Blockchain and the EU General Data Protection Regulation

Pei Lin Hsu

CTBC Business School

I. Introduction 2

(II) The GDPR Supervisory Framework and Blockchains 3

1. Core Principles and Rights of GDPR 3

2. Blockchain Features 3

(II)Permissionless and Permissioned Blockchains 4

1. Permissionless Blockchain 4

2. Permissioned Blockchain 5

3. Data Protection in the Permissionless Blockchain 6

Personally Identifiable Information (PII) 7

(I)Lex Cryptographica 7

(II)Pseudonymisation and Anonymous in the Blockchain 9

1. Pseudonymisation 9

2. Standard of Anonymity 11

(III) One-way Hash Function 13

III. Personal Data Security and Privacy Protection 14

(I) Strengthening of Personal Data Protection by the GDPR 14

(II) Zero-knowledge Proofs 15

IV. Data Control and Processing for the Blockchain 17

(I) Data Controller 17

(II) Data Processing 19

V. Implementation and the Future of Personal Data Protection for Blockchain 20

(I) Analyze applicability for each case 20

(II) Evolution of Encryption Technology and Legal Risks..... 21

I. Introduction

The vibrant development of digital technologies in recent years has led to personal profiles and data being applied on a massive scale by technologies such as Big Data, Mobile Internet, Internet-of-Things (IoT) and Cloud Computing. GDPR provides a complete and consistent framework for the implementation of personal data protection against this digital tsunami by each member nation. The General Data Protection Regulation (EU) 2016/679 ("GDPR") was formulated in 2016 by the European Parliament and European Council to protect the processing and free movement of personal data belonging to natural persons. [1]EU GDPR replaces the EU Data Protection Directive (EU Directive 95/46/EC) from 1995 and formally took effect in all EU member states on May 25, 2018. [2]

---

[1] RECITAL (171) EU GDPR: directive 95/46/ec should be repealed by this regulation. Processing already under way on the date of application of this regulation should be brought into conformity with this regulation within the period of two years after which this regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation.Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed.

[2] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(II) The GDPR Supervisory Framework and Blockchains

1. Core Principles and Rights of GDPR

The core principles proposed by GDPR include the lawful, fair and transparent processing of data, only collect data for specific purposes, not process data for an incompatible purpose, and the data held must be adequate for the purpose and limited to what is necessary (data minimization); data should be accurate and kept up to date; data should only be stored for as long as necessary and processed in a safe manner.[3]GDPR provides personal data the following key rights and protections:

(a)Transparency and Modalities: The main body of information is transparent information, communication and communication to exercise its rights.(b) Information and access to personal data Right to Access: Information provided when collecting personal data of the data subject).(c) Information Obligation of the Controller Prior to Processing: Information to be provided where personal data have not been obtained from the data subject.(d) Right of access by the data subject.(e) Right to Erasure, Rectification and Restriction.(f) Right to Object.(g) Right to Data Portability.(h) Automated individual decision-making, including profiling.[4]

2. Blockchain Features

Blockchain has the following features: Decentralization, flexibility and immutability, transparency, pseudonymisation, autonomy, consensus mechanism, and incentive measures. The low-level protocols of blockchain applications operate on lex cryptographica. Decentralized blockchain technology operates

---

[3] Luis-Daniel Ibáñez, Kieron O'Hara, and Elena Simperl, On Blockchains and the General Data Protection Regulation, Ibanez, Luis-Daniel, O'Hara, Kieron and Simperl, Elena (2018) On Blockchains and the General Data Protection Regulation EU Blockchain Forum and Observatory 13pp. Published date: 6 July 2018, https://eprints.soton.ac.uk/id/eprint/422879, at 3.

[4] Sandra Wachter, Brent Mittelstadt and Chris Russell of University of Oxford co-authored "Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR" to explore how the GDPR normative framework can be applied to automated decision making.

across national bounders without being subject to the controls of a single central organization. The rules change greatly or even conflict with each other between the countries it passes through resulting in a variety of different outcomes from the application of law. The question of jurisdiction for illegal online behavior has proven to be a major challenge for national courts.

