



U4 Issue 2020:7

Blockchain as an anti-corruption tool

Case examples and introduction to the technology

By Per Aarvik
Series editor: Arne Strand

CMI CHR.
MICHELSEN
INSTITUTE

Disclaimer

All views in this text are the author(s)', and may differ from the U4 partner agencies' policies.

Partner agencies

Australian Government – Department for Foreign Affairs and Trade – DFAT

German Corporation for International Cooperation – GIZ

German Federal Ministry for Economic Cooperation and Development – BMZ

Global Affairs Canada

Ministry for Foreign Affairs of Finland

Ministry of Foreign Affairs of Denmark / Danish International Development Assistance – Danida

Swedish International Development Cooperation Agency – Sida

Swiss Agency for Development and Cooperation – SDC

The Norwegian Agency for Development Cooperation – Norad

UK Aid – Department for International Development

About U4

U4 is a team of anti-corruption advisers working to share research and evidence to help international development actors get sustainable results. The work involves dialogue, publications, online training, workshops, helpdesk, and innovation. U4 is a permanent centre at the Chr. Michelsen Institute (CMI) in Norway. CMI is a non-profit, multi-disciplinary research institute with social scientists specialising in development studies.

www.U4.no

U4@cmi.no

Cover photo

Clifford Photography on Unsplash (CC cc0) <https://unsplash.com/photos/TekPZz1YP3A>

Keywords

blockchain - corruption - development - e-government - illicit financial flows - money laundering - sustainable development goals - transparency

Publication type

U4 Issue

Creative commons

This work is licenced under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International licence (CC BY-NC-ND 4.0)

The technology behind bitcoin and other cryptocurrencies was supposed to end poverty, eliminate corruption, and provide financial inclusion for all. The very financial institutions it was created to exclude are adopting the technology to increase transactions' security and reduce costs. Its degree of success is more contextual than related to the technology itself.

Main points

- Blockchain has the potential to be a game changer in anti-corruption efforts. Whether it is successful or not largely depends on contextual elements – infrastructures, legal systems, social or political settings – rather than on the technology itself.
- Implementation of blockchain technologies in governance affects fundamental aspects of society, such as trust in institutions, identity, transparency, and data and privacy protection.
- A blockchain is designed to operate in environments where trust in data/code is greater than trust in individuals or institutions.
- Records entered in the blockchain are transparent and immutable. Because of these features, there may be conflicts with individual rights such as the right to privacy or the right to be forgotten, as described in the European Union General Data Protection Regulation (GDPR).
- When blockchains hold registries of physical items, trusted gatekeepers have to ensure that the physical reality and digital information correspond.
- Digital infrastructure, governing regulations, and digital literacy should be in place before blockchain-enabled registries are rolled out, particularly in developing countries.
- Decision makers should have an understanding of the technology before deciding on whether or not it is appropriate.

Table of contents

An overview of blockchains and cryptocurrencies	2
The blockchain and Bitcoin: A brief history	2
Consensus mechanisms	3
Power consumption and energy footprint	4
Sovereign and corporate cryptocurrencies	5
The four major types of blockchain	7
Confusing definitions	8
Prerequisites for blockchain technologies	9
Properties of blockchain relevant for anti-corruption	10
Trust in people and trust in code	11
Trust in gatekeepers	11
Transparency vs privacy	13
Distributed or re-centralised power?	14
Blockchain applications	14
Land rights	14
Digital Identities	18
Remittances and global transactions	21
Regulating the flow of crypto assets	22
Blockchain, provenance, and logistics tracking	23
Digital literacy as a prerequisite to harness the blockchain's potential	24
Methodology	24
References	26

About the author

Per Aarvik

Per is an independent writer on applied digital technology for humanitarianism, development, governance and anti-corruption. Social media data, satellite imagery, geographical information systems, and applied artificial intelligence are among his interests. He holds a Master's degree in Democracy Building from the Department of Comparative Politics, University of Bergen, Norway. His thesis focused on the potential of crowdsourced civil society election monitoring as a tool to combat election fraud. His background is from journalism, advertising and higher design education – as a practitioner, educator, and in managerial roles. In recent years he has led digital humanitarian work during disasters and in democracy projects.

