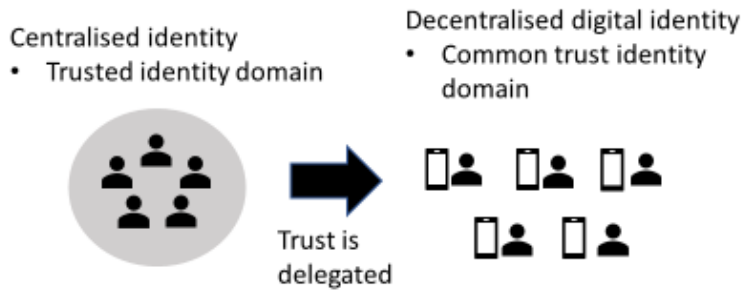
[131] Ibid., p. 11.

[132] Capisizu L.A., Digital identity, 2020, p. 257.

[133] Ibid., p. 258.

emphasised in figure 3 below. The digital identity today is described as decentralised, because the identity remains in the control of the person that created it.[134]

Figure 3. Digital identity management paradigm shift



One of the main threats of applying blockchain technology to digital identity management is legal unclarity and the problem seem to me more about technical implementation than doctrinal. In the case of digital identity management solution based on blockchain, similarly to all online innovations, the solution could be used by multiple people from different jurisdictions and most notable under the jurisdiction of the GDPR, which the UN identifies as "legal benchmark for privacy and data protection in the digital economy".[135] Nevertheless, international privacy frameworks cover multiple jurisdictions, granting extensive data subject rights outside EU as well, encouraging an international approach for solving the legal issues.

[134] The decentralized digital identity could easily be called centralized digital identity if the concept is viewed in the point of view of the creator of the digital identity. As the person who has created the digital identity never hands over the control of the identity, the identity stays in "centralized" control in the hands of its creator. Due to this fact, the term decentralized identity can be somewhat misleading.

[135] UN Economic and Social Council Harnessing blockchain for sustainable development: prospects and challenge Distr.: General 4 March 2021E/CN.16/2021/3, para 81.

4.2 Emerging digital identity laws and regulations

Meanwhile the potential to use blockchain technology in digital identity management solution is explored by international organisation, the digital identity frameworks are being developed to facilitate the application of the potential solution. ID2020 alliance and USAID are focusing on creating digital identity for those without proper identification and UN is encouraging this initiative by its Sustainable Development Goals (SDG).

Despite the blockchain technology decreasing the dependency on intermediaries and increases the trust in peer-to-peer activities, the power to regulate blockchains nevertheless remains on state governments.[136] The traditional way would be to pass laws in order to regulate the blockchain technology. It is desired to legislate digital identity technology neutrally in order to the legislation to be flexible with future technological developments that could emerge more rapidly than it takes legislation to be amended. This suggests that policies and guidance is the appropriate way to start regulating blockchain technology in the beginning and the digital identity management solution could be facilitated by technology neutral identification framework.

There are two main difficulties in regulating the blockchain technology and the first being the high-tech characteristics and management model oftentimes making it contradictory to regulatory requirements. Second, it has been discovered that attempting to frame data protection legislation to blockchain technology reveals further ambiguity of how to apply the data protection legislation and unclarity with anonymity, data subject's rights and identifying data controllers have been detected.[137] On one hand, legislations such as the GDPR have been

---

[136] De, Filippi. Blockchain and the Law, 2018, p. 173.

[137] EPRS, Blockchain and the General Data Protection Regulation, 2019, p. 96.

designed on broad principles in order to be technology neutral and flexible towards the emerging technologies like blockchain. On the other, this inflicts the uncertainty upon how to correctly apply the legislation to the technology in practice. In my view, the current international privacy frameworks need not to consider blockchain technology particularly, but additional guidance and policies should be presented on international scale, as it would be most efficient way to prevent the risk of regulatory fragmentation.

