# TMC's ADVISOR

*Covering IT and Telecom from a Canadian Viewpoint* — *May 2018 , Volume 5 Issue 4*

## Blockchain—Why It's a Game Changer *By Peter Aggus*


It used to be synonymous with Bitcoin—but the actual technology is a Peer-To-Peer, secure, distributed database with far-reaching consequences for internet-based data management. Blockchain provides a P2P transaction 'trust', which has historically only been provided by centralized trusted brokers like Big Banks, or Governments, or even Facebook. Could this be another new era of cultural disruption like the creation of the Internet? Or will the big guys just take it over?

## *Data Stewardship: The Essentials* *By Guy Robertson*

"In my organization, I'm the Director of Common Sense," says Robert, an IT manager in a BC government agency. "I'm in charge of data stewardship, which covers basic and essential aspects of managing data. I handle tasks that everybody takes for granted. Frankly, without me, our agency would be in dire straits."



## Smart City Contest *By Ellen Koskinen-Dodgson*


The Smart Cities Challenge is an Infrastructure Canada initiative intended to push communities of all sizes to make plans to use more data and connected technology. There are four prizes of $5 to $50 million for the current round with new competitions to be offered annually. Obviously, the percentage of winners will be small but benefits will flow to all participants.

## Trusted Partners Expose Data *By Lee-Ann Dittrich*

Digital Shadows, a cyber monitoring service, has published the results of their recent 3 month global scan of some of the most ubiquitous file sharing services across the Internet. They found a shocking amount of publicly exposed data - over twelve petabytes – across open Amazon S3 buckets, rsync, SMB, FTP servers, misconfigured websites, and NAS drives. They report how and why this data is being exposed.

| Highest Exposure | |
|---|---|
| **EU** 538 Million | **USA** 340 Million |
| **Asia-Pacific** 220 Million | **UK** 64 Million |
| **Nordics** 39 Million | **Middle East** 30 Million |

 ISSN 2369-663X

# Blockchain—Why It's a Game Changer *By Peter Aggus*

It used to be synonymous with Bitcoin—but the actual technology is a Peer-To-Peer, secure, distributed database with far-reaching consequences for internet-based data management. Blockchain provides a P2P transaction 'trust', which has historically only been provided by centralized trusted brokers like Big Banks, or Governments, or even Facebook. Could this be another new era of cultural disruption like the creation of the Internet? Or will the big guys just take it over?

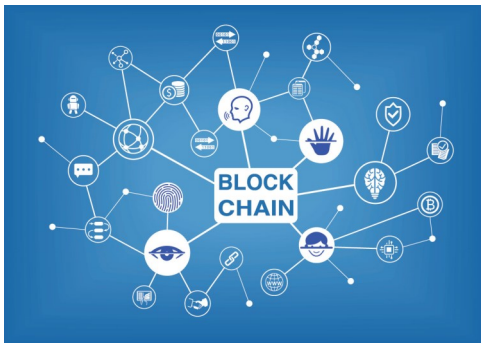
## What Is Blockchain?

When you perform a 'transaction', whether spending money or selling goods, there is a degree of 'trust' involved. The 'seller' wants to know that the 'buyer' has real funds and the 'buyer' wants to know that the 'seller' has real goods—which they then exchange.

With a blockchain, the seller can register the product in a publicly viewable form for the buyer to see before the seller registers his funds in the same way. These two equivalent registrations are then simply swapped and the buyer now has title to the product and the seller has title to the funds. The 'trust' is established because the blockchain is a shared (Peer-To-Peer) database that exists on many distributed servers around the world—making it impossible to forge. It is one of those 'amazing but simple' innovations.

## Applications

Bitcoin is the example most people know about. It shows how trust in 'currency' does not actually need a central bank—which is something essential to real currency. There are examples of blockchain technology being deployed in other fields.




Synereo and Akasha are social networks (like Facebook) but user sharing of data is done by blockchain rather than central servers. There is inherently more privacy and the trust obtained is much higher because users retain total control over their data and simply 'license' it to others as required.

OpenBazaar is a marketplace similar in concept to eBay or Amazon and Mycelia is a service for musicians to market their recordings and get direct compensation from users.

