Technology Trends

Blockchain

Enterprise Architecture, Chief Technology Officer Branch

Version 0.1
Date 2019-5-8

Shared Services Canada
Services partagés Canada

Canada

Table of Contents

Business Brief

Blockchain is a list of digital records (called blocks) that are securely linked together to form a chain using secure encryption and time stamps. Blockchains form a digital ledger, which is a history of transaction records that can be accessed by multiple users but cannot be individually modified.

The theory behind blockchain was first described in 1991. The desire was to create a system in which documents could be timestamped and linked together digitally or cryptographically. In 2008, someone or a group of people, known as Satoshi Nakamoto, created the first cryptocurrency known as Bitcoin. The creation of Bitcoin in 2008 also unveiled the technology behind it - Blockchain. Blockchain provides the means for recording bitcoin transactions (as a shared ledger), which can be used to record any transaction and track the movement of any asset that is tangible, intangible or digital.

Due to increasing mistrust around data sharing by some large corporations, as well as the financial crisis earlier that year, there was a growing desire for a means in which personal data or currency could be held individually. It needed to be decentralized and needed to reduce the requirement for middlemen, such as banks, brokers, or insurance companies. As the first of its kind, blockchain technology was revolutionary.[i]

While blockchain technology has begun to expand since its creation, when it first began, users were exclusively individuals. While individual uses involving cryptocurrency such as Bitcoin are still in existence, companies such as Ethereum, Golem, and Blockstack have since emerged and also employ blockchain technology for the rendering of "smart contracts" between individual parties, the sharing of computer processing power and open-source app development respectively. However, the technology is still deemed immature and underutilized. Of the respondents to Gartner's 2018 CIO Survey, only 1% have invested in and deployed blockchain technology.[ii]

Technical Brief

In contrast to traditional records of transactions, which often require an intermediary such as a bank or other administrator, and involve multiple records of the same transaction, the data or transaction records contained within a blockchain are decentralized. For example, in a traditional purchase, a consumer would have a record, the merchant would have a record, a supplier would have a record, and an auditor or accountant would have a record. The bank would also have a record. All of these records are kept separately. Therefore, this process requires a great deal of trust between the individual parties that one record will not be tampered with or lost.

With a blockchain transaction, each of the parties involved (called nodes, users or miners), all have the same replica of a ledger, which is contained in the blockchain on a peer-to-peer (or node-to-node) network. As a result, the bank and the traditional

merchant databases traditionally used to record and organize the data in ledger would be eliminated (i.e. transaction time and date, product, buyer).

In order to form a block or a blockchain, each user requires a specialized computer and mining software. A blockchain is managed and verified collaboratively on a network accessed by multiple users or nodes. These users work collaboratively and use mining and "consensus algorithms" to solve complex mathematical problems. A consensus algorithm is an agreed-upon process for solving calculations and there are several used in blockchain technology depending on the type of calculation to be solved and the type of data to be verified.

Blockchain's decentralized, open and cryptographic nature allows people to trust each other and perform perform peer to peer transactions, which removes the need for intermediaries. It is resistant to hacking attacks that impact centralized intermediaries like banks because to succeed, an attacker would need to hack both the specific block in a blockchain as well as every one of the other potentially million ledgers in the network simultaneously. This would be a difficult endeavor given that the blocks are secured with both public and private keys and require verification by multiple individual users and computers. Even if it were possible, they would also need to update every subsequent transaction in the chain and overwrite every other copy of the ledger in the network to ensure integrity of the new chain.

Despite this natural resistance to attacks, it was reported in the MIT Technology Review that security holes are increasingly appearing in cryptocurrency and smart contract platforms. In some cases, the security issues are fundamental to the way the platforms were built. By gaining control of more than half of the network's computer power, a hacker was attempting to rewrite the transaction history of the exchange platform for cryptocurrency called Coinbase, allowing for the same cryptocurrency to be spent more than once to a total value of $1.1 million.[iii]

Industry Use

The most well-known use of blockchain is in support of cryptocurrencies, such as Bitcoin. A digital currency launched in 2009, Bitcoin does not rely on a monetary authority to monitor verify or approve transactions, but rather relies on a peer-to-peer computer network made up of its users' machines to do that. Blockchain can be used for all sorts of inter-organizational cooperation. In 2017, Harvard Business Review estimated that approximately 15% of banks are expected to be using blockchain.[iv]

Although Bitcoin is the first and most well-known use of the blockchain technology, it is only one of about seven hundred applications that use the blockchain distributed ledger system. Blockchain is a digital ledger on top of which organizations can build trusted applications, via a secure chain of custody for digital records.