As stated in the Joint Inspection Unit (JIU) Report on blockchain applications, it is too early for rigid regulation of blockchain and instead, minimum standards and policies should be introduced.[138] Digital identity solution is only one of multiple possible blockchain technology applications and the blockchain use cases vary a lot, meaning that even issuing minimum standards that consider wide range of applications but are not too broad to have on effect will be challenging. Though, blockchain-based digital identity solutions can be developed while disregarding the current legal ambiguities over who is the controller of the solution. Ideally, guidelines on controllers of blockchain solutions are issued sooner than later and this would most probably lead to emergence of blockchain-specific intermediaries which is a good thing because expertise on the blockchain technology would increase data security.

International organisations have a major impact on international custom and major part of international law is created by or within international organisations.[139] Most commonly international organisations are created by states by the means of a treaty to fulfil a purpose that the states cannot or will not fulfil themselves, for example UN for collective security and

[138] Blockchain applications in the United Nations system: towards a state of readiness Report of the Joint Inspection Unit JIU/REP/2020/7 Geneva, 2020, p. 44.

[139] Klabbers, International Law (2017), p. 91.

World Bank for development.[140] The international organisations are built around functions and can therefore act significantly more efficiently globally than states that are bound on territory. Although some organisations are heavy in their nature and formed as platforms for states to discuss and debate on issues rather than making fast decisions.[141] International organisations are able to create projects under their supervision as one way to streamline research and problem solving regarding emerging issues. Prime examples of previous are EU's Blockchain Observatory and Forum and OECD's Global Blockchain Policy Forum.[142]

To grasp the potential of blockchain technology, industry standards are already being produced and in near future the problem would not be the lack of standardised guidance but the inconsistent and disjointed national standards.[143] National Institute for Standards and Technology of the United States of America is exploring blockchain-based identity management systems and The European Blockchain Partnership is in the middle of establishing an European blockchain services infrastructure to facilitate cross-border digital public services.[144] It appears that the JIU have already identified the International Organization for Standardization (ISO) to be the competent organisation to lead the standardisation of blockchain technology. In fact, ISO has already published an early consideration for privacy and personally identifiable information regarding blockchain and

---

[140] Klabbers, International Law (2017), p. 91.

[141] E.g., the UN General Assembly consist of all 193 members of the UN.

[142] The purpose of these forums is to monitor and promote coordination of blockchain initiatives in Europe and across the globe and share knowledge in European and global setting. See more https://www.eublockchainforum.eu/about and https://www.oecd.org/finance/oecd-blockchain-policy-forum.htm.

[143] JIU/REP/2020/7 p. 46

[144] Ibid.

other distributed technologies.[145] What is more, The International Telecommunication Union's Telecommunication Standadrization Sector (ITU) have produced technical standards for blockchain applications which is significant since ITU is an intergovernmental institution with backing of UN member states.[146]

According to the UN General Assembly, the United Nations Commission On International Trade Law (UNICITRAL) is "the core legal body within the UN system in the field of international trade law, aimed at increasing coordination of, and cooperation on legal activities of international and regional organisations active in the field of international trade law, including legal issues relating to the digital economy"[147] UNICITRAL is able to establish principles and practises and give recommendations to minimise divergence regarding the state regulation on new issues typically caused by emerging technologies such as blockchain technology.[148] Through conventions, UNICITRAL is able to establish legally binding obligations.[149] By unified efforts of UNICITRAL and UN member states on legal issues surrounding blockchain technology, it could be possible to achieve harmonised and consistent laws, guidelines and/or principles that would prevent fragmented national legal response to blockchain technology. Thus, the way to coherently fill the legislative gaps regarding blockchain technology would be the combination of national and international legislative powers to achieve the best regulatory guidance on how to apply data protection principles to

---

[145] ISO/TR 23244:2020, available for a fee.

[146] JIU/REP/2020/7 p. 47.

[147] United Nations, General Assembly, resolution 74/182, Report of the United Nations Commission on International Trade Law on the work of its fifty-second session, doc. A/RES/74/182, para 9.

[148] A Guide to UNCITRAL Basic facts about the United Nations Commission on International Trade Law, UN Vienna, 2013 p. 13.

[149] Ibid.

blockchain technology. In addition, these guidelines shall be combined with the technical standards produced by international organisations.

