Observatory of
Public Sector Innovation

Blockchain and its Use in the Public Sector

June 20, 2018

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

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

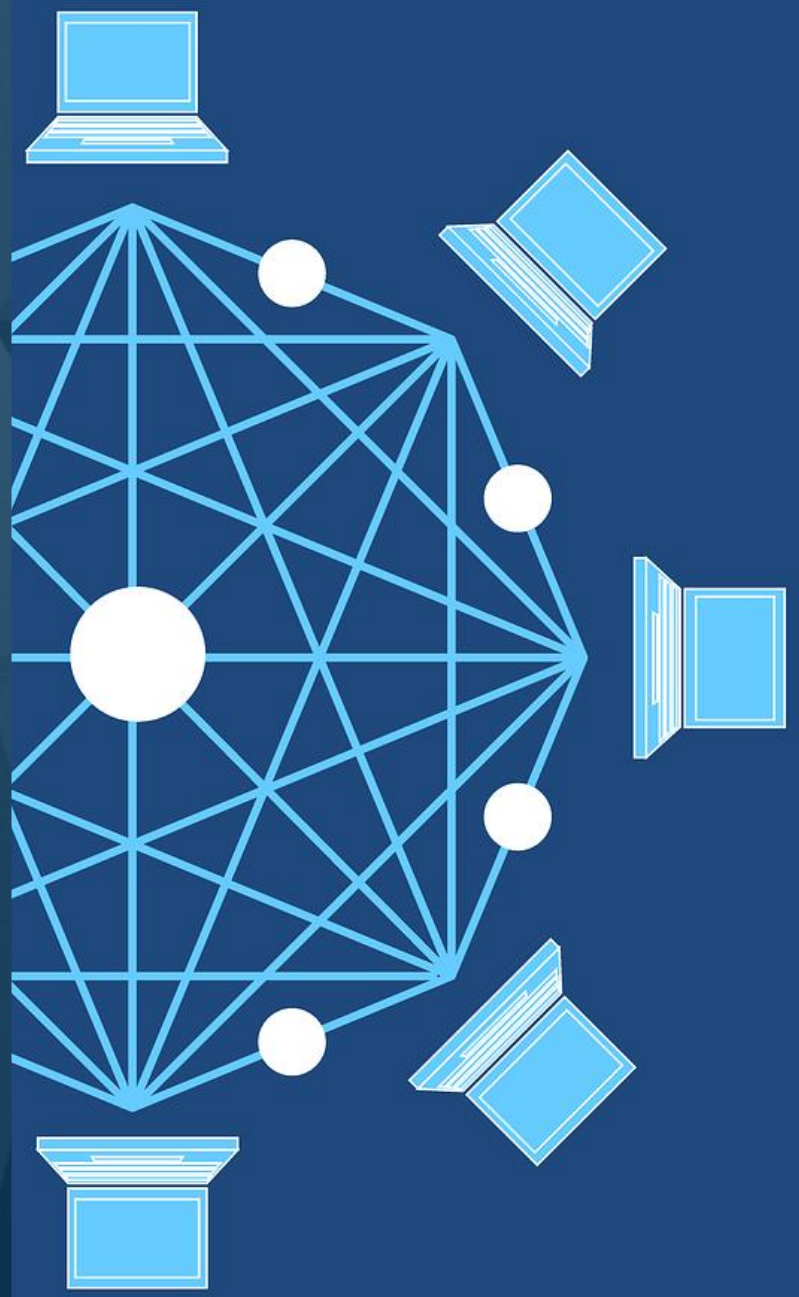
Identifying new practices at the leading edge of government, connecting those engaging in new ways of thinking and acting, and considering what these new approaches mean for the public sector.

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.



Blockchains Unchained Guide

Many public servants have come to OPSI about how blockchain fits within government.

Because of blockchain's complexity and its association with Bitcoin, it can be confusing to look past the hype and understand the potential uses and implications it can have in the public sector.

To help address this, OPSI created the Blockchains Unchained (http://oe.cd/blockchain) guide to:

- Explain simply what blockchain is and isn't
- Make the case for public servants to build knowledge and capacity around blockchain
- Make sense of blockchain's potential impacts in government
- Explore existing public sector use of blockchain

Blockchain Basics

OPSI

Types of Problems Blockchain Can Solve

Two analogies…

E-MAIL

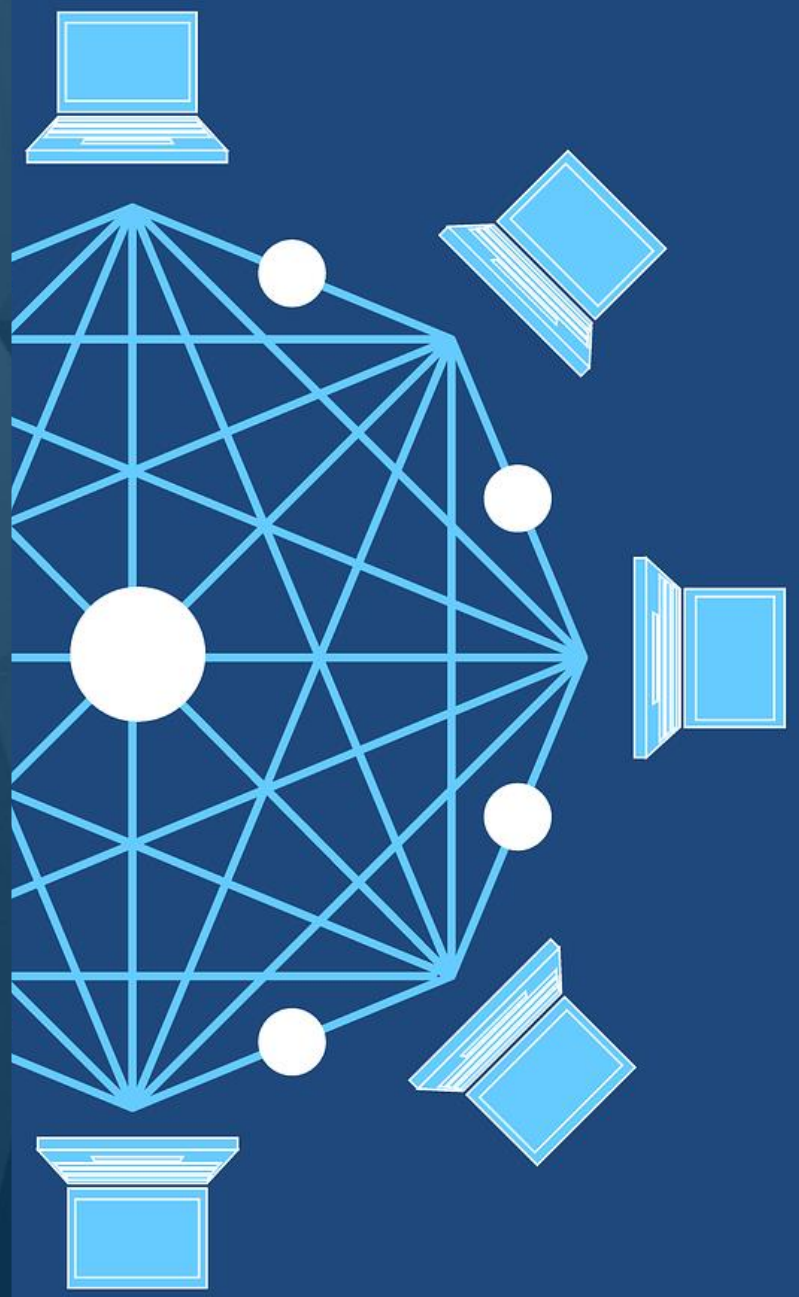
It is common to share documents in e-mails among colleagues and peers, resulting in repeated duplication of the document. The duplication can be theoretically never-ending.

