Data privacy-related issues arising from the use of blockchain technology

Dr. Umut Kolcuoglu
Managing Partner
ukolcuoglu@kolcuoglu.av.tr

Can Baykut
Associate
cbaykut@kolcuoglu.av.tr

Kolcuoglu Demirkan Kocakli Attorneys at Law

EVEN THOUGH blockchain technology has a lot to offer, it comes with the need for careful consideration and new issues that must be addressed, as innovation often does. Blockchains are decentralized digital ledgers that are generally open to the public, which are comprised of "blocks" of information attached to each other by way of cryptographic hashing. These are extremely difficult to tamper with, and their decentralized, public and unalterable nature brings the question of what will happen to personal data that is entered into the blockchain.

In a broader sense, one can argue that the public keys (these can be compared to conventional banking system IBANs) which anyone can track, provide sufficient network user anonymity. However, contrary to popular thought, pseudonymous data such as public keys do not provide full anonymity and can be traced back to the user. Further, some blockchains allow users to enter much more detailed data than basic transactions which can be tracked by public keys.

One issue concerning personal data that is entered into a blockchain is determining the jurisdiction in which that data is being processed. While blockchains' decentralized nature provides trust and security, it also leads to uncertainty in terms of the applicable law. As the public digital ledgers of permissionless public blockchains are distributed around the world to any node wanting to join the network, blockchains can easily be acknowledged as having no borders. In this regard, the governing law necessary to handle the personal data in a blockchain or any relevant legal disputes that may arise is unclear.

Another major issue arising from blockchain usage is the data controllers' identification within a blockchain. As per Law on Protection of Personal Data numbered 6698 (the "Data Protection Law"), data controllers are individuals or legal entities that determine the purpose and the means through which personal data is processed. In terms of the personal data stored in private and permissioned blockchains, the data controllers can easily be identified. However, when it comes to public and permissionless blockchains, such as the Bitcoin blockchain, data controller identification is not as clear. Three main data controller actors under discussion are the programmers, miners (a broader term could be validating nodes), and users.

The "Blockchain and the GDPR" report dated 2018 prepared by the EU Blockchain Observatory and Forum clarifies that the relevant blockchain coding programmers should not be the data controllers, as they are merely the technological tool creators and have no say in the actual usage. The status of miners as data controllers, however, is slightly more controversial as they oversee the network's functionality and security. Contradicting views exist as to whether this control over the network means that they determine the purpose and means of data processing or not. As for the network users, the Blockchain and the GDPR report states that they may be deemed as data controllers within the blockchain if their purpose concerns commercial activities. Nonetheless, the question of how to penalize such users remains.

The final data privacy-related issue that comes with the use of blockchain technology is the difficulty to alter data within a blockchain. According to the Data Protection Law, if the grounds for collecting personal data no longer exist, the data controller must erase, destroy, or render the personal data anonymous ex officio or upon the data subject's request. However, it is almost impossible for data entered into a blockchain to be altered or deleted once entered. Most blockchains permit alteration of past data only if the majority (the ratio of which may vary depending on the consensus algorithm used) of the network nodes agree to do so. Considering the vast number of nodes in a large sum of blockchains, the majority consensus is objectively troublesome to achieve.

Considering both the disruptive and innovative nature of blockchain technology and that current data privacy laws do not take distributed ledger-type databases into account, blockchain technology will inevitably give rise to new legal complexities in this area. We believe that to achieve true blockchain technology potential and, at the same time, protect personal data, the existing data privacy legislation needs to be adapted continually to match technological innovations. Despite the risk of such legislation going against the nature of blockchains, for blockchain technology to survive the age of mass regulation, it may indeed be required.