CCITAGS

Canadian Conference on IT Audit, Governance and Security

April 2-4, 2019
The Globe and Mail Centre, Toronto

Prepare for Blockchain Disruption: The Basics and What It Means

The Institute of Internal Auditors Toronto Chapter

The Institute of Internal Auditors
L'Institut des auditeurs internes Canada

CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Why Blockchain is a Disruption?

US$20 billion

The Blockchain market is expected to be worth around US$20 billion by 2024.

90%

Around 90% of the banks in North America and Europe are exploring blockchain and its underlying technology, while globally it stands around 69%.

28 million

There are 28 million blockchain wallet users worldwide.

13,309

There are 13,309 currently open positions in the blockchain space according to LinkedIn's job search tool.

42

42 systematically important financial institutions are doing active research on Blockchain.

US$1.1 billion

Approximately US$1.1 billion have been invested in Blockchain technology.

8-12 billion

Blockchain technology could save banks between $8-12 billion annually.

86.7%

By 2022, Canada will enjoy the second-fastest growth in blockchain spending globally, with the CAGR hitting 86.7% after Japan's 108.7%.

CCITAGS

What is Blockchain?

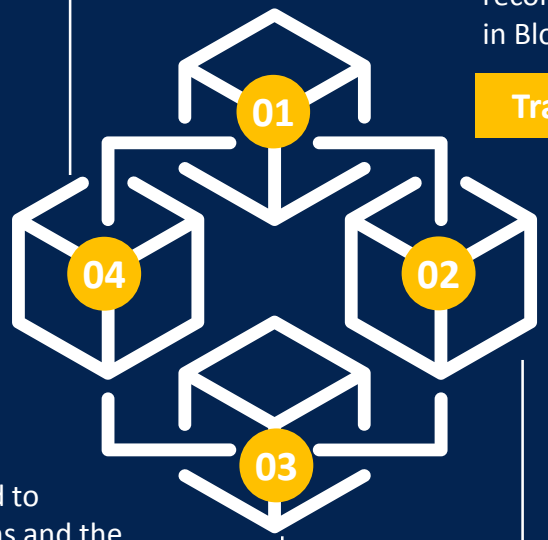
Blockchain is a distributed digital ledger technology in which transactions are recorded chronologically and publicly. Originally developed as the technology underpinning the Bitcoin cryptocurrency, it uses consensus and cryptography to validate each transaction while also protecting the identities of all participating parties. It can operate in permissioned and permission less models.

Provenance

Blockchain is shared between all parties that participate in the events.

Transparency

Every transaction in a blockchain is fully recorded and traceable to individual participants in Blockchain.



Consensus

Blockchain technology can operate without any central authority as the record of events can only be updated after a consensus of the participants, and once information is entered it can never be erased, sometimes referred to as immutability.

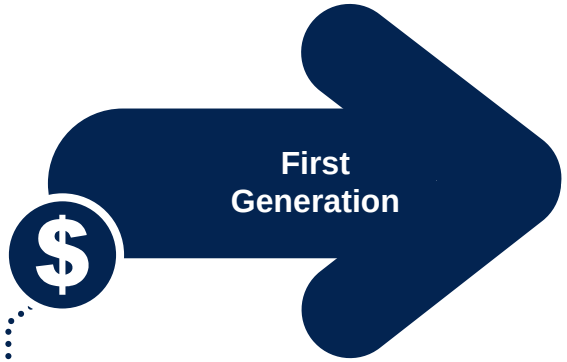
Immutability

Blockchain technology can be leveraged to facilitate peer-to-peer (P2P) transactions and the exchange of value or information between any two parties.

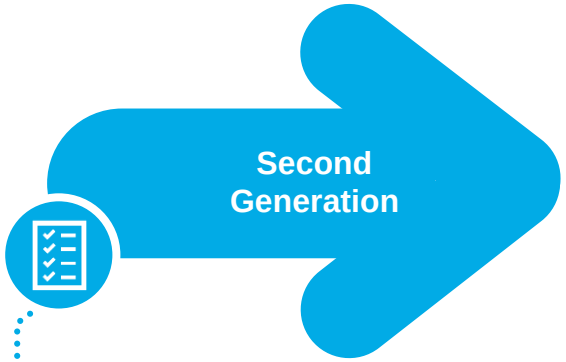
CCITAGS

The journey so far…

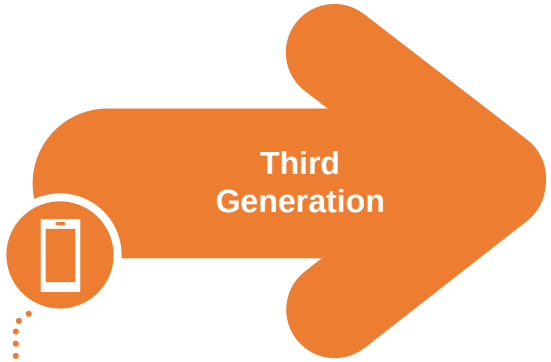
Blockchain has evolved in ways that provide important implications and opportunities for the every industry, ensuring the foundation to manage evidence that can prove to be truth. As a result, blockchain has delivered a mechanism to re-architect certain aspects of the business model:



- Blockchain technologies (which traditionally supported Bitcoin) based on capturing unique identities, protecting sensitive customer data and maintaining a payments transaction audit trail



- **Content** (contracts, documents, claims forms, invoices that link end transactions with client and policy or claims documents)
- **Access to third-party information**



- **Programmable services** (indexation of assets – driving third-party automation or verification services)
- **Internet of Things data integration**

The Advantages Blockchain brings…

No Single Control

- Blockchain evolution removes the reliance on one individual/entity to control and maintain updates to the accounting system.

