



Blockchain Technology Brief

Overview

A blockchain is a write-only database dispersed over a network of interconnected computers that uses cryptography (the computerized encoding and decoding of information) to create a tamper-proof public record of transactions. Blockchain technology is transparent, secure and decentralised, meaning no central actor can alter the public record. In addition, financial transactions carried out on blockchains are cheaper and faster than those performed by traditional financial institutions. These properties are at the heart of this technology's rapid expansion.

Bitcoin was the first blockchain. It was implemented in 2009 to create the cryptocurrency bitcoin as an alternative to fiat money/currency (paper money or coins of little or no intrinsic value but made legal by a government). It has a market capitalisation of \$15 billion CAD as of November 2016. A number of second-generation blockchains have been created in recent years with Ethereum being the best known example. Transactions on the Ethereum blockchain include financial transactions but can also include general-purpose database records and programs known as "smart contracts" that can be executed directly on the blockchain. Smart contracts interpret legal or business contracts into computer programming, bringing blockchain properties to commercial transactions. In addition, cryptographically signed **Decentralized applications** ("**Dapps**") can duplicate the functionality of commercially available apps, but in a decentralized and low cost environment. Dapps are applications that execute smart contracts. Examples include ride sharing, crowdfunding, notary services to publicly store ownership data, decentralized electrical power sales, task management, decentralized messaging services (like Twitter), identification and record-keeping, and other governmental services.

Financial Times: [How bitcoin and its blockchain work](#) and [The Ethereum Project](#)

Policy Considerations

Blockchain technology presents a safe, transparent, rapid and affordable digital solution to many government challenges. It could facilitate payments, benefits distribution, identification, record keeping and certification to name a few. On the negative side, there is concern that cryptocurrencies like bitcoin could also be used to facilitate anonymity in criminal transactions and pose legal and security [challenges](#). However, a 2015 UK government [report](#) found that because all bitcoin




Government
of Canada

Policy Horizons
Canada

Gouvernement
du Canada

Horizons de politiques
Canada

Canada



transactions are public, bitcoin had the lowest risk of being used for money laundering. Blockchain innovations like the Ethereum-based DAO present an opportunity for facilitated funding of start-up enterprises. This may be of interest to a country like Canada where Small and Medium-sized Enterprises play an important role in the economy. Similarly, the service sector plays an important role in the Canadian economy and blockchain holds the promise of reducing friction in digital commerce and services by reducing financial transaction costs. These costs are a disproportionate burden on small enterprises with large numbers of small transactions.

Blockchain technology has repeatedly broken [crowdfunding records](#) due to the amount of interest by investors. The global banking community as well as technology and communications industry leaders are funding projects to learn how to make use of this innovation. Fundamentally, this technology is decentralised and can be perceived as a threat to large institutions, potentially including governments. Bitcoin is a currency backed by no nation and controlled neither by banks nor central actors. Unlike the internet, which is run on servers, on soil controlled by nation-states and owned by companies, decentralised software may present entirely new legal challenges in terms of liabilities, rights, and jurisdictions.

While the technology is only seven years old, the inherent nature of open source software allows for blockchain innovations to be rapidly and widely distributed. Waiting to see if initiatives will pan-out, instead of preparing for when such ambitions will become widely successful may prove to be a risky approach.

Advantages

Blockchain technology has the potential to reduce the cost of banking services by providing a near-zero cost alternative. One example is international money transfers. While many currency exchanges will charge a fee (perhaps 2-3%) on the amount exchanged, bitcoin transaction fees are about [5 to 10 US cents](#) regardless of the amount exchanged. Another advantage is speed. Instead of financial trades settled by banks in one to three days, blockchains are capable of clearing transactions in fewer than [15 seconds](#). The decentralised and transparent public record-keeping provided by blockchains can create the trust needed to engage in a transaction with an unknown individual without the need of a jointly trusted third party like a bank or a lawyer. In doing so, blockchain technologies may become a key element in the rise of rapid and inexpensive peer-to-peer transactions for the exchange or sale of goods and services, thus potentially expanding choice and supply in the market place. The use of private blockchains is being explored by a number of sectors to lower the cost and increase the speed and security of their operations. Overall, blockchain technology may raise consumer purchasing power by reducing transactional costs throughout the value chain.

Limitations

One consequence of having universal, decentralized records is that any errors or software faults must occur in the open, and will be rapidly discovered by the global community. This has led to well-publicized thefts, such as the failure of the [Mt. Gox](#) bitcoin exchange, and the [Bitfinex](#) bitcoin hack. While blockchain public ledgers are cryptographically protected and are not vulnerable to most forms of tampering, accompanying services may be just as vulnerable to attack and theft as other digital technologies. Recent discoveries of flaws in the code of one of Ethereum's most ambitious spin offs, the [DAO](#) (Digital Autonomous Organization), has demonstrated that while blockchain technology promises to be transformational, it is still early in its development.

Companies, sites and venues currently accepting bitcoin are few and far between despite [rapid expansion](#), leaving the currency a poor substitute for national currencies and banking services. A general lack of understanding of the technology and a shortage of skilled and knowledgeable talent is perhaps the largest barrier to the wider deployment of blockchain technology.

Policy Horizons Canada is exploring plausible futures for Canada over the next 10 to 15 years in the area of governance, sustainability, infrastructure, and the digital economy. For more information, please contact us at questions@horizons.gc.ca.

Sources

[Digital Currency: you can't flip this coin! - Report of the standing senate committee on banking, trade and commerce](#)

[Device democracy: saving the future of the Internet of Things](#)

[Cryptocurrency 2.0 Report - CoinDesk](#)

Government of Canada

The Bank of Canada gaining first-hand experience with the technology.

Wall Street Journal - [Bank of Canada's Carolyn Wilkins Sees Potential for Blockchain, But Not Just Yet](#)

Policy Horizons Canada - www.horizons.gc.ca

Other Jurisdictions:

- [Blockchain to transform Estonia's e-residency by allowing shareholders to vote in shareholder meetings.](#)
- [Georgia Pilots and Sweden Ponders – Is Blockchain the Future for Europe's Land Registries?](#)
- [Dubai to use blockchain technology for all government documents by 2020](#)
- [Chinese government's primary information technology ministry has published a research paper](#)

[detailing blockchain's benefits](#)

- [Singapore's Central Bank Pairs Up With R3 to Create Blockchain R&D Center](#)
- [UK Government Trials Blockchain Welfare Payments System](#)
- [Blockchain Support Bill Passes Vote in US Congress](#)

Best in Class

- [R3 Cev](#) is leading a partnership between 50 global banks in developing a private blockchain under the project name Corda.
- [Bitnation](#) offers governmental services and emergency assistance for those in need of representation like refugees or aspiring global citizens.
- [Hyperledger](#) is an open protocol and standards project between industry leaders such as IBM, Cisco, Intel, London Stock Exchange, etc... led by the Linux Foundation.
- [Everledger](#) is a diamond database used to fight theft and fraud and help insurance and law enforcement.
- [Zcash](#) is a cryptocurrency offering privacy and selective transparency.
- [The DAO](#), decentralised autonomous organisation was an ambitious project to create a decentralised company whose members could all vote on the many ventures the company would fund.

This document does not attempt to predict the future. The purpose is to stimulate reflection and dialogue and support the development of public policy that is more robust and resilient across a range of plausible futures. The views contained in this document do not necessarily represent the views of Horizons, the Government of Canada or participating departments and agencies.

PH4-171/2016E-PDF
978-0-660-07025-4

© Her Majesty the Queen in Right of Canada, 2016.