It is possible that **one could be amended and tampered** with independently of all others. As amended copies duplicate, the history of changes becomes ambiguous: which document becomes the correct one? **Which one can be relied upon to 'state the truth'?**

BANK

Digital payments been become a part of daily life. We expect a bank to act as a trusted third-party to verify that user identities are known, that the sender has the necessary funds, and the funds are transferred to the correct person.

The central ledger held by the bank becomes a **single point of failure** (e.g., target for hacking). The potential exists for accessing and **altering the data** without a trace.



Blockchains Unchained Guide

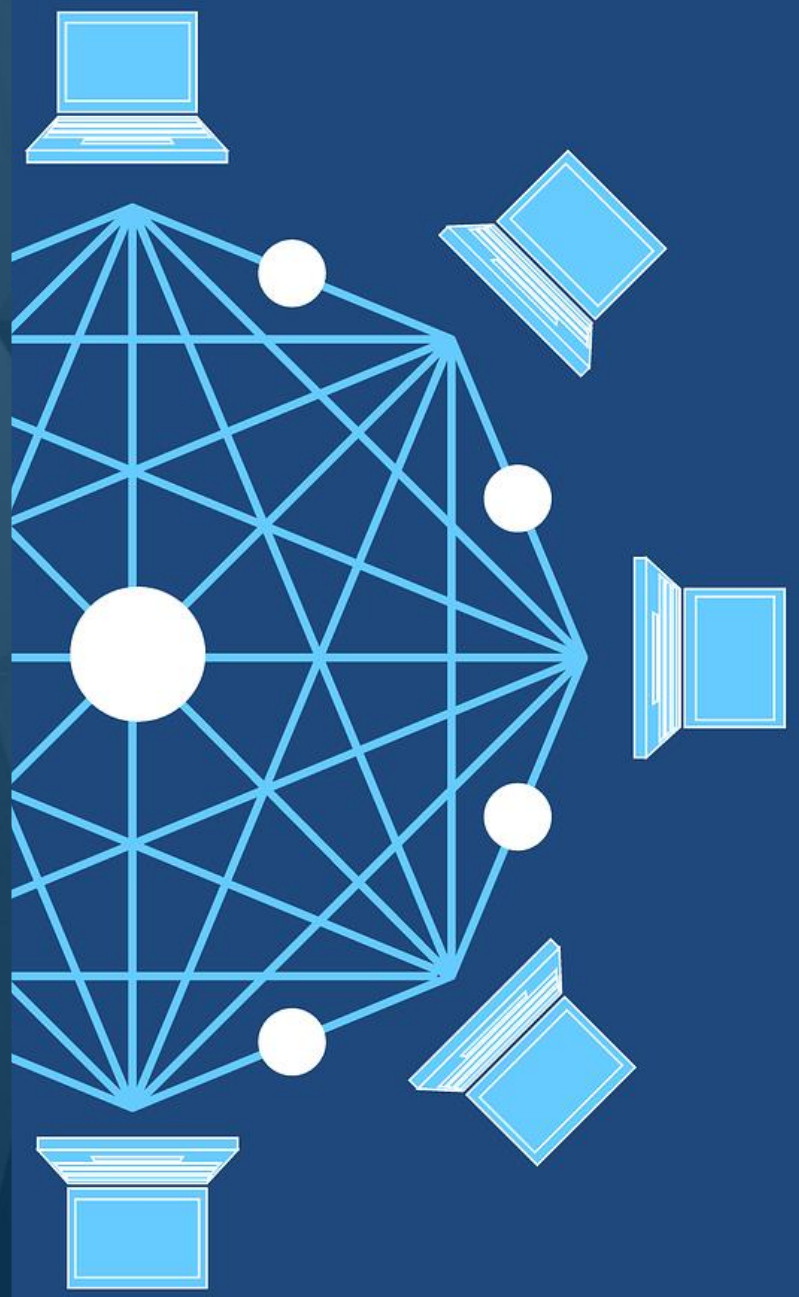
The basic and inter-related goals of blockchain are to:

- Reduce or **eliminate the need for a central authority** (e.g., banks, government)
- Eliminate **central points of failure**
- **Enable trust** among people who don't know each other to directly conduct transactions

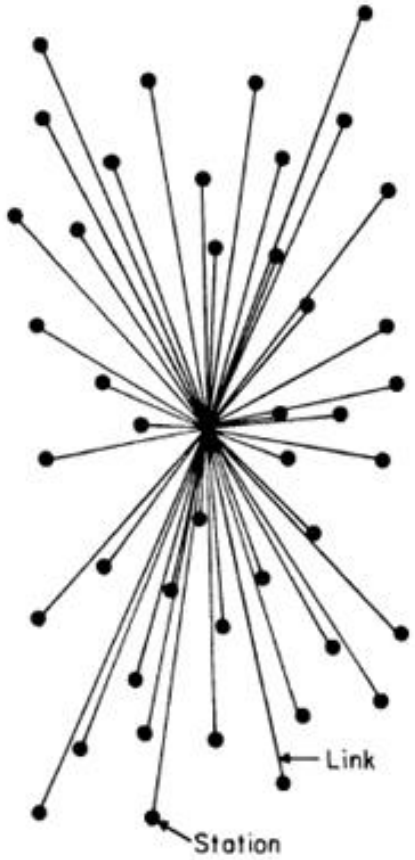
To achieve this, instead of an authority running a central database, every user can have a copy of the full database and can see every transaction that has ever taken place. This is a **distributed ledger.**