No Dependence on Central Author

- When compared with the legacy ledger, which relies on the author maintaining it centrally, blockchain is much harder to interfere and tamper with.

Expandable

- Blockchain can also be extended to include the ability to automate and codify rules that enforce “digital” or “smart” contracts based on the information stored within it.

No Dependence on Third Party

- Blockchain has the ability to execute transactions without the help of a third-party intermediary, such as a bank.
- The blockchain ledger is distributed across thousands of computers, so hacking the ledger is nearly impossible.

Provides Transparency

- Blockchain also provides greater transparency over traditional model of private ledger keeping.
- At every stage in a blockchain transaction, the network of participants in the event must agree to the latest block of transactions. This agreement is reached through majority consensus, with duplicate entries eliminated.

CCITAGS

The recent trends observed…

Established players, such as banks and exchanges, are looking for ways to **refine and improve all kinds of transactions**, while integrating blockchain technology and trying to learn how best to connect to and complement these business processes.

Large financial institutions are developing strategic plans to **set parameters for blockchain** technology risk taking.

Financial institutions are focusing on **protecting intellectual property** as they are exploring new collaborative opportunities with customers, suppliers, and competitors.

Market participants of blockchain technology are **starting to develop the processes** that surrounds the transactional layer.

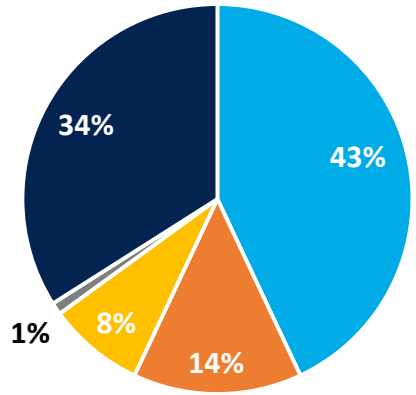
Venture capitalists are **heavily funding blockchain startups** in order to increase R&D activity in this field.

Impact of Blockchain on Organizations

How are organizations going forward with Blockchain?

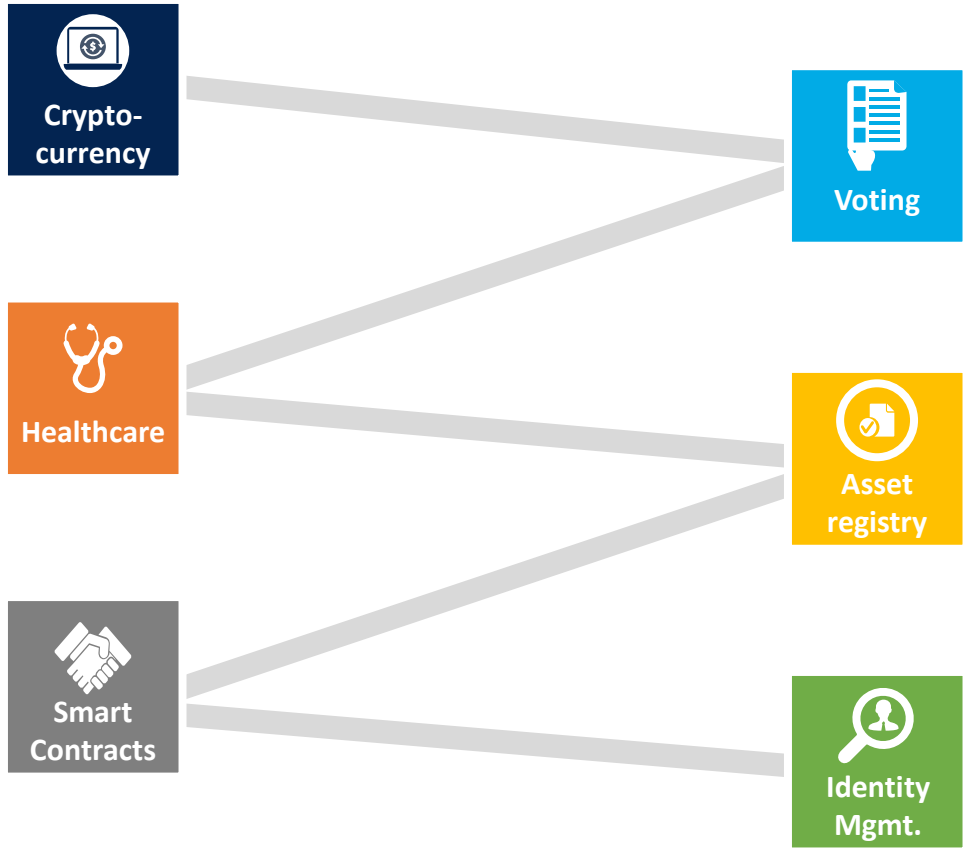
A 2018 Gartner survey of CIOs revealed that only 1% had blockchain deployed in their organizations; **that number has grown to 3.3% today**.

