COSMOS
Navigate the Compliance Universe

CEP Magazine - April 2023

**Segev Shani** (segevshani@neopharmgroup.com) is Chief Compliance & Regulatory Officer at Neopharm Ltd., Petach Tikva, and Senior Lecturer at the Department of Health Systems Policy & Management & School of Pharmacy at Ben-Gurion University in Beer Sheva, Israel.

# Blockchain and privacy: Can they live together?

By Segev Shani

The amount of data in our world is rapidly increasing. In the Big Data era, data is constantly being collected and analyzed, leading to innovation and economic growth. Companies and organizations use the data they collect to personalize services and optimize the corporate decision-making process, among other things. Today, data is a critical asset in our economy. While we appreciate the benefits of a data-driven society, there is a growing public concern about user privacy. Centralized organizations—both public and private—amass large quantities of personal and sensitive information. Individuals have little to no control of how data about them is stored or used.

As a consequence of public concern regarding the use (or abuse) of personal data, legislators tried to update privacy laws to cope with recent data use technological development, mainly due to social media and other applications (Web 2.0). The European Union (EU) General Data Protection Regulation (GDPR) became binding in May 2018. The GDPR establishes a framework of fundamental rights protection based on the right to data protection in Article 8 of the EU Charter of Fundamental Rights.[1] The GDPR was followed by other privacy legislation worldwide, including the California Consumer Privacy Act (CCPA), etc. The objective of privacy law is to protect natural persons through the fair processing of their personal data and respect their fundamental rights and freedoms—particularly their right to protect personal data. For that purpose, privacy rules create obligations for data controllers—the entities determining the means and purposes of data processing; they allocate many rights to data subjects—the natural persons to whom personal data relates that can be enforced by data controllers.

Blockchain technology has evolved in the last two decades to become one of the most hyped technologies publicly debated in recent years. However, blockchain technology and data privacy laws and regulations have largely developed independently. Heightened global data protection regimes with dramatically increased potential fines drive businesses to further reevaluate their privacy practices. Organizations currently face significant ambiguity and complexity in applying data privacy requirements to blockchain technology and associated services.

This article aims to explain blockchain technology, including its core elements; to discuss key similarities and differences between the use of blockchain and data privacy laws and regulations compliance; and to suggest potential measures for mitigating compliance risks and enabling the use of personal data on blockchain while assuring data privacy.

## Blockchain

The term "blockchain" refers to a specific subtype of distributed ledger technology. This software infrastructure provides a synchronized and shared data structure that multiple participants can access and modify over a peer-to-peer network. The ledger chronologically links each newly published data block to previous blocks of

transactions using a cryptographic hashing process to form a chain. Participants, or nodes, generally store a complete copy of the ledger with previous transactions.

The blockchain's essential utility is a decentralized and tamper-resistant store of data that can act as a single irrefutable source of truth without needing a trusted centralized intermediary. This has enabled use cases such as document verification, digital asset storage and transfer, and supply chain tracking, with these applications built on top of blockchain networks.

This is achieved by using consensus mechanisms in which a defined majority of participants are required to verify the legitimacy of and agree on each new ledger transaction request, taking the place of a traditional centralized administrator. Some consensus models include:

- Proof-of-work—mostly in public blockchains—induces participants to compete for the right to verify and settle blocks of transactions by solving computationally intensive puzzles.
- Proof-of-stake sets block publishing rights according to participants' known investment in the blockchain.
- Proof-of-authority verifies a participant's identity and authorization level before granting block publishing rights, typically in private blockchains of known participants.

Blockchain networks differ from conventional databases in two ways:

- Data is stored in a decentralized fashion. In a blockchain network, copies of the ledger are hosted on multiple nodes, which often exist across different jurisdictions. Addition of new data onto the chain must be validated and accepted by a majority of network nodes ("consensus"), after which the new data will be replicated across copies of the ledger within the network.
- Stored data is tamper-resistant. The blockchain is designed to be append-only, meaning that records committed on the chain cannot be edited or deleted. This grants blockchains a degree of tamper-resistance and transaction finality (i.e., immutability).

These two attributes allow for a high degree of trust in the data on-chain. However, when personal data is written on a blockchain, the decentralized and tamper-resistant attributes give rise to issues with accountability and immutability in complying with the obligations of keeping data private.