Key term: Distributed Ledger
A List of transactions that are spread across many users (not central)

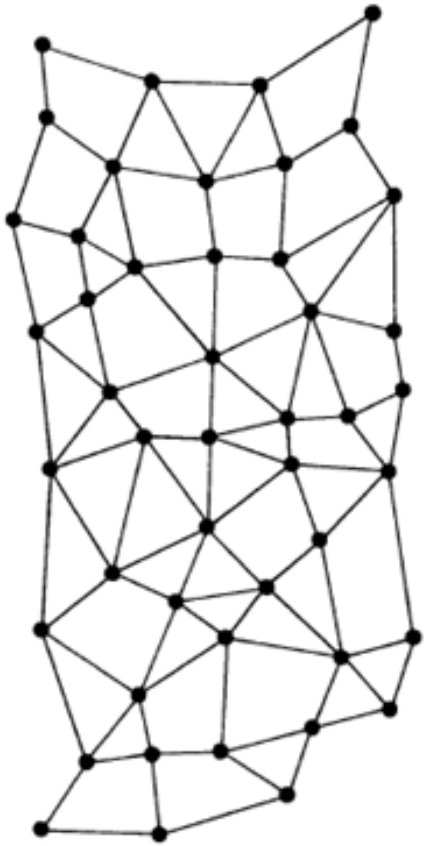
Key term: Node
Another word for a user on a blockchain network running blockchain software and holding a copy of the ledger



Centralized vs. Distributed

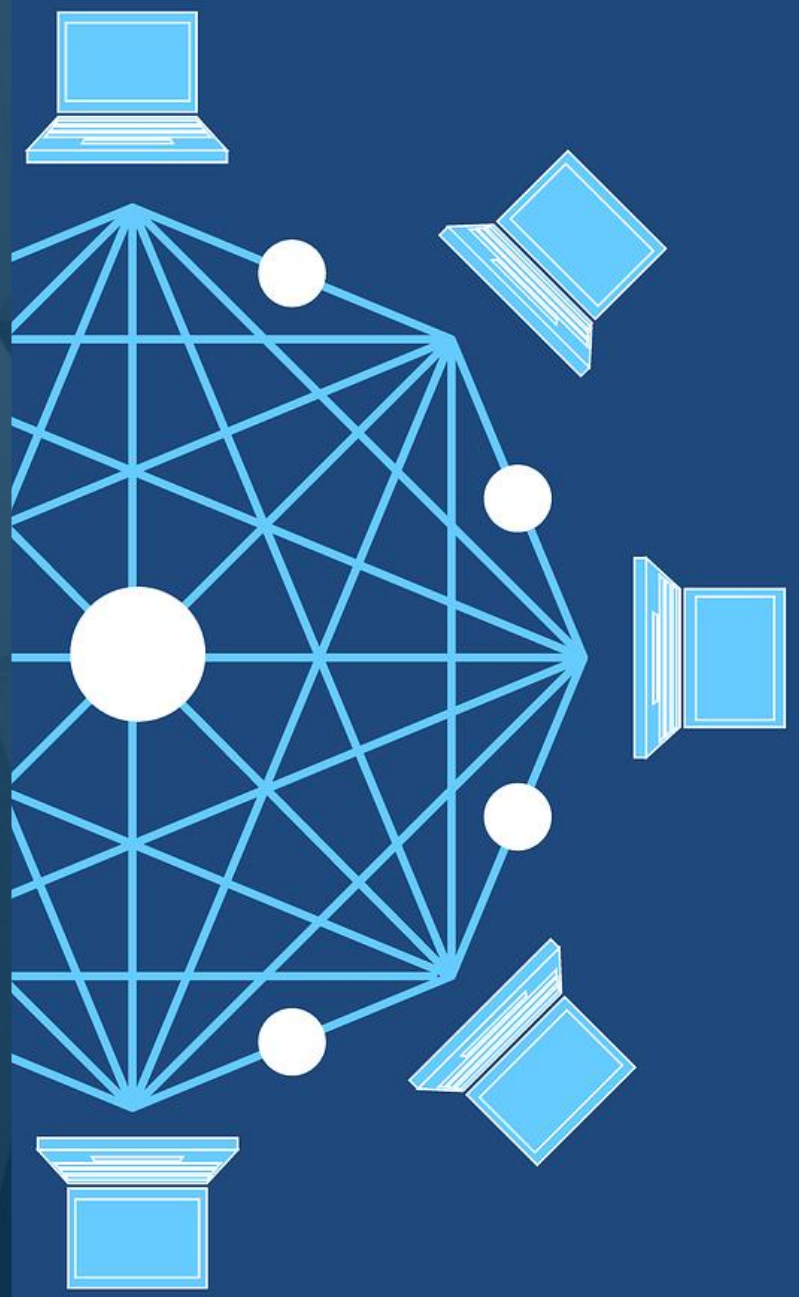


CENTRALIZED



DISTRIBUTED

Source: Baran, Paul, 1964, “On Distributed Communications: Introduction to Distributed Communications Networks”, United States Air Force Project Rand

