Blockchain

Re-imagining Multi-Party Transactions for Businesses

Produced by

ISCA

Global Mindset, Asian Insights

IBM

Contents

Blockchain

Re-imagining Multi-Party Transactions for Businesses

Blockchain is a shared, immutable ledger that enables trusted multiple party transactions. Blockchain offers us the opportunity to relook existing business networks, and re-imagine how we perform, record and secure transactions. By making transactions shared and distributed, we break down silos of information control. This makes the transactions faster and more efficient, while completely preserving notions of privacy, authenticity, and auditability.

Blockchain has been popularised by Bitcoin, the cryptocurrency. However, there are many other potential applications. This article focuses on how blockchain can be applied to businesses, especially in highly regulated industries like financial services. We will describe some of the key concepts in blockchain for businesses, potential use cases, and considerations for adopting the technology.

1. Basic concepts

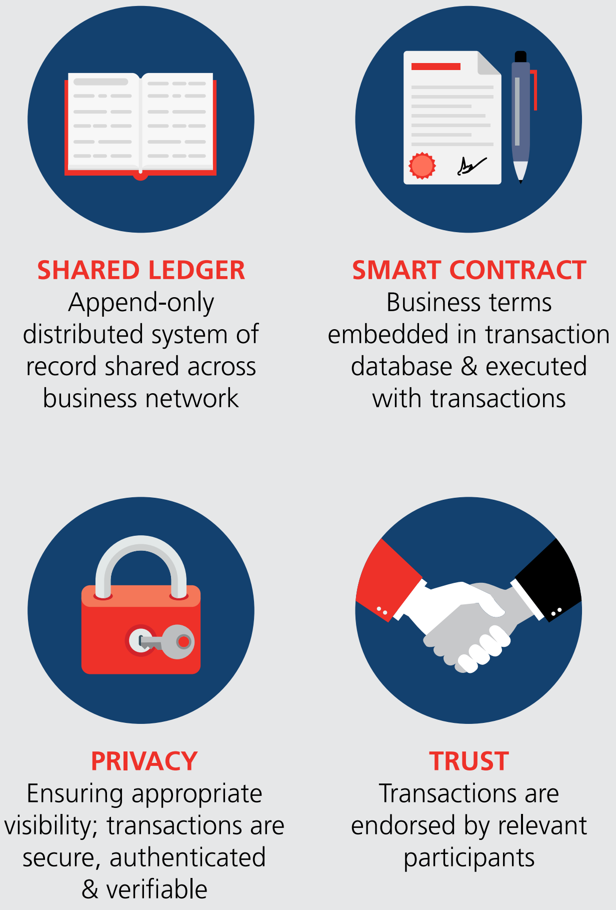
Blockchain leverages the solid underpinnings of existing disciplines like distributed systems, cryptography and transaction management coming together for the first time on the back of the sensation created by Bitcoin.

In this section, we introduce four concepts of blockchain that are key to understanding how the technology could be applied to businesses.

Shared ledger vs centralised databases

With centralised systems, individual participants in the business network (e.g. banks, government, logistics) have their own version of the system of record and need to reconcile their version with that of trusted intermediaries. Centralised systems also have their system of record stored in one place. This could potentially be costly, time intensive and vulnerable to attacks.

▼ **Figure 1** Key blockchain concepts



SHARED LEDGER
Append-only distributed system of record shared across business network

SMART CONTRACT
Business terms embedded in transaction database & executed with transactions

PRIVACY
Ensuring appropriate visibility; transactions are secure, authenticated & verifiable

TRUST
Transactions are endorsed by relevant participants

Blockchain introduces the concept of an append-only distributed system of record shared across the business network. When there is an update of the records by one party, the same copy of the system of record is copied to all member nodes in the network.