Blockchain Plans of Organizations



- On the radar, but no action planned
- In medium or long-term planning
- In short-term planning/actively experimenting
- Have already invested and deployed

Blockchain Application by Industry

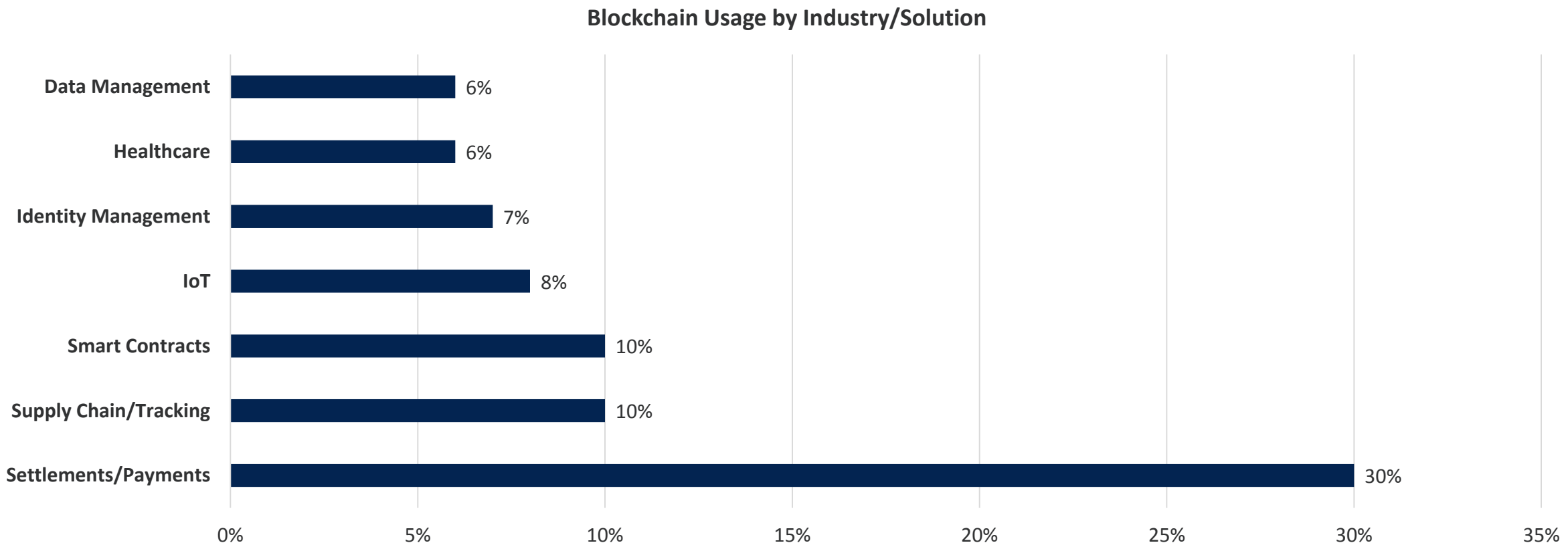


CCITAGS

Application by Industry/Solution

Among companies deploying or considering deploying blockchain, here's the breakdown of what they plan to use it for.

Settlements/payments clearly dominate early deployments.



Understanding Blockchain Business Models

Three ways companies may get involved in Blockchain

Building a Blockchain:

A company may chose to create a Blockchain for their application(s). Creating a new Blockchain can be done using open source platforms such as Ethereum, EOS, NEO, ICON, etc.

Partnership:

A company may chose to partner with an existing Blockchain company. The partnership can be Software as a Service (SaaS), Blockchain as a Service (BaaS) or a consortium between multiple stakeholders. Examples of this include Ripple, R3, Digital Assets, B3i

Asset Holdings/Custodian:

A company may utilize Blockchain technology for asset storage, transactions with partnered Blockchain companies, retail payments, or exchange trading, thus holding cryptocurrencies which fluctuate in value.

CCITAGS

Blockchain and its Risk Environment

CCITAGS

A look at its risks

Scalability
- The time required to put a transaction in the block.
- The time required to reach a consensus.

Data privacy
- Transaction transparency on the blockchain not easily compatible with the privacy needs in banking.

Decentralized Autonomous Organization
- Who is responsible if laws are broken?
- What, if, any, is the liability of DAOs and their creators?
- Who or what is claimed against in the case of a legal dispute?

Jurisdiction
- Complex jurisdictional issues as nodes are located anywhere in the world and require careful consideration in relation to the relevant contractual relationships.