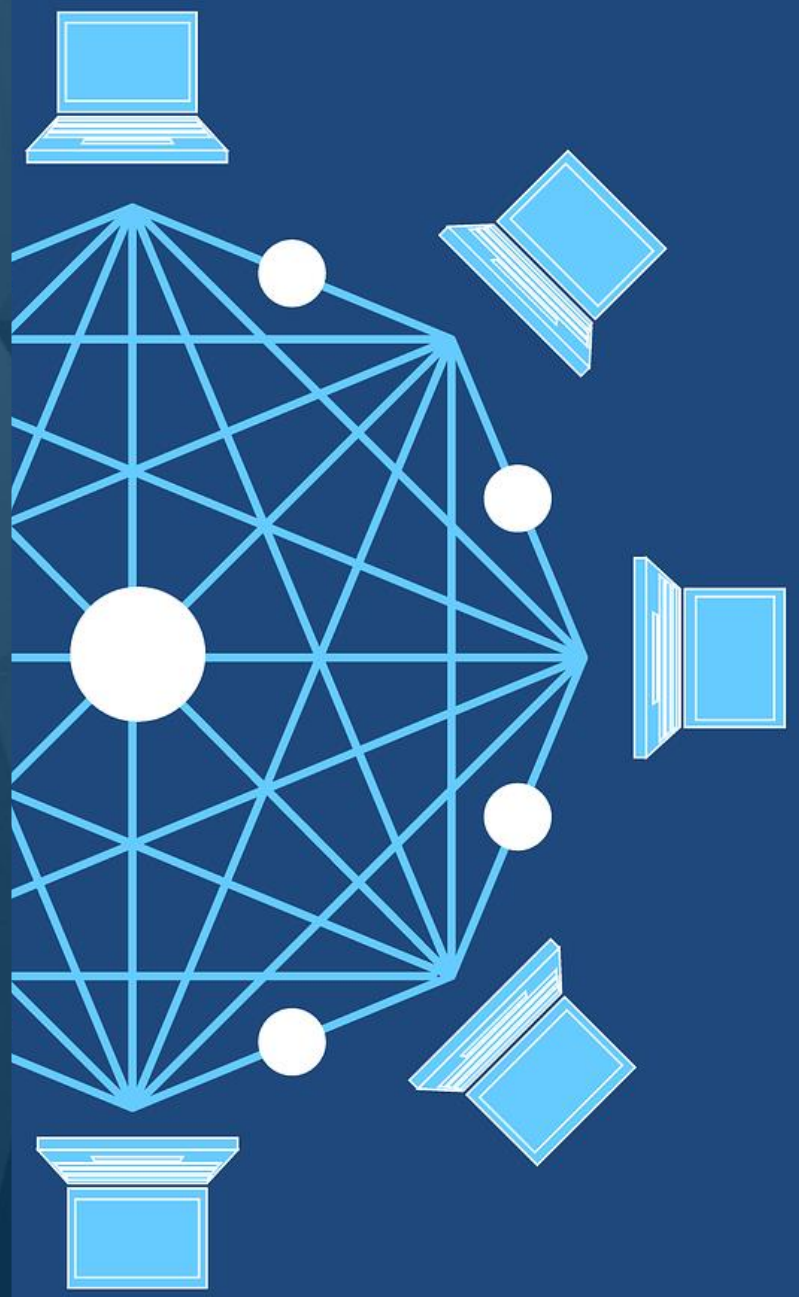


Validating Transactions

Ok, so everyone can have a copy of the ledger and see all of the transactions. **But how can they be sure these transactions are valid?**

- To submit a transaction, a user must digitally sign it using a "cryptographic **key**".
- When a user submits a transaction, it propagates throughout the network in seconds or minutes. **Every node checks** to ensure the transaction is feasible and was properly signed. If yes, they continue to propagate, if not, they discard the transaction.
  - If **more than 50%** agree that is it valid, it is considered a valid transaction.
  - *But… these are not part of the blockchain yet.*

Key term: Cryptographic Key
Old decryption technology. All users have a "public key" and a ***linked*** "private key". The public key is widely known. The private key must never be shared. A user signs their transactions with the private key, and then **all users can verify** that it was truly the right person by checking it against their public key.



Mining Transactions

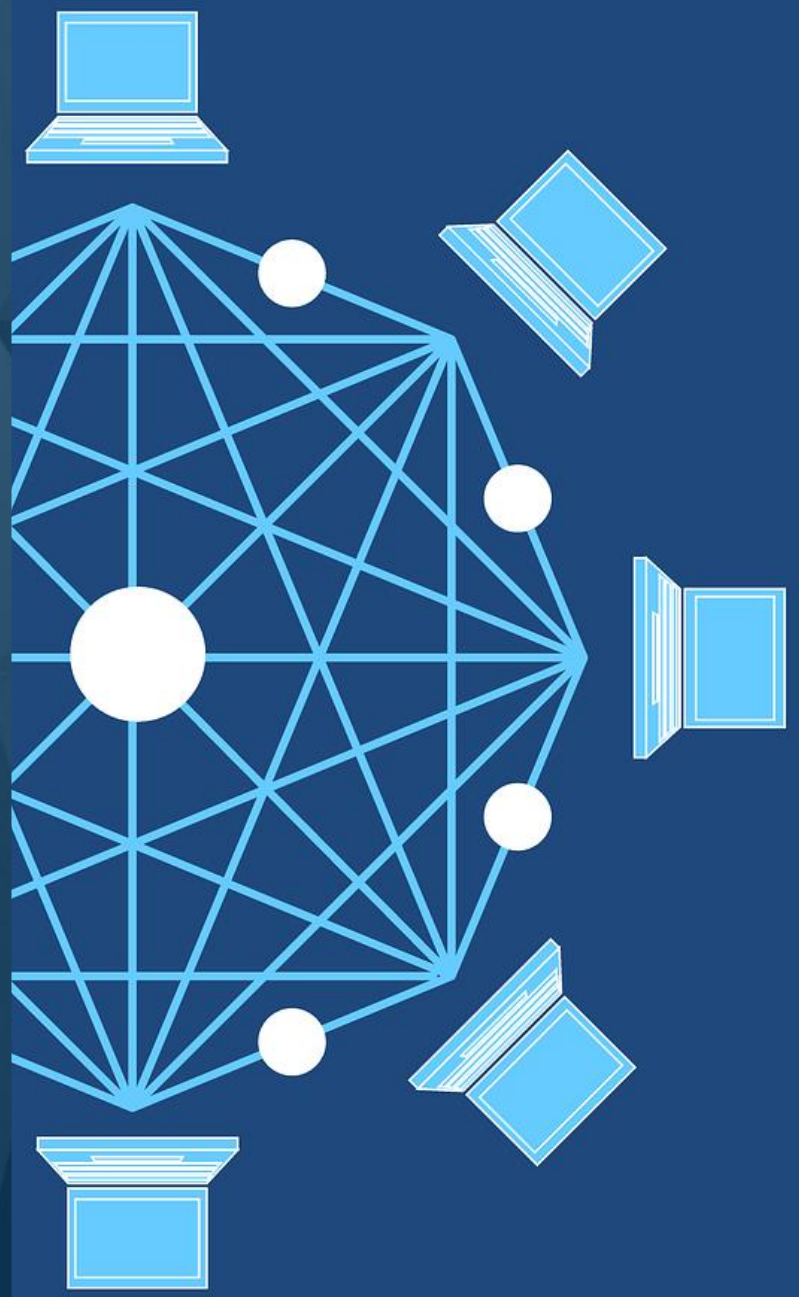
After transactions are validated, they wait in a queue until they are "mined" by a "mining node".

- A mining node will **validate a set of transactions** from the queue and group them into a "block".
- The mining node then **publishes the block** to the chain and begins to broadcast the new block across the network.
- The mining node discards any invalid transactions

Although this is complex, it is all done automatically with blockchain software.

Key term: Mining

The act of again validating a group of transactions from the queue and publishing them as new block to a chain. The agreed-upon "consensus model" (a very complicated concept to be explained shortly) for the blockchain determines who can do this. Sometimes it's competitive. Sometimes it's based on user permissions.



