OPSI Observatory of Public Sector Innovation

Blockchains for Public Sector Innovation

4instance: The potential of Blockchain in the Public Sector

May 15, 2018

Jamie Berryhill
jamie.berryhill@oecd.org

OECD
BETTER POLICIES FOR BETTER LIVES

OPSI

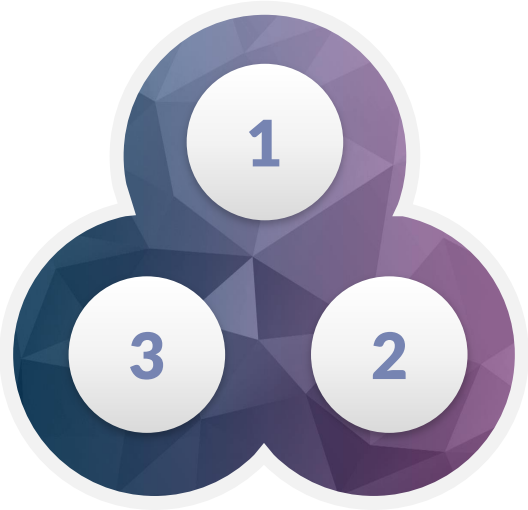
OPSI is a forum for **shared lessons and insights** into the practice of innovation in government. Since 2014, it has worked to meet the needs governments around the world, providing a collective resource to identify, collect and analyse **new ways of designing and delivering** public policies and services.

UNCOVERING WHAT IS NEXT

Identifying new practices at the leading edge of government, connecting those engaging in new ways of thinking and acting, and considering what these new approaches mean for the public sector.

PROVIDING TRUSTED ADVICE TO FOSTER INNOVATION

Sharing guidance and resources about the ways in which governments can support innovation to obtain better outcomes for their people.



TURNING THE NEW INTO NORMAL

Studying innovation in different public sector contexts and investigating potential frameworks and methods to unleash creativity and innovation and ways to connect them with the day-to-day work of public servants.

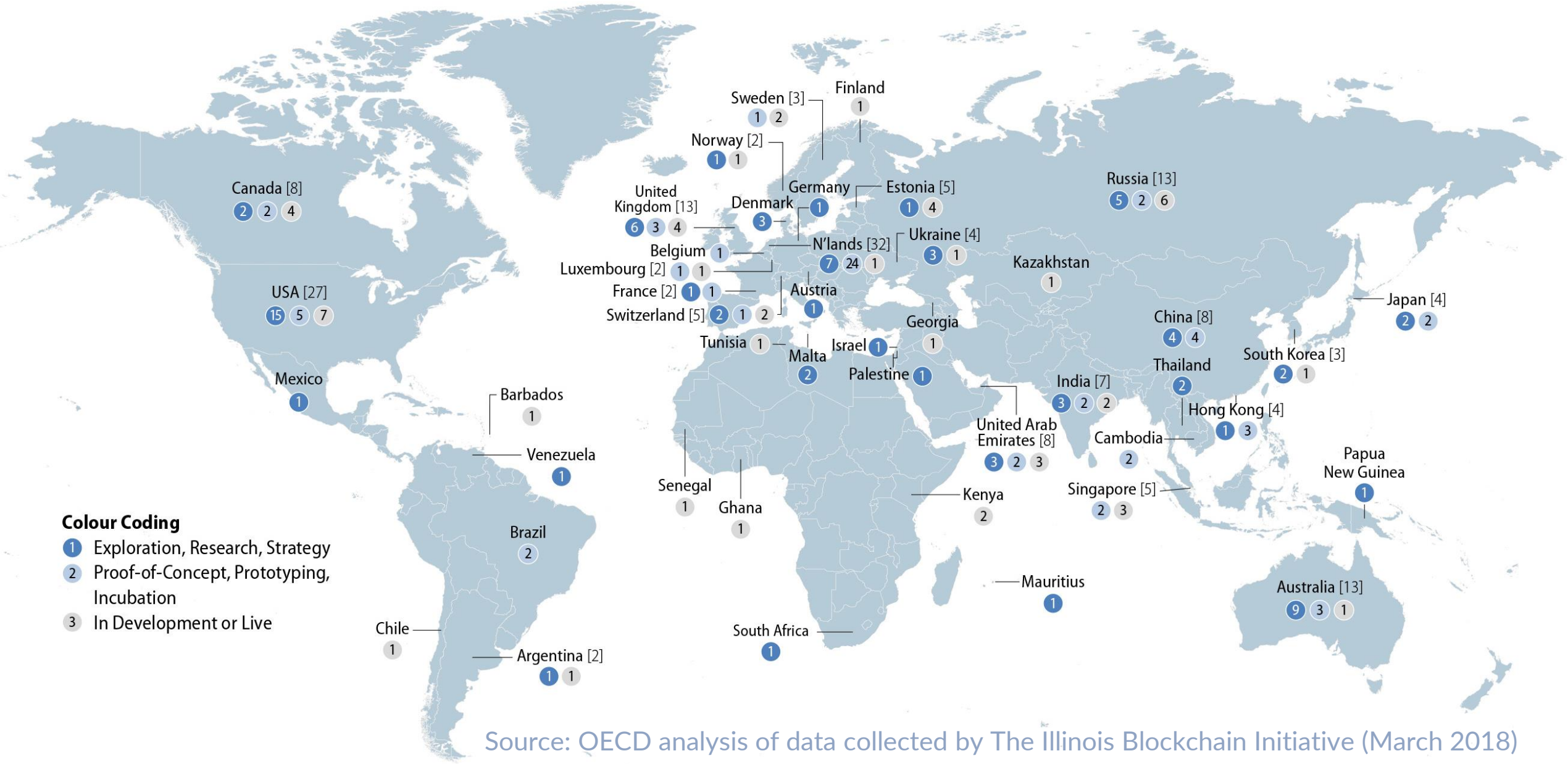
One year ago: 117 Initiatives in 26 Countries