Canadian Government Use

Canada does not currently have a federal policy on blockchain. While blockchain is an important emerging technology, how it could be used by the Government remains to be seen. At this point, the ideal GC use case for blockchain would be a system of public record to register secure transactions from multiple contributors toward distributing a single source of truth in a non-refutable fashion.

According to Gartner, there is no Government around the world that is operating a true blockchain initiative , although some (State of Georgia, Hong Kong, United Arab Emirate) are operating pseudo-initiatives and starting to experiment with the technology.[v] Treasury Board of Canada notes highlights a few specific initiatives: Estonia uses an eHealth Foundation partnership to accelerate blockchain-based systems to ensure security, transparency, and auditability of patient healthcare records. Singapore employs the use of blockchain to prevent traders from defrauding banks through a unique distributed ledger-based system focused on preventing invoice fraud.[vi]

In 2017, "The Blockchain Corridor: Building an Innovation Economy in the 2nd Era of the Internet" was developed, discussing ways to turn Canada into a global hub for the "Blockchain revolution." Written by a high-tech think tank and prepared for / partially funded by the federal Department of Innovation, Science and Economic Development (ISED), the report lays out a few proposals regarding how to cement Canada's role as a world leader in blockchain technology. The Canadian Government announced in July 2017 the intention to run at least 6 select pilot projects on the use of blockchain.[vii]

This included establishing a digital economy commission, which will be tasked with developing solid recommendations regarding how Canada can become a leader in developing technologies such as blockchain, quantum computing, artificial intelligence and self-driving vehicles. It also recommended getting governments currently using blockchain to transform their own operations and provide examples of how the technology can benefit public sectors in Canada and abroad. Governments could use blockchain to verify the payment of taxes and manage public services more efficiently.

Implication for Shared Services Canada (SSC)

Value Proposition

Collaborative technologies like blockchain promise the ability to improve the business processes that occur between organizations and entities, radically lowering the "cost of trust." As a result, blockchain may offer significantly higher returns for each investment dollar spent than that of traditional internal investments, but in doing so means collaborating with customers, citizens, suppliers and competitors in new ways.[viii]

Blockchain offers a numbers of benefits to the Government of Canada, such as a reduction in costs and complexity, trusted record keeping and user-centric privacy control. It offers significant opportunities in terms of a single source for public records, support for multiple contributors and a technology ideal for multi-jurisdictional interactions. Due to its decentralized, collaborative nature, it potentially aligns well with policies and practices around Open Government, which aim to make Government services, data, and digital records more accessible to Canadians.

By eliminating the duplication and reducing the need for intermediaries, blockchain technology could be used by SSC to speed-up aspects of service delivery. A challenge for SSC in terms of blockchain will be to identify which enterprise solutions emerge as leaders and how they deal with privacy, confidentiality, auditability, performance and scalability.

Currently, a number of Government agencies are engaged in Blockchain in a number of ways. Maybe SSC could support the following departments in their initiatives to explore how Blockchain can help solve these issues:

Elections Canada – practical applications to support Voter List Management, Secure Identity Management, and management of electoral geography.

Financial Transactions and Reports Analysis Centre of Canada – exploring implications for anti-money laundering and counter-terrorism financing.

Public Safety Canada – focused on various uses and misuses of virtual currencies, such as extortion or blackmail.

Natural Resources Canada – use as a public registry for the disclosure of payments under the Extractive Sectors Transparency Measures Act.

Bank of Canada – exploring a proof of concept model alongside Payments Canada, Canadian commercial banks and the R3 consortium.

ISED – engagement with Government departments, provincial-territorial-municipal partners, and key industry players.