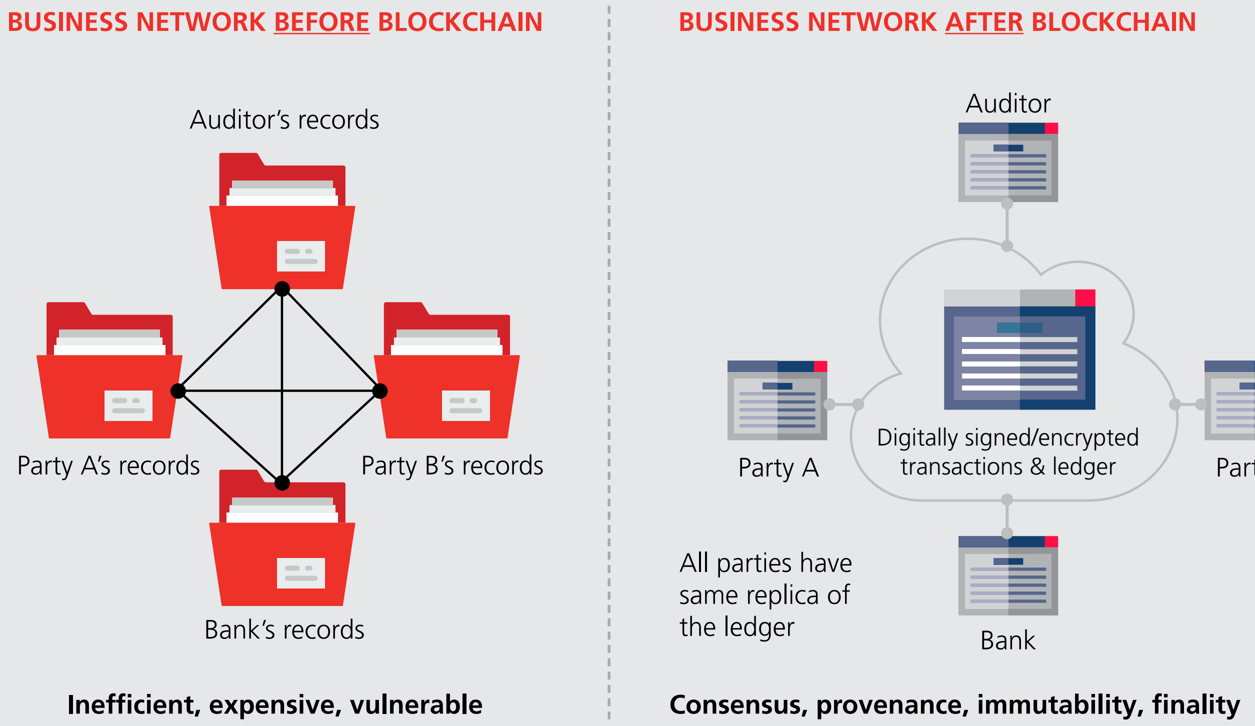
All the confirmed and validated transaction blocks are linked and chained from the start of the chain to the most current block – hence the name blockchain. The blockchain permanently records, in blocks, the history of asset exchanges that took place between the peers in the network. It thus acts as a single source of truth, and members in a blockchain network can view only those transactions that are relevant to them.

This makes it hard for the data to be tampered with. Once data is written into one block of the blockchain, it is immutable – it cannot be changed. What this creates is a permanent record of the transactions in the blockchain's history. This overcomes the challenges of a single party unilaterally altering records. Malicious organisations or individuals would not be able to cover their tracks after tampering with the database, such as after embezzling funds for example. This high risk of detection can deter fraud.

Blockchain could potentially be a game changer by alleviating the challenges associated with complex reconciliation efforts between parties involved in a business transaction. Imagine the example of an international trade transaction, which will involve four parties – the buyer, the seller, the buyer's bank and the seller's bank. Traditionally, each party would maintain their own database of transaction records, even though the transactions are interdependent. The seller will ship the goods ordered, after knowing that the buyer's bank has issued a letter of credit in the seller's favour to the seller's bank.