## Decentralisation

Traditionally we have turned to central services to establish trust. For example, eBay do not ship product or store it, they simply provide a platform for buyers to search for products and know that they can 'trust' that the eBay supplier will deliver the advertised goods. If that 'trust' could be certified independently, we would not need the expensive middle agent. This is why Bitcoin is seen as such a threat to the central banks.

With blockchain, transactional trust can be established without central mega-companies, so the wealth they syphon off can be eliminated.

It is not all good news, though. Blockchain is causing a proliferation of vast power-hungry server farms and this will need to be addressed.

## Will Giants Take Over?

So what stops the Big Guys from simply taking over by buying or creating blockchains? It turns out that there's no point as they cannot establish a monopoly nor can they make vast sums of money at it.

It is early days yet but the view of the future for blockchain is very bright. If you employ transactions, and who doesn't, it will be your future.

This article is reproduced from the May 2018 edition of ***TMC's Advisor***



*Peter, as an engineer & technology management consultant, has developed innovative & cost-effective solutions for clients in many industries.*

# Data Stewardship: The Essentials By Guy Robertson

"In my organization, I'm the Director of Common Sense," says Robert, an IT manager in a BC government agency. "I'm in charge of data stewardship, which covers basic and essential aspects of managing data. I handle tasks that everybody takes for granted. Frankly, without me, our agency would be in dire straits."

## Counter-Intuitive

Robert's office shelves are crammed with three-ring binders that contain IT policies, guidelines, procedures, contracts, and training materials. He regularly produces updated documents online and in hardcopy.

"In the best of all possible worlds, I'd keep all of our policies and procedures in electronic form, but distributing hardcopy allows me to reinforce key messages clearly, often, and face-to-face with people. As any data steward will tell you, reinforcing messages through repetition in different formats is one of the best ways to get people to comply. I don't often put my CEO in a half nelson to get him to take me seriously. Usually I rely on repetition to inculcate the importance of effective data stewardship."

## What's Involved?

Roberts activities include:

- Writing, editing, and regularly updating data policies so that they are clear and readable. He recommends using plain language as much as possible
- Examining vital data to ensure its integrity and overall quality; resolving problems as they arise

- Overseeing metadata for all online records; updating obsolete metadata and creating new terminology as required
- Maintaining and enhancing data security tools, orientation and training packages, and procedures, both regularly (i.e. monthly) and whenever the risk of a security breach becomes evident
- Maintaining state-of-the-art backup procedures and technology for agency networks and standalone systems
- Working with the Purchasing Department as well as IT colleagues to ensure that IT contracts are clear and comprehensive, and that vendors have solid reputations. A corollary task involves reviewing vendors after any merger or acquisition that could affect their performance or reliability
- Determining retention periods for all agency data. Data that are no longer necessary are securely deleted; archival data are retained permanently and securely
- Maintaining an IT disaster response plan (DRP) that allows agency users to access data promptly after a disaster such as a fire, flood, or earthquake
- Complying with all Privacy regulations and guidelines for government organizations, and keeping up-to-date on new regulations

"These days I'm training a colleague to take over these tasks while I'm on vacation," says Robert. "If I am not available for an extended period, or I retire, there will be a new Director of Common Sense to take my place."

This article is reproduced from the May 2018 edition of *TMC's Advisor*



*Guy Robertson is a senior planner at TMC and an instructor at the Justice Institute of BC and Langara College. He has written five books and numerous articles on corporate security and disaster planning, and offered workshops and lectures at conferences across North America and in the UK.*

# Smart City Contest *By Ellen Koskinen-Dodgson*

The Smart Cities Challenge is an Infrastructure Canada initiative intended to push communities of all sizes to make plans to use more data and connected technology. There are four prizes of $5 to $50 million for the current round with new competitions to be offered annually. Obviously, the percentage of winners will be small but benefits will flow to all participants.

## Impact Canada

The Canadian Government has created the Impact Canada platform in an effort to engage a diverse range of Canadian innovators and problem solvers. They've created a website where government departments can post challenges and financial prizes to incent creative proposals.

Infrastructure Canada has posted the Smart City Challenge with prizes of $50 million (all population sizes), two of $10 million (population under 500,000 residents) and $5 million (population under 30,000).