Acknowledgements

Niklas Kossow, PhD at Hertie School, The University of Governance in Berlin, and Jan Isaksen, CMI Emeritus, have contributed valuable inputs and comments to the report. Thanks also to Arne Strand, director of U4, for his guidance and conversations in the making of the text.

Abbreviations

AML – Anti-Money Laundering

CBDC/NDC – Central Bank Digital Currency also referred to as National Digital Currency

CDD – Customer Due Diligence

CFT / CTF – Countering the Financing of Terrorism / Counter Terrorist Financing (used)

DBVN – Decentralized Borderless Voluntary Nation

DAO – Decentralized autonomous organisation

FATF – Financial Action Task Force

Fork – A blockchain fork is the split occurring when consensus is not reached on a new block

GDPR – General Data Protection Regulation (Europe)

ISA – Information System Authority (Estonia)

KYC – Know Your Client / Know Your Customer

NAPR – National Agency of Public Registry (Georgia)

P2P – Peer-to-Peer networks without a central hub or decision maker

PoS – Proof of Stake – consensus algorithm in blockchains such as Ethereum

PoW – Proof of Work – consensus algorithm in blockchains such as the Bitcoin

VA – Virtual Asset / Virtual Goods – non-tangible assets or goods

VASP – Virtual Asset Service Provider

Stablecoin – A cryptocurrency linked to fiat currencies or other values for stability

SSO – Single Sign On – offered by corporations such as Google, Facebook or Twitter

SSI – Self Sovereign Identity – ID system proposed by Blockchain Bundesverband, Germany

Bitcoin, cryptocurrencies, and the blockchain technology behind them, have gained a lot of attention in recent years. Bitcoin was introduced in 2008 when trust in financial institutions was at its lowest. The technology was later repurposed for thematic areas other than digital currency. Some experts predicted that blockchain technologies would end poverty, eliminate corruption, and provide financial inclusion for all. Things have changed. Financial institutions and digital corporations are adopting the technology to increase efficiency and to create new financial products.

Blockchain technologies are attracting development organisations and anti-corruption communities because of their potential to prevent corruption and protect public registries from fraud and tampering.

Blockchain technologies also attract development organisations and anti-corruption communities as tools that can potentially prevent corruption and protect public registries from fraud and tampering. These technologies have even been suggested as a tool to fulfil Sustainable Development Goals (SDGs) related to legal identity and financial inclusion. In humanitarian contexts, the blockchain has, in some cases, replaced traditional banking services to reduce transaction costs and to facilitate tracking of funds and audits in cash-based interventions. Diamonds, luxury objects or gemstones are recorded on blockchains to provide proof of provenance and prevent illegal goods from entering the market. The technology has many uses and can be implemented to increase efficiency and profit, or to reduce the risk of disputes and increase traceability.

Blockchain is the underlying platform for Bitcoin and other cryptocurrencies. The technology, designed for a borderless digital currency, was intended to be free from the control of countries and financial institutions, which are now adopting it and modifying it to fit their needs. Digital currencies such as the Libra, part of a project launched by a consortium of companies and NGOs, challenge lawmakers and regulators.

Blockchain is a method for storing records, where cryptography is used to link data in a chained structure. Through its verification mechanisms, the blockchain promises to establish trust where trust is absent. Its distributed nature, where a ledger is duplicated among several nodes, prevents unnoticed attempts to falsify records.

