GBBC Global Blockchain Business Council

Open Learning Forum

Algorand's Approach to the Right to Be Forgotten

Executive Summary written by GBBC

Introduction

The European Union's sweeping General Data Protection Regulation (GDPR), which went into effect in May 2018, includes a provision that has presented a dilemma for blockchain firms: the right to be forgotten (RTBF). As stated in the GDPR, a 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," with "undue delay" being defined as roughly one month. This is seemingly antithetical to blockchains, which are by nature immutable, transparent, and distributed, meaning one centralized entity cannot delete personal information.

Algorand's Approach

Algorand has an advantage in this domain over Bitcoin and other blockchains: it is a balance-based blockchain (BBB), meaning that "in order to validate new payments, the participants in the consensus protocol are not required to look up and validate past payments. Rather, they need only keep and update a small amount of information: namely, the current balance of each key in the system." Because the consensus protocol is based on balances rather than transactions, it is possible for a user to erase their personal information. However, this principle only applies to payment transactions; there is no balance available for pure data transactions. To address this problem, Algorand has modified the usual structure of blocks and transactions by separating erasable and non-erasable data while permanently storing a hash of any erasable data. This enables the Algorand protocol to remove personal information in response to RTBF requests without compromising the integrity of the blockchain.

Conclusion

Laws and regulations are not written in stone, and it is possible that the RTBF could be strengthened or weakened in the future. Algorand's approach to transaction and block structure enables it to adjust which personal information should be included in the erasable or non-erasable components of future transactions. They also note that it is possible for any blockchain, regardless of consensus mechanism, to become RBTF compliant by using the same transaction and block structure. Importantly, the approach also demonstrates that blockchain technology is far from being stagnant and at the mercy of regulators and lawmakers; the technology is constantly evolving, and entities are finding innovative ways to adapt to the world around them.