GDPR changes the model for personal data protection. Roles such as data controllers and data processors as defined by GDPR are required to ensure that their procedures for the processing and handling of data comply with GDPR regulations. The technical characteristics of blockchain technology have influenced the data protection regulations of GDPR in a number of ways as well. For example, blockchains can enhance the security of data protection. Engineers can design blockchains that solve special GDPR requirements on traceability or immutability during data processing. As for differences across regions, national boundaries and supervisory systems, connecting blockchains together to form a transparent and open "Global Cloud" may lead to the creation of a new mechanism for trans-national governance. Blockchain attributes such as openness, democratization and decentralization may provide fairest and most effective transnational supervisory mechanism. [5]

(II)Permissionless and Permissioned Blockchains

1. Permissionless Blockchain

Bitcoin and Ethereum are both "Permissionless" blockchains where anyone can use the "open source software" to access and use the blockchain over the Internet. The identity of the user does not have to be disclosed during the process either. The openness, decentralized nature and pseudonymisation of permissionless blockchains raise concerns over their potential for criminal abuse when applied

[5] Melanie Swan 著，沈佩誼譯，區塊鏈-未來經濟的藍圖(Blockchian: Blueprint for a new Economy)，碁峯出版社，2018 年 2 月初版 2 刷，頁 55。

to banking and financial transactions or supervision. Regulators and financial institutions are therefore required to strengthen their tracking and screening of participants' identities in order to deter illegal activity. [6]

2. Permissioned Blockchain

The reverse of the permissionless blockchain (also referred to as the public blockchain) is the permissioned blockchain (or referred to as the private blockchain). Permissioned blockchains rely on P2P networking and is not open to everyone. The identity of the participants are screened and controlled. They are frequently found in governments' supervisory applications or regional alliances such as the Consortium Chain of European banks. [7] Members of a blockchain alliance can select who has permission to visit the shared database or to share data. [8] A well-known example is the Ripple protocol that uses approved blockchains to facilitate the exchange of currencies and the storage of other value. Currencies that it has been used with include USD, Euro, Australian Dollar and even gold. Hidden within the Ripple protocol is a consensus mechanism different to the Proof of Work (PoW) used by Bitcoin and Ethereum. This particular mechanism relies on trusted sub-networks within the Ripple network to process and validate transactions. Bitcoin is an example of Blockchain 1.0. Ripple allows transactions of fiat money to be completed by banks within seconds at a very low cost. Ripple can operate process a number of widely used currencies in real-time so a number of financial institutions have already integrated the Ripple protocol into the payment infrastructure of their own banks. From this, we can see that blockchain can improve the operational efficiency of traditional exchange markets and offshore banks. Customers do not have to convert their existing USD or Euro deposits into a digital currency to enjoy the efficiency and low-cost transactions provided by blockchain technology. [9]

---

[6] Primavera De Filippi and Aaron Wright 著，王延川譯，區塊鏈與法律-程式碼之治，元照出版社，2019 年 2 月初版。

[7] Introduction to the bank alliance chain, reference URL: https://www.blocktempo.com/r3-corda-settler/

[8] Allison Berke, “How Safe Are Blockchains? It Depends,” Harvard Business Review, March 7, 2017, https://hbr.org/2017/03/how-safe-are-blockchains-it-depends.

[9] Primavera De Filippi and Aaron Wright 著，王延川譯，區塊鏈與法律-程式碼之治，元照出版社，2019 年 2 月初版，頁 87-89。Bryant Gehring, “How Ripple Works?” Ripple, October 16 2014, http://ripple.com/knowledge_center/how-ripple-work/.

Compared to the powerful consensus of trust mechanism in a permissionless blockchain, permissioned blockchain's authentication mechanism means that it cannot guarantee that some nodes may eventually collude against other participants in the network to tamper with the low-level blockchain. As only a small number of people can validate and write data to the blockchain, the participants then become a single point of failure or control. There is therefore a higher risk of technical failure or damage from hacker attacks. [10] "Trust" can be unpredictable and the security limitations of the permissioned blockchain may lead to catastrophic consequences especially if is used for developing a key pillar of support for social or economic systems. [11]Nevertheless, the permissioned blockchain offers the advantage of speed as validation is carried out by chosen participants. [12] Private blockchains may have less difficult with GDPR compliance however since permissioned blockchains are controlled by specific persons with supervision or validation handled by core members.

3. Data Protection in the Permissionless Blockchain

Blockchain technology encompasses both permissioned and permissionless blockchains. Private permissioned blockchains are not decentralized blockchains so it is quite feasible for a programmer to develop a mechanism that complies with the legal requirements on data protection. The research focus of this paper is therefore the public blockchain as public blockchains can be used to perform legitimate work or for supporting all kinds of hard-to-trace illegal activities. Whether the data stored in a decentralized public blockchain operating under lex cryptographica is subject to GDPR supervision, and whether pseudonymisation in permissionless blockchains operating under the GDPR supervisory framework can be excluded from the scope of GDPR supervision are issues that this paper seeks to explore.