Currently, the reconciliation of records among the parties would be a cumbersome, time-consuming process, and could be fraught with the risk of disputes. With blockchain, the parties involved would be operating on a shared ledger, and therefore have end-to-end visibility of the process and transactions. The visibility could potentially speed up the resolution of any potential disputes.

▼ **Figure 2** A business network before and after blockchain


BUSINESS NETWORK BEFORE BLOCKCHAIN
Auditor's records
Party A's records
Party B's records
Bank's records
Inefficient, expensive, vulnerable
BUSINESS NETWORK AFTER BLOCKCHAIN
Auditor
Party A
Digitally signed/encrypted transactions & ledger
Party B
All parties have same replica of the ledger
Bank
Consensus, provenance, immutability, finality

Smart contracts

Smart contracts encode the rules that govern a business transaction using programming language. The business rules implied by the contract are embedded in the blockchain, and executed with the transaction. Smart contracts may have many contractual clauses that could be made partially or fully self-executing, self-enforcing, or both. For example, you could define contractual conditions under which a corporate bond transfer occurs.

The purpose of smart contracts is to provide a form of security that is superior to traditional contract law, while reducing the costs and delays associated with traditional contracts.

Consensus and decentralised decision making

Another key concept of blockchain is that of consensus. This is the process by which transactions are verified by parties on the network. In existing business networks, decision making is centralised, and a single operator could decide what is updated in the system of record, which subjects it to potential abuse.

Blockchain changes that paradigm by enabling decentralised decision making. Consequently, there is no central authority that controls what is updated on the blockchain.

There is a variety of mechanisms to achieve consensus on a blockchain network. One popular mechanism is the use of Proof of Work (POW), which is the cryptographic mining technique used in Bitcoin. This enables verification by anonymous participants, but comes at a significant computing cost. When participants are known, it is possible to do the verification at a much lower cost.

Besides POW, there are multiple alternatives such as:

1. **Proof of Stake (POS)** – where fraudulent transactions cost validators (e.g. transaction bond)
2. **Multi-signature** – for example, where 3 out of 5 participants agree
3. **Practical Byzantine Fault Tolerance (PBFT)** – an algorithm that is designed to settle disputes among competing nodes/network participants, when a node generates different output from others in the set.

In practice, different business networks have different levels of friction and trust. Consequently, each network would require different consensus mechanism that caters to the characteristics of each business network.

Privacy

Public blockchains, such as the Bitcoin blockchain, support anonymous transactions on a public network. The information is public and is sent to all the nodes in the network, so all participants are aware of the details of the transactions. Meanwhile, the transactions are verifiable by all parties, so participating members can verify the hashes all the way to the genesis block, and ensure that they match.

Meanwhile, in highly regulated industries such as banking and healthcare, there is a need to ensure confidential information is shared with parties on a need-to-know basis only. To support this requirement, enterprises are increasingly looking towards private blockchains, such as those offered under the Linux Foundation Hyperledger.

Private blockchain implementations support this requirement through the use of private transactions, which ensure that identities are not linked to a transaction. At the same time, transactions need to be authenticated, so that parties can only see those transactions that they are authorised to see. Cryptography is central to these processes.

If there is confidential information that should not be read even by other users of a private blockchain, one way to preserve confidentiality is to store the data off the blockchain, and link to it back to the blockchain by a reference code.

For example, confidential details in a contract document need not be included in the blockchain; nevertheless, the reference link from the blockchain to the contract document can be inscribed on a block record, should there be a potential need for legal enforcement. It is also possible to encrypt confidential data and allow access to selected persons holding the key to decrypt the data.

2. Use cases and adoption patterns

Where can blockchain be used?

Blockchain shows great promise across a wide range of business applications. It can help to significantly improve industries, beginning with the financial industry, and transform other types of industries spanning the legal system, the Internet of Things, healthcare, supply chains, manufacturing, technology, government, and more.