Technological innovations relating to internet know no boundaries and therefore I believe it would be best to issue the policies and guidance on international level. On one hand, more people would gain access to the innovations, at least more rapidly, and on the other the technical solutions would be more coherent and therefore it would be easier to implement legislation that would ensure that the technological solutions have room to develop to admired direction. More importantly, the international guidance would guide the innovations to worldwide, user-safe, and secure direction and could at least establish rules for best-practises.

UN have published SDGs that provide guiding principles that should be taken account with emerging technologies.[150] Out oof all SDGs, the SDG 1.4, which aims for equal rights to ownership, basic services, technology, and economic resources, is the most relevant to blockchain-based digital identity solutions. The key goal is to find user-friendly methods and tools in managing private keys and overall use of blockchain in digital identity solutions. Digital identity could enhance the goal of financial inclusion and identity for developing countries.[151] In fact, a digital identity project is being developed in Thailand and Turkey to create a national digital identification platform which is built on blockchain technology and used for authentication and verification of digital identities.[152] Indeed, UN have identified

[150] There 17 sustainable development goals in total, see more https://sdgs.un.org/goals visited 6.3.2022.

[151] Ibid. Chapter III.A.

[152] see more. Harnessing blockchain for sustainable development: prospects and challenges Geneva, Switzerland 18-22 January 2020 https://unctad.org/system/files/non-official-document/CSTD_2020-21_c30_B_Thailand_en.pdf visited 6.3.2022.

identity as one of the SDGs that blockchain could have direct relevance on.[153] According to UN, there is more than one billion people around the world living without legal identification, which is restricting their access and different rights.[154] In accordance with SDG 16.9, legal identity shall be provided for all by 2030 and UN Office of information and communication technology have stated that a blockchain based digital identity could provide a solution to firstly receiving a digital identity and secondly, protecting the digital identity from unauthorised use.[155]

The UN have released in 2019 principles on identification for sustainable development (the Principles) which includes principles on inclusion, design and governance.[156] The purpose of the Principles is to strengthen the identification systems in order to "support development and the achievement of the Sustainable Development Goals".[157] According to the Principles, identification systems should be robust, context-appropriate and interoperable.[158] In addition, the Principles demand, similarly to the GDPR, privacy by default in order to protect user privacy and for this purpose privacy shall be considered especially from the point of view of

---

[153] UN Office of information and communication technology, Blockchain – What does it mean for the UN, June 2018 (2 of 3) Emerging technologies whitepaper series: Blockchain and distributed ledgers https://unite.un.org/sites/unite.un.org/files/emerging-tech-series-blockchain.pdf.

[154] Ibid.

[155] UN Office of information and communication technology, Blockchain – What does it mean for the UN, June 2018 (2 of 3) Emerging technologies whitepaper series: Blockchain and distributed ledgers https://unite.un.org/sites/unite.un.org/files/emerging-tech-series-blockchain.pdf.

[156] UN Principles on Identification for Sustainable Development: Toward the Digital Age, https://www.osce.org/files/Identification%20Principles%20FINAL_0.pdf, p. 1, visited 6.3.2022.

[157] Ibid., p. 2.

[158] Ibid., p. 12.

end user/data subject.[159] As previously provided, blockchain technology complies with privacy by default principles, including Principle 6 "protecting user privacy and control through system design", without requiring action from data subject to actively protect its personal data.[160] The UN has pretty much identified the same issues as presented previously in this study, including the lack of data privacy being global issue and that harmonised approach is required, users are not fully in control of their data and solution should provide transparency and security among other things.[161] Blockchain technology has this ability to give users control over their personal data through Self Sovereign Identity systems, where the users would control the storing of their own data. Especially the Principle 8, which provides a guide for comprehensive legal framework in order to safeguard data privacy, security and user rights, emphasise why blockchain technology should be applied for digital identity solution.[162] In accordance with the Principle 8, the identification legal framework should "protect end-users against inappropriate access and use of their data by third parties' for undue commercial surveillance or unlawful profiling".[163] When it comes to user rights, identification services under the identity framework should provide end-users with genuine choice and control over the use of their data, including the ability to selectively disclose only those attributes that are required for a particular transaction".[164] If one replaces "legal framework should" with "the Self Sovereign Identity (SSI) has the ability to", the sentence would still be correct. The SSI is a potential digital identity management system that

---

[159] UN Principles on Identification for Sustainable Development: Toward the Digital Age, p.14.