Color coding key

- In progress
- Planned
- Announced

Source: Deloitte analysis in conjunction with the Fletcher School at Tufts University (March 2017)

Now: 203 Blockchain Initiatives in 46 Countries



Source: OECD analysis of data collected by The Illinois Blockchain Initiative (March 2018)

Top 10 types of projects and industries

Rank	Types of projects (count)*	Industries (count)*
1	Strategy/Research (42)	Government Services (174)
2	Identity (Credentials/Licenses/Attestations) (25)	Financial Services (74)
3	Personal Records (Health, Financial, etc.) (25)	Technology & Internet of Things (26)
4	Economic Development (24)	Healthcare (23)
5	Financial Services/Market Infrastructure (20)	Real Estate (22)
6	Land Title Registry (19)	Supply Chain (19)
7	Digital Currency (Central Bank Issued) (19)	Energy (13)
8	Benefits/Entitlements (13)	Transportation (13)
9	Compliance/Reporting (12)	Education (8)
10	Research/Standards (12)	Telecom (4)

Source: OECD analysis of data collected by The Illinois Blockchain Initiative (March 2018)
*Initiatives may be tagged with more than one type of project/industry.

Potential Use Cases

Use Case	Description
Identity	Establishing and maintaining identities for citizens and residents (birth certificates, marriage licenses, visas, death records).
Personal records	Interoperable health records, insurance records, etc.
Land title registry	Details and historic records related to real estate and property transactions.
Supply chain management, inventorying	Tracking an asset from its creation, transportation, purchase, and inventorying.
Benefits, entitlements, and aid	Social security, medical benefits payments, domestic and international aid. Anticipatory/automated payments could be automated through Smart Contracts.
Contract and vendor management	Tracking and paying vendors, managing purchase commitments and transactions, and monitoring schedule performance. Can allow for perfect transparency of government expenditures.
Voting	Enabling new methods of digital voting, ensuring eligibility, accurate counting, and auditing (e.g., to avoid ballot-rigging).
Streamlining interagency processes	Blockchains and smart contracts can automate transaction handling and improve information sharing – allows each agency to better focus on their own mission and tech without as much need to consider others tech.

Communities of Practice &Public-Private Partnerships

Two of the fastest growing best practices

COMMUNITIES OF PRACTICE

Cross-sector communities (public, private, civil society) **learning** about blockchain together and exploring the use and implications of Blockchains in government.

For example, the U.S. **Emerging Citizen Technology Office** (ECTO) has been created to provide a common guidance and vision for emerging tech in the U.S. government and to share ideas and connect innovators. Bring in insights from other sectors.