In the financial industry, blockchain can reduce duplicative record-keeping, eliminate reconciliation, minimise error rates and facilitate faster settlement. This, in turn, may mean reduced risk and lower capital requirements for financial enterprises. These benefits are critical and relevant to an industry that is focused on de-risking, and maintaining trust and compliance to industry regulations.

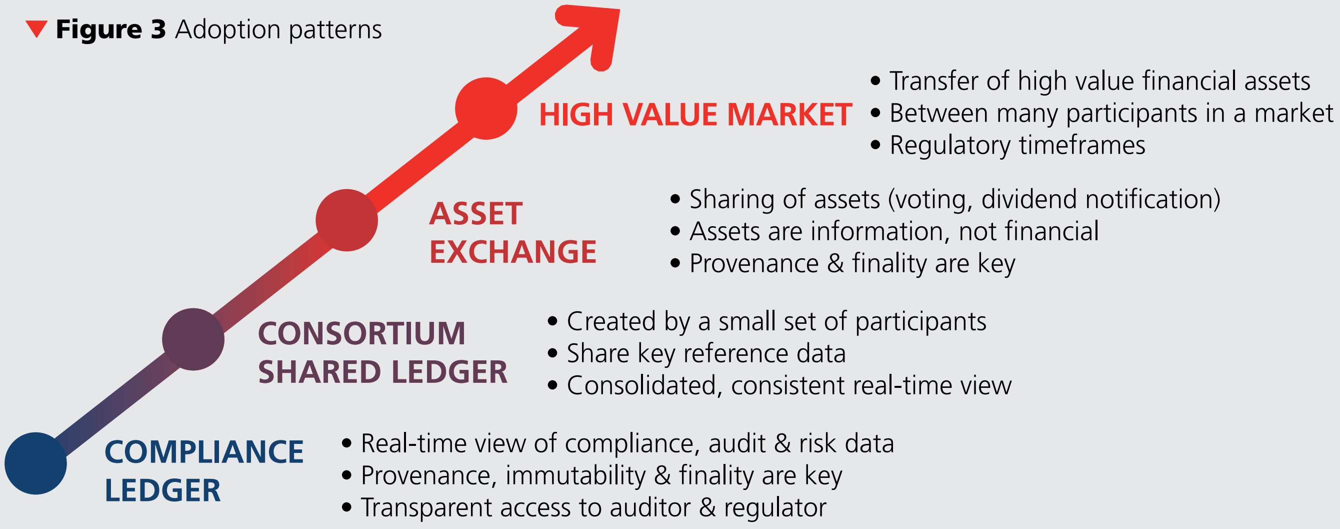
In the legal industry, blockchain helps to provide a shared record of the contract status, which is updated as it progresses through the purchase and delivery stages. It enables information to be made available to all parties to the agreement, their banks, and partners. Accordingly, we can help to improve efficiency, transparency and risk management through the near real-time update of all contracts. This works well for the legal industry, given that business-to-business contracts may require privacy control to protect sensitive business information from being disclosed to outside parties that also have access to the ledger.

Meanwhile, manufacturers can reduce the need for whole-scale product recalls by sharing production logs with original equipment manufacturers (OEMs) and regulators, which would help pinpoint more precisely the affected products that need to be recalled. Businesses of all types can manage more closely the flow of goods and related payments, with greater speed and less risk.

While financial services is leading the field in experimenting with and implementing blockchain technology, it is essentially suitable for any enterprise that involves multi-party and multi-layered transactions. Consequently, the implementation of blockchain technology often involves multiple parties across industries, and requires a cross-industry collaborative effort.

Blockchain use cases tend to fall into one of these four categories below. The categories towards the bottom of the chart tend to be easier to implement because they have fewer participants to influence, or require less regulatory involvement. Use cases in the categories towards the top of the chart may take longer to come to fruition, but are highly valuable and transformative.