[160] Ibid., p. 16.

[161] Ibid., p. 18.

[162] Ibid.

[163] Ibid., Principle 8, p. 12

[164] Ibid.

Another organisation seeking after digital identity solution is ID2020 Alliance, which is with UN's assistance, attempting to provide safe, verifiable, and persistent digital identity system using blockchain technology by 2030 in accordance with SDG 16,9 in order to offer legal identity for all and assist millions of refugees globally in near future.[165] ID2020 alliance is formed by governments, NGOs, and private sector companies, including Microsoft and Accenture.[166]

In EU's approach, the European Commission have proposed amendment to legislation regarding the establishing a framework for a European Digital Identity (eID) by amendment to regulation (EU) No 910/2014 (EIDAS).[167] The EIDAS framework aims to build trust in the online environment.[168] What is more, EIDAS is expected to support the development of emerging technologies such as blockchain technology.[169] The eID seeks to create a wallet containing identity of a person.[170] The wallet would be available on a device such as mobile phone. The eID system would be provided by EU member states based on national electronic identification systems.[171] The use of wallet would be accepted both by public and private

---

[165] EPRS study on technological innovation for humanitarian aid and assistance, (STOA) PE 634.411 – May 2019, p. 58 and ID2020 approach https://id2020.org/digital-identity#approach visited 27.2.2022.

[166] ID2020 Governance https://id2020.org/alliance visited 27.2.2022.

[167] 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, 2021/0136 (COD), Brussels, 3.6.2021 .

[168] Regulation (EU) No 910/2014, Recital 1.

[169] Preliminary Opinion on privacy by design, Opinion 5/2018, European Data protection Supervisor 31.5.2018, para 104

[170] 2021/0136 (COD) Explanatory Memorandum, p. 3.

[171] Ibid.

sector for provision of services.[172] The purpose of the wallet is to enable online and offline identification and store and share information received from public authorities and trusted private sector entities.[173] By utilising blockchain technology, the eID can be provided as self-sovereign identity. Because EIDAS' definition for electronic document includes all information stored in electronic form, this could be interpreted to include data stored on blockchain's blocks. Perhaps surprisingly, it seems that the EU has legal framework in place for blockchain-based digital identity as soon as the identified ambiguities regarding anonymity and exercising data subject rights are cleared. However, it takes a long time to see this proposal in application because it takes time to go through negotiations within EU and the statute would not ordinarily be given legal effect until 24-48 months after adaptation. However, if the proposal is passed, it would have potentially significant implications for electronic identification and trust services in general, including validation of digital identity solutions such as SSI systems.

While the EU is building its own digital identity framework, the US have just started to develop its counterpart for digital identity under USAID with a more international approach.[174] The USAID report for identity in a digital age: infrastructure for inclusive development follows the UN's SDGs and addresses and recommends the use of blockchain technology explicitly.[175] The report identifies multiple use cases for "blockchain-backed ID" including humanitarian cash transfers and economic ID for keeping record of transaction history and problems it could solve including resilience against destruction and loss which

---

[172] 2021/0136 (COD) Explanatory Memorandum, p. 3.

[173] 2021/0136 (COD) Article 1.

[174] For the sake of clarity, USAID should be hyphenated to US AID, not USA ID, but the name of the organization is an amusing coincidence, nevertheless.

[175] Identity in a Digital Age: Infrastructure for Inclusive Development, USAID, September 2017, p.1-3.

could be extremely useful in unsettled states.[176] The report acknowledges that there are multiple ongoing international processes in search for blockchain application and highlights identity solutions, however admitting that none are ready for operation.[177]

All in all, a lot is happening on multiple fronts in relation to blockchain technology and digital identity. New use cases are emerging, and key privacy issues are being identified and demanded to be solved. I forecast the developers and stakeholders from various industries start soon pushing for clarifying policies and guidelines in order to get rid of security and operational risks and the tension between data protection legislations and blockchain technologies. Meantime, states and international organisations are developing digital identity frameworks because the potential and rapidly increasing demand for digital identification solutions have been realised. The international legal framework for blockchain-based digital identity solution like SSI consists of international privacy frameworks and the emerging identification legislations such as EU's eIDAS Regulation in addition to technical standards.