Challenges

There are weaknesses in terms of technological complexity, intensive computational and storage demands and a requirement for common software across all nodes. There are significant challenges particularly important within a governmental process. Truly digital assets with a single copy can be destroyed and a government network housing such assets would represent a very public target for malicious actors. [ix]

It is important to remember that Blockchain, while a technological innovation in transactional business and chain of digital custody, is not a single solution to transactional challenges facing the GC.

The amount of time and energy required to maintain the blockchain and create new blocks is not small and this is a frequent criticism of the technology. Conventional database entry, such as using SQL, takes only milliseconds, compared to blockchain, which takes several minutes. Due to the length of time required as well as the need for multiple computers to verify the blocks, blockchains consume an enormous amount of energy. However, as technology advances, the blockchain consensus process takes closer to three minutes with Ethereum, which is currently among the most advanced blockchains available.xxiii Even older blockchains, such as Bitcoin, are still faster than traditional financial transactions, such as the stock exchange, which can take days to be verified and finalized. Despite this, services or transactions that require rapid speed, may not be suitable for blockchain.

There are also some concerns with respect to privacy. Since blockchain is built on the premise of decentralization and transparency, the data within the chain is technically available for anyone on the network, provided they have the computational power and knowledge to gain access. Instead of being identified on the network by name, users have encryption keys, which is a list of seemingly random numbers and letters. While more private than a name or other demographic information, users could still be identified by their keys over time. Also, any data contained within a block that may have personal information that an individual wishes to keep private, such as medical records for example, may not be well suited for a blockchain as it will be transparent and visible to other users.[x]

Considerations

By using an agreed upon consensus algorithm, collaborative technology like Blockchain promises the ability to improve the business processes that occur between organizations and entities, radically lowering the "cost of trust." The cost of trust is lowered because there is only one record of a transaction that needs to be kept and all stakeholders trust that record.

In a traditional transaction, all stakeholders have to keep a record of the transaction and in the case of a discrepancy, it was more difficult / costly to determine the accuracy of a record. As a result, Blockchain may offer significantly higher returns for each investment dollar spent than that of traditional internal investments. However, to doing so, it means collaborating with customers, citizens, suppliers and competitors in new ways. [xi]

Further research is needed to understand the potential impacts that blockchain could have on SSC as a service provider as well on the usage amounts the GC would require. SSC should consider the identification of client areas where blockchain may be

leveraged. It may be required that client departments self-identify spaces which could benefit from blockchain processes. A challenge for SSC will be to identify which partner organizations and enterprise solutions require priority blockchain pilot projects as well as be able to identify departments that emerge as leaders and how they deal with privacy, confidentiality, auditability, performance and scalability.

Lastly, SSC and the GC should consider the capacity issues in resources, network capabilities, and time required to create and maintain blockchain networks on its own. Blockchain is not a pedestrian technology, it will require dedicated teams that are appropriately resourced and financed in order for the technology to be deployed as any other service. SSC may wish to consider looking for private sector companies that specialize in providing Blockchain as a Service (BaaS), and determine the risk and cost benefits of outsourcing this process altogether.

References

[i] George Gilder, Life After Google: The Fall of Big Data and the Rise of the Blockchain Economy, Gateway Editions, July 2018.
[ii] David Furlonger and Rajesh Kandaswamy, *Hype Cycle for Blockchain Technologies, 2018*, July 2018
[iii] Mike Orcutt, *Once hailed as unhackable, blockchains are now getting hacked*, MIT Technology Review, February 19, 2019.
[iv] Harvard Business Review, A Brief History of Blockchain, 2017.
[v] Gartner conference call.
[vi] Treasury Board of Canada
[vii] Digital Operations Strategic Plan: 2018-2022 - https://www.canada.ca/en/government/system/digital-government/digital-operations-strategic-plan-2018-2022.html
[viii] Treasury Board of Canada, *Blockchain: Ideal Use Cases for the Government of Canada*, 5.
[ix] Treasury Board of Canada, 7.
[x] Henning Diedrich, Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations, Sept 2016.
[xi] Treasury Board of Canada, *Blockchain: Ideal Use Cases for the Government of Canada*, 5.