PUBLIC-PRIVATE PARTNERSHIPS (PPPs)

Efforts to bring public agencies and private firms together in **developing and implementing** Blockchain systems. Often, private firms assist government agencies with the technological aspect of the work.

For example, the **ID2020** initiative (UN agencies, companies such as Microsoft Accenture) seeks to provide formal identities to the 1.1 billion individuals who lack one, including millions of refugees.

Example 1: Vehicle Wallet (Denmark)

Problem:
During a car's lifecycle it undergoes various phases and activities (tests, repair, loan, insurance and changes in ownership). When a car is sold from one person to another, there can be a lack of information from either the buyer or seller. On the seller's side, the car could have undergone an undesirable re-build or even be stolen. On the buyer's side, the buyer could never re-register the car, which could result in continuous taxes for the original seller.

Solution:
Vehicle Wallet is a partnership between payment service provider and the Danish Tax Administration. It is a supply chain management tool where data concerning the car is saved in one distributed ledger and creates one agreed and shared record of the vehicle history as it is transferred across the supply chain. This reduces risks for buyers and sellers, and helps ensure Denmark receives all proper taxes.

Example 2: BenBen (Ghana)

Problem:
For land property, Ghana lacked a systemic way to determining the legal existence of parcels and to track land ownership titles. This prevented authorities and property owners from having clear certainty and visibility over what belongs to whom, resulting in regular disputes. In addition, because previous processes were on paper, it could take over a year to register the sale/purchase of a property, which was a fraud risk for both sellers and buyers.

Solution:
BenBen provides an Ethereum-run digital register system of all land registries across Ghana. It is able to certify land information through the cross-cutting of satellite imagery and on-the-ground verifications, working hand-in-hand with local stakeholders in the land market. It aggregates all the information such that financial institutions and the Lands Commission have real-time access to the data. Property transaction times have been reduced by 75% and court disputes have been reduced.

Example 2: Project Ubin (Singapore)

Problem:
The Monetary Authority of Singapore (MAS) conducted a study that found that Inter-bank payments within Singapore and cross-border financial transactions were inefficient and slow.

Solution:
MAS partnered with R3– a consortium of banks and regulators to create a prototype for a Blockchain-based digital Singaporean dollar to facilitate digital transactions. This would allow for incorruptibility of records through a decentralised trust system, but also 24 hour processing with no centralised – i.e. human-based – checks required. The partnership has successfully developed software prototypes of three different models for decentralised inter-bank payment that are now being explored. MAS has published the source code as open source software on GitHub.

Challenges & Limitations

Blockchain is not a cure-all

01

IMMUTABILITY

A Blockchain is an add-only list. Once data is added, it can't be removed. Perhaps not a good fit when updating/deleting data is a regular occurrence.

02

DATA STORAGE

Databases are often used to store large amounts of data (images, docs, apps, etc.). However, Blockchain is designed for small pockets of data. If data storage is needed, Blockchain may not be a good fit, or a hybrid solution may ne needed.

03

TALKING ABOUT BLOCKCHAIN

The act of explaining blockchain to public officials and civil servants is difficult. De-linking blockchain from Bitcoin and discussing how it can improve efficiency and strengthen mission effectiveness can help.

04

COSTS

Higher short-term costs associated with a still-emerging technology prevent its widespread use for the time being. Blockchain-as-a-service products are starting to be offered that can allow for experimentation.

05

BLOCKERS

People often flag issues such as energy consumption and scalability as Blockchain blockers. However, many of these are irrelevant to government Blockchain implementations.

06

CODING & GOVERNANCE MODELS

Blockchains are known for eliminating the need for central authority, but this is not entirely true. They must be coded and governed by those entrusted with key roles. Governments must build a technical knowledge base to ensure these decisions are made well (even if the actual coding is outsourced).

Innovation in Government: **The New Normal**

20-21 November 2017 - Paris, France - #opsi2017

OPSI


Search ...
English
OPSI
Observatory of
Public Sector Innovation
Innovation
Blog
About Us
3
OPSI
Innovation
Far far away, behind the word mountains, far from the countries Vokalia and Consonantia
Blog
there live the blind texts. Separated they live in Bookmarksgrove
Community
right at the coast of the Semantics, a large language ocean

OPSI | @opsi

2 minutes ago Profile completion 84%

What's new, OPSI?

