A Practical Guide to Using Blockchain within the United Nations
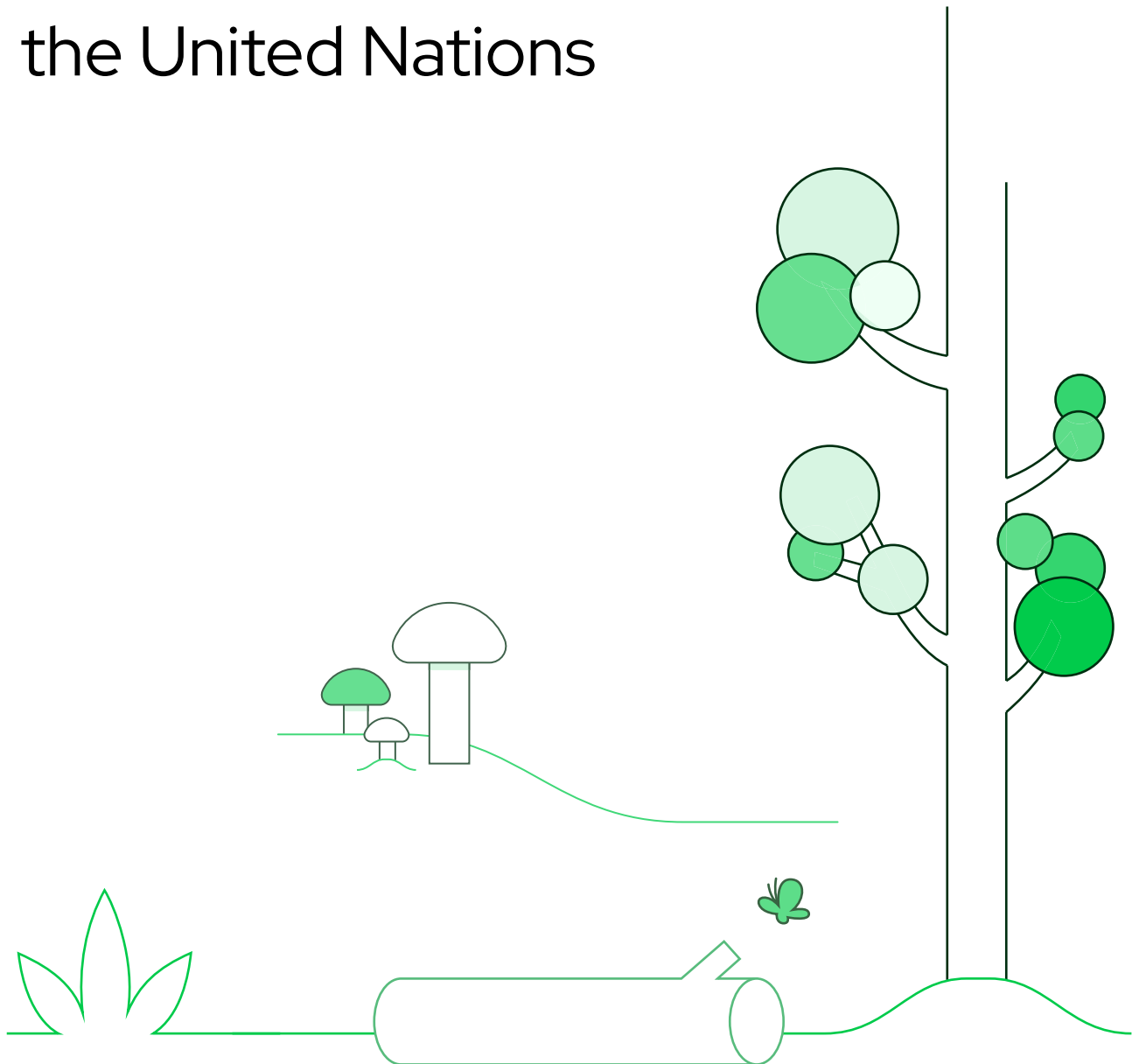
Table of Contents

The UN Innovation Network is pleased to offer an accompanying online tool, The Atrium, to the UN community. Visit: www.atrium.uninnovation.network

Preface

This Practical Guide looks to give a basic understanding of blockchain and general guidance on how to determine if blockchain could help solve a particular problem. This guide does not include all details related to the functioning of the technology but is meant to serve as starting point to evaluate blockchain use cases and introduces ways in which the UN is approaching these technologies in a systematic way.

Why are there plants and fungi throughout the paper?

In many forests, fungi and mycelium are vast underground networks that are critical to plants' survival but are often never seen. We scattered this as a metaphor for blockchain networks because we think that some of the same attributes are shared between fungi and mycelial networks, and blockchain as a technology. Both networks do not exist for just one purpose but serve many different opportunities. They are both decentralised, lacking a single point of authority and rather work to balance out the environment around them. Like how fungi networks allow for the exchange of information, blockchains operate as a network of computers which work together to maintain information securely, without central coordination.

Join the UN blockchain community online at www.uninnovation.network/blockchain or follow us on Twitter at @UN_Innovation.

If you have questions related to this guide, please reach out to blockchain@uninnovation.network or on Twitter at
Chris Fabian @hichrisfabian
Christina Lomazzo @crlomazzo
Mehran Hydary @mehranhydary
Ariana Fowler @arianasfowler
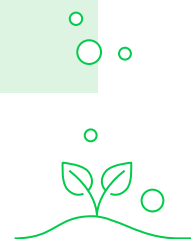
1. Introduction to blockchain

1.1 What is blockchain

Blockchain is a type of software made up of records of digital transactions that are grouped together into "blocks" of information and shared securely across computers on a shared network. When a new block is added, it is connected or "chained" to the previous block, making it difficult to change past information. All computers on the shared network retain a complete record of transactions as they occur, representing the entire blockchain. These computers are called nodes. Transactions submitted to a blockchain can only be added and previous data cannot be removed or modified.[i]
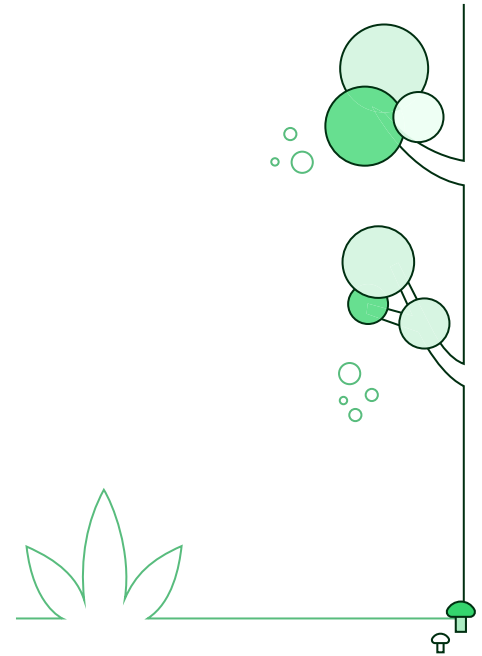
Blockchain is often **incorrectly used interchangeably** with Bitcoin. While Bitcoin was the **first use** of blockchain, it is only one application of **how** the ledger can be used to store information.

How blockchains work
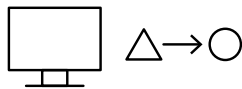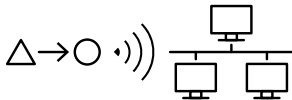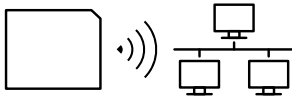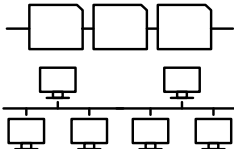
1	Transaction is submitted to a blockchain		Transactions are constantly being sent to the network by users.
2	Network receives the transaction		The transactions are received by computers who verify that the transactions are valid.
3	New block created and propagated		One computer then packages the transactions into the next block and sends it out to the network.
4	Blockchain updated and transaction completed		The newest block is added to the chain of blocks, and the transactions are confirmed.