---

[10] Primavera De Filippi and Aaron Wright 著，王延川譯，區塊鏈與法律-程式碼之治，元照出版社，2019 年 2 月初版，頁 45。

[11] Allison Berke, “How Safe Are Blockchains?”, March 07, 2017, https://hbr.org/2017/03/how-safe-are-blockchains-it-depends

[12] Vitalik Buterin, “On Public and Private Blockchains,” Ethereum (blog), Au- gust 7, 2015, https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

Personally Identifiable Information (PII)

Article 2 of the GDPR stipulates the scope of application of the entity, and the Paragraph 1, Subparagraph 1 of the same article excludes of the same article excludes the regulation of personal data in the course of an activity which falls outside the scope of Union law.

However, Article 3, paragraph 2, states this Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not, including Subparagraph (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union.

There is for example no need to disclose your own location or personal information during Bitcoin transactions. This encrypted digital currency network imposes no restrictions on user identity however so its service might be provided to EU residents. Its actual scope should therefore include blockchain networks that can provide global cross-domain services.

(I)Lex Cryptographica

Blockchain make extensive use of cryptography in its operation. Bitcoin for example involves cryptographic keys (private and public keys), symmetric encryption, asymmetric encryption, Hash, and Elliptic Curve Cryptography (ECC). [13]Autonomous protocols and services based on blockchain technology use the aforementioned cryptographic techniques form an autonomous system of rules referred to as lex cryptographica. [14] The implementation of cryptographic

---

[13] Elliptic Curve Cryptosystem is a general term for public key cryptography, digital signature and key exchange cryptography using elliptic curves.

[14] Primavera De Filippi and Aaron Wright 著，王延川譯，區塊鏈與法律-程式碼之治，元照出版社，

rules on a decentralized point-to-point network allows blockchain protocols and services to run themselves without any intervention from a central agency. [15]

Data stored in a blockchain can be divided into two categories. One is "transaction data" such as all the different transactions and message sent between users; the second is "public key.": that is, the user's personal identification code. Every participant and miner has a public key that is used for identifying the publisher and recipient in a transaction. This includes the transaction itself as well other information such as text certificates or asset contracts.

GDPR Article 4, Paragraph 1 defines "personal data" as defined in Article 4, Paragraph 1 of the GDPR means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Personal Data" refers to any information that directly or indirectly linked to the natural person whether it is identifiable, or whether it can be made identifiable through analysis with technical tools. GDPR regulations generally cover identifiable through analysis by: Data controller, exercising of rights, implementation of appropriate protections and security obligations. The central question in this study is whether GDPR is applicable to blockchain and how personal data should be handled by blockchain applications. [16]

Paragraph 2 of the same article stipulates "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation,

---

2019 年 2 月初版，頁 69-71。

[15] Primavera De Filippi and Aaron Wright 著，王延川譯，區塊鏈與法律-程式碼之治，元照出版社，2019 年 2 月初版，頁 69-71。

[16] Paul Voigt, Axel von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide, Springer, Berlin Germany(2017), at 11. 2017.9, A guide to blockchain and data protection https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf

structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Paragraph 2 of the same article stipulates pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

(II)Pseudonymisation and Anonymous in the Blockchain

1. Pseudonymisation

Participants in a Bitcoin for example do not need to disclose their real identity and all users can create a pseudonymous key pair at any time. The public key in the Bitcoin blockchain is visible to everyone and is held by the service provider. Even though it is a pseudonym, information analysis techniques can still be used to obtain identifying information for that person. The public key records may be linked to a natural person or legal entity. By analyzing the IP address or other links on the website, it may be possible to obtain personally identifiable information from the public key records. [17] If a public key becomes associated with a specific person or organization then it may qualify as personal data.

Recital 26 EU GDPR: "The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to

[17] A guide to blockchain and data protection,(2017.9) https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf

identify the natural person directly or indirectly."