“Immutability”

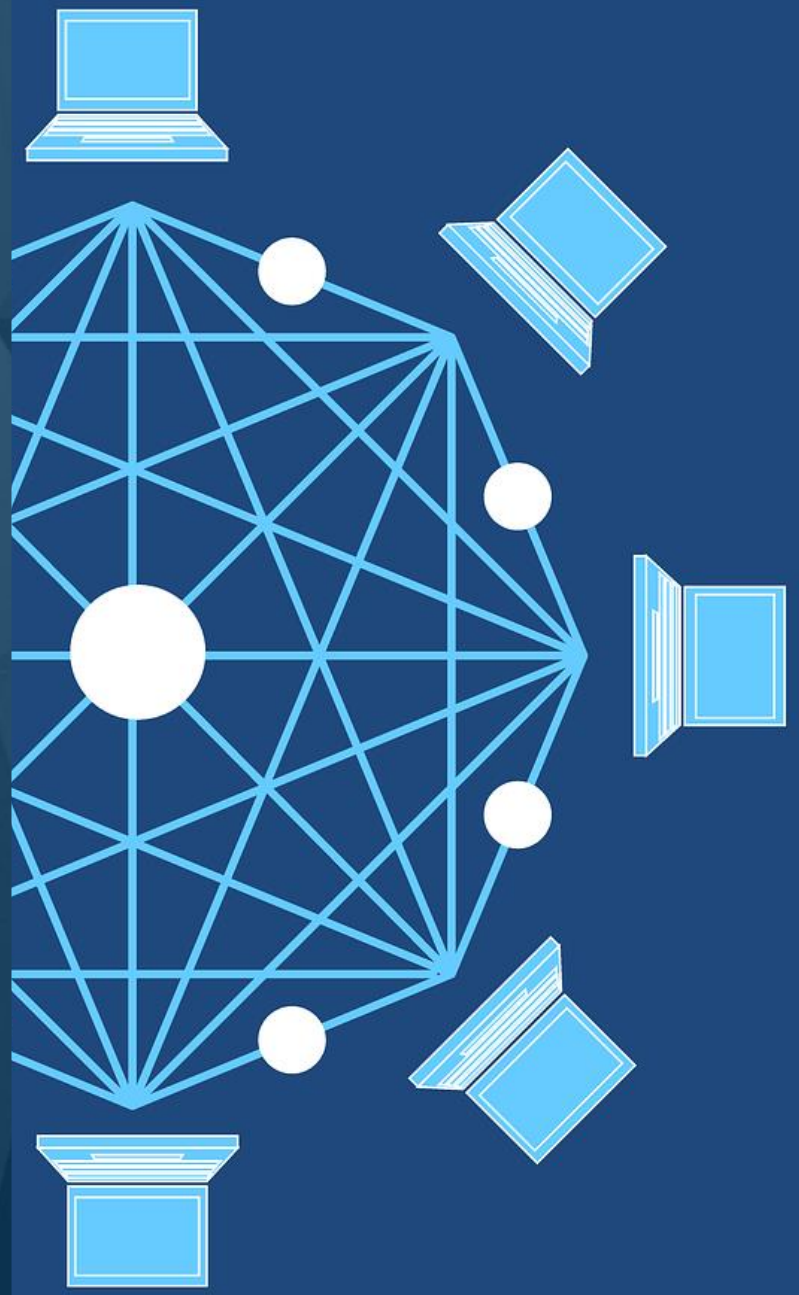
In addition to they key principles of:

1. Distributed: everyone holding a copy of the ledger and these copies are automatically synchronised
2. Shared: all transactions being transparent to everyone

There is a key third principle: ***Immutability***

Key term: Immutability
Once data has been written to a Blockchain, no one, not even a system administrator, can change it. This helps to ensure trustworthiness.

Immutability is a result of how blockchain technology is designed.



How Blockchains are Designed

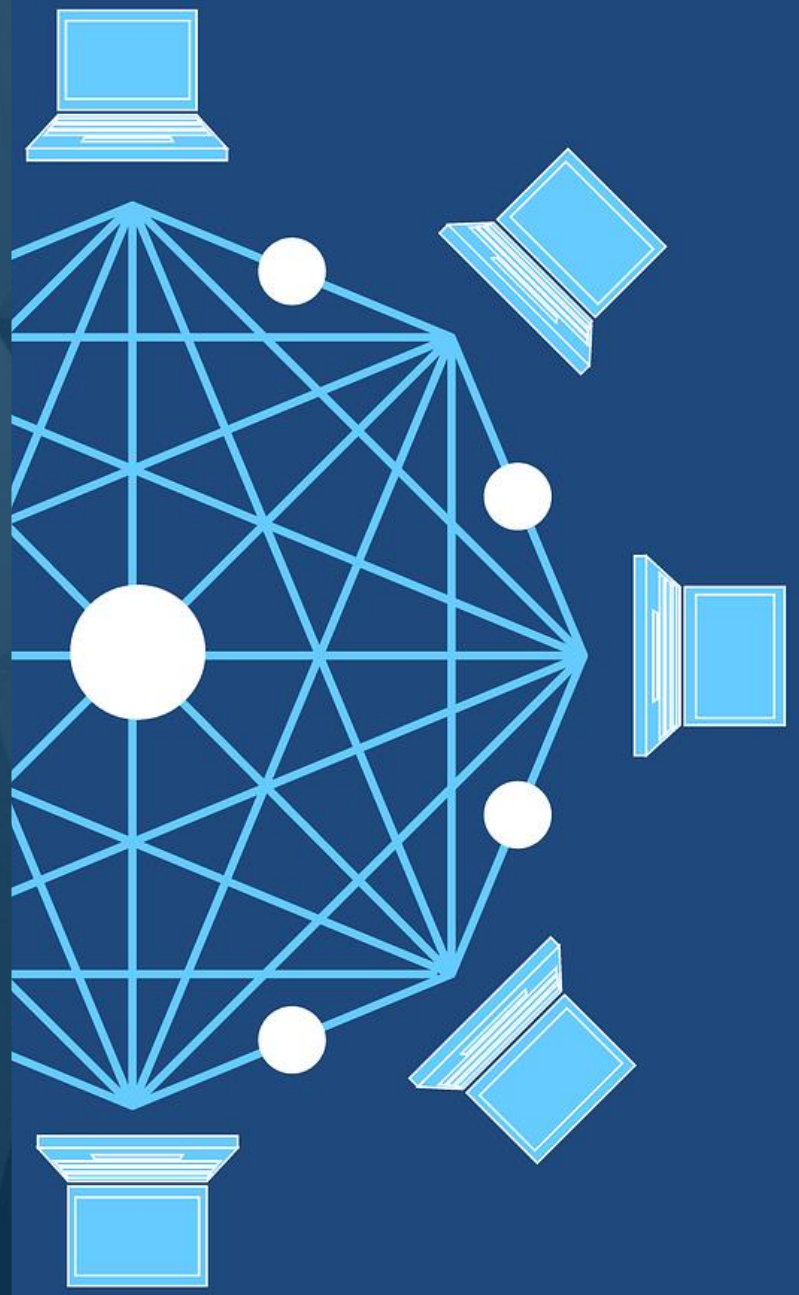
A “blockchain” is literally a chain of blocks