Diagram 1

Blockchain is a form of Distributed Ledger Technology (DLT). While this guide focuses on blockchain, some of the content can apply more broadly. Different configurations of blockchains are possible, including whether the information will be viewable by all (e.g. in a public blockchain), and who can maintain and update the information.[ii]

Main functions

Blockchains perform three main functions: they store information, track the exchange of value, and can digitise and automate rules through smart contracts. Traditionally, databases are used to store information and are centrally hosted and managed. Blockchains can store vast amounts of information in multiple places all governed by a predetermined set of rules. Like accountants using ledgers to maintain the debits and credits of an account, a blockchain maintains the balances and the transfer of value between accounts.

Finally, similar to programming a bank account to automatically pay rent on the first of each month, smart contracts can be created to automatically perform a function if certain criteria are met. Smart contracts are code that can automatically execute actions.

Blockchain, a modernized ledger? A ledger is a book of records traditionally kept by an accountant which has debits (withdrawals) and credits (deposits). Ledgers are typically used by banks to maintain a record of balances and by business to keep track of transactions; however, they are centrally managed and not transparent to everyone. If the ledger is lost, stolen or damaged, this could be problematic for maintaining the information. A public blockchain is a digital ledger which is maintained by thousands of computers around the world, rather than a central intermediary such as a bank or accountant and is viewable by anyone at any time.[ii]

1.2 Key features of blockchain

Trust

Blockchains have a decentralised architecture and governance structure, meaning there is no one entity that is solely responsible for the state of the ledger and can make changes. A predetermined set of rules dictate which transactions are valid, and how new information is added to the ledger. Because there is no one owner of the system, and all rules are pre-defined, this creates a level of trust between unknown parties.

Security

Blockchains duplicate the same information across all its nodes, which in some cases are in the thousands and are distributed geographically. This creates a redundancy of information, which is beneficial in the case of a network outage in a region or a malicious attack on the network. Cryptography is used to secure communications between parties, so that anything that is intercepted is not comprehensible unless sent to an intended recipient with appropriate permissions. Cryptography can also act as a way of authenticating whether communications are in fact from a specific individual or organisation.[vi]

Immutability

Information on a blockchain cannot be changed once added to the ledger, making it append-only. Because transactions are batched into blocks which are then cryptographically linked together, information in past blocks cannot be changed. Because information is immutable this makes blockchain ideal for record keeping or when needing to create a single source of truth between multiple parties.

Transparency

Transactions published to a public blockchain are viewable by anyone at any time. All records are accessible through a web-based browser and can be validated. Blockchains create a new level of transparency of information, increasing accountability and reducing the need for third-party verification or audits.

Coordination

Because blockchains create a common set of information across multiple parties, this reduces the need for reconciliation and can expedite the processing of certain actions by using smart contracts that automatically execute if the predetermined conditions are met. In the case of cryptocurrencies, the transfer of value can take place around the world without the need for all traditional intermediaries.

1.3 Where blockchain can help

Blockchain has three primary use cases: record keeping, transfer of value and automated logic, increasing from the most basic application to the most complex.

1.3.1 Immutable record keeping

As its most basic function, a blockchain serves as an immutable ledger, meaning that once information has been verified and committed to the system, it cannot be edited or deleted – creating a permanent record. Because of the construct of blockchains, different parties can access the same information seamlessly, breaking down data silos that often plague organisations – particularly those with multiple agencies, partners, vendors, etc. When designed properly, blockchain can facilitate data sharing across partners that may not trust each other or may not be able to use a common centralised database.

Examples of where blockchain can be used for immutable record keeping could be for digital certificates of educational credentials, digital ownership of physical assets such as land titles, digital medical records such as vaccinations, beneficiary entitlement tracking or supply-chain tracking such as with precious metals.[vii, viii]

1.3.2 Transfer of value

Another benefit of blockchain technology is the frictionless movement of value that can occur by leveraging the ledger of blockchain to record the transfer of an asset. By utilising blockchain, third-party processors and clearinghouses play a lesser role, reducing transaction costs and the time delay that typically occurs when moving value between parties.

Systems that use blockchain to record and move financial value are often known as cryptocurrencies – with common examples being bitcoin and ether. In these two cases, the blockchain stores records of "Amount, From, To, Date" in a cryptographically secure, distributed ledger.

Other examples of where blockchain can be used to transfer value within an ecosystem could be for intellectual property rights when a patent is transferred, to record the transfer of value in a closed loop solar energy ecosystem for payment of services, or the transfer of asset ownership, such as property between individuals or organisations.[ix]

1.3.3 Automated rules, smart contracts

Smart contracts are a feature within certain blockchains which automate logic. Smart contracts can be used in the context of an organisation to streamline and expedite administrative processes. Smart contracts use an information source, called an oracle, to determine if conditions have been triggered, and as a result, generate a new transaction which is added to the ledger. Despite the name, smart contracts are not legally binding, therefore doing so usually requires traditional paperwork to accompany the digitised rules.

Smart contracts can be used in the organisational context as it relates to processes such as official sign offs, vendor payments, insurance claim payouts, financial asset trading, triggering dispute resolution, and asset transfer.[x]

One common problem when exploring the possibility of using blockchain is not fully understanding blockchain's key characteristics, in order to evaluate if they can help solve the problem at hand. Reference Appendix I to understand some of the key differentiators between databases and blockchain.
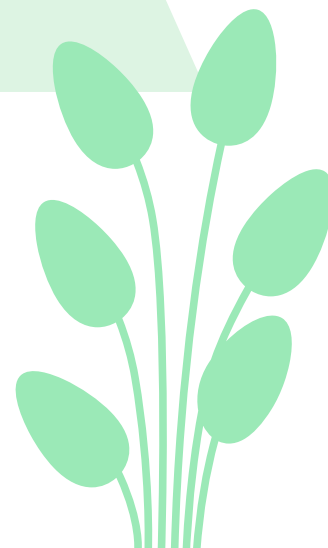
2. The road to blockchain

2.1 Determining if blockchain is the right fit

Before exploring whether blockchain is the right technology, have a clear understanding of the problem you are trying to solve and the goals you are trying to achieve. The problem should be approached from a user's perspective and the ecosystem components should be evaluated (users, community, infrastructure, financing, and technology).[xi] During the phase of problem definition and goal setting, the [Principles of Digital Development](#) should also be considered and the requirements for the solutions defined.[xii]

Below is a set of questions meant to help determine whether blockchain could be beneficial for solving a problem and achieving desired outcomes. The more "Yes" answers you have, the more likely that blockchain could provide value.

Questions   Yes

Does the solution require a database?

Will there be multiple writers updating/inputting information?

Is there a lack of trust among participants?

Is there a lack of a trusted intermediary?

Can a consistent set of rules help achieve the outcome?

WIll governing rules be consistent over time?

Is transparency of the transactions an important feature?

Is an immutable, auditable record of transactions important?

Are transactions dependent or interrelated?

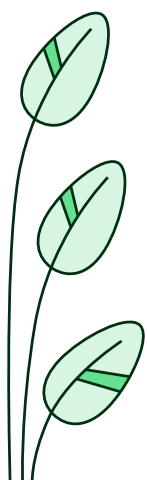Can a distributed infrastructure reduce the risk of censorship or attack?

0/10
LESS LIKELY

10/10
MORE LIKELY

Diagram 2: Adapted from The Beeker Center and Georgetown University[xiii]

If the signs point to blockchain being a fit, it is important to determine which configuration of blockchain would best suit the problem you are trying to solve. There are several aspects to consider when determining a blockchain configuration — primarily, who should see the information and who should maintain the infrastructure.[xiv]

Public blockchains

A public, permissionless blockchain is one where anyone can see all transactions taking place, and anyone is able to participate in the network and help maintain the ledger. This is the most decentralised configuration of a blockchain from a governance and architecture standpoint. Consensus mechanisms (such as Proof of Work) are used

to select a node in the network to contribute the next block and set of transactions, distributing the power in the network.

Permissioned blockchains

A private, permissioned blockchain is where both the information and the maintenance of the network are restricted to a selected group, often referred to as a consortium. Consortiums use private permissioned blockchains to share information across multiple entities to create a single source of truth. Typically, members of the network are known and therefore consensus mechanisms which require lower computational effort can be used (for more on consensus mechanisms, see Appendix I)[xv].

Note that other configurations of blockchains are possible, where the information being shared could be internally stored until it reaches a state where it is valuable and feasible to be shared publicly (ex. think of any type of license – it might not be appropriate to share all personal details, but the status of the license could be shared publicly). Think through the data architecture and consider where and when information can and should be shared.