OPSI wrote a new post, **How can leadership and HR professionals catalyse innovation?** 14 days ago

The case for public sector innovation has been steadily growing for years. Citizens' expectations continue to grow and evolve, and governments need to rethink and re-imagine how they deliver value to citizens. T [...]

Members

Newest | Active | Popular

OPSI
2 minutes ago

Philip McGrath
5 days ago

Jamie Berryhill
11 days ago

Julia Tyszko
19 days ago

Robin Bode
3 months ago

Who's Online

OPSI

Groups

New | Active | Popular | A-Z

OPSI Website User Testing
active 2 weeks ago

OPSI

Observatory of
Public Sector Innovation

Join our newsletter at http://tiny.cc/opsinewsletter

oecd-opsi.org | @OPSIgov | opsi@oecd.org

The e-mail analogy

The status quo: It is a common process to share documents among peers and colleagues through the use of e-mails. This translates in the duplication of the document. There are automatically two copies: the sender's, which is saved on one's personal device or drive, and the e-mail recipient's. This process can be reiterated an infinite number of times – thus the duplication of one document is theoretically never-ending.

The issue: Such a process cannot exclude the possibility that one of these copies, and one of these copies only, be amended and tampered with independently of all others. As amended copies duplicate exponentially, the history of changes becomes ambiguous: which document becomes the correct one? Which one can be relied upon to 'state the truth'?

Types of Blockchains

Blockchain ledgers can be public or private. In a **public network** (such as Bitcoin), anyone can have access, whereas in a **private network** only specific authorised users can participate. This draws an important distinction between *permissionless* (or "public") and *permissioned* (or "private") ledgers.

Permissionless (public) ledgers, such as Bitcoin, "allow anyone to contribute data to the ledger and for everyone in possession of the ledger to have identical copies"

Permissioned ledgers, on the other hand, limit contributions to a restricted set of users who have been given rights. Access to view transactions on permissioned ledgers may also be restricted, or could be public, depending on the ledger's settings. Permissioned ledgers **may be the most applicable types of ledgers for the public sector.**

The bank analogy

The status quo: Digital financial transactions and transfers have become a common and fully accepted aspect of peoples' economic lives. In such contexts, we expect a bank to act as a **trusted third-party to verify and confirm** that:

- The identity of the sender is valid and it is indeed them, and not someone else
- The sender has the necessary funds to make the transfer
- The recipient is indeed the one aimed for, and not someone else.

The issue: This single ledger held by the bank and the bank can ultimately create a single point of failure, whereby hackers may gear cyberattacks to this specific entity – which, if not protected enough, can enable access to sensitive information. The outcome is a rather grave one: the trust placed upon the third party no longer holds and transactions are no longer believed to be secured. In addition, digitally enabled economies require ledgers that can be quickly accessed by multiple people from multiple places. Digital information [today] can be erased, updated or altered without leaving any discernible trace of such activity"

Proof of Work (PoW) Consensus Model

The PoW model—the most common consensus model used, including for the Bitcoin platform—requires that for a mining node to post a block to the Blockchain, they must expend processing resources in order to solve a difficult puzzle. Their accurate solution to the puzzle serves as proof that they conducted the work needed to publish the block. The process to solve the puzzle is intentionally costs money in terms of processing time and electricity, but the process to check that the solution is correct is intentionally very easy.

The PoW model is well suited for permissionless ledgers, which allow anyone to contribute data to the ledger and for everyone in possession of the ledger to have identical copies. Since anyone can contribute, there is a mutual distrust among users. The PoW model helps to ensure that each user has roughly the same likelihood of being able to solve the puzzle, thereby preventing certain users from being able to control which blocks are added to the chain

Proof of Authority Consensus Model

Proof of Authority provides the ability to validate and publish new blocks to the Blockchain for **authorised users, called *validators***. Unlike consensus models like Proof of Work and Proof of Stake, a user's identity must be known and verified. This is critical, as identity is the sole verification of a user's authority to add new blocks to the chain. When compared with models such as Proof of Work, Proof of Authority is a much faster model for processing new blocks, as there is no need for lengthy and resource intensive computer processing.

This consensus model may seem the most familiar to users who have experience working with databases in which only specific authorised users may edit or add data to a database. Thus, it **may be the most applicable for many applications of Blockchain technologies in the public sector**, as it can be adapted to represent the complexity of government review and decision-making processes.