Five challenges to the adoption of distributed ledger technologies in the telecoms industry

October 2017

Enrique Velasco-Castillo

Operators' interest in distributed ledger technologies (DLTs)[1] and their use cases is high, and they are beginning to scrutinise the potential costs and benefits involved more carefully. Vendors and innovators must address the five challenges described in this article to demonstrate the superiority of DLTs over existing solutions for the telecoms industry. The current state of DLTs suggests that there are few compelling applications for the technology in the telecoms industry at present.

Telcos' internal platforms do not currently have a strong requirement for DLTs

Telcos' current BSS and OSS platforms (for billing or SIM provisioning, for example) do not have strong requirements for decentralisation or trust-less access to data, which are the features that set DLTs apart from other distributed data storage and verification technologies. Scalability, high availability, resiliency, and cost are arguably more important factors for telcos. Other reasons why DLTs may be unsuitable for telcos include a centralised database topology being simpler to implement, a centralised authority being necessary to verify and authenticate autonomous devices, or international payments having to be settled within the constraints of national banking systems. However, this may change as an increasing number of network functions, such as billing or SIM provisioning, become virtualised.

DLTs must integrate with legacy systems to work in a telco environment

DLT solutions will have to be integrated with legacy telco systems, which may require development of specialised solutions.

- **OSS/BSS integration.** DLTs' integration with operators' internal systems may require middleware layers in operators' technology stacks. This transition could be facilitated by digitalisation of more functions in operators' network stacks.
- **Third-party integration.** A centralised interoperability solution may be required to integrate with other operators and third parties (to verify users' access credentials, for example).

Operators will need to assess whether the cost of integrating DLTs offsets their benefits. The need to implement centralised authentication systems, for example, could negate the advantages of decentralised ledgers over other data architectures.

[1] The term DLT is sometimes used interchangeably with blockchain, but it is not equivalent. Blockchains are a subset of DLTs, and generally involve a computationally expensive process (in CPU cycles, electricity, and specialised hardware) to verify the integrity of the data stored in the blocks.

External use cases, such as IoT or payments, are attractive, but operators have a more limited role in the value chain

DLTs' goals of decentralisation, immutability, and security are important for use cases in unregulated environments where agents with asymmetric resources and disparate goals need to transact, even if they do not necessarily trust each other. Players in cryptocurrency markets fall under those conditions and blockchain technologies have so far gained the most traction in those applications.

There are telecoms use cases with similar requirements for decentralisation and trust-less data exchange between multiple parties. These include:

- IoT (for example for the exchange of data between different smart city or industrial applications)
- transactional digital services (such as mobile money, including direct carrier billing and international remittances).

Telcos tend to have a more limited role in those industry verticals. However, some operators are investing heavily in playing greater roles in financial services or IoT, and will look for solutions that help them integrate more deeply into those value chains.[2]

DLTs create new security challenges

DLTs' implementation costs may have to include non-technical factors such as regulation or usability. Organisations are still not good at keeping data (including encryption keys) safe, regardless of the sophistication of the latest encryption technologies.

Some operators are active in highly-regulated industries in which the security and consistency of sensitive data are essential, such as finance or healthcare. Regulatory compliance may increase the implementation costs of DLTs, or even bring their suitability for those applications into question. Alternative solutions to this issue have been proposed, such as off-chain data storage. This refers to using the blockchain to store the hashes of the data, but not the data itself, which is stored in a separate database. The party storing the data would add some degree of centralisation to the system, and end users would need to trust that the data in this repository is correct and consistent. This negates the security advantages of DLTs by adding implementation complexity and increasing the potential attack surface.

DLTs will need to become standardised, which will take years

Standards for any technology in the telecoms industry only appear after a long process of consensus among operators, vendors and industry bodies. DLTs will be no exception and their standardisation process will take years, as most tend to do. Vendors will present a variety of solutions, and compete for awareness and adoption. The most technically-advanced solution may not necessarily be the one that succeeds.

Operators will ultimately balance the potential of DLTs against the practical realities of implementing production-ready telco systems. There are few compelling applications of DLTs in telecoms so far, but this may

[2] For examples of operators' roles in digital banking, see Analysys Mason's Report *Digital banking operator case studies: Orange, Telefónica and Telenor*. Examples of operators' efforts to embed themselves in the IoT value chain are discussed in Analysys Mason's Article *Four operator approaches for IoT as the market opens up*.

change as operators embrace network function virtualisation. For a more detailed discussion of the potential and challenges of DLTs, see our recent report *Blockchain in telecoms: revisiting telco use cases and challenges*.