Examining differences

	DATABASE	PERMISSIONED BLOCKCHAIN	PUBLIC BLOCKCHAIN
TYPE	Permissioned	Permissioned	Public
CONTROL	Centralised	Determined by a selected group	Public
ARCHITECTURE	Client-Server architecture	Closed Peer-to-Peer architecture	Public Peer-to-Peer architecture
DATA PERSISTENCE	Non-persistence	Immutable	Immutable
CHANCE OF FAILURE	Yes	No	No
PERFORMANCE	Extremely fast	Slow to medium	Slow

Diagram 3: Adapted from 101blockchains[xvii]

The key features of trust, security, immutability and transparency are typically achieved with public and permissionless blockchains (see Appendix II for the evolution of blockchain technology). For permissioned blockchains the value proposition is slightly different. The two most common public, permissionless blockchains are the Bitcoin and Ethereum networks. The Hyperledger blockchains are permissioned networks.

It might not be immediately clear what type of blockchain you should use to solve a problem. The following section presents a key set of questions that should be asked to determine exactly how to approach blockchain both in the design and the implementation.
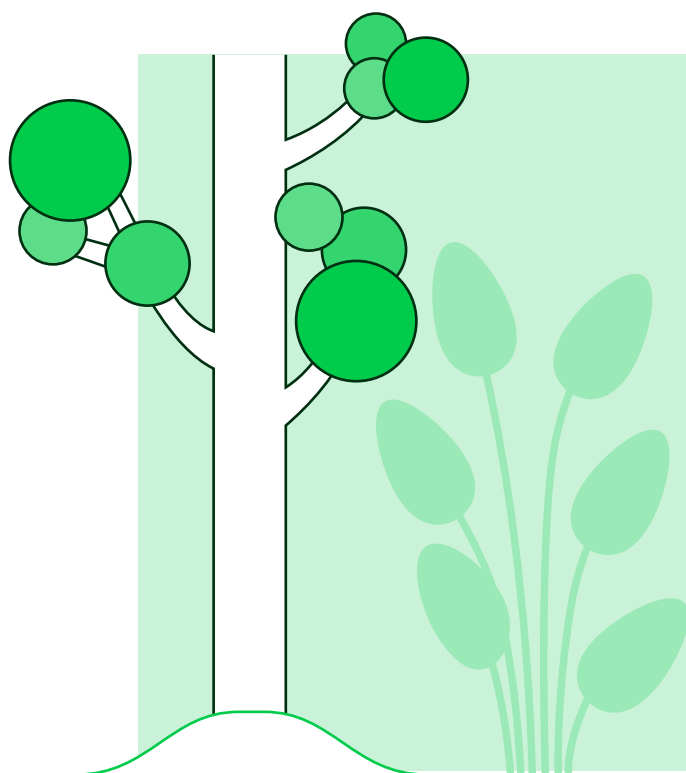
When talking about blockchain, it is important to clarify what type of blockchain is being discussed, as each setup has different advantages and disadvantages.

2.2 Types of blockchains

Key questions to consider

Blockchain has a set of core competencies which should be considered when evaluating whether it is a suitable technology for a specific challenge. Typical use cases where blockchain could prove valuable are in cases where there are multiple entities who require access to a specific set of information, when the information being shared has value being immutable, and when there is value for the data to be made transparent to all. Other potential scenarios that could be a match for using blockchain would be situations where information needs to be shared freely without controls imposed, for example, by censorship or where the transfer of value in an expedient manner would be beneficial.

A step by step flow-chart and a key set of questions have been curated to help guide your decision making on when blockchain is the right fit.

(diagram on next page)

Blockchain decision tree

Start

This chart should be used as a starting point in determining if blockchain could be a good fit; it is advisable to consult with someone who is familiar with databases and blockchain technology.

Can you articulate the problem you are trying to solve? → **NO**

↓ **YES**

Are you trying to store structured information? → **NO**

↓ **YES**

Do multiple parties need to access or audit this information? → **NO**

↓ **YES**

Do the parties fully trust each other?

↓ **NO**

Would all the participants trust a third party? → **YES**

← **NO**

Is there value in the data being public? → **YES** → Do you need to control who can make changes to the blockchain software?

↓ **NO**

YES ↓

Is the database likely to be attacked or censored?

YES → (from Do the parties fully trust each other)

↑ **NO**

Is there value in having multiple copies of the information? → **NO**

YES ↓

Do you need high throughput? (>30 transactions per second) → **YES** → Is the database likely to be attacked or censored?

↑ **NO**

(Do you need high throughput) **NO** →

YES (Is the database likely to be attacked or censored) ↓

YOU MIGHT NEED A PUBLIC BLOCKCHAIN

YOU MIGHT NEED A PERMISSIONED BLOCKCHAIN

YOU DON'T NEED A BLOCKCHAIN
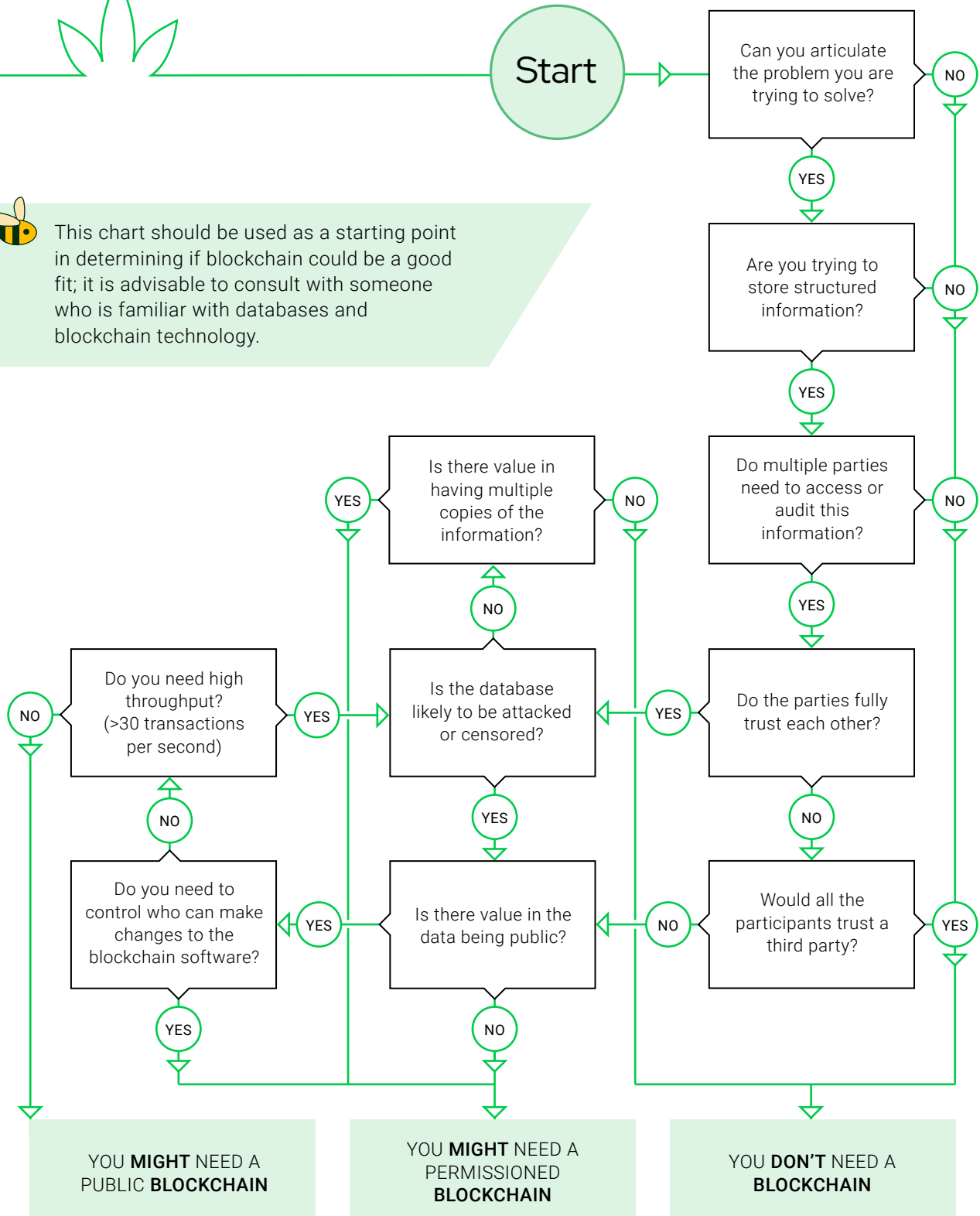
Diagram 4: Modified from IEEE[xviii]

Diagram 2 and 4 above are tools meant to determine if blockchain could provide value, and if so, what type of blockchain could potentially be the best fit. As conversations are being had about using blockchain technology, consider the context in which you are working, the participants involved, rules and regulations, and the type of data being stored. The following questions are meant to supplement the decision tree above, and to elaborate on key considerations.