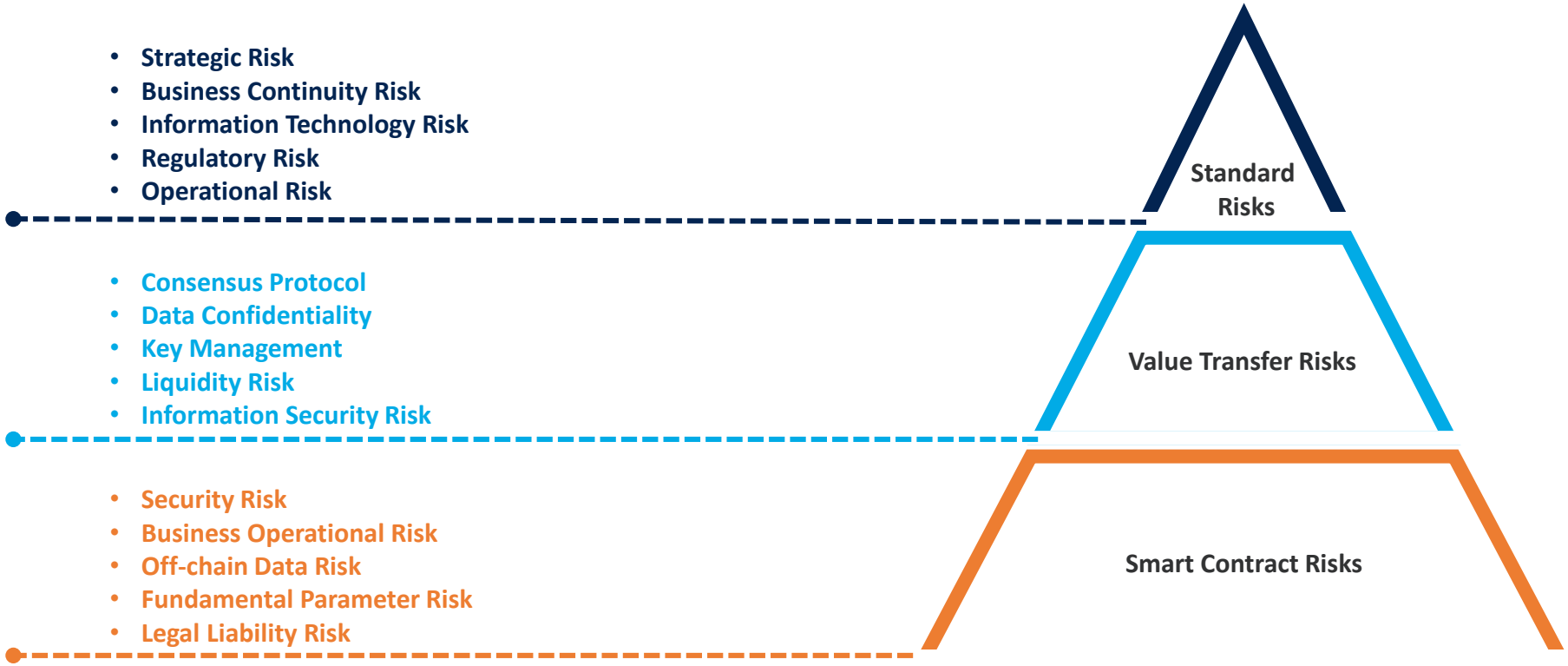
Encryption
- Anyone with the encryption key can read the encrypted data if the key is made public, while if the key to unlock the blockchain is lost you can never get it back.

CCITAGS

Risk Management and Blockchain

Types of Inherent Risks

- Strategic Risk
- Business Continuity Risk
- Information Technology Risk
- Regulatory Risk
- Operational Risk



These are the risks which are similar to the one's associated with current business processes.

- Consensus Protocol
- Data Confidentiality
- Key Management
- Liquidity Risk
- Information Security Risk

These are the potential risks to which interacting parties are exposed to which were earlier handled by central intermediaries.

- Security Risk
- Business Operational Risk
- Off-chain Data Risk
- Fundamental Parameter Risk
- Legal Liability Risk

These are the risks associated with one to one mapping of complex business, finance and legal arrangements on the blockchain.

CCITAGS

Canada as one of the Blockchain's leading Territory

Scenario of Blockchain in Canada

Most active segment in Canada with respect to blockchain usage is **Digital currency/payment**

Crypto-currency contributes the most with respect to experimenting blockchain as crypto regulations are gentle as compared to other jurisdictions.

In 2016, Bank of Canada, experimented with a digital currency called **CAD-COIN** as a way to better understand the technology first-hand.

In the blockchain realm, Canada stands in the third rank after the US and the UK

Canada is home for the inventor of the **Ethereum blockchain, Vitalik Buterin** and thus, the hub for blockchain innovation.