- As discussed, each block contains a group of validated transactions.
- These blocks are added one-by-one to the chain in a **linear, chronological** manner.
- *Critically*, every block is ***inextricably linked*** to the previous blockchain using a process called “**hashing**”.
- Each block’s contents are “hashed”, and each block gets a unique “hash code”, which ***links blocks together***

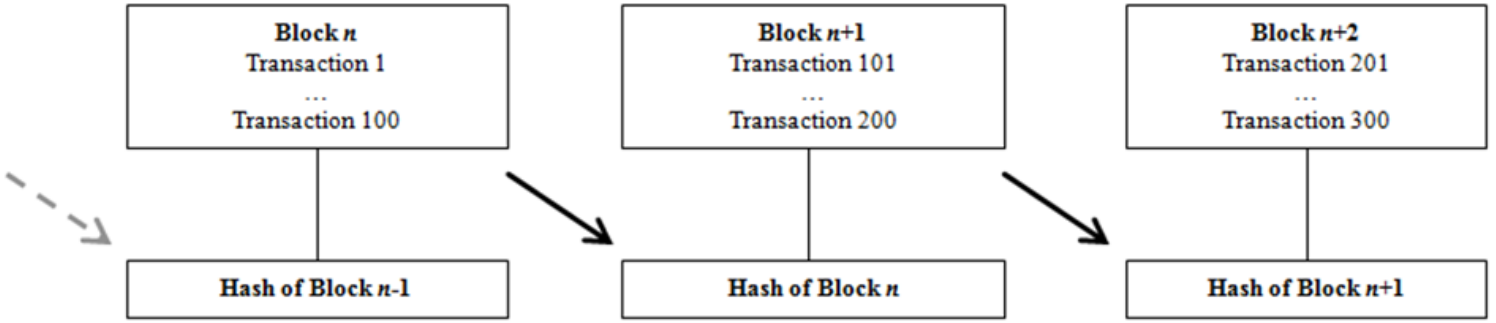
Key term: Hashing

An encryption function that converts any input (text, image, etc.) into a fixed-length code. The same input will always result in the same code. However, even the most minor change will entirely change the code.

Input	Hash
OPSI	6057121102B54E7210E021645C5305F4DD3F154ECAF8CE6DA69AED5FE4317428
OPSi	E23F99DF38E5A29119853DBACB40ED647CF7F9D6FA3850A76EF170AC11E46732

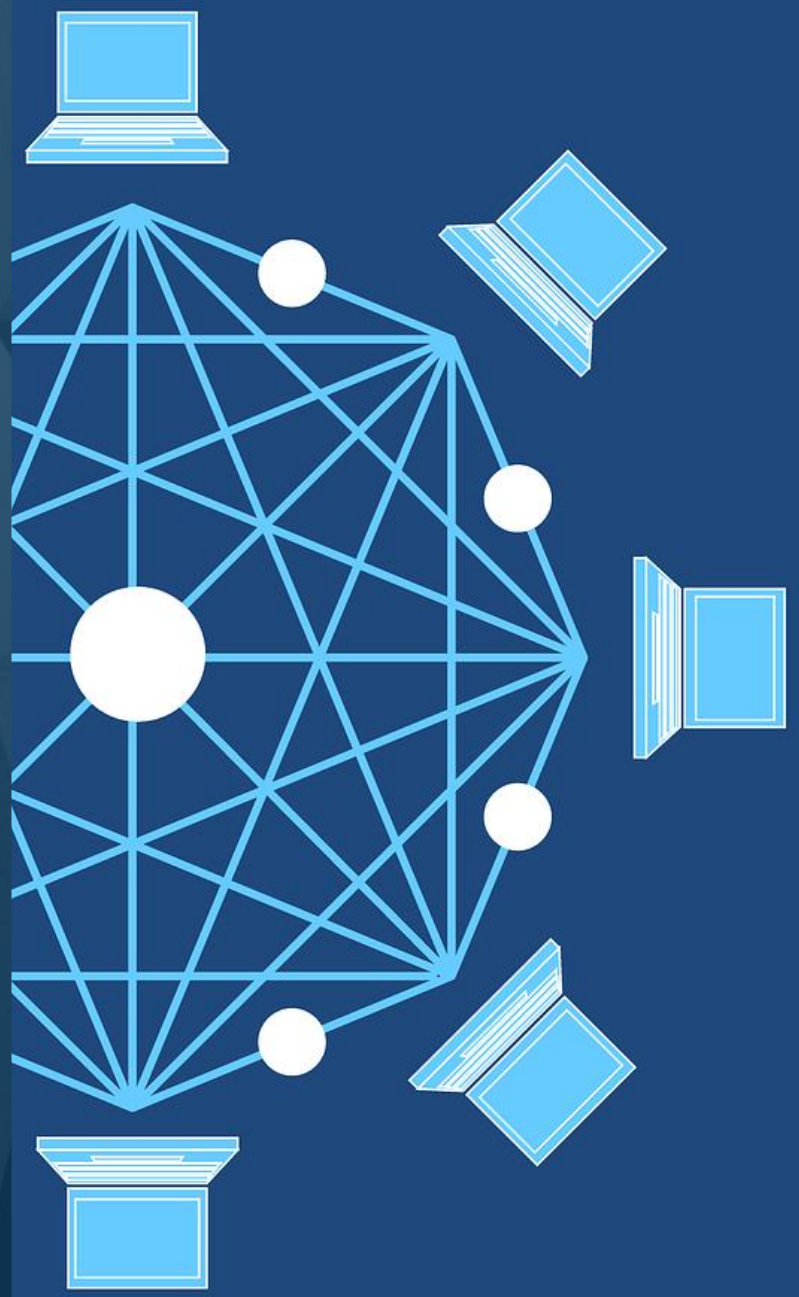


Linking of Blocks



If anyone tried to alter even the smallest piece of a transaction, it would **completely change** the hash code for the transaction and the block. This would cause **cascading effects** for all of the connected blocks.

This would **immediately be noticed** by the nodes and discarded.



