Blockchain and General Data Protection Regulation (GDPR) compliance issues (2019)

Blockchain and General Data Protection Regulation (GDPR) compliance issues (2019)

I. Brief

Blockchain technology can solve the problem of trust between data demanders and data providers. In other words, in a centralized mode, data demanders can only choose to believe that the centralized platform will not contain the false information. However, in the decentralized mode, data isn't controlled by one individual group or organization[1], data demanders can directly verify information such as data source, time, and authorization on the blockchain without worrying about the correctness and authenticity of the data.

Take the "immutable" for example, it is conflict with the right to erase (also known as the right to be forgotten) in the GDPR.With encryption and one-time pad (OTP) technology, data subjects can make data off-chain storaged or modified at any time in a decentralized platform, so the problem that data on blockchain not meet the GDPR regulation has gradually faded away.

II. What is GDPR?

The purpose of the EU GDPR is to protect user's data and to prevent large-scale online platforms or large enterprises from collecting or using user's data without their permission. Violators will be punished by the EU with up to 20 million Euros (equal to 700 million NT dollars) or 4% of the worldwide annual revenue of the prior financial year.

The aim is to promote free movement of personal data within the European Union, while maintaining adequate level of data protection. It is a technology-neutral law, any type of technology which is for processing personal data is applicable.

So problem about whether the data on blockchain fits GDPR regulation has raise. Since the blockchain is decentralized, one of the original design goals is to avoid a large amount of centralized data being abused.

Blockchain can be divided into permissioned blockchains and permissionless blockchains. The former can also be called "private chains" or "alliance chains" or "enterprise chains", that means no one can join the blockchain without consent. The latter can also be called "public chains", which means that anyone can participate on chain without obtaining consent.

Sometimes, private chain is not completely decentralized. The demand for the use of blockchain has developed a hybrid of two types of blockchain, called "alliance chain", which not only maintains the privacy of the private chain, but also maintains the characteristics of public chains. The information on the alliance chain will be open and transparent, and it is in conflict with the application of GDPR.

III. How to GDPR apply to blockchain ?

First, it should be determined whether the data on the blockchain is personal data protected by GDPR. Second, what is the relationship and respective responsibilities of the data subject, data controller, and data processor? Finally, we discuss the common technical characteristics of blockchain and how it is applicable to GDPR.

1. Data on the blockchain is personal data protected by GDPR?

First of all, starting from the technical characteristics of the blockchain, blockchain technology is commonly decentralized, anonymous, immutable, trackable and encrypted. The other five major characteristics are immutability, authenticity, transparency, uniqueness, and collective consensus.

Further, the blockchain is an open, decentralized ledger technology that can effectively verify and permanently store transactions between two parties, and can be proved.

It is a distributed database, all users on the chain can access to the database and the history record, also can directly verify transaction records. Each nodes use peer-to-peer transmission for upload or transfer information without third-party intermediation, which is the unique "decentralization" feature of the blockchain.

In addition, the node or any user on the chain has a unique and identifiable set of more than 30 alphanumeric addresses, but the user may choose to be anonymous or provide identification, which is also a feature of transparency with pseudonymity[2]; Data on blockchain is irreversibility of records. Once the transaction is recorded and updated on the chain, it is difficult to change and is permanently stored in the database, that is to say, it has the characteristics of "tamper-resistance"[3].

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

Therefore, if data subject cannot be identified by the personal data on the blockchain, that is an anonymous data, excluding the application of GDPR.

(1) What is Anonymization?

According to Opinion 05/2014 on Anonymization Techniques by Article 29 Data Protection Working Party of the European Union, "anonymization" is a technique applied to personal data in order to achieve irreversible de-identification[4].

And it also said the "Hash function" of blockchain is a pseudonymization technology, the personal data is possible to be re-identified. Therefore it's not an "anonymization", the data on the blockchain may still be the personal data stipulated by the GDPR.

As the blockchain evolves, it will be possible to develop technologies that are not regulated by GDPR, such as part of the encryption process, which will be able to pass the court or European data protection authorities requirement of anonymization. There are also many compliance solutions which use technical in the industry, such as avoiding transaction data stored directly on the chain.

2. International data transmission

Furthermore, in accordance with Article 3 of the GDPR, "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. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (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 behaviour as far as their behaviour takes place within the Union".[5]

In other words, GDPR applies only when the data on the blockchain is not anonymized, and involves the processing of personal data of EU citizens.

3. Identification of data controllers and data processors

Therefore, if the encryption technology involves the public storage of EU citizens' personal data and passes it to a third-party controller, it may be identified as the "data controller" under Article 4 of GDPR, and all nodes and miners of the platform may be deemed as the "co-controller" of the data, and be assumed joint responsibility with the data controller by GDPR. For example, the parties can claim the right to delete data from the data controller.

In addition, a blockchain operator may be identified as a "processor", for example, Backend as a Service (BaaS) products, the third parties provide network infrastructure for users, and let users manage and store personal data. Such Cloud Services Companies provide online services on behalf of customers, do not act as "data controllers". Some commentators believe that in the case of private chains or alliance chains, such as land records transmission, inter-bank customer information sharing, etc., compared to public chain applications: such as cryptocurrencies (Bitcoin for example), is not completely decentralized, and more likely to meet GDPR requirements[6]. For example, in the case of a private chain or alliance chain, it is a closed platform, which contains only a small number of trusted nodes, is more effective in complying with the GDPR rules.

4. Data subject claims

In accordance with Article 17 of the GDPR, The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay under some grounds.

Off-chain storage technology can help the blockchain industry comply with GDPR rules, allowing offline storage of personal data, or allow trusted nodes to delete the private key of encrypted information, which leaving data that cannot be read and identified on the chain. If the data is in accordance with the definition of anonymization by GDPR, there is no room for GDPR to be applied.

IV. Conclusion

In summary, it's seem that the application of blockchain to GDPR may include: (a) being difficulty to identified the data controllers and data processors after the data subject upload their data. (b) the nature of decentralized storage is transnational storage, and Whether the country where the node is located, is meets the "adequacy decision" of Article 45 of the GDPR.

If it cannot be met, then it needs to consider whether it conforms to the transfers subject to appropriate safeguards of Article 46, or the derogations for specific situations of Article 49 of the GDPR.

Reference:

[1] How to Trade Cryptocurrency: A Guide for (Future) Millionaires, https://wikijob.com/trading/cryptocurrency/how-to-trade-cryptocurrency
[2] DONNA K. HAMMAKER, HEALTH RECORDS AND THE LAW 392 (5TH ED. 2018).
[3] Iansiti, Marco, and Karim R. Lakhani, The Truth about Blockchain, Harvard Business Review 95, no. 1 (January-February 2017): 118-125, available at https://hbr.org/2017/01/the-truth-about-blockchain
[4] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques (2014), https://www.pdpjournals.com/docs/88197.pdf
[5] Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN
[6] Queen Mary University of London, Are blockchains compatible with data privacy law? https://www.qmul.ac.uk/media/news/2018/hss/are-blockchains-compatible-with-data-privacy-law.html

Links

- How to Trade Cryptocurrency: A Guide for (Future) Millionaires
- The Truth About Blockchain
- Directive 95/46/EC (General Data Protection Regulation)
- Are blockchains compatible with data privacy law?

Download

- Opinion 05/2014 on Anonymisation Techniques [pdf]

Juan, Yun-Chien
Associate Legal Researcher

Release : 2020/03