▼ **Figure 3** Adoption patterns



HIGH VALUE MARKET
- Transfer of high value financial assets
- Between many participants in a market
- Regulatory timeframes

ASSET EXCHANGE
- Sharing of assets (voting, dividend notification)
- Assets are information, not financial
- Provenance & finality are key

CONSORTIUM SHARED LEDGER
- Created by a small set of participants
- Share key reference data
- Consolidated, consistent real-time view

COMPLIANCE LEDGER
- Real-time view of compliance, audit & risk data
- Provenance, immutability & finality are key
- Transparent access to auditor & regulator

High-Value Market – interdependent transactions which are created by multiple parties across industries that do not share a common database. A classic example is found in trade finance, where the seller is at risk for shipping the goods before payment, and the buyer is at risk for paying before receiving the goods. The banks provide financing for the network and are operating in a highly regulated market.

Asset Exchange – where recording the chain of historical data of ownership (the "provenance") is integral. An example is the diamond blockchain by the London-based startup Everledger, which allows stakeholders such as buyers and sellers, jewellers, insurers and banks, to verify the authenticity of the registered diamonds.

Consortium Shared Ledger – where reference data, such as customer identity, is shared among a small set of participants. For example, The Seam – a US commodities trading software provider – formed a consortium with IBM to develop a blockchain platform for the supply chain and international trading of cotton. Customer information needs to be captured only once and it can be shared with other partners on the blockchain platform.

Compliance Ledger – real-time sharing of compliance data is provided. Take a hypothetical example of a car manufacturer placing the emission testing of their cars on a compliance ledger. The auditors and regulators for emission standards can participate in the ledger with end-to-end visibility of emission compliance in real-time.

What is the state of development of blockchain applications?

Bitcoin is the most established blockchain application so far, but the technology has since evolved. Private blockchains and smart contracts are some of the more recent innovations that are catching on. The legal framework to govern blockchain operations on a large commercial scale is still lacking though.

The financial sector has been particularly keen on developing blockchain, and many "proof of concept" projects are ongoing (see Case 1).

Case 1: Standard Chartered and DBS in Tradesafe

In late 2015, Standard Chartered and DBS Group Holdings Ltd developed and tested a blockchain to reduce the risk of multiple-invoice fraud. In trade finance, the invoice is a seller's asset that can be used for factor financing. Multiple-invoice fraud occurs when the invoice is used as collateral for debt financing for multiple times, and then the culprit defaults on the debt. The idea behind the trial project code-named TradeSafe, which involved 60 mock invoices, is as follows:

- The invoice number and the Bill of Lading number are used to generate a unique reference number that is stored on the blockchain.
- Commercially confidential information, such as terms of financing, are excluded.
- The bank receiving the invoice attaches one of four processing states – received, being processed, financed or rejected -- to that reference number.
- If another bank enters the same invoice data into the blockchain, it would generate the same reference number alerting the second lender that the invoice already exists on the ledger -- and what stage of processing it was at.
- Based on the stage of processing, the other bank can then decide what it wants to do with that invoice.

In the next phase of the project, the working team will widen the participation to include other industry stakeholders, including government agencies such as Singapore Customs and other banks based in Singapore, to join as partners and contribute to the commercial adoption of this initiative.

Sources: Bloomberg, Financial Times

As of early 2017, there are now a few live applications of private blockchain. IBM Global Financing (IGF), the financing arm of the technology corporation which has an office in Singapore, is already using a blockchain solution to make its work more efficient (see Case 2). A small part of the future is already here.

Case 2: IBM Global Financing

IBM Global Financing (IGF) provides financing for the purchase or lease of capital IT equipment to more than 125,000 clients in over 60 countries for over US$ 44 billion. With such a vast network of suppliers and partners, IGF faces major challenges with over 25,000 disputes a year, tying up more than US$ 100 million in capital at any given time.

IGF reduced time spent resolving financial disputes by 75% using blockchain technology. The time for dispute resolution falls from more than 40 days to less than 10 days, and achieved 40% capital efficiency in disputes. Blockchain provides comprehensive visibility across the entire transaction lifecycle which allows stakeholders to prevent or speed up the resolution of disputes. The advantages of a blockchain solution are:

- Full details of the dispute as it occurs;
- Reduces time researching issues;
- Instant action gets work back on track;
- Fast resolution frees up funds.