Lastly, I will attempt to provide a possible solution, based on the parameters established before, for a digital identity management solution utilising blockchain technology.

4.3 Self sovereign identity

By studying the applicable international privacy frameworks regulating the processing of personal data and restrictions they may have on the use of blockchain technology, I have been able to identify self-sovereign identity (SSI) as a possible solution that could, in practice, provide the means and methods for utilising blockchain technology and enable the data

[176] Identity in a Digital Age: Infrastructure for Inclusive Development, USAID, September 2017, p. 2.

[177] Ibid.

subjects to take control over and manage their digital identities as well as facilitating the storing of personal data.

As presented before, the blockchain technology could change digital identity from the present centralised digital identity paradigm to decentralised digital identity paradigm. The SSI can provide a form of data management with increased data protection and features that benefit the data driven economy and enables data subjects to take back the control over their personal data that relates to them in digital environment. The emerging digital identity legislations will likely help to facilitate this shift. In the decentralised digital identity model, the user is placed at the centre of the identity framework, but still most of the user's data is dependable on the issuance of others.[178] For example, passports and driving licenses are issued by central authorities.

The concept of SSI consists, firstly, of the person's ability to control their identity and, secondly, of all the data that can be linked to the identity of that person. Hence, the person has the means to create and control individual identifiers and the facilities for the storage of the created data linked to the identity.[179] This means that the person can share only the data that they choose to, regardless of the data content, from social media data, payment transaction history or proof of identity issued by public authority, personal data included.

What is more, the person can, due to the ability to gather, control and store data from different sources, create multiple different digital identities which the person can then share depending on the context.[180] The SSI has not been invented until recently, because there have not been the technological capabilities to build it upon. It is necessary to have technologies in place to

---

[178] Capisizu L.A., Digital identity, 2020, p. 260.

[179] Ibid.

[180] Ibid.

create and control their identities that are called decentralised identifiers (DIDs) and technologies to store the DIDs, which could be done by creating digital wallets.[181] The term "mobile wallet" originally refers to the persons possibility to make payments on smartphones, which was not so long ago considered revolutionary as the first fully functioning banking app was launched in 2011.[182] The handing of the private data over to a third party underlies the need for strengthening the digital privacy protections of personal identity information stored in mobile wallets.[183] Digital wallets are mobile wallets that store the DIDs and able the person to control their own digital identity. The proposal for eIDAS expressively mentions digital wallets and gives the wallet a purpose of requesting and validating personal identification data and electronic attestations of attributes.[184]

The objective for GDPR Article 17 is to facilitate the data subjects' control over their data by the means of erasing their data in almost all circumstances, including when there is no unlawful procession to exercise the right of freedom of expression and information.[185] The SSI could provide just that and more. To start with, based on research findings concerning applicable international law, the blockchain-based digital identity solution should 1) be built on a private blockchain 2) use state-of-the-art pseudonymisation and encryption techniques for the purpose of data security and protection and 3) store the personal data off-chain in order to achieve compliancy with data subject rights, especially with right to be forgotten and right to

---

[181] Capisizu L.A., Digital identity, 2020, p. 260.

[182] Royal Bank of Scotland launched the banking app in May 2011 https://www.natwestgroup.com/heritage/history-100/objects-by-theme/going-the-extra-mile/banking-app-2011.html visited 20.10.2020

