Technology deep dive: DLT and blockchain

Description of technology

DLTs¹ are public or private networks recording transactions across distributed infrastructure.

Stored transactions are encrypted through unique, unchangeable hashes (for example, SHA 256 algorithm).

Multiple nodes verify items based on permissions or economic incentives to reach majority consensus to add transactions to the ledger, called consensus mechanisms.²

Blockchain is a type of DLT, a public network with a shared ledger without central authority controlled by economic incentives for nodes to update the ledger.

In a public network, economic incentives for transaction verification promise rewards to nodes as they credibly prove that transactions are legitimate; this is called mining.

Technology maturity

Technical maturity

Mass adoption

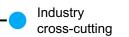
By 2027, up to 10% of global GDP could be associated with blockchain-enabled transactions

Fundamental

research

Industry applicability







What it enables companies to do

Immutability of records



Encryption of transactions ensures that any alteration to the ledger would recognized by the network and be rejected

Auditabilitv

Sequential and indefinite recording of transactions create an indelible audit trail³

Traceability of positions

Transactions can be tracked down to their current position as it is always known where it was sent from and arrived at

Embedded security



Consensus from the network and encryption mechanisms ensure security is natively incorporated into operations

In private networks, permission designs determine degree of DLT/blockchain properties, and hence benefits apply

1. Distributed-ledger technologies. 2. Two consensus mechanisms exist: the first is private blockchain, using big trusted corporations (smaller share of market) and the second is public mass-market blockchain. 3. Technically, blockchains could be reverted/deleted; however, there is minimal risk if designed properly. 4. Know your customer.

Main opportunities

Example use cases

Reduced risk and lower compliance costs As trust in the system replaces trust in the counterparty, fewer risk checks are needed (eg, KYC⁴ guidelines) as actors and transactions are approved through consensus

Cost-efficient transactions No middleman required to authenticate transactions as system is based on high security, consensus, and

verification via economic incentives

Automated and secure contract fulfillment Deployment of smart contracts that trigger transactions automatically upon fulfillment of contract criteria, ie, less reconciliation

Network transparency

Network members can view status of transactions or item positions any time (eg, proof of provenance within supply chain)



Use case deep dive: DLT and blockchain

Proof points

Use case	Situation and approach	Impact
■ Reduced risk and lower compliance costs	Existing KYC ¹ processes are outdated and generate costs of up to \$500 million/year/bank New DLT ² system is proposed to reduce verification costs and improve customer experience	KYC verification in DLT system is only conducted once for each customer and then shared between the different financial institutions
		Cost-efficient transactions
Process could be reduced to less than 4 hours from issuing to approval of the letter of credit		
Usually, process takes 10 days		
Automated and secure contract fulfillment	One retailer sought to streamline its supply-chain management by recording all processes and actions from vendor to customer and coding them into smart contracts on blockchain	Retailer yielded several benefits: 1) Improved transparency (easier to trace food provenance leading to safer consumption)
		2) Fewer human actions in the chain
		3) Improved tracking of lost products

1. Know your customer.

2. Distributed-ledger technology.

Expected technologydevelopment horizons: DLT and blockchain

Expected technology-development horizons in next 5 years

Growth of

blockchain as a

Growth of federated DLT networks

Type of private blockchain in which multiple authorities can control the preselected nodes to validate transactions, instead of only one authority

Along with increasing possibilities to digitize values of physical assets (tokenization), federated blockchains will grow industry adoption

1. Distributed-ledger technology.

service (BaaS) Cloud-based service to build digital products for DLT¹ and blockchain environments without any setup requirements for infrastructure

Big Tech companies are leading the efforts (eg, Amazon and Microsoft), likely accelerating diffusion of DLT/blockchain technology Interoperability across DLT/ blockchain networks and outside system

Enabling disparate DLT/blockchain and external systems to view, access, and share data while maintaining integrity

Interoperability needs to take place on three layers: business model, platform, and infrastructure

Hardware standardization and scalable consensus algorithms will enable crossnetwork use cases (eg, the Internet of Things on DLT/Blockchain infrastructure)

Enablers

Economic uncertainty as predictor of uptake of DLT/blockchain initiatives given independence of centrally regulated systems (eg, fiscal monetary system, public-cloud solutions)

Increased pressure from regulators and customers to institutionalize supply-chain transparency from provenance to end consumer (eg, German supply-chain law initiative)

Growing number of successful pilots and validation of use cases attracting network members (eg, Walmart)



Limits to scalability for well-known applications, including transaction throughput and energy or infrastructure requirements

Uncertainty about regulatory and governance developments, including jurisdiction and enforceability of smart contracts, financial regulations, and offshore data storage

Lack of standards for deployment of DLT/blockchain solution (eg, terminology, programming practices, or platforms) and incompatibility with legacy systems

Unresolved threats of cyberattacks (eg, quantum brute-force attacks) Efficient consensus for effective consensus mechanisms that require less or no energy

Trust architecture