Difference Between Blockchain and Bitcoin

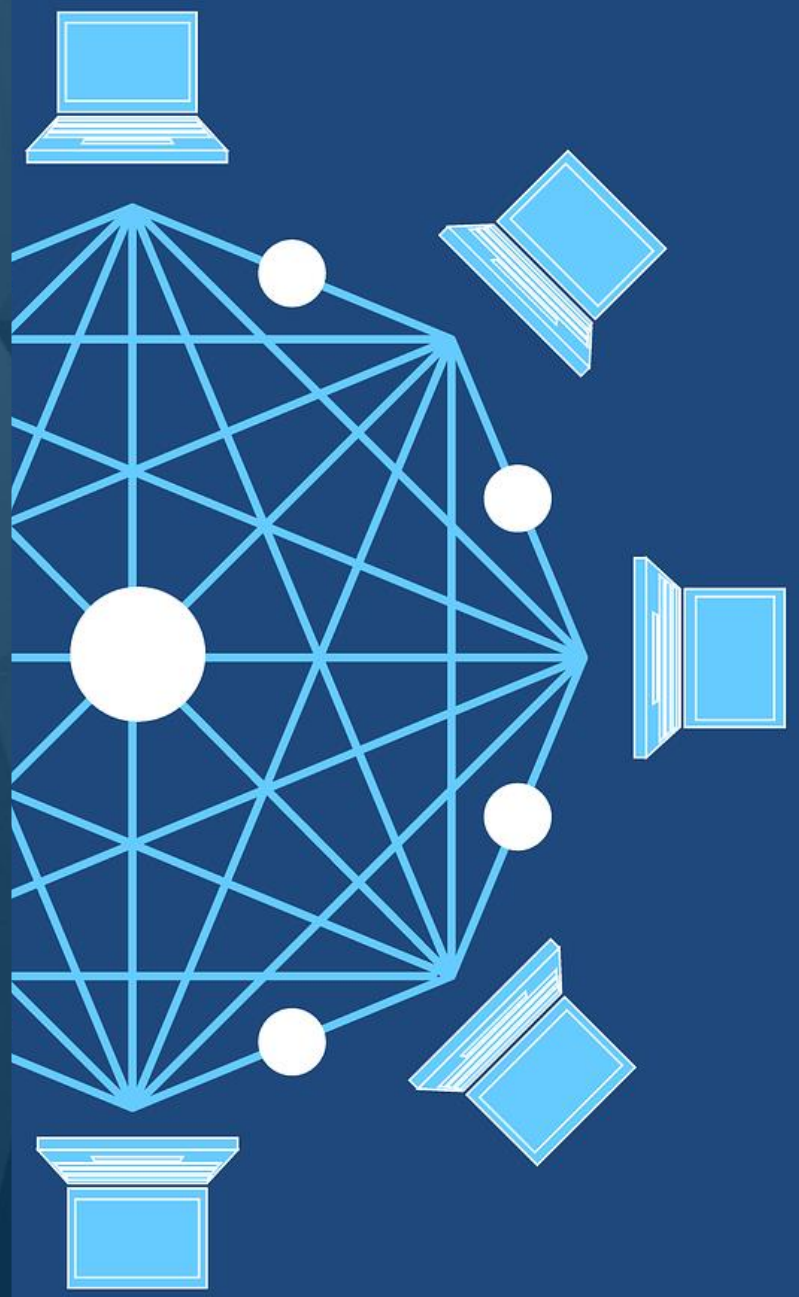
One of the biggest challenges for blockchain is that it is **conflated with Bitcoin**.

- Blockchain was born with Bitcoin and remains the largest blockchain *platform*
- However, hundreds or **thousands of other platforms** now exist
- The underlying technology has uses and implications that go **far beyond Bitcoin** or cryptocurrencies in general

Some platforms have developed innovative new features. Most notably, "**smart contracts**"

Key term: Smart Contracts
Self-executing contracts where the terms are written directly in software code on the blockchain.

Each smart contract is an automated "if/then" scenario that executed when a specific trigger occurs.



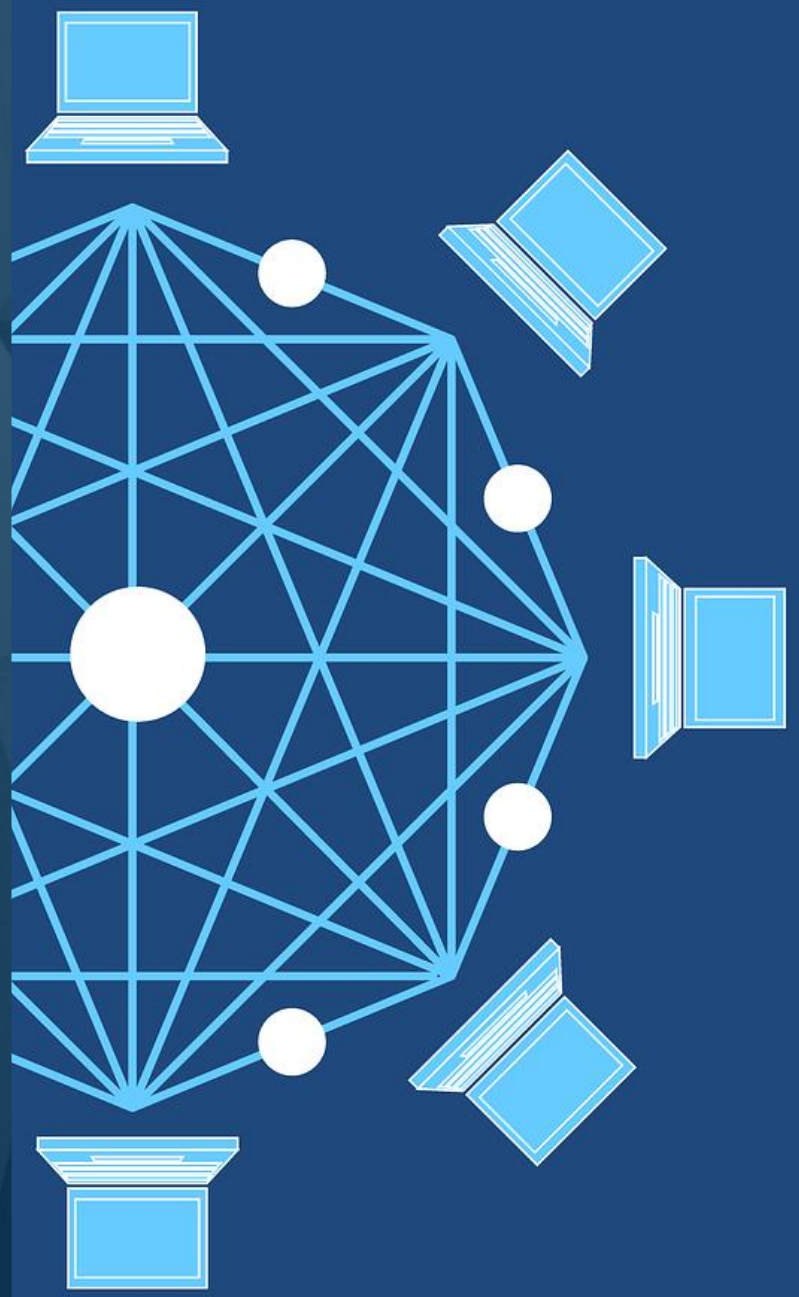
Public versus Private Blockchains

Blockchain ledgers can be public ("permissionless"), or private ("permissioned"). The distinction between the two is much like the *internet* versus an *intranet*.

