INSURANCE - INDIA

Blockchain technology in insurance sector

September 04 2018 | Contributed by Tuli & Co

AUTHORS

Celia Jenkins

Anuj Bahukhandi

Swathi Ramakrishnan

Blockchain technology

Blockchain is a relatively new form of technology that acts as an incorruptible digital ledger and keeps a virtual record of all data and transactions.(1) Broadly speaking, as a digital ledger, blockchain can record a wide range of quantities, from physical assets to electronic cash.

Over the past few years, India has seen a few segmental adoptions of the technology, with some public authorities and private entities acknowledging its potential benefits, including the Insurance Regulatory and Development Authority of India (IRDAI).

Adoption in insurance industry

Insurance business is built in large part on policyholders' trust in the accountability of insurers. Incidents that compromise the protection of policyholders' personal and proprietary data may not only result in regulatory consequences for the defaulting parties, but also undermine the policyholders' confidence in the sector. Since the technology and design of a blockchain is broadly believed to be secure, the integration of blockchain into insurers' databases may help to cater to the sector's need for data integrity and management.

Recent press reports have indicated that some Indian insurers have started contemplating various ways in which to implement the technology. It is reported that a consortium of the 15 leading Indian life insurers has partnered with a global technology firm to develop a blockchain solution facilitating cross-company data sharing for the specific purpose of reducing fraud and money laundering in the sector.(2)

Blockchain and Cybersecurity Guidelines

Notwithstanding the foregoing, not all blockchains are created equal, and it is imperative to consider whether the technology could be considered at odds with the existing data protection and security regime in India.

The IRDAI has on more than one occasion stressed the need for data security and storage in the insurance sector and issued various circulars and guidelines in this regard. In 2015 the IRDAI set out the Guidelines on Information and Cyber Security of 7 April 2017 (Cybersecurity Guidelines). These guidelines require all insurers to put governance mechanisms and requisite IT infrastructure in place to ensure the security of all data created, collected, maintained and shared, irrespective of its form or place of storage.

However, implementation of a new technology such as blockchain may not necessarily completely comply with the existing insurance statutory and regulatory framework. Thus, below is an analysis of the Cybersecurity Guideline's framework for blockchain technology, bearing in mind its potential use in the Indian insurance sector in future:

- Per Paragraph 5.17 of the Cybersecurity Guidelines, insurers must identify and address any possible risks to their organisational systems and information while engaging vendors and third parties. Paragraph 5.17.2.1 additionally requires insurers to share information with third parties only on a need-to-know basis. Since an encryption key may protect each blockchain, access to its data may be restricted only for the permitted purposes of such data by granting the key to authorised individuals, thus controlling access to data by an unidentified third party.
- To ensure the security of information systems, Paragraph 12.8(a) of the Cybersecurity Guidelines stipulates that "direct back-end updates to database should not be allowed except during exigencies". However, blockchain by its very nature hinges on the automatic updating of records in tandem with ongoing transactions or data entries. Although sufficient controls may be built in to ensure that an audit trail is maintained (Paragraph 12.7(d)), no unauthorised modification is carried out (Paragraph 12.8(c)) and the regulatory intent of restricting the unauthorised use of data is satisfied, it is unclear whether the inherent working of the technology could be considered to be a back-end update. Therefore, it will be interesting to see how this is viewed if blockchains were implemented on a wider scale.
- Paragraph 21 of the Cybersecurity Guidelines sets out the norms on maintaining insurers' data on cloud infrastructure, stipulating that they must have a framework for regulating data hosted "on cloud or on any external hosting infrastructure". Additionally, insurers must implement appropriate access control mechanisms to establish a logical segregation of duties between the service providers and third parties and the data is not shared accidently with other users. Broadly speaking, since blockchain technology is designed to store data in a manner that restricts access to or meddling by any unauthorised persons, if an insurer integrates it across all of its storage infrastructure, this may reduce the chances of manipulation and misuse.
- Considering the trend in cybercrime, consumerisation, the rise in cloud computing systems, the significance of business continuity and the increase in internal threats (eg, relating to employee fidelity), Paragraph 11.1 of the Cybersecurity Guidelines requires insurers to implement a data security policy. In this regard, Paragraph 11.1 requires that "consistency & accuracy of data entered into the system should be verified through a maker checker process (3) wherever applicable" and audit trails "should be secured to ensure the integrity of the information captured, including the preservation of evidence". Since each blockchain is understood to provide a comprehensive audit trail and be self-correcting in nature, introduction of the technology may possibly eliminate or minimise the need for additional people to be involved in verifying the integrity of data.
- Per Paragraph 16 of the Cybersecurity Guidelines, insurers must define data retention and destruction schedules and ensure that multiple copies of data stored across different locations are destroyed once the retention timeframe has lapsed or on request. This could serve as an interesting point of contention if blockchain is introduced, as a blockchain is immutable and the data stored in each block can neither be modified nor deleted.

In the wider data protection context, certain additional challenging questions are raised by this technology:

- While blockchains where the origin of the data is hidden may offer anonymity to parties and individual records could be made private and encrypted, it is concerning that where a party loses its access key to such encrypted blockchain, it also loses all of its data.
- A blockchain ledger allows for the addition of data across a network of machines, but in order to prevent data tampering and fraud, the data can neither be deleted nor modified. For example, where any personal data is stored on a blockchain by an insurer, it is unclear whether a party will be able to exercise its right to rectification or right to be forgotten under Articles 16 and 17 of the General Data Protection Regulation 2016/679.

Comment

While the collective effect of the existing Indian insurance statutory and regulatory framework on data security is to minimise misuse and unauthorised tampering of any organisational data belonging to insurers and other entities, it will be interesting to see whether the new technology is discussed or accommodated for within the existing guidelines.

It is still too early to comment on whether and to what extent the insurance sector will assess this technology to meet its data security and integrity requirements going forward.

For further information on this topic please contact Celia Jenkins, Anuj Bahukhandi or Swathi Ramakrishnan at Tuli & Co by telephone (+91 11 4593 4000) or email (celia.jenkins@tuli.co.in, anuj.bahukhandi@tuli.co.in or swathi.ramakrishnan@tuli.co.in). The Tuli & Co website can be accesses at www.tuli.biz

Endnotes

(1) Blockchains are comprised of a linear chain of blocks, created by linking new blocks of validated entries to older blocks, which successively reveal each transaction made in the history of that blockchain. Subsequently, this chain is continually updated so that every database in the network is the same.

(2) "Leading Indian Life Insurers Partner with Cognizant to Develop Industry-Wide Blockchain Solution for Secure Data-Sharing and Improved Customer Experience" (Cognizant, 16 April 2018).

(3) In the maker-checker process, while one individual may create a transaction, another individual must be involved in confirmation and authorisation of the same.