In Jan 2018, the Canada Revenue Agency re-affirmed its stand that bitcoin payments should be treated as **barter transactions**. The Canadian federal government also announced its intention to regulate bitcoin through its anti-money laundering and counterterrorist financing legislation

Leading Government Blockchain Experiments in Canada

In Canada, there are several cases of experimentation and proof of concepts (PoC) under way or completed. Indeed, government departments will benefit from experimenting with **DLT (Distributed Ledger Technology)** and increasingly deploying it strategically. Leading DLT adopters include:

1. **National Research Council:** NRC is using DLT to record contribution agreements and make government research grant and fund information more transparent to the public.

2. **Bank of Canada:** The Bank of Canada completed a one-year Blockchain pilot project named Jasper and concluded that DLT is not yet mature enough to run a national interbank payment settlement system.

3. **Canada Revenue Agency:** The Agency is looking into cryptocurrencies and the risks they pose to the Canadian tax base to inform future risk assessment and audit approaches, in addition to developing the means for detecting tax non-compliance.

4. **Toronto Restaurant Operators:** The Government of Canada, Province of Ontario, and City of Toronto undertook a PoC that explored using Blockchain to reduce the time that business owners take to open a restaurant in the city.

5. **Corporate Registries:** IBM Canada, the Province of British Columbia, and the Digital ID & Authentication Council of Canada (DIACC) collaborated to develop a PoC to explore the viability of Blockchain technology as a tool. Their purpose was to enable more secure, effective, and efficient corporate registrations.

Blockchain and GDPR

About the GDPR

This regulation was created to provide individuals with greater control over how their **personal data is collected, stored, transferred and used by organizations.** It impacts companies that conduct business in the European Union (EU) as well as companies that maintain and process EU personal data.

Who has Authority?

The European Union enacted this law to protect the data privacy of people within its member states. To enforce this new regulations, each member state will have a **Supervisory Authority,** which are individual organizations, that will be responsible for monitoring GDPR. These organizations will be coordinated with the **European Data Protection Board**, who is responsible for the consistent application of data protection in the EU.

Potential Investigation Triggers

Three main channels to get on the Supervisory Authority's investigation list are:

- Data Subject Complaints
- Data breach by Controller
- Data breach by Sub-Processors

Additionally, individuals can also file Class Action Suits against companies directly for violating this regulation.

First Enforcement Action

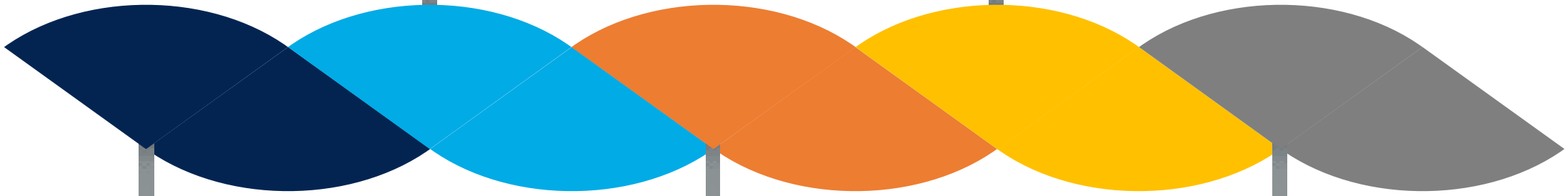
On July 6, 2018, the ICO sent an Enforcement Notice demanding that Canadian company AggregateIQ comply with the GDPR within 30 days. AIQ's continued retention of UK citizens' data is likely to have caused "damage or distress" to those affected and the company is in breach of Articles 5 and 6 of GDPR, the ICO said. The enforcement notice comes as the ICO has hit a string of companies with the highest fine – £500,000 – possible under previous data protection legislation.

CCITAGS

How Blockchain and GDPR are interlinked?

A blockchain network generally contains personal data, where the GDPR is applicable.

Blockchain can be used to manage consent between data subjects, processors and controllers.



There is no contradiction in principle between the goals of the GDPR and those of blockchain technology.

Using Blockchain in KYC process can be helpful in satisfying the data portability requirement

Design of GDPR is technology agnostic & flexible enough to support for Blockchain disruption.

CCITAGS

Tensions between Blockchain and GDPR

There is a direct clash of function, but, on ideological grounds, the aim of both the GDPR and blockchain is the protection of data. The tensions between the GDPR and blockchain revolve mainly around three below issues:

Identification and obligations of data controllers and processors: While there are many situations where data controllers and data processors can be identified and comply with their obligations.

The anonymization of personal data: What does it take to anonymize personal data to the point where the resulting output can potentially be stored in a blockchain network?

Exercise of some data subject rights: Blockchain implies an environment and operating paradigms that may make it difficult to exercise some data subject rights such as the right to erasure or rights related to automated processing.

How GDPR and Blockchain can co-exist?

According to recent researches, beside challenges presented by GDPR, Blockchain technology can exist by making its principles compatible with the regulations under GDPR. There is no such thing as a GDPR-compliant blockchain, but there are only GDPR-compliant use cases and applications:

Principle 1. Start with the big picture: How is user value created, how is data used, and do companies really need blockchain?