All objective factors must be considered when determining what constitutes reasonable means of identifying the data subject, including: The cost and time required for identification. Existing technologies and the level of technological development should also be taken int account. Data protection rules does not apply to anonymous information. That is, information that is not already identifiable or can be used to identify the subject, or personal data that has been made anonymous through methods that make the subject impossible to identify, or cannot be identified again. The processing of anonymous information like this for statistical or research purposes this is therefore not covered by these regulations. [18] Paragraph 30 in the preamble of GDPR states that natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

The nature of the public blockchain means that a record of every transaction is broadcast and linked to the public key issued by a specific user. Private keys are encrypted so while the blockchain's transaction records are public and open to investigation, nobody can directly identify the user's personal identity or corporate entity. Though direct identification through a private key is impossible, when the public key is reused it may be possible for a supervisory unit or an interested party to analyze the public key and discover the real identity of the person. In practice, the purpose of the public key is to select the other party to the transaction and confirm that the transaction is happening with the right person. When it becomes associated with a specific person then the public key qualifies as personal data under GDPR. Later on, more robust encryption was developed by blockchain technology that allowed for non-disclosure of the public key. In this situation, applicability of GDPR under personal data may

[18] Recital 28 EU GDPR： "The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection."

change. [19]GDPR should be applicable to situations where a link to personal information can be established through analysis of public key records. As it is possible to analysis the public key it then conforms to GDPR's definition of personal data.

Blockchain can be applied to the transfer of assets, for ensuring the traceability of related records, and even for the execution of smart contracts. The last concept refers to an independent procedure that "freezes" the agreement made by two persons in the blockchain in the form of an algorithm. No part of the blockchain involves the processing of personal data. In practice however, the applicable of blockchain technology requires the manipulation of information and content relating to the participants. [20]

2. Standard of Anonymity

Opinion 05/2014 (WP 216) issued by the Article 29 Working Party of the European Commission in 2014 provided an explanation on the difference between pseudonymised and anonymized data. [21] The distinction between pseudonymisation and anonymization is critical to determining the application of data protection regulations. Data protection regulations does not apply to anonymized data because it can't be traced to an individual or organization. The threshold to qualify as anonymous data is extremely high. [22]

As stated in the opinion, "anonymization results from processing personal data

---

[19] A guide to blockchain and data protection. (2017.9), https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf

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

[21] The "Article 29 Working Party" is the short name of the Data Protection Working Party established by Article 29 of Directive 95/46/EC. It provided the European Commission with independent advice on data protection matters and helped in the development of a harmonised implementation of data protection rules in the Member States of EU . It contributes to the development of a unified data protection policy for member states of EU. This working group is composed of representatives of national regulatory of EU member states.

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

in order to irreversibly prevent identification." [23]The data controller should consider all the reasonable ways that can be used for identification be it by the controller or a some other third party. Hashing allows for the linking of records so it is often considered a pseudonymisation technique rather than anonymization technique. EU GDPR continued to adopt the high standard set out in this opinion. [24]

It is generally possible to trace encrypted personal data to a specific person if experts are willing to put in enough effort or if someone has the decryption key. Encrypted data, including anonymized data, does not necessary satisfy the requirements for personal data. What this means is that privacy regulations will under most circumstances apply to at least some of the data in the blockchain system. [25]

In the case of *Patrick Breyer v. Bundesrepublik Deutschland*, the Court of Justice of the European Union (CJEU) issued a ruling in 2016 on whether dynamic IP addresses should be classified as personal data. The court's opinion on what constituted "personal data" influenced how personal data should be defined by GDPR in blockchain applications. CJEU ruled that the dynamic IP address (a temporary IP address issued to computing equipment when it connects to the Internet) may be classified as "personal data" even if additional information sufficient to identify the subject is only held by a third party (the Internet Service Provider in this case) - under certain circumstances. The possibility that the data can be combined with such additional information must satisfy the definition of

---

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

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

25Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, 06 November 2018, https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data

"all the means reasonably likely to be used to identify" the person. [26]

(III) One-way Hash Function

Hash function is used in blockchain technology to compare the fingerprint of the data and confirm that both parties have identical information. One-way hash function has an input and output. The output is referred to as the value while the input is the message. [27]The message is used by the one-way hash function to calculate the value. The value can be used to verify the integrity of the message. The core components of the block header are a unique fingerprint and time stamp for all the transactions in that block along with a hash to the previous block. Hash is a generated using a standard encryption hash function invented by the U.S. National Security Agency (NSA). A series of symbols and numbers form a unique fingerprint that represents all the transactions in a block as well as the block itself. [28]