## Everyone Wins

There will only be four winners out of the many hundreds of applicants, yet everyone wins. As part of the process, applicants have:

- Held public consultations to crowdsource ideas about which problems to solve and how to best solve them
- Engaged internal and external expertise to identify other ideas and approaches
- Completed a formal planning process to assess and select the ideas that will deliver the best value


This valuable brainstorming and planning is often minimized in favour of day to day operations and 'putting out fires'. However, once completed, there will be no turning back.

Public expectations will have increased and the highest levels of municipal management will have imagined the possibilities. These are important ingredients in raising 'smart city' initiatives towards 'must have' status.

## Vancouver/Surrey

As an example, Surrey and Vancouver have submitted a joint application to implement Canada's first two collision -free corridors, one in each city. The corridors will include autonomous vehicles and smart technologies.

## Toronto

Toronto's submission aims to significantly reduce child poverty for children living in Toronto's older high-rise rental apartment communities by enhancing economic opportunities for their families by removing barriers to employment, providing education, training, and social and cultural opportunities.

## Other Programs

The BC government is providing similar incentives (on a much smaller scale) to small communities.

The City of Orillia, Ontario is directly partnering with Bell to develop a model smart city. The partnership includes digital kiosks to promote local businesses, a public Wi-Fi network, and solutions to monitor sewer status and snowplow progress.

## Leading by Example

This process of government 'gamifying' creative solutions will spark enthusiasm and interest by the public, which will, in turn, motivate local politicians to get involved.

This article is reproduced from the May 2018 edition of ***TMC's Advisor***



*Ellen Koskinen-Dodgson is President and Managing Partner of TMC IT and Telecom Consulting Inc. She is an IT and Telecommunications Management Consultant, electrical engineer, author, speaker, media resource and Expert Witness.*

# Trusted Partners Expose Data *By Lee-Ann Dittrich*

Digital Shadows, a cyber monitoring service, has published the results of their recent 3 month global scan of some of the most ubiquitous file sharing services across the Internet. They found a shocking amount of publicly exposed data - over twelve petabytes – across open Amazon S3 buckets, rsync, SMB, FTP servers, misconfigured websites, and NAS drives. They report how and why this data is being exposed.

## 1.5 Billion Files

While the majority of countries are affected (>95%), the United States has the most unintentionally exposed files of any single country.

Amazon S3 buckets get the most attention but only account for a small percent of exposed data discovered. Older, yet widely used, technologies were a bigger problem:

- SMB: 33%
- rsync: 28 %
- FTP: 26 %
- Amazon S3 buckets: 7%

## Sensitive Information

Highly sensitive information was found during the scanning. There was personal information, intellectual property, and security assessments.

The most common employee data found was payroll (700,000 files) and tax return (60,000 files).

Over two million .dcm files (Digital Imaging) were found. These contained medical tests (like MRIs) as well as other personal health information.

In the intellectual property category, they found yet-to-be-released product designs on social media, sometimes in the format of photographs taken in a company's warehouse.

| Highest Exposure | |
|---|---|
| **EU** 538 Million | **USA** 340 Million |
| **Asia-Pacific** 220 Million | **UK** 64 Million |
| **Nordics** 39 Million | **Middle East** 30 Million |

They also found source code testing results.

In the security category, they found almost 6000 security audit files, almost 2000 'network infrastructure' details, over a thousand network diagrams as well as hundreds of penetration test reports.

Some files included images of the organization's physical set-up of production servers. Some revealed details on insecure servers including server locations and hosting IPs, missing software patches, port information, CVE numbers, and vulnerability descriptions.

This information could allow easy access for an attacker to modify data, inject malicious code, or perform man -in-the-middle attacks.

## Why?

Third parties and contractors were among the most common sources of sensitive data exposure. In trying to back-up or share files, they inadvertently made the information public.

Contractors, suppliers and employees took actions to allow files to be accessed from home or from offsite locations.

## Next Steps

There are many ways to mitigate the risks and these ways are well known (authenticate, disable guest/ anonymous access, IP whitelist…). As the massive amount of exposed data demonstrates, best practices are often ignored.

Organizations must educate staff, contractors and consultants about best practices and the risks of copying and archiving work files at home.

This article is reproduced from the May 2018 edition of *TMC's Advisor*



*Lee-Ann is a researcher and business analyst that oversees benchmarking studies.*