Deloitte.

Which control principles are essential for blockchain adoption on a global scale?

01 Standard for Blockchain Development

02 Interoperability and System Integration Controls

03 Audit Rules

04 Cybersecurity Controls

05 Enhancement of Traditional ICT Controls

06 Business Continuity Planning

Distributed Ledger Technology has attracted significant attention in the global financial services community. Researchers and investors are increasingly interested in the transformative and disruptive ability of this technology to

- Facilitate an exchange of value
- Enable the safe storage of value
- Achieve operational efficiencies
- Secure cost savings
- Increase industry transparency
- Enhance customer experiences

01 Standard for Blockchain Development

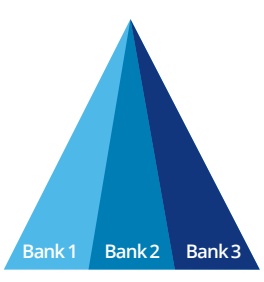
3 macro factors which are essential to the widespread adoption of private Distributed Ledger Technology within the financial services in the long term are:

- Governance
- Legal and Regulation
- Standards

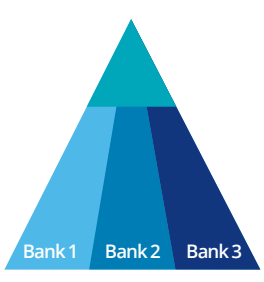
Governance

To develop appropriate structures for DLT adoption within the financial services community three different governance models must be considered:

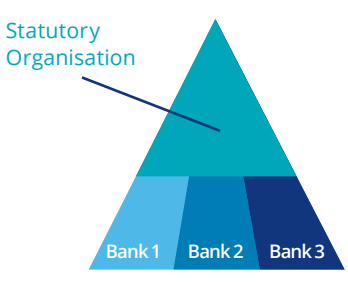
A Consortium



B Joint Venture



C Statutory Organisation



02 Interoperability & System Integration Controls

When introducing DLT into the enterprise, it is essential that DLT system is capable of integrating and interoperating with other systems, including other blockchain solutions or technologies, and need to consider:

- Security considerations
- Data integration
- Integration with legacy systems
- Security mechanisms

03 Audit Rules

The use of blockchain platforms will not remove audits nor the need for an independent auditor. Rather, it will transform the way in which auditors extract, test and analyse data. Layering blockchain technology with audit analytics could yield standardised, sophisticated audit routines and analysis that enable near real-time evaluation of transactions across the blockchain.

04 Cybersecurity Controls

DLT is intrinsically linked with Cybersecurity considerations. The foundation of Blockchain technology is private and public key cryptography, digital signing and cryptographic hashes. Cybersecurity considerations related to the cryptographic and immutable nature of blockchain technology include:

- Key management
- Risk of an attacker overpowering a private blockchain
- Centralisation of authority within the network
- Privacy and the right to be forgotten

05 Enhancement of Traditional ICT Protocols

The decentralized nature of DLT requires a differing approach to the management of ICT controls:

- Security management
- System development and change management
- Information processing

06 Business Continuity Planning

While blockchain itself is a new and powerful technology, its components are well understood. Ensuring high quality business continuity planning for Blockchain solutions will involve collation and aggregation of these existing processes into a unified package.