Context: What is the problem you are trying to solve and what does the ecosystem around it look like?

Before launching a project, ensure that the context in which the project will operate, and the goals are fully understood. Understanding the users and the risks of the project ecosystem are critical. From a user perspective, taking a human-centered approach helps to better understand what you are trying to solve and the environment in which the solution will operate in (ex. low connectivity, low literacy, etc.). Insights can be gained by conducting interviews and testing at each stage. Engaging with a variety of stakeholder groups at the outset could lead to a greater chance of success.[xix]

Because blockchain technology is fairly new, the number of people around the world with skills to design, build and maintain these types of projects is still limited. Therefore, when deciding to proceed with a blockchain project, a decision needs to be made about how the project will be implemented: through a vendor, hiring new talent, or a combination of both. It will need to be decided how the staff, vendors and other operational costs will be covered. Moreover, other major considerations should include how the platform will be managed on a day-to-day basis and how to deal with updates to the software when required.
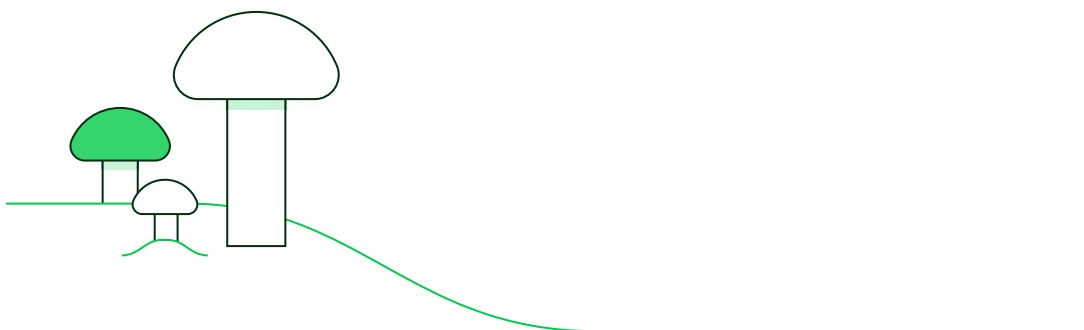
Participants: Who needs access to the data?

One of the key suitability criteria for using blockchain is when there are multiple parties who need to share and view a common set of information; therefore, most blockchain projects involve multiple entities working together towards a common goal. If information has value in being viewable by anyone, consider a public blockchain. If only a limited group should have access to the information, consider a permissioned blockchain.

For permissioned blockchains, consortiums form to be the governing group to oversee a project, however, consortiums introduce their own complexities. A framework needs to be established in order to determine how to deal with challenges, such as how decisions are made within the context of the project, who is responsible if something does not go as planned with the project, how disputes are handled and defining the terms of the membership.

If it is determined that there is value in sharing information across parties, it then needs to be determined if all parties need equal access to the data, or, if there are certain parties who are contributors of data, and others who are simply consumers of data. Understanding elements such as data privacy help better inform the overall technology choice and also access controls.

Rules: Is there an element of mistrust?

Since blockchain provides a distributed way to manage information, it creates an avenue for groups who traditionally would not work together to reimagine what is possible. A wide definition of mistrust should be used to assess whether blockchain could be beneficial. Frank conversations need to be had about the willingness of all parties to share information in a traditional database. Additionally, it should be discussed whether the parties would be willing to use a third party to manage and share information. If there is an unwillingness to trust a central party, blockchain could be a potential solution.

When mistrust between parties is present, determining the rules of operation is critically important. Public blockchains have their own set of rules around how the ledger is maintained. In a permissioned scenario, the parties involved need to determine how the system will be designed, taking into consideration how the ledger will be maintained (i.e. the type of blockchain and the way that consensus will be achieved). If using a permissioned blockchain, it is important for all parties to agree on how voting will take place, and whether all parties will have an equal amount of nodes (i.e. copies of the ledger), or if some organisations

will have more validating power because they are greater consumers of the network. Ultimately, this is a decision that should be decided by the governing board and the technological setup should match the decisions made offline.

The other consideration related to the system and maintaining its integrity, is whether the system is likely to be attacked or censored. If there is a chance that the system will be attacked, increasing the decentralisation of the information increases the resiliency, because if one node is compromised, there are still other unaffected copies. If censorship is a concern, public blockchains can serve as a solution given there are no limitations on who can participate.

Data: What type of data are you storing?

Due to the permanency of information which will be stored on a blockchain, having strong data practices in advance of putting any information on a blockchain is crucial. Often, deciding on standardised information to share across all parties in the network is a large exercise for data quality assurance (ex. meters versus square feet, euros versus rupees, etc.).

Particular attention should be paid to data privacy, since information placed on a blockchain is immutable. Due to this permanency, it is recommended that no sensitive information be stored on a blockchain, but instead a digital fingerprint of the data (known as a hash) or reference to where the information exists, be captured on the blockchain.[xxii]

If a public blockchain is being used to store information or deploy applications, this will require an organisation to pay a small fee, in cryptocurrency, to the network for these tasks. Organisations will need to establish processes to acquire and utilise the necessary cryptocurrency.

What is cryptocurrency

Cryptocurrencies (also known as "crypto") are digital assets which are maintained by a blockchain through distributed computing and cryptography and enables peer-to-peer transactions.

Contrary to fiat currencies which are solely issued by central banks, cryptocurrencies are digital assets which are not created by a central bank.[xxiv,xxv] Cryptocurrencies are built on top of blockchains and rely on thousands of computers around the world to maintain the ledger, including who has sent and received various amounts of the crypto, and when. Bitcoin is considered the first major implementation of crypto, at scale.[xxvi] The value of cryptocurrencies is determined based on supply and demand, scarcity of the asset, public sentiment about the cryptocurrency and, lastly, their perceived usefulness.[xxvii,xxviii]

There are currently over 2,400 cryptocurrencies, valued at a total of $241B USD (as of 13 May 2020).[xxix] The two largest cryptocurrencies, with a combined $186B USD market cap, are *bitcoin* (BTC) and *ether* (ETH). Each operates as the currency (or the *native token*) of their associated blockchains (respectively called the Bitcoin blockchain and the Ethereum blockchain).

For the bitcoin ecosystem, bitcoin with a lowercase "b" refers to the cryptocurrency (or BTC for short), while Bitcoin with an uppercase "B" refers to the blockchain. In the case of the Ethereum ecosystem, the cryptocurrency is called ether (or ETH for short), and the blockchain is referred to as the Ethereum blockchain.

3. Uses in a UN entity

The Public Sector is the industry in which blockchain could have the most impact. Many entities within the United Nations have already begun researching, prototyping and implementing blockchain based solutions.[xxxi,xxxii]

This section will highlight a few ways in which blockchain technology can be used. It should be noted, however, that this document only provides samples and is not exhaustive. As mentioned before, blockchain has three primary functions: storing information, tracking the exchange of value, and automated logic.

To learn more about use cases of blockchain and cryptocurrency within the UN, see Appendix III.

General use cases for blockchain

USE CASE	Public records	Supply-chain tracking	Other	Digital financing	Cryptocurrecny	Other	Smart contracts	Incentivisation	Other
RECORD	Data			Value exchange			Efficiency		
PLATFORM	Blockchain								

Diagram 5: Modified from Imperial College[xxxiii]

3.1 Acting as a single source of truth

Public records

> *"Tenneh, a local business owner in Freetown, is able to provide her financial institution proof that she is who she says she is, and a record of her restaurant licenses with ease."*

Registries are an obvious use for blockchain as they enable a large group of people to know the status of a registration in real-time, should be tamper proof and can exist in perpetuity.