Principle 2. Avoid storing personal data on a blockchain: Making full use of data obfuscation, encryption and aggregation techniques in order to anonymize data.

Principle 3. Continue to innovate, and be as clear and transparent as possible with user.

Principle 4. Collect personal data off-chain or, if the blockchain can't be avoided, on private, permissioned blockchain networks. Personal data should be carefully considered when connecting private blockchains with public ones.

CCITAGS

Blockchain and Internal Audit

Internal Audit in Blockchain Disruption

Is Internal Audit ready for Blockchain?

Blockchain technology offers the promise of a safe, transparent, rapid and affordable digital solution to many industry challenges.

However, this same technology also poses challenges and opportunities to auditors wishing to provide maximum value to their organizations.

To capitalize on the opportunities, IA departments must be able to place auditors – **well trained** on both blockchain technology and projects **right from their inception**.

The steps ahead for Internal Audit

Early Involvement: Internal auditors need to get involved at the planning stage of blockchain-based applications. All systems must have adequate governance, risk management, and controls.

Updated Knowledge and Skills: Before adopting blockchain, training internal auditors on blockchain is a necessity.

Adapt to the New Environment: Internal auditors need to update themselves with the new technical environment and they must be able to access information contained in this environment.

CCITAGS

Blockchain: Disruption for Audit Processes

The explosion of new applications of blockchain technology will drive traditional internal audit process to a great extent. Below are some of the major disruptions:

Effective Automated Controls

Auditors need to assess whether **effective automated controls** are in place to validate transactions before they are executed.

Effective Disaster Recovery

Auditors need to have **effective disaster recovery and loss mitigation procedures** in place.

Phishing Attacks

Auditors need to determine whether internal controls to **prevent and detect phishing attacks** are indeed operating effectively.

Real-time Access to Information

Blockchain-based applications provide real-time access to information. **Continuous auditing will allow internal auditors** to use this real-time access to transactions to increase the value they bring to their organizations.

Work Collaboratively Across Organizations

There are public blockchains, such as Ethereum, **that applications may be run on and that have pre-existing governance structures**, but there are also private/consortium blockchains that are only open to identified stakeholders.

Triple-entry Accounting

Auditors may require to verify the application of blockchain mechanisms or protocols. This could be accomplished through "triple-entry accounting," **where existing double-entry accounting systems are retained with blockchain ledger entries.**

Ways to Approach Blockchain in Audit

Implementation and Oversight

- Project Sponsorship and Business Case
- Scope and Requirements Definition
- Budgeting and Resourcing
- Quality Assessments and User Acceptance Testing.
- Deployment

Technology General Controls (Blockchain Apps)

- Application Security
  - Provisioning and Deprovisioning
  - Authentication Requirements
  - Privileged Access
  - Periodic User Recertification
- Interface Change and Program Management
  - Change Process
  - Acceptance Testing/Management Approval
  - Segregation of Environments
  - Emergency Changes
  - Developer: Segregation of Duties
- Interface & Application Layer Operations
  - Data Back up and Retention
  - Disaster Recovery and Business Continuity
  - Job Scheduling and Issue Resolution

Private Key Management

- Key Fragmentation/Repository
- Private Key Recovery (BCP)
- Segregation of Duties

Data Governance and Integrity

- Data Classification (Public Blockchain)
- Interface: Completeness and Accuracy
- Manual Entry (Application GUI)

Data Governance and Integrity

- Data Classification (Public Blockchain)
- Interface: Completeness and Accuracy
- Manual Entry (Application GUI)

Blockchain Regulatory Requirements

- ICO Requirements (SEC)
- Consumer Protection Requirements (NYDFS)
- Taxation (Currency Holdings)
- Jurisdiction

Operations*

- Liquidity
- Anti Money Laundering
- Know Your Customer
- Smart Contracts
- Supply Chain
- Trading
- Financial Transactions and Disclosures

***Note: Operational risk will vary depending on the usage and purpose of the Blockchain and Cryptocurrency.**

CCITAGS

Appendix

Other key terms associated with Blockchain

1 Distributed Ledger Technology

Distributed Ledger Technology is a consensually shared and synchronized database spread across multiple sites. Any changes made to this chain gets reflected and copied to all participants within seconds i.e. real time synchronization.

2 Permissionless or Public Blockchain

Permissionless or public blockchain network is a completely open network i.e. anyone is free to join and participate in the core activities of the blockchain network.

3 Permissioned or Private Blockchain

Permissioned or private Blockchain allows entry of only verified participants, through an authentic verification and a validation from the network administrator or defined protocols to make a change or access the data.