- **Permissionless ledgers** (e.g., Bitcoin) allow anyone to make transactions and to hold identical copies of the full ledger.

- **Permissioned ledgers** limit contributions to a limited set of users who have been given permission. Access to view records can be restricted or public, depending on the settings of the ledger. In fact, many different aspects of the blockchain can be customized to meet different needs. **These are likely to be the most useful for public sector use.**

The types of "**consensus models**", which are the rules that determine who has the right to publish the next block, vary depending on type of blockchain at hand.



Consensus Models

There are a growing number of consensus models that determine **which node has the right to publish the next block**. The two below are examples.

Proof of Work – Always for permissionless ledgers (e.g., Bitcoin)

- Since no trust exists, in order to keep one or a few users from taking control, a complicated process exists to help even the playing field.
- Each user competes to solve a puzzle that is intentionally resource intensive (e.g., processing power, and by extension, electricity) to solve.
- The winner publishes the next block and earns financial reward.

Proof of Authority – Usually for permissioned ledgers

- User identities must be known and verified.
- Ability to publish new blocks is dictated by user permissions (not unlike a traditional database).
- No issues related to processing power or electricity.

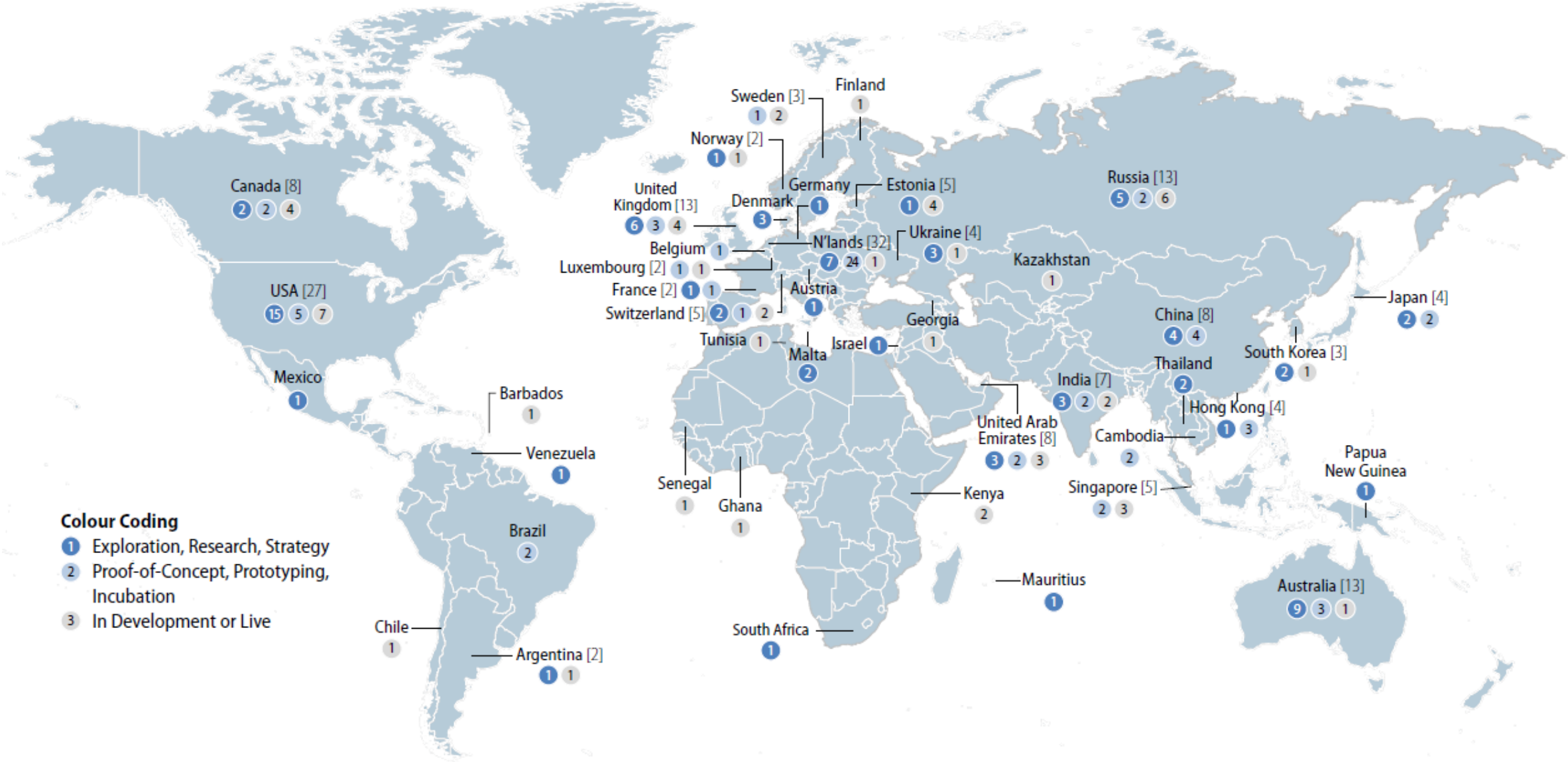
Blockchain in the Public Sector

OPSI

One year ago: 117 Initiatives in 26 Countries

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

Now: 202 Blockchain Initiatives in 45 Countries



OPSI

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

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.

Top 10 types of projects

Rank	Types of projects (count)*
1	Strategy/Research (42)
2	Identity (Credentials/Licenses/Attestations) (25)
3	Personal Records (Health, Financial, etc.) (25)
4	Economic Development (24)
5	Financial Services/Market Infrastructure (20)
6	Land Title Registry (19)
7	Digital Currency (Central Bank Issued) (18)
8	Benefits/Entitlements (13)
9	Compliance/Reporting (12)
10	Research/Standards (12)

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

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. 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 (i.e., only apply to Proof of Work consensus on permissionless/pubic blockchains).

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).

Observatory of
Public Sector Innovation

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

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