To increase the difficulty of generating a hash for each block, Satoshi Nakamoto added a target constraint to the PoW for Bitcoin. Each hash must start with a designated number of leading zeros. A block can only be generated when PoW calculates a SHA-256 hash smaller than the target value. Nodes trying to generate a valid hash must perform repeated computations in order to satisfy the strict requirements set by the Bitcoin protocol. This type of activity is known as "mining." [29]Article 29 Working Group of the European Commission considered hashing to be a pseudonymisation technique rather than an anonymization technique in Opinion 05/2014. [30]

---

[26] *Patrick Breyer v Bundesrepublik Deutschland*, Judgment in Case C-582/14, Luxembourg, 19 October 2016, PRESS RELEASE No 112/16 , Court of Justice of the European Union.

[27] 結城浩著，吳嘉芳譯，密碼學與比特幣原理，碁峯出版社，2017 年 12 月初版 2 刷，頁 189。

[28] Primavera De Filippi and Aaron Wright 著，王延川譯，區塊鏈與法律-程式碼之治，元照出版社，2019 年 2 月初版，頁 29。

[29] Primavera De Filippi and Aaron Wright 著，王延川譯，區塊鏈與法律-程式碼之治，元照出版社，2019 年 2 月初版，頁 29。

[30] Article 29 Working Party considers in its Opinion 05/2014 that hashing is a technique of

III. Personal Data Security and Privacy Protection

In the previous chapter on pseudonymisation, we see that privacy protection is an issue in blockchains because pseudonymisation makes it possible for people to be traced and identified. Despite the many advantages offered by blockchain, the problem of privacy protection must still be overcome before individuals or institutions can be convinced to make use of public blockchains and use them to store their data on public databases. [31]

(I) Strengthening of Personal Data Protection by the GDPR

Article 6, Paragraph 4 of the GDPR on the lawfulness of processing personal data specifies that where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23, Paragraph 1, the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: ...(e) The existence of appropriate safeguards, which may include encryption or pseudonymisation. Chapter 4 of the GDPR sets out the responsibility of the data controller and processor. In Article 25 on data protection by design and default, Paragraph 1 states taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles,

---

pseudonymisation, not anonymisation. https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data

[31] Vitalik Buterin, Privacy on the Blockchain, January 15, 2016, https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/.

such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

Art. 32 Security of processing states taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Paragraph 1 states that pseudonymisation of personal data and encryption technologies can be implemented to protect the privacy of data subjects.The permanent storage of data in the public blockchain creates difficulties for complying Article 17's right to be forgotten during actual operation. However, if personal data that is non-identifiable is not removed, it improves the security of the blockchain while constructing a secure safe for protection of personal data. Such a combination may offer a suitable form of compliance. The use of more hybrid anonymization techniques to protect privacy and data security should be considered by blockchains. As long as it is absolutely impossible to identify a person by tracing the data on the chain then it falls outside of GDPR protections on personal data. More complex and advanced encryption techniques that provide stronger anonymization include "The Holy Grail", "Ring Signatures", and "Zero-Knowledge Proofs." [32]

(II) Zero-knowledge Proofs

Once virtual currencies were added to the scope of the Money Laundering Control Act, regulation of crypto-currencies such as Bitcoin based on blockchain technology continues to be a technical challenge. Under the Bitcoin transaction mechanism, the only way to do this is to enforce Know-Your-Customer (KYC) verification procedures at virtual currency brokerages or exchanges like MaiCoin. Bitcoin is an open source anonymous network so there is no need to go through banks, create an account or provide personal details for exchanging

[32] Vitalik Buterin, Privacy on the Blockchain, January 15, 2016, https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/.

Bitcoin. Even as programmers are beginning to pay attention to increasing the legitimacy of transactions, new services have emerged that aim to increase the illegitimacy of digital currencies. "Dark Wallet" for example mix together different types of un-related transactions to make it harder for third-party regulators to trace the flow of funds. [33] Conversely, anonymization techniques can be used in blockchains to strengthen privacy protection and data security. If it is absolutely impossible to identify a person by tracing the data on the blockchain then it falls outside of GDPR protections on personal data.

More advanced cryptographic techniques such as Zero-knowledge Proofs and Ring Signatures developed by anonymous digital currencies aim to muddy the source, destination and amount of blockchain transactions to further evade financial regulation and anti-money laundering efforts. [34]

Zcash for example is a joint project between Israeli and American cryptographers. The project allows members of the Zcash network to transfer digital currency (referred to as z-coin) anonymously over the blockchain. Zero-knowledge proofs makes it almost impossible to trace Zcash transactions because it creates something that seems quite paradoxical: Private transactions on a transparent and generally accessible blockchain.