4 Public Key

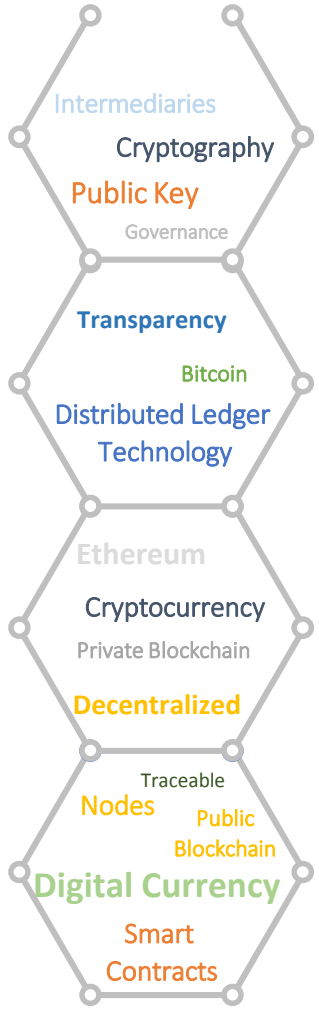
Public key can be obtained and used by anyone to encrypt messages intended for a particular recipient.

5 Smart Contracts

Smart contracts are self executing contracts with defined parameters directly written into lines of code that are built on a blockchain. They not only define the rules and penalties around an agreement in the same way that a traditional contract does, but also automatically enforce those obligations.

6 Cryptography

The main purpose of this component of blockchain technology is to create a secure digital identity reference when 2 or more individuals want to transact over the internet.

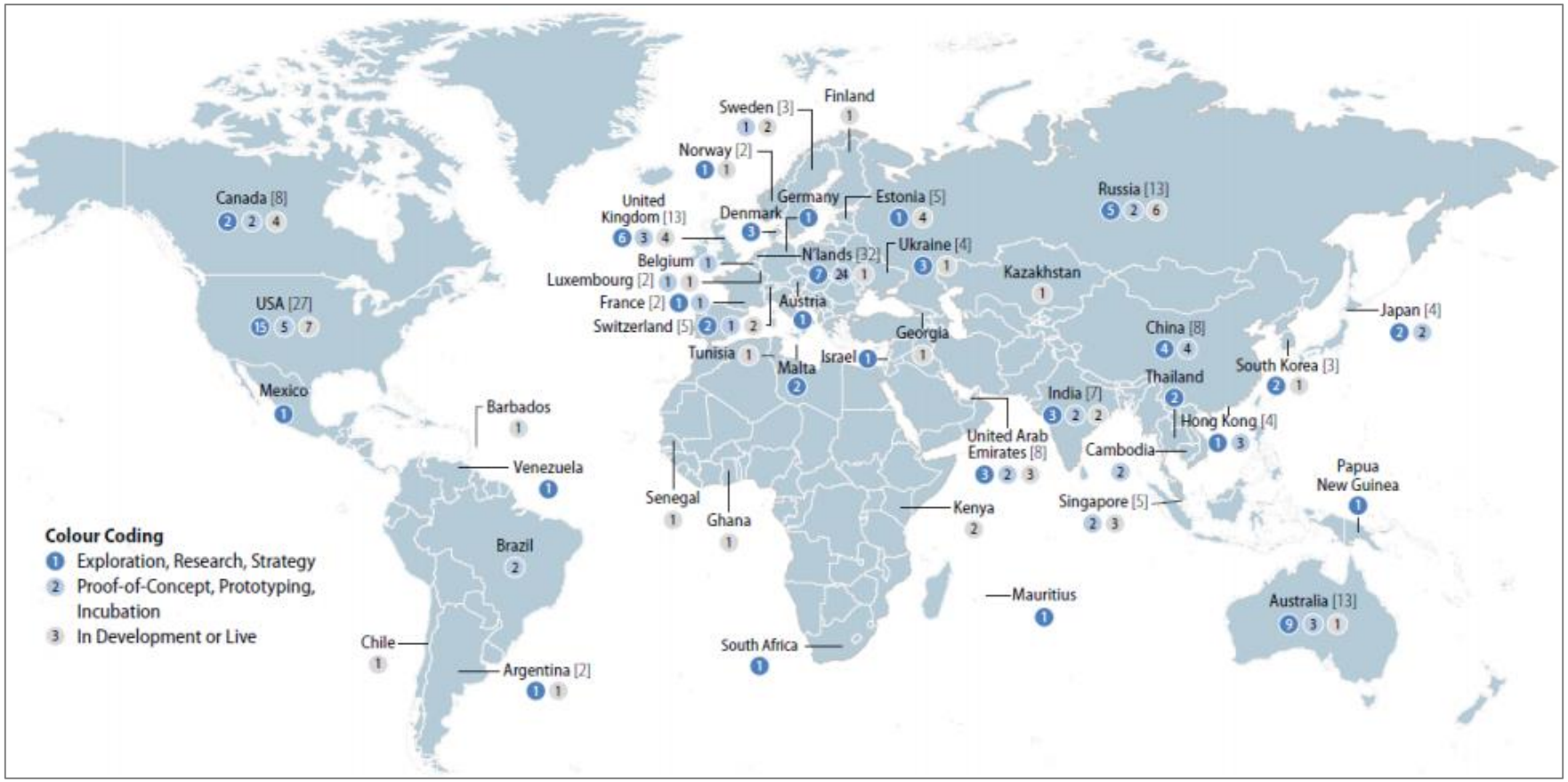


CCITAGS

Global Blockchain usage by Geographies

There has been a significant rise in blockchain experiments by governments in past one year from **117 Initiatives in 26 countries in 2017** to **202 Blockchain Initiatives in 45 countries — including 8 in Canada.**