Source: IBM

Other recent examples include the Walmart-sponsored food safety network, Maersk's global trade digitisation solution, and Northern Trust's private equity network.

What are the roles in a blockchain network?

We have characterised the following common roles in a blockchain network:

DEVELOPER

The developer conceptualises and develops the blockchain software (including its embedded rules and validation mechanisms), in consultation with the blockchain users to reflect their operational needs.

USERS

- Users are participants in the transactions posted on the blockchain, e.g. buyers and sellers in a trade finance application of blockchain.
- Depending on the design of the blockchain, they can read anything in the blockchain (public blockchain), or can read transactions related to them (private blockchain).
- They can post transactions to the blockchain network that may later become recorded once validated.

VALIDATORS

- In a public blockchain, anyone can be a validator. The validator would require an incentive for validation (e.g. financial rewards in the form of bitcoins) in return for their service in validating a transaction as a non-interested party.
- In a private blockchain, a closed group of users act as validators.

NETWORK OPERATOR

- Sets up and maintains the blockchain network. The network operator is responsible for onboarding members to the network.

3. Considerations for blockchain for businesses

How do I know I need a blockchain?

It is important to first define and understand the business problem without any technology or solution bias, instead of using a solution to look for a problem. Here is a set of questions that businesses should consider in deciding whether to embark on a blockchain project:

- **Is there an identifiable business network with a need to share information?** Ideally these are separate companies, but in large organisations, autonomous units are fine. A regulator can be a participant.

- **Is there a set of assets that require management within that business network?** Identify a set of assets that need to be shared. Often, assets will be transferred between participants.

- **Does the status of assets need to be recorded? (e.g. "delivered", "received")** Blockchain is suitable for recording transactions about assets in a business network. Think about the ownership lifecycle of an asset by the participants.

- **Do the participants require a relatively high degree of collaboration?** Good blockchain projects support the need for participants to collaborate, for example in a market, consortium or at the request of a regulator.

- **Is there a need to maintain the history of all updates to the assets ("provenance")?** Blockchain provides both provenance and immutability, which are significant benefits for assets with relatively sophisticated lifecycles – such as the ownership history of diamonds.

- **Are there rules which govern properties of the asset (e.g. how transfer of ownership between participants can occur)?** A blockchain can enforce business rules in contractual relationships, through smart contracts. If there are no business rules behind the transfer of assets, an alternative technology might be more appropriate.

How to get started

Here are some suggestions for your firm to get started on blockchain:

- **Consider agile proofs of concept, and incrementally expand scope for major business results:** Use insights from earlier, more limited projects to re-engineer and implement larger efforts. Identify the most compelling use cases – consider which frictions are holding back your enterprise. Experiment in discrete areas where the attributes of blockchains drive rapid impact.

- **Recognise the need for global standards:** Blockchain innovation may accelerate faster and scale further than the internet ever did. This requires global standards to be developed even sooner. Place your bets and invest your time now.

- **Open governance:** Explore the role of alliances and consortiums in making blockchains scalable, open and interoperable. Blockchains will benefit from open-standard governance. An example is the Hyperledger project, founded by The Linux Foundation. Hyperledger is a collaborative effort to advance cross-industry blockchain technologies. It is deemed an "umbrella" for developer communities building open-source blockchain and related technologies. The Hyperledger project was launched on 9 February 2016 with 30 member sponsors, including 11 Premier sponsors comprising the permanent members of the Governance Board. As of May 2017, there are 130 members.

- **Play for the long term:** Consider how your ecosystem could best benefit from network effects, and how profit pools might be redistributed in your industry or ecosystem. Then, evaluate your role in this disruption. Consider whom you should partner with to create the optimal business network.