Blockchains have been used to track official registries issued by public sector entities, academic institutions, and medical entities, among others. Blockchain can be used by governments and public institutions to issue official permits and licenses that must be approved and processed by a trusted entity. Instead of relying on a paper copy of a license, which could be fraudulent, lost, or difficult to verify, blockchain can be used to ensure that a license has been issued by a valid entity and that the license is in good standing.[xxxiv] Blockchain-based registries have increased value when they are on public blockchains.

Supply-chain tracking

> *"Maya, an importer in Ethiopia, is able to track her most recent shipment of goods in real-time. Because of the digitised and streamlined process, she now receives her shipment in days rather than weeks."*

Because blockchains allow multiple parties to view a common set of information, and agree upon a common history, supply-chain

has commonly been considered a prime blockchain use case. Creating this shared set of real-time, immutable information empowers each entity in the ecosystem with a new level of information to make better informed decisions and more precise modeling and forecasting.[xxxv]

Using blockchain to track the lifecycle of a product can bolster transparency and provide a single source of truth between producers, distributors, and consumers. In the context of using blockchain for the lifecycle of vaccines, authentic vaccinations can be given a unique QR code or tag (such as RFID) upon creation. Throughout the vaccine's journey to health care providers, Internet of Things (IoT) devices can capture the temperature at which the vaccine is stored to ensure it is kept at an appropriate temperature and create a blockchain-based record. Finally, when a doctor is administering the vaccine, they can verify that the vaccine is usable and can then transfer information about the vaccine to the individual's digital medical charts. Should there ever be a recall on a product which is being tracked in a blockchain-enabled supply-chain, the source and those who may have come in contact with the product can be identified quickly. Supply-chain projects can be either public, private, or hybrid, depending on the nature of the information being collected.

3.2 Tracking the exchange of value

Digital finance

"Bassam is a Syrian refugee who lives in the Za'atari camp. He shops for the ingredients he needs from a grocery store inside the camp. Bassam doesn't worry about losing a food voucher or an external bank having his data — and he pays with a digital voucher at checkout."

Blockchain can be used to increase the transparency and efficiency of financial transactions which take place within or between organisations. In this case, blockchain would be used to increase the transparency and accountability of when, where and how funds are being allocated.

Blockchain can also be used to create a common view of beneficiary data and entitlements across organisations. In doing so, organisations would be able to access a comprehensive view of who is receiving benefits. Digital cash systems could be used in a closed ecosystem environment where beneficiaries receive a digital entitlement and have vendors who accept the digital entitlement. The process could be streamlined where a digital record of entitlements and expenditures could be batched, and one payment can be made to the outlet on a regular basis, therefore reducing transaction costs (i.e. banking fees). Options for using the entitlement outside of the designed outlets must also be considered. Given that some of this information may be sensitive, it is likely to be stored on a private, permissioned blockchain.[xxxvi]

Cryptocurrency

"Prescrypto, a Mexican based startup working on digital prescriptions, can pay their employees around the world in mere seconds, and with full transparency to all investors in the company, who can verify where the funds went."

Cryptocurrencies allow organisations to leverage a new type of asset to transfer value between parties around the world. Cryptocurrencies are faster than traditional banking solutions and typically have public history to trace where funds have come from and are transferred to. Cryptocurrencies also allow individuals around the world to easily transfer funds to one another without traditional intermediaries.

Cryptocurrencies offer an alternative for individuals looking to make cross-border transfers. Specifically in the case of migrants, remittance systems tend to be slow and expensive whereas cryptocurrencies represent a cheaper, more efficient alternative. While traditional transfers can have high fees, which are often passed on to the customer, cryptocurrencies can be sent for a fraction of traditional fees. Some migrants also consider using cryptocurrencies to avoid local currency volatility or international exchange fees. Cryptocurrencies are also an alternative solution for individuals who are unbanked or live in underserved communities.[xxxviii]

3.3 Increasing organisational efficiency

Smart contracts

"The Digicus platform is a digital portal that allows the streamlined processing of the disbursement of funds, making it faster and more transparent, leaving more time to focus on programme delivery."

Because smart contracts reduce the need for manual interaction points, they can help organisations increase the efficiency of their operations by codifying logic which automatically executes if certain conditions are met. By putting the interaction on a blockchain, this provides all parties with a new level of information which can be utilised to increase the efficiency of planning and decision making and increases the level of accountability of all parties.

When a contractual commitment with a monetary value is made between organisations, this relationship can be codified on a blockchain and when a predetermined milestone is met, payment can automatically be sent. Throughout the duration of the partnership, any new critical events can be recorded on the blockchain for all parties to maintain a record of the event. Traditional banking systems can be linked to the blockchain to create a digital record of the payment sent by the paying institution, or cryptocurrency can be used as payment. By using smart contracts, parties can have confidence that the agreement will be respected if the terms are met. If using blockchain for the purposes of increasing the accountability and transparency of contractual relationship management, it is likely that this will be a private blockchain implementation unless there is a public interest in the interaction.

Digital engagement

"Marcin, a UN employee is collecting digital impact tokens as he completes learning modules. The tokens create verifiable proof of participation and can be redeemed to provide nutritional bars to children in need, creating double the impact."

Blockchain and cryptocurrency create opportunities for entities to engage with individuals in new ways. Blockchain platforms give organisations the opportunity to solicit individuals around the world to contribute to tasks, with a construct that is designed to demonstrate to the worker that the funds are there to be paid, and that payment will be completed in an expedient manner as long as verification of task completion is provided.[xxxix] Micro jobs, where individuals can complete small tasks and be paid accordingly, are also well suited for blockchain projects and cryptocurrency payments.

Using a beach cleanup as an example, small amounts of cryptocurrency could be offered for each bag of garbage collected. A photo with the bag of garbage and an item that proved the date (such as a newspaper) would then be submitted to the blockchain-based platform that pays out the reward. Platforms like these provide opportunities for individuals to earn alternative incomes and give organisations a platform to make an impact around the world with little local infrastructure.

4. Mechanisms for systematic use

4.1 Exploring blockchain across the UN

Blockchain is a powerful tool that can help organisations achieve their objectives if used effectively. As entities learn to use the technology, the UN can explore ways to strategically integrate blockchain into its work in order to maximise its benefits and avoid potential pitfalls.

Providing tools

Entities of all sizes need to innovate and modernise to stay relevant. To support this innovation, the UN needs tools to help entities learn about blockchain. To reduce the risk involved in innovating, it would be ideal for entities to experiment on a common, secure platform to build a basic understanding of the technology. Additionally, to reduce the duplication of work, blockchain applications created by entities should be shared across the UN.

The Atrium

The UN Innovation Network, in partnership with United Nations Development Programme (UNDP), UNICEF and The World Food Programme (WFP), has launched The Atrium, an inter-agency platform that allows any UN entity to learn and experiment with blockchain technology. The Atrium has a curated list of introductory-to-advanced learning resources and a repository of UN blockchain based projects where individuals can share project documentation and code. Instead of starting from scratch, UN entities can leverage work that has already been done and customise to their needs. A private Ethereum blockchain is also run, which allows entities to quickly test their applications and learn how to run a node.

When WFP wanted to create digital certificates to issue on blockchain, instead of starting from scratch, The Atrium provided the code for a certificates project. By leveraging some-thing that had already been created by UNICEF, WFP saved eighty percent development time and was able to launch their certificates via blockchain in under 24 hours.[xl]


Sharing knowledge

As entities start their learning journey, project leads and team members should have a medium to share what does and does not work and to learn from colleagues how to strategically approach problems. Through this forum, colleagues can discuss projects and developments in the area of blockchain and cryptocurrency. This group can share their insights across the UN system across all levels. This forum would ideally operate in person and online to allow different types of collaboration, and to allow global participation.

UNIN blockchain learning group & courses

The UN Innovation Network (UNIN) has launched a Blockchain Learning Group, as well as an Introduction to Blockchain course which are both **open to anyone within the UN to join**. The Learning Group is meant to serve as a forum for interested parties to ask questions, share lessons learned, and find potential areas of collaboration. This group is open to all levels to join and complements the digital platform, The Atrium, also launched by UNIN to support blockchain learning.