Following is a indicative list from OECD that highlights usage of blockchain in public sector for 2018:



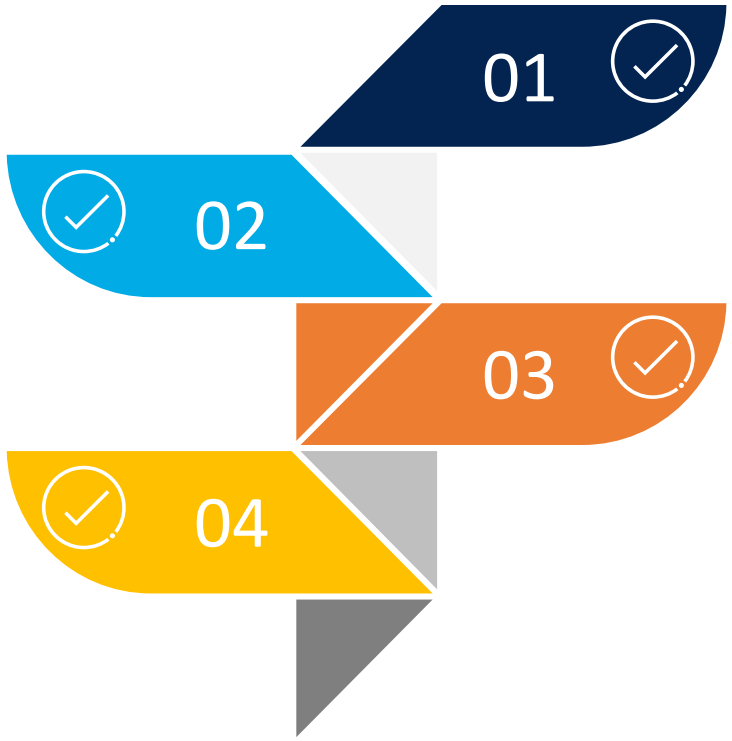
CCITAGS

Difference between Blockchain and Bitcoin

One of the biggest challenges and misconception for blockchain is that it is conflated with Bitcoin.
Here are some points that can bifurcate blockchain from bitcoin:

Blockchain technology has uses and implications that go far beyond Bitcoin or cryptocurrencies in general.

Bitcoin is limited to trading as a currency, but blockchain can easily transfer anything from currencies to property rights.



Blockchain was born with Bitcoin and remains the largest blockchain platform.

Hundreds or thousands of other platforms now exist that work on blockchain platform.

CCITAGS

Post GDPR Highlights

Big Players, Big Targets

- Google and Facebook were sued within minutes by Privacy Activists and EU regulatory bodies due to data breaches which affected million of users.
- U.S. Websites denied access to EU Visitors to avoid compliance costs.
- WHOIS information limited by Registrars
- Plaintiffs' class action lawsuit filed against Nielsen

Unforeseen Aftermath

- Opt-In Fatigue: the endless wave of "tick-the-box" compliance to wave companies operating in EU.
- Expectation of hyper-personalized online interactions in lieu of detailed information
- Complying with GDPR requirements now a paid model for otherwise "free services" for EU companies.

The Wakeup Call

- Businesses realize that more care needs to be given to regulated data, and users should have more rights over their data.
- Increase in responsibilities of Risk Management: strategic, operational & IT departments.

Way Forward for Internal Auditors

Blockchain certainly has the potential to enable numerous new digital solutions to many of the challenges large organizations face.

Internal Auditors must, however, take the necessary steps today to ensure that the blockchains of tomorrow are subject to the same high standards as all other business systems and processes. Otherwise, we risk that potential being unrealized.

Internal audit must be prepared to perform a detailed analysis of the technical architecture of the blockchain, a familiar task for internal audit functions that have been involved in systems development. Beyond that, internal audit must develop strategies for maintaining a sufficient level of transparency and verifying that the blockchain and related applications are performing as intended.

CCITAGS

Key Inherent risks

Off-chain Data Risk

- **Second Layer (Off-Chains)** are built on top of the main blockchain and do not require any fundamental changes to the actual blockchain. The bulk of transactions are 'off-loaded' to the secondary channels to reduce network congestion and facilitate faster processing speeds.
- **Off-chain transactions are harder for the public to verify**, and it could also create compliance issues. Users could also be disillusioned if they aren't given a say in these updates.
- If static data is stored off-chain, **the blockchain can nonetheless record a cryptographic hash of that data** to allow its integrity to be checked.

Fundamental Parameter risks

Below are the risks associated with fundamental parameters of smart contracts:

- Decentralization is expensive
- Decentralization is hard to guarantee
- Identity is hard to manage
- Lost identities are a bigger problem

Thank You

CCITAGS