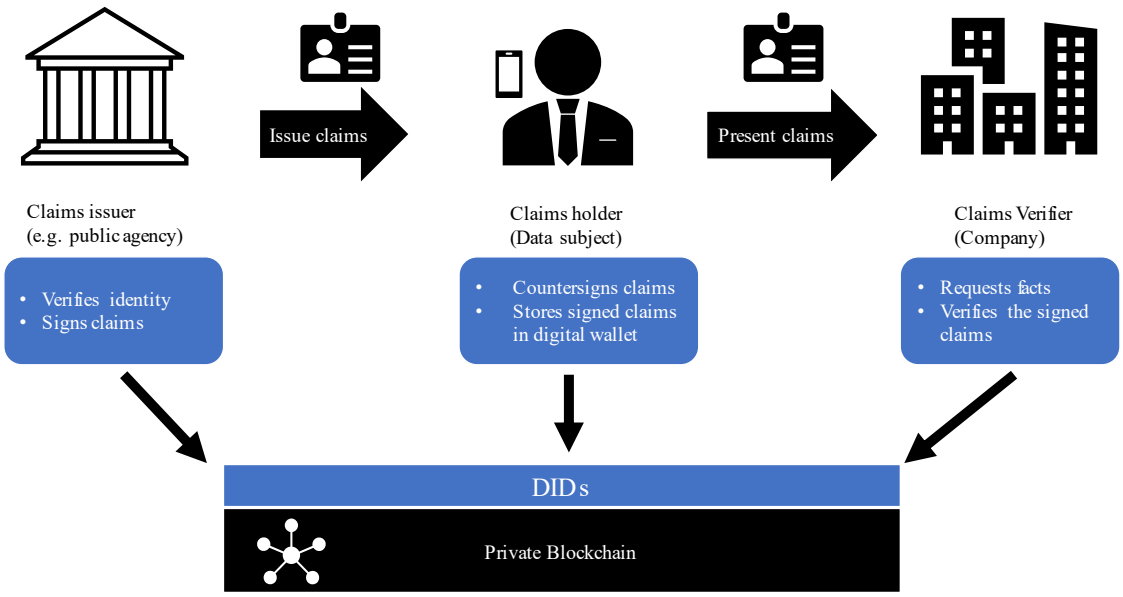
[183] Ross, Elisabeth Sara, Nobody puts blockchain in a corner, 2017, p. 372.

[184] Proposal for amending Regulation (EU) No 910/2014 Article 4(a)(2)-

[185] GDPR 17.3(a) Right to be forgotten.

erasure. The sharing of digital identity is implemented in SSI system that utilised blockchain technology. The shared digital identity or DIDs are not stored on the blockchain but the blockchain is rather used for purpose of ensuring that the recipient of the data can be sure of the accuracy and validity of the data shared from another source. The blockchain technology includes by default multiple features designed to facilitate the creation of DIDs as well as the blockchain provides the decentralised infrastructure to control the accessing of the data. In the SSI system any individual can use a simple, standardised, and portable digital wallet and DIDs to prove their identity, establishing trust and providing verifiable data in any context—without ever surrendering control of their personal data. The use of DIDs enable SSI as presented in the figure 4, below.

Figure 4. Self-sovereign identity



Daily, people prove something about themselves when using physical documents, for example passports, and trust in these documents are based on the organisations that issue them. The purpose and value of these documents are widely understood. The development of blockchain technology is enabling this new framework for digital identity. Digital identity is to be

considered a new legal concept and only strengthening this argument is the SSI which is a digital identity management enabling the control of DIDs from which the digital identity consists of. The SSI enables the data subject to share reliable information from trusted authorities, for example proving their identity, while keeping the digital identity under their control and it could be even argued that with SSI, the data subject becomes the controller of their data.[186] In the decentralised paradigm a person can create an SSI that would corresponds to an identity identified in the physical world. This provides better personal data management while improving authentication of identity online and promoting data sovereignty. As emphasised in figure 4, above, SSI provides the means to create and manage personal data of the identity by utilising the blockchain technology. The personal data is not stored on the blockchain, but the blockchain is used to ensure that the recipient of the data can otherwise verify the accuracy and validity of the data with the zero-proof technique.

To conclude with, based on the findings of this study, private blockchain should always be opted when personal data processed. Additionally, unless the legal ambiguities of how the right to rectification and erasure are technically implemented, the off-chain solution is recommended in order to achieve compliance with data protection regulations.[187] The right to erasure and the right to rectification can be secured by storing data off-chain which would mean no personal data is stored on blockchain. In addition, the data stored off-chain shall be encrypted to ensure sufficient level of data protection. What is more, the link between off-chain and blockchain shall always be hashed. The access to personal data would be provided by design when data is stored on blockchain. However, in off-chain solutions such as a digital wallet facilitating the SSI, access shall be managed, and the data subject identified upon

[186] If the data subject would be considered the controller, it would reduce corporate responsibility and improve compliance.