Because of its potential and its different applications, the technology generates diverging, if not contradicting, opinions. Enthusiasts describe it as a “revolution in trust,” while sceptics criticise it for potentially leading to a society trusting code and

technology more than humans. Some view blockchain as the most “promising disruptive technology in the fight against corruption” and as a reliable alternative in countries where data maintenance is poor and corruption rampant. Others warn against deploying it unless a number of prerequisites are in place, such as internet connectivity, digitised public records, and a tech-savvy population.

The following U4 Issue attempts to identify core functions of blockchain technology and to evaluate its applicability in anti-corruption and integrity-related projects.

An overview of blockchains and cryptocurrencies

The blockchain and Bitcoin: A brief history

A paper on the issue of time-stamping a digital document describes how, in the early 1990s, cryptographers tackled the problem of certifying the authenticity of digital content such as text, video, or audio. Digital content could be easily modified or duplicated. It was difficult to certify the date of creation or alteration of a certain document or file. The proposed solution was to digitally timestamp documents and link these “certificates” in a chain using cryptography and digital signatures. The aim was to make it impossible to back-date or forward-date digital content and thereby to provide proof of authenticity. The concept was further developed, clustering several documents in groups – or blocks. The term blockchain was coined.

Almost simultaneously, electronic cash started making its appearance. Ecash first appeared in the mid-nineties and was used for micropayments. The technology was adopted by some European banks, such as Credit Suisse and Deutsche Bank, but later abandoned.

The predecessor of Bitcoin was the Bit Gold, which, however, never reached markets. In 2008, a famous white paper, written under the pseudonym of Satoshi Nakamoto, described a radical, libertarian, global, and entirely digital currency. The currency would not be governed by any institutions, but managed by a network of volunteer stakeholders, bypassing central banks.

Although Bitcoin is the most well-known cryptocurrency and one of the first players to appear in the crypto money world, there are now hundreds of competitors. All

transactions ever made are visible on the Bitcoin blockchain. They are written on the ledger, clustered in blocks, and linked to each other in an unbreakable chain by the use of cryptographic hashes. The complete ledger is replicated among all full nodes in the network. The nodes are the computers running the software behind Bitcoin. A computational algorithm is used to prevent double spending of coins, ensure that only valid transactions are accepted, and protect the blockchain from attacks. This is the consensus mechanism, which is crucial to ensure trust in the blockchain.

Consensus mechanisms

When new transactions are made, they are communicated to all nodes. A computational challenge is used as a consensus mechanism aiming to agree on the cryptographic hash for the next block and verify the transactions recorded in the previous block. The work is rewarded with transaction fees and new Bitcoins. This process is referred to as “mining.” Different consensus mechanisms are at play for different types of blockchains.

Proof of Work (PoW) is the original consensus mechanism behind Bitcoin. It includes a mathematical task which is time-consuming and demanding in terms of computational power but where the desired result is easily detected. The result has to be a cryptographic hash with a value equal to or lower than a predefined target. This target is set by the network and adjusted so that a new block is added to the network about every 10 minutes. The hash is found by trial and error, by inserting an integer in the algorithm, a “nonce” or a number used only once. The first node to identify this value, is given the right to name the next block in the chain. The task is rewarded with coins, hence the term “mining.” The computational costs of fraudulent behaviour are designed to be higher than the potential gains. Trust is secured by the programmed structure of the network. The PoW algorithm typically enables 5-8 transactions per second. This poses a major scalability challenge for Bitcoins.