The Introduction to Blockchain course is a facilitated five-week course which covers the basics of blockchain technology, how to identity when blockchain is the right fit, as well as UN blockchain use cases. In this course, students use a blockchain-enabled application to complete homework, and also write their first smart-contract. This course will continue to run in 2020 with both online and in-person options.[xli]
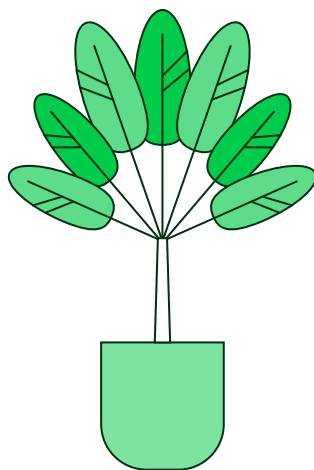
Scanning the horizon

Further understanding of cryptocurrencies and the role they could play at the United Nations, within and between Member States, as well as individuals around the world is needed. It is suggested that a group of experts from all sectors have targeted discussions on topics such as custodianship of crypto assets, decentralised financial applications and the potential drawbacks and challenges of using cryptocurrency. While entities and Member States may have different approaches to cryptocurrency, these conversations will better equip entities to operate in a digitally financed future.

| Cryptocurrency working group |
| --- |
| As UN entities continue to learn about blockchain and cryptocurrency, more focused conversations around particular elements of the technology will be needed. In response to the growing interest and use of cryptocurrency, a Cryptocurrency Working Group has been formed to explore topics such as decentralised finance, Central Bank Digital Currencies (CBDC) and the digitisation of physical assets onto a blockchain. The Working Group will share lessons learned publicly but will also convene industry experts to share their work and facilitate conversations around the impact cryptocurrencies can have on the way the UN operates. This group also advises senior leadership on the topic of cryptocurrency. |
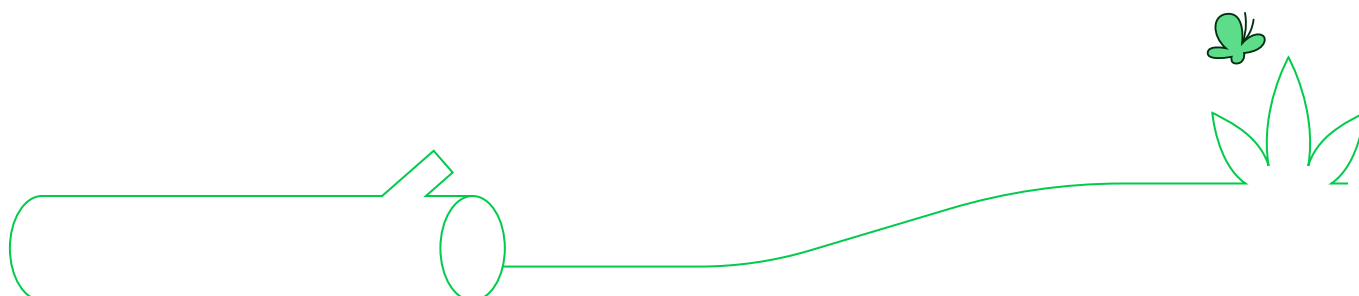
Investing in the future

Blockchain and cryptocurrency projects continue to be built around the globe. Investing strategically in [digital public goods](#) allows entities to learn what is going on in the ecosystem by having inside access to projects as they develop. This approach also allows UN entities to ensure that the technology is being built with the most vulnerable in mind by mentoring and guiding these initiatives. Investments are needed in regions or in populations that traditionally do not receive large investment attention; this could be achieved through a pooled fund which makes strategic investments in key projects.

UNICEF Venture Fund

UNICEF's Venture Fund is a $29M pooled Fund investing in early stage, open-source, emerging technology with the potential to impact children on a global scale. It also provides product and technical assistance, support with business growth, and access to a network of experts and partners. The UNICEF Venture Fund is the first financial vehicle of its kind in the United Nations and enables UNICEF to learn from and to shape markets of emerging technology that exist at the intersection of $100 billion business markets and 1 billion persons' needs.

To date, the Venture Fund has made strategic investments in digital public goods in the areas of machine learning and artificial intelligence, drones, augmented reality and virtual reality, accessibility and blockchain. There have been 85 investments in digital public goods across 55 countries. By providing flexible funding to early-stage innovators, it allows UNICEF to quickly assess, fund and grow open-source technology solutions that show potential to positively impact the lives of vulnerable children. [xlii]
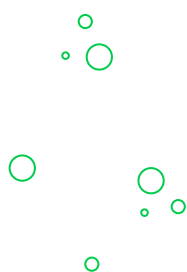
Appendix

Appendix I:
Differentiating features of blockchains

Consensus mechanism

In order to maintain a single source of truth amongst dozens or even thousands of computers, blockchains rely on *consensus mechanisms*, a predetermined set of rules that all parties follow to maintain the network. Blockchains such as the public Bitcoin or Ethereum blockchains use a consensus mechanism called Proof of Work (POW) to maintain constant agreement on the information that the blockchain should include.

The nodes in these networks are constantly accepting transactions from the network, while simultaneously working to be the first in the network to solve a difficult mathematical problem. Once a computer solves the problem, a block (which includes a batch of transactions) is sent to other nodes in the network and all blockchains are updated. All nodes then begin trying to solve the next mathematical problem to be able to propose the next block.[xliii]

Miners are incentivised to maintain the network by receiving a reward for being the computer that solves the difficult mathematical problem, called a *block reward*. The winning computer also receives the transaction fees of all the transactions that will be included in the block. The current block reward for the Bitcoin network is 6.25 bitcoin and 2 ether for the Ethereum network. Because of slightly different rules between the two networks, the new blocks are added to each network at different speeds. In the Bitcoin network, a new block is added to the blockchain approximately every 10 minutes. This means that it takes approximately 10 minutes for a transaction to be processed.[xliv] For the Ethereum network, transactions are processed within ten to twenty seconds.[xlv]

Many different blockchains exist outside of Bitcoin and Ethereum, which have special characteristics. Blockchains rely on different types of consensus mechanisms to maintain a constant state of agreement amongst nodes. Other common consensus mechanisms are Proof of Stake and Proof of Authority.[xlvi] Public blockchains using Proof of Work consensus mechanisms are energy intensive. Permissioned blockchains that rely on alternative consensus mechanisms require less energy since computers typically do not need to compete to add the next block.[xlvii]

Decentralisation

Since blockchains have consensus mechanisms to keep them in sync, no central authority is required to be the arbiter of whether a transaction is valid, since the rules are predetermined when the blockchain is initially set up. Because anyone can participate in public networks such as the Bitcoin or Ethereum blockchains, this means that nodes around the world maintain the blockchain and have a copy of all the information. Since the network is self-managed, blockchains are referred to as being decentralised, because no one person or organisation owns them and can single handedly control them. At the time of writing, there are approximately 10,000 Bitcoin nodes and 7,000 Ethereum nodes around the world.[xlviii, xlix]

Cryptography

Cryptography is a way to secure communications between parties, so that anything that is intercepted is not comprehensible unless sent to an intended recipient with appropriate permissions. Cryptography can act as a way of authenticating whether or not communications are from a specific individual or organisation. In the case of blockchain, a specific technique called *hashing* is used to take large amounts of data and create a unique identifier based on the contents. If any of the data is altered, the unique identifier known as the *hash*, will not match the original. For each block in a blockchain, a hash is created making a unique fingerprint for the block. In the following block, the previous hash is used as part of the information that creates a new hash, in effect, binding the two blocks together; this process continues to link the blocks together, making it extremely difficult to change the history of the blockchain.

| BLOCK 75	BLOCK 76	BLOCK 77
PREVIOUS HASH: f85539bc40d6b2a21a847b4578c2a5ab0175031e17ebdb4ac4a701daeac7688e	**PREVIOUS HASH:** 9ed261f584fa341daa11e64564646e2955bc11525d9dd09d7bc803b8a9ca44cc	**PREVIOUS HASH:** ee5efeb71b038ed8a1cb61a9def740f3bfe8d1e0c87413bd30e20e8828080b53
DETAILS FOR: Transaction 1 Transaction 2 Transaction 3 ….	**DETAILS FOR:** Transaction 1 Transaction 2 Transaction 3 ….	**DETAILS FOR:** Transaction 1 Transaction 2 Transaction 3 ….
BLOCK HASH: 9ed261f584fa341daa11e64564646e2955bc11525d9dd09d7bc803b8a9ca44cc	**BLOCK HASH:** ee5efeb71b038ed8a1cb61a9def740f3bfe8d1e0c87413bd30e20e8828080b53	**BLOCK HASH:** 3ccb1d53c65fb77939cd40dac74eba7511e5c0f819c7dea81f9aac7160c7e4da

Public key cryptography is a way of verifying a digital signature on a transaction without exposing any sensitive information.[li] A public key and a private key together produce a unique digital signature; a miner can validate that the transaction is from a valid account by only knowing the public key. The concept of public key cryptography is used in the context of blockchain to prove the author of the content, or ownership of an asset.