Glossary:

Append-only distributed system – The word "append-only" means records can be added to but not deleted from or modified in the blockchain. A new transaction will have to be initiated to compensate for the previous erroneous record. Distributed assumes that the records are kept in multiple locations. In a blockchain, there are multiple sets of records, where each set is as credible as any other set, housed in multiple computers (called nodes) in a network. This makes it a distributed system. By design, these records are consolidated in blocks and linked sequentially. Hence new records are appended in blocks after the latest block.

Finality – The character or condition of being final, settled, irrevocable, or complete.

Hash – An abbreviation of an original data generated by a mathematical tool called hash function. A hash has a useful property. It is easy to verify that the hash originates from a data, but as there are many possibilities, it is difficult to predict what hash will be produced from any data.

Immutable – Unchangeable, indelible. A blockchain is designed such that once a block is verified and accepted, changing any record in the block requires rebuilding the blockchain from that block onwards and triggering re-validation of subsequent blocks all over again. This makes change very difficult, if not impossible.

Member node – A computer in the network in the blockchain

Open governance – Suggests the way the group is structured and who provides direction and oversight to the group.

Open standard – Suggests interoperability through open, published interfaces and services.

Ownership lifecycle – The processes that identify and measure the creation, holding, transfer and destruction of the property rights of an asset by participants.

Private blockchain – A blockchain where the validation (and hence writing) of records is by a close group of known participants.

Provenance – A complete record of ownership history.

Public blockchain – A blockchain whereby anyone in the public (provided pre-requisites are met) can read and send transactions to.

Shared ledger – A set of records where the authority to create records is not by one party, but rather by consensus of several parties to ensure the reliability of the records.

Notes and resources:

- **Blockchain for dummies (E-book)**
  https://goo.gl/tlWahj
- **Linux Foundation Hyperledger Project**
  https://www.hyperledger.org/
- **Maersk and IBM Industry-Wide Cross-Border Supply Chain Solution on Blockchain**
  https://goo.gl/g2q00i
- **KBank Reduce Complexity in Corporate Credit with Blockchain**
  https://goo.gl/tLvOqF
- **JPX - Applicability of Distributed Ledger Technology to Capital Market Infrastructure**
  https://goo.gl/14yMro
- **Northern Trust – Private Equity Administration**
  https://goo.gl/kLUviU
- **Blockchain Basics and Getting started with IBM Blockchain**
  https://www.ibm.com/blockchain/
- **Thought leadership papers from IBM Institute of Business Value – Blockchain**
  https://goo.gl/waeFlD
- **Blockchain basics: Introduction to distributed ledgers**
  https://goo.gl/I2dKFw

ABOUT THE INSTITUTE OF SINGAPORE CHARTERED ACCOUNTANTS

The Institute of Singapore Chartered Accountants (ISCA) is the national accountancy body of Singapore. ISCA's vision is to be a globally recognised professional accountancy body, bringing value to our members, the profession and wider community. There are over 32,000 ISCA members making their stride in businesses across industries in Singapore and around the world.

Established in 1963, ISCA is an advocate of the interests of the profession. Possessing a Global Mindset, with Asian Insights, ISCA leverages its regional expertise, knowledge, and networks with diverse stakeholders to contribute towards Singapore's transformation into a global accountancy hub.

ISCA is the Administrator of the Singapore CA Qualification and the Designated Entity to confer the Chartered Accountant of Singapore - CA (Singapore) - designation.

ISCA is an Associate of Chartered Accountants Worldwide (CAW). CAW brings together 11 chartered accountancy bodies connecting and representing the interests of over 1.6 million members and students globally.

For more information, visit **www.isca.org.sg**.

INSTITUTE OF SINGAPORE CHARTERED ACCOUNTANTS

60 Cecil Street
Singapore 049709

Tel: (65) 6749 8060 | Fax: (65) 6749 8061
Email: isca@isca.org.sg

www.isca.org.sg

Global Mindset, Asian Insights