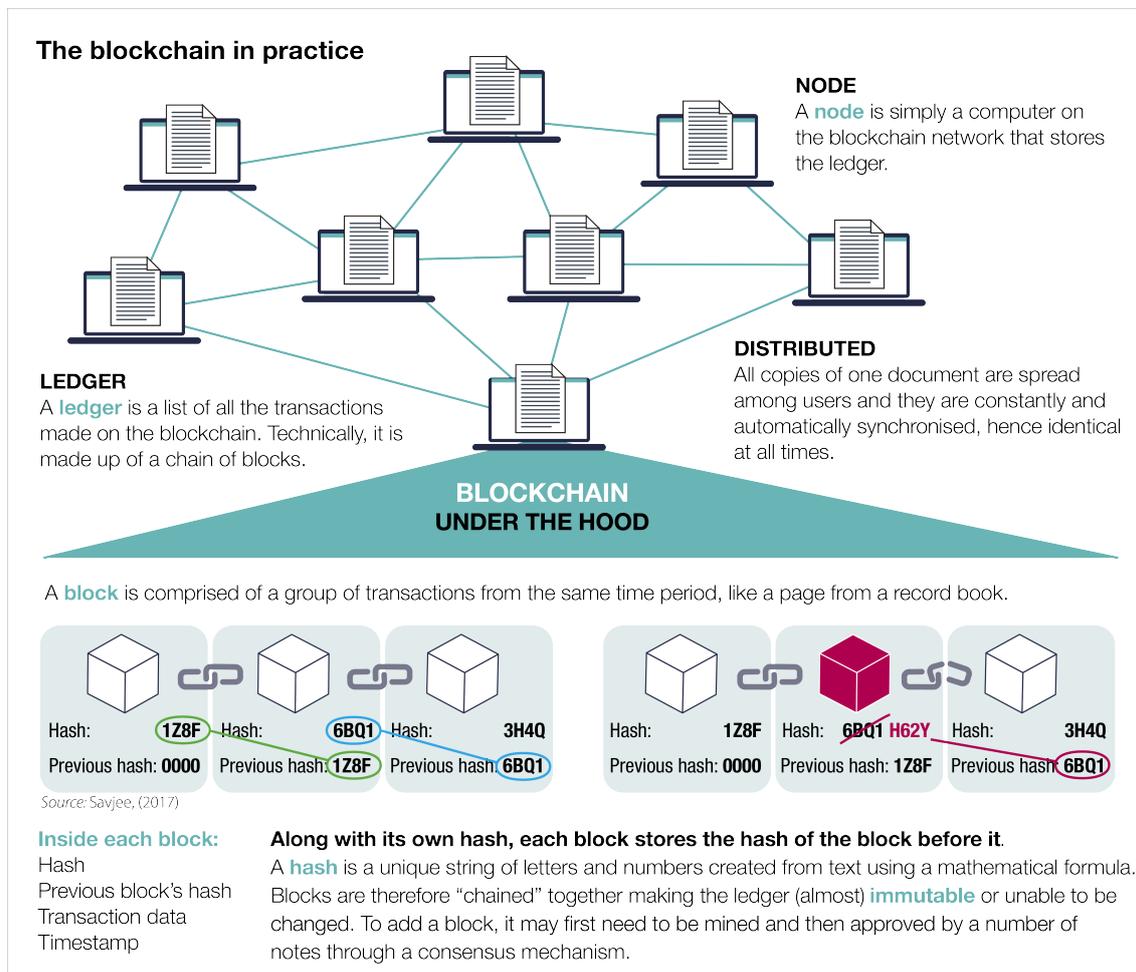
An alternative verification method called Proof of Stake (PoS) selects a random number of nodes to perform validation. The nodes have to lock up funds to be selected. These funds are released after the calculations are completed and the new blocks are accepted. Compared to PoW, PoS can cut energy consumption by 99%. The Ethereum blockchain is planning to convert to PoS in 2020.

Finally, a method called Proof of Authority (PoA) is driving the verification process in some private blockchains. In PoA systems, one or more of the nodes have the authority to verify and add blocks. As explained in a post on the subject, this method does not

provide the benefits of a fully distributed public blockchain but can handle far more transactions per second for a significantly lower computational cost.

Holders of cryptocurrencies or other digital documents access and manage their assets through a digital wallet. The software can run on a laptop, tablet, or smartphone. The access codes are often kept offline for security reasons, for example on a specialised USB stick. The wallet holds cryptographic keys to access assets on the blockchain. If the digital keys are lost, there is no way to restore them in an open blockchain. Without any form of central governance, individuals are fully responsible for their own assets.