Network economics, decentralised computing and cryptography have existed for many decades; however, Bitcoin brought these concepts together in 2008.[lii]

Smart contracts

Some blockchains include the ability to create digital logic which determines the rules by which users interact. This logic can be specified so that if certain conditions are met, then, subsequently, a result should occur, also known as "if/then" statements. When a smart contract is invoked, a new transaction is generated and added to the ledger.[liii] Examples of blockchains with inherent smart contract functionality are Ethereum and Hyperledger.[liv] An example of a smart contract application could be for farmers who have signed up for an agriculture insurance premium; "*if* there is no rain in Jaipur, India for greater than sixty days, *according to* theweathernetwork.com, *then* pay the farmer 1.5% the value of their insured crops."
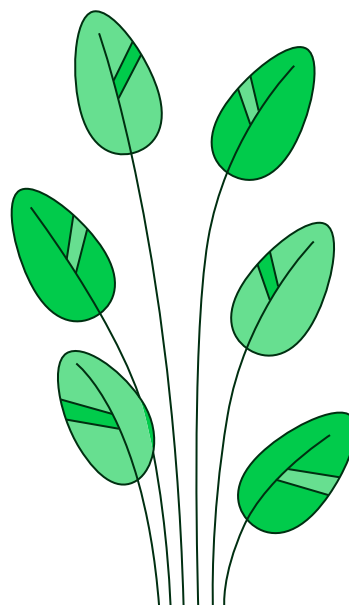
Appendix II:
The evolution of blockchains

Many components that make up blockchain, such as decentralised computing and cryptography, have existed for decades, but bitcoin was the first major implementation at scale. Bitcoin, the first use case of blockchain technology, is a peer-to-peer electronic cash system introduced in a whitepaper in 2008 by an individual or group using the pseudonym Satoshi Nakamoto. The paper introduced the idea of users being able to send payments to one-another without using a central authority such as a bank, and instead, relying on computers around the world to verify transactions and maintain balances. A year later, in 2009, Satoshi released 30,000 lines of code and the first bitcoin transaction took place on 12 January 2009.[lv] The rules set in the original code dictated that only 21 million bitcoin would ever be created (note: a bitcoin is divisible to the eighth decimal place). The original code also determined the speed at which bitcoin would be released into the network through block rewards, and how transactions would be sent, verified and added to the network through the Proof-of-Work consensus mechanism.

The Ethereum blockchain, often referred to as "blockchain 2.0", allowed new types of information to be easily stored and introduced the concept of smart contracts for blockchains.[lvi] In 2015, Vitalik Buterin presented Ethereum as a platform that could store different types of information, such as land titles, provenance information, and beneficiary entitlements.

Since then, organisations have been exploring whether this new technology could be applied in an enterprise context for various use cases. In late 2015, the Linux Foundation launched Hyperledger, an enterprise-grade blockchain.[lvii] Hyperledger has since evolved into six blockchain codebases that focus on specific use cases such as digital identity or supply-chain.[lviii]

Appendix III:
Showcase of UN projects using blockchain and cryptocurrency

Public records

Use Case	Land record management in Afghanistan
Entity	United Nations Office of Communication and Information Technologies (UN-OICT), UN-Habitat

In Afghanistan, blockchain is being used to track the ownership of parcels of land. As part of the UN-Habitat's "City for All" initiative, UN-OICT and UN-Habitat are working together to build the digital registry. By leveraging blockchain technology, an immutable version of land records is created, which can then serve as the basis for other government services such as urban planning, citizen engagement and revenue generation.[lix, lx]

Supply chain tracking

Use Case	Transparent supply-chain between Djibouti and Ethiopia
Entity	World Food Programme (WFP)

The tracking of the movement of goods between countries can be difficult due to disparate information, which can often lead to delays in critical aid delivery. The World Food Programme is exploring digitising the supply-chain process and using a blockchain-based system to share a common set of information between relevant parties to both reduce the administrative burden and increase the transparency of information. In this pilot between Djibouti and Ethiopia, it is estimated that the current shipping process which takes 15-20 days can be reduced to three to five days.[lxi, lxii]

Digital finance

Use Case	Cash transfers in refugee camps in Jordan
Entity	WFP and UN Women

Blockchain technology is being used in refugee camps to track cash entitlements that are disbursed to the people WFP serves. Cash value from WFP or other partners is stored in an 'account' for individual recipients and is maintained on the blockchain. The cash that people receive or spend on goods and services is paid to retailers through a commercial financial service provider that is built on a private, permissioned blockchain, and integrated with UNHCR's existing biometric authentication technology—WFP has a record of every transaction. This not only saves on financial transaction fees in the camp setting but ensures greater security and privacy for Syrian refugees. The project currently coordinates the delivery of food assistance for over 100,000 Syrian refugees.[lxiii, lxix]

Use Case	Tracking chocolate production in Ecuador
Entity	United Nations Development Programme (UNDP)

When a chocolate bar is purchased through a new UNDP pilot, the purchaser receives an impact token which the consumer can send directly back to the farmer or can use for a discount on future products. When four tokens are sent back to a farmer, a new cocoa tree is planted, with the intent that this allows the farmer to increase their production and therefore their income. Because the token is issued using a blockchain, the tokens transfer can be tracked by anyone, creating an immutable and transparent proof of impact. This model is being currently tested in other value chains and products, as a new marketing strategy mechanism to leverage resources from the private sector for the SDGs.[lxv]

Cryptocurrency

Use Case	Making investments in start-ups using cryptocurrency
Entity	UNICEF

Nearly four years ago, UNICEF set up the first investment fund of its kind in the UN. This fund makes investments into early-stage start-ups in UNICEF programme countries who are working on solutions to better the lives of children. Building on this innovation, in October 2019, UNICEF announced the first cryptocurrency-denominated fund of its kind in the UN. Following the same principles as the fiat denominated fund, the CryptoFund makes investments into startups, but instead of receiving investment in United States Dollars or local currencies, the investment is made in bitcoin or ether, the two largest cryptocurrencies by market capitalization (as of May 2020). By providing funding in the form of cryptocurrency, there is transparency of where funds come from, where they are invested and also where the investees use their funds. Bitcoin and ether allow the transfers to take place in a few seconds, regardless of where the investees are around the world. This new asset class allows organisations such as UNICEF to transact in a digitally financed world and leverage a new donation type.[lxviii]
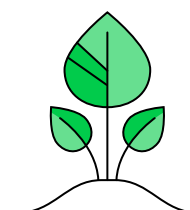
Smart contracts

Use Case	Vendor payment leveraging smart contracts
Entity	UNICEF Kazakhstan

UNICEF works with many partners to deliver its mandate and is innovating in managing those relationships. UNICEF recently leveraged blockchain to digitise and consolidate UNICEF's agreements with its implementing partners on the ground in Kazakhstan (governments, NGOs, academic institutions) by using smart contracts. The goal of the prototype was to develop a platform to streamline processes related to cash transfers to improve the transparency and accountability of partnerships and related transfers of resources. Ultimately, the platform allowed for streamlined verification of the results achieved by partners and allowed the blockchain-based smart contract to automatically release the payment, after verification and authorisation. This platform, called "Digicus", allows all parties to have a common understanding of what stage a project is at, what goals have been achieved, and showcases how smart contracts can be used to expedite processing of paperwork and payment.[lxix]

Digital engagement

Use Case	Incentivising employees with the Unite Token
Entity	United Nations Office of Communication and Information Technologies (UN-OICT)

The Unite Token, a blockchain-based token, can be used to gamify collaboration among UN employees. A typical use would be to give staff a number of tokens at the beginning of the year which they can donate to colleagues to thank them for their support. The resulting balance of tokens shows one's achievements in collaboration and support as seen by peers, not by their managers. Unite Token can be used to incentivise innovation, greening the UN, diversity or any other mindset or behavior we want to encourage in employees.[lxx]

Use Case	Linking youth to the future of work
Entity	UNICEF South Africa and UNDP South Africa

Zlto (zlah-toh) is an innovative digital rewards system that is aimed at reducing employment barriers youth face such as work experience, the cost of work seeking, and access to credible networks by rewarding them for "doing good". The micro jobs performed by the youth are stored as a "work asset" on the blockchain which are validated on the platform by recognized reviewers and serve as credible, verified work experience which can assist them in their search for employment. With the rewards earned through Zlto, young people can access quality opportunities including education, formal jobs, and small business finance. An added advantage of Zlto is that young people earn credits for the micro jobs they perform which can then be exchanged for products and services ranging from basic food supplies such as bread and milk to transport, airtime and electricity.