[187] In theory and on technical point of view, the SSI system should work similarly as described in figure 4, whether the blockchain is public or private.

registration. The GDPR requires data to be processed with integrity and confidentiality in a transparent manner, all of which blockchain technology can provide by default and design.[188] Consequently, this means that the blockchain solution for identity management should process personal data by implementing appropriate technical and organisational measures, for example pseudonymisation and integration, necessary safeguards in order to comply with the GDPR and protect the data subject rights.[189] The SSI meets the design and default requirement and the key to compliance lies in the choice of specific blockchain and the anonymisation technique used in the SSI. Nevertheless, SSI can be considered viable digital identity management solution that also is, in the present, in compliance with all current international privacy frameworks.

5 SUMMARY

Despite advanced hashing techniques, personal data stored on blockchain still falls under the scope of current international privacy frameworks because the personal data can be reversibly encrypted, and hashed data is still considered pseudonymous data. Additionally, because immutability is integral part of blockchain's design, personal data cannot be, in order to be in compliance with international privacy frameworks, stored on blockchain. However, private blockchain provides an additional layer to blockchain technology which enables the utilisation of blockchain technology in storing of personal data. What is more, in addition to personal data, innovative solutions can provide and facilitate the ability to manage digital identities.

The international framework for digital identity management is two-folded, consisting firstly, on international privacy frameworks applicable on processing of personal data, and secondly,

---

[188] GDPR Article 5.

[189] GDPR article 25 and recital 78.

on emerging rules, regulations regarding digital identity. The relevant international privacy frameworks that the blockchain-based digital identity management solution needs to be in compliance with are OECD Privacy Framework, the GDPR, APEC Privacy Framework and WAPIS Guide because the digital identity consists of DIDs which will inevitably constitute as personal data. These privacy frameworks provide data subjects multiple rights of which right to rectify and erasure and right to be forgotten raise the biggest concerns over the application of blockchain technology as the data stored on blockchain violates the key rights since the blockchain's immutability would obstruct the ability to delete or amend the personal data stored on the blockchain. Notwithstanding, off-chain solution provides the compliancy with current international privacy frameworks. If the erasure and deletion of data would be interpreted loosely and not literally, restricting access irretrievably to personal data stored on blockchain could offer compliance. However, legal ambiguity still remains over the definition of erasure and the classification of pseudonymous data. Additionally, classification of hashed personal data as pseudonymous data would clarify and possible open the door for other solutions in addition to off-chain solution. Finally, the identification of data controller in decentralised digital identity management is an important question that this study did not provide an answer but is nevertheless an issue that needs further consideration.

There are emerging rules and regulations relating to digital identity on multiple fronts. The ISO and the ITU are creating technical standards for application of blockchain technology, EU's eIDAS Regulation aims to support the facilitation of blockchain-based digital identity management and ID2020 Alliance and USAID are seeking for digital identity managements solutions with particular focus on helping the ID-less. Out of all international organisations, I believe UNICITRAL could provide the most meaningful guidance on best practices on digital identity solutions.

The SSI is a digital identity management solution that is, when built on a private blockchain that uses state-of-the-art encryption techniques and hashes and storing personal data off-chain in a traditional data base, in compliance with current international privacy frameworks. Consequently, only the hash of the personal data is stored on blockchain, and, upon request,

the personal data can be easily deleted from the traditional data base rendering the decryption of the hash stored on on-chain useless. What is more, the SSI uses zero-proof technique which provides additional benefits of data minimisation and data security. However, this method is criticised because it lacks the benefit of transparency that blockchain technology would otherwise provide by default. Still, this results in compliancy with the applicable international laws by enabling the exercise of key data subject rights. The ability to utilise blockchain technology in storing of personal data could potentially result in paradigm shift and promotion of data sovereignty because in the SSI system, the data subjects maintain the control over their personal data instead of surrendering the data over to companies.

In mathematics, a theorem is a statement that is true and in order prove the theorem, it has to be provided with logically established “proofs”. I would like to think that the key result of this study is that the SSI is to be considered as a valid digital identity management solution for compliant storing and sharing of personal data and for which this study has provided legal “proofs”.