The use of Zero-knowledge proofs allow members of the Zcash network to camouflage and conceal their transaction volume through advanced encryption algorithms. The identify of those sending and receiving z-coin can also be obscured. Here Zero-knowledge proofs is used to confirm that the sender has sufficient z-coin for the transaction. No information relating to the transaction needs to be disclosed to the network at all. The design of Zcash makes it difficult for Zcash accounts to be linked to real-world identities. Accounts on the Zcash network are pseudonymous. The Zcash blockchain does not store any information on the source and destination of "private" Zcash transactions.[35]Not

---

[33] See DarkWallet, http://darkwalet.is/. Primavera De Filippi and Aaron Wright 著，王延川譯，區塊鏈與法律-程式碼之治，元照出版社，2019 年 2 月初版，頁 92。

[34] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, Madars Virza, Zerocash: Decentralized Anonymous Payments from Bitcoin, in 2014 IEEE Symposium on Security and Privacy, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6956581, at 459-474.

[35] Primavera De Filippi and Aaron Wright 著，王延川譯，區塊鏈與法律-程式碼之治，元照出版社，2019 年 2 月初版，頁 93-94。

all Zcash users are anonymous however and over 90% of the transactions do not make use of the anonymization function. Anonymization is optional for users due to its higher cost. "Monero" (XMR) on the other hand is a "privacy coin" that enforces 100% anonymity. The low-level technology of XMR is similar to Bitcoin and Ethereum. Its source code is open, transparent, decentralized and open to participation by anyone. Monero is also a development of blockchain technology distinguished by its emphasis on privacy and anonymity. There are absolutely no addresses of transactions amount to be found in the Monero blockchain. Addresses cannot be used to check the remaining amount and transaction record of addresses either. Confidentiality is enforced throughout the entire network. [36]

IV. Data Control and Processing for the Blockchain

(I) Data Controller

Any discussion on the legitimacy of blockchain operations should first establish who will have legal liability as the data controller and data processor as defined under Chapter 4 of the GDPR. Defining the identity of the controller and processor in an application based on distributed ledgers may cause difficulties.

GDPR Article 4, Paragraph 7 defines “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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

GDPR Article 4, Paragraph 8 defines “processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

---

[36] https://xmr-tw.org/monero-advantage/

GDPR Article 4, Paragraph 2 defines “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

GDPR Article 4, Paragraph 9 defines “recipient” means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. 2However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

GDPR Article 4, Paragraph 10 defines “third party” means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

In a decentralized blockchain, its long-term operating structure doesn't actually contain a single controller with the power to decide the purpose and method of data processing. From a DApp perspective, as the logic and purpose of data operations are all written into the contract by program code so the contract's creator is the data controller with responsibility for the maintenance and removal of personal data. In the Consortium Chain, miners or validators are picked and authorized by Consortium members, so they are the data controller. Since they have control over the transactions the protection or deletion of data is processed by Consortium members working together. In a public blockchain, each node can decide for itself whether to engage in mining or not. Mining only verifies the PoW for block generation so it doesn't actually process the data on the blockchain and has no control over the data either. Take for example Bitcoin, with its more than 10,000 mining nodes around the world. Considering the scope, content, purpose and risk to data subject from the data being processed, enforcing Article 24 of the GDPR is probably not practical at all. If controller responsibility is implemented for a private chain then there may end up being multiple controllers that fall under Article 26 covering "joint controllers." The participant then uses

the governance protocol to determine the responsibility of each controller. [37]

(II) Data Processing

The roles defined by Article 4 of the GDPR include data controller, processor, recipient and third party. In a blockchain, identifying each role is a complicated affair as there is considerable overlap between roles and data processing.

GDPR Article 4, Paragraph 8 defines "processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. GDPR Article 4, Paragraph 2 defines processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

GDPR also places responsibility for data protection on the data processor. If we compare a blockchain with a distributed cloud computing system, the data processor for the cloud computing system is the system operator while the data controller uploads data to the cloud system. In a decentralized blockchain system however, the users simply run the program created by the blockchain platform's developer and there is no central administrator. [38] The responsibilities of the data processor and controller are clearly allocated under the roles defined by the GDPR. In a centrally managed organization, it refers to personal data being collected by a certain organization then outsourced to a data processor to be processed. There is no centralized organization for blockchain however. It is run by multiple parties so individual roles are hard to assign. [39]

---

[37] W. Maxwell and J. Salmon, "A guide to blockchain and data protection." https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf, 2017.