Notes

i	https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf
ii	http://beeckcenter.georgetown.edu/wp-content/up-loads/2018/06/The-Blockchain-Ethical-Design-Framework.pdf
iii	https://www.dictionary.com/browse/ledger
iv	https://www.europarl.europa.eu/RegData-/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf
v	https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274
vi	https://economictimes.indiatimes.com/definition/cryptography
vii	https://www2.deloitte.com/us/en/insights/industry/public-sec-tor/understanding-basics-of-blockchain-in-government.html
viii	https://assets.kpmg/content/dam/kpmg/pdf/2016/06/kpmg-block-chain-consensus-mechanism.pdf
ix	https://www.oecd-ilibrary.org/docserver/3c32c429-en.pdf
x	https://www2.deloitte.com/us/en/insights/industry/public-sec-tor/understanding-basics-of-blockchain-in-government.html
xi	http://beeckcenter.georgetown.edu/wp-content/up-loads/2018/06/The-Blockchain-Ethical-Design-Framework.pdf
xii	https://digitalprinciples.org
xiii	http://beeckcenter.georgetown.edu/wp-content/up-loads/2018/06/The-Blockchain-Ethical-Design-Framework.pdf
xiv	http://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf
xv	https://assets.kpmg/content/dam/kpmg/pdf/2016/06/kpmg-block-chain-consensus-mechanism.pdf
xvi	https://101blockchains.com/blockchain-vs-database-the-difference
xvii	https://www.dhs.gov/sites/default/files/publica-tions/2018_AEP_Blockchain_and_Suitability_for_Government_Applications.pdf
xviii	https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain
xix	http://beeckcenter.georgetown.edu/wp-content/up-loads/2018/06/The-Blockchain-Ethical-Design-Framework.pdf
xx	https://cointelegraph.com/news/blockchain-will-be-most-in-demand-hard-skill-in-2020-linkedin
xxi	https://www2.deloitte.com/content/dam/Deloitte/us/Documents/-financial-services/us-fsi-taking-blockchain-live.pdf
xxii	https://www.ibm.com/downloads/cas/LA8XBQGR
xxiii	https://blockgeeks.com/guides/what-is-cryptocurrency
xxiv	https://www.investopedia.com/terms/f/fiatmoney.asp
xxv	https://consensys.net/knowledge-base/what-is-cryptocurrency
xxvi	https://www.ivey.uwo.ca/scotiabank-digital-banking-lab/education/bitcoin-crash-course
xxvii	https://www.coinbase.com/learn/where-do-cryptocurrencies-get-their-value
xxviii	https://cointelegraph.com/explained/how-cryptocurrency-prices-work-explained
xxix	https://coinmarketcap.com
xxx	https://bitcoin.org/en/vocabulary#bitcoin
xxxi	https://www.mckinsey.com/business-functions/mckinsey-digital-/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value
xxxii	https://drive.google.com/file/d/1FuT1mP_NaA3D_ooIe5TZPRzDo7mXW6aK/view
xxxiii	https://www.slideshare.net/OECD-DAF/blockchain-and-competi-tion-mulligan-june-2018-oecd-discussion
xxxiv	https://publicsectordigest.com/article/mythical-busi-ness-one-stop-holy-grail-government-business-service-delivery
xxxv	http://www3.weforum.org/docs/WEF_Building-Blockchains.pdf
xxxvi	https://drive.google.com/file/d/0B--8okvw4smiNnFEWjF1M2NSaW8/view

xxxvii	https://www.dummies.com/software/other-software/the-transparency-of-bitcoin
xxxviii	https://ec.europa.eu/jrc/sites/jrcsh/files/blockchain_and_remittances_online.pdf
xxxix	https://breakermag.com/thanks-to-crypto-incen-tives-3-tons-of-trash-were-removed-from-manila-bay
xl	https://www.unicef.org/innovation/stories/blockchain-collaboration-across-un
xli	https://www.unicef.org/innovation/stories/UNINblockchain
xlii	https://www.unicef.org/innovation/venturefund
xliii	https://assets.kpmg/content/dam/kpmg/pdf/2016/06/kpmg-block-chain-consensus-mechanism.pdf
xliv	https://cointelegraph.com/explained/bitcoin-halving-explained
xlv	https://media.consensys.net/the-thirdening-what-you-need-to-know-df96599ad857
xlvi	https://assets.kpmg/content/dam/kpmg/pdf/2016/06/kpmg-block-chain-consensus-mechanism.pdf
xlvii	https://www.cnbc.com/2018/02/23/bitcoin-blockchain-con-sumes-a-lot-of-energy-engineers-changing-that.html
xlviii	https://bitnodes.io
xlix	https://etherscan.io/nodetracker
l	https://economictimes.indiatimes.com/definition/cryptography
li	https://www.ivey.uwo.ca/scotiabank-digital-banking-lab/education/bitcoin-crash-course
lii	http://www3.weforum.org/docs/WEF_Building-Blockchains.pdf
liii	https://hyperledger-fabric.readthedocs.io/en/re-lease-1.4/smartcontract/smartcontract.html#smart-contract
liv	https://www.lawtimesnews.com/archive/are-we-ready-for-smart-contracts/263509
lv	https://u.today/first-bitcoin-btc-transac-tion-was-made-11-years-ago-by-satoshi-what-was-its-purpose
lvi	https://www.mckinsey.com/industries/advanced-electron-ics/our-insights/blockchain-2-0-whats-in-store-for-the-two-ends-semiconductors-suppliers-and-in dustrials-consumers
lvii	https://www.hyperledger.org/resources/publications/hyperledger-annual-report
lviii	https://www.hyperledger.org/wp-content/uploads/2018/11/Hyper-ledger_DataSheet_11.18_Digital.pdf
lix	https://sociable.co/technology/un-enlists-blockchain-in-af-ghanistan-for-transparency-in-rebuilding-process
lx	https://reliefweb.int/report/afghanistan/city-all-investing-sustainable-urbanization-afghanistan
lxi	https://innovation.wfp.org/blog/how-un-innovation-network-seeks-acceleratesdgs-innovation
lxii	https://www.delltechnologies.com/it-it/perspec-tives/how-blockchain-is-bringing-food-security-to-refugees
lxiii	https://innovation.wfp.org/project/building-blocks
lxiv	https://www.unwomen.org/en/news/stories/2018/9/press-re-lease-un-women-and-wfp-harness-innovation-for-economic-empowerment-in-crisis
lxv	https://www.fastcompany.com/90413242/this-new-blockchain-choc-olate-bar-is-brought-to-you-by-the-un
lxvi	https://coinmarketcap.com
lxvii	https://www.unicef.org/press-releases/unicef-launches-cryptocurrency-fund
lxviii	https://www.unicef.org/press-releases/unicef-launches-cryptocurrency-fund
lxix	https://www.unicef.org/innovation/blockchain/digicus
lxx	http://bit.ly/UNIN2019Q2
lxxi	https://www.ted.com/talks/paul_stamets_6_ways_mushrooms_-can_save_the_world/transcript?language=en
lxxii	http://www.bbc.com/earth/story/20141111-plants-have-a-hidden-internet