[38] W. Maxwell and J. Salmon, "A guide to blockchain and data protection." https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf (2017).

[39] Luis-Daniel Ibáñez, Kieron O'Hara, and Elena Simperl, On Blockchains and the General Data

Article 29 of the GDPR states that the data processor should process data under the data controller's authority. [40]In smart contract applications, the data subject and data controller use special settings to express initial, updated and withdrawal. This design can be applied to all kinds of smart contracts and can be deployed to the blockchain initially agreed upon. Initial agreement, withdrawal and each update are all managed by the smart contract where each contract represents a different version of the agreement. The smart contract system can also validate which is the correct and final version. Blockchain can confirm the validity and integrity of both parties' content. The blockchain programming also mechanisms in place to control agreement versions and send withdrawal notifications.[41]

V. Implementation and the Future of Personal Data Protection for Blockchain

(I) Analyze applicability for each case

The data controller and data processor in a decentralized public blockchain is difficultly to define. It is also difficult to implement centralized control over operations. The facts of each case should therefore be analyzed to determine the applicability of the GDPR, how the programming of its blockchain operates, the applicable data roles, as well as their corresponding responsibilities and obligations. Blockchain based on distributed ledger technology may lead to two scenarios: One is that the users use a certain centralized platform for processing data transactions and blockchain serves as a back-end tool; The other is users

---

Protection Regulation, Ibanez, Luis-Daniel, O'Hara, Kieron and Simperl, Elena (2018) On Blockchains and the General Data Protection Regulation EU Blockchain Forum and Observatory 13pp. Published date: 6 July 2018, https://eprints.soton.ac.uk/id/eprint/422879. at 5. (This work is licensed under a Creative Commons “AttributionShareAlike 4.0 International” license.)

[40] Art. 29 GDPR :The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

[41] Konstantinos Rantos1, George Drosatos2, Konstantinos Demertzis1, Christos Ilioudis3 and Alexandros Papanikolaou3, Blockchain-based Consents Management for Personal Data Processing in the IoT Ecosystem, science and technology Publications, at 575. https://www.scitepress.org/papers/2018/69110/69110.pdf

making direct transactions over the blockchain. The first scenario is similar to the service structure of the traditional Internet. The platform provider may qualify as the data controller while the nodes or other service providers serve as the data processor. The second scenario may lead to problems with who qualifies as the data controller. Whether participants can be considered data processors is also open to doubt. If the subject can control his or her own data through private key, whether the user can then be considered to be the data controller is a question worth looking at. Subjects use the blockchain for different purposes as well. For example, if an individual submits personal data to the chain then the subject may qualify as a controller of personal data. Differences in blockchain application scenarios makes it too difficult to find a one-size-fits-all solution.

(II) Evolution of Encryption Technology and Legal Risks

The nature of the decentralized blockchain means it doesn't really conform well to the centralized supervisory framework of GDPR. Blockchain however can provide better security and privacy for data protection. How blockchains operate means they cannot erase data on demand as required by Article 17 of the GDPR. Article 17, Paragraph 1, Subparagraph a however states that if the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her. Nevertheless, the data controller of a public blockchain is harder to define and the erasure of data is no technically feasible either. Compliance is therefore in doubt. Article 16 on the right to rectification is also extremely hard to implement due to the immutability of the blockchain.

Blockchain should perform better when it comes to satisfying the requirements of data security. Article 5, Paragraph 1, Subparagraph f of the GDPR states that data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures. Article 25 on data protection by design and by default states that the controller shall implement appropriate technical and organizational measures, such as pseudonymisation when processing data. The use of more hybrid anonymization techniques to protect privacy and data security

should be considered by blockchains to meet the data protection requirements of the GDPR. As long as it is absolutely impossible to identify a person by tracing the data on the chain then it falls outside of GDPR protections on personal data. More complex and advanced encryption techniques that provide stronger anonymization for protecting data and privacy include "The Holy Grail", "Ring Signatures", and "Zero-Knowledge Proofs." Blockchain can also be applied to automated execution scenarios to provide a high-level of traceability and transparency. This may provide new impetus for the protection of personal data.