The blockchain in practise



The ledger of all transactions in a blockchain is duplicated to all participating nodes in the network. The cryptographic hash of one block is included as content in the next, shaping a chain which can't break without being detected. (Illustration cred. OECD Blockchain Primer)

Power consumption and energy footprint

The Bitcoin Energy Consumption Index provides updated footprint calculations for the cryptocurrency. Bitcoin mining uses the same amount of electricity consumed by

countries like Chile or Austria – about 77 Terawatt-hour (TWh) annually. A single transaction equals the electricity consumption of three weeks of the average US household, close to 650 kilowatt-hour (kWh). Much of the mining happens in China, where coal-fuelled electricity adds to the carbon emissions. The global carbon footprint of Bitcoin mining matches New Zealand’s total annual emissions – more than 36 megatonnes of CO₂.

The algorithms that verify transactions and the search for cryptographic hashes to name new blocks are complex activities that demand a huge amount of computing power. This is a consequence of the PoW consensus mechanism. The electronic waste, amplified by the need for the latest and fastest hardware, further reduces the sustainability of the cryptocurrencies using the PoW protocol.

With a maximum rate of only 5-8 transactions per second, blockchains relying on the PoW consensus mechanism also have a scalability challenge. VISA, for instance, handles an average of 1,700 transactions per second. PoS or PoA are less costly, more energy efficient and also better able to handle a greater number of transactions. Different consensus mechanisms or reduced numbers of nodes could compensate for the scalability and energy problems.

A McKinsey report from 2018 acknowledges that distributed ledgers may serve niche applications “within insurance, supply chains, and capital markets, in which distributed ledgers can tackle pain points including inefficiency, process opacity, and fraud.” But for most applications, including international payment systems, they suggest simpler solutions.

Sovereign and corporate cryptocurrencies

Hundreds of alternative cryptocurrencies based on blockchain technology have emerged since the creation of Bitcoin. Some have a setup similar to that of Bitcoin, others are linked to a government-issued currency, a fiat currency. Bitcoin has some major challenges connected to its slow transaction rates, energy-consuming computational complexity, and its vulnerability to speculation resulting in short term volatility. Stablecoins are an attempt to avoid issues of volatility. They are in fact backed by a reserve, much like fiat currencies are supported by a central bank. Venezuela has, for example, issued its own sovereign cryptocurrency, the Petro. Backed by oil reserves, the Petro was meant to be a stable asset to meet the challenges of a free-falling Bolivar and avoid US sanctions. It has not been a success, and citizens now flock to other cryptocurrencies as a refuge against hyperinflation.

The most recent cryptocurrency project which gained attention and triggered concern by regulators is the corporate cryptocurrency Libra. Facebook has formed a consortium of tech companies and NGOs to govern the development of Libra. The currency is meant to be backed by fiat reserves. But the project has received mixed reactions. A currency managed by a giga-company such as Facebook with its 2,4 billion users could overnight become a powerful financial player, possibly the world's largest bank. The currency could overrun small sovereign currencies and deprive governments of control over their financial systems. Regulators are following its development carefully, concerned about a currency detached from the ordinary financial system.

During the OECD Global Blockchain Policy Forum in 2019, the French Minister of Finance, addressed similar concerns for a private, global currency and stated that France would reject the development of Libra on European soil. Major partners such as Visa, Mastercard, and PayPal have pulled out of the project.

A few months later, China's president Xi Jinping encouraged the development of blockchain technologies during a speech to the Central Committee. He stated that China will "seize the opportunity" and support blockchain research, development, and standardisation. His speech signals a change in attitude of the Chinese leadership. Since 2017, the use of Bitcoins has been banned in China. Still, the country hosts a substantial portion of Bitcoin miners, and has initiated work to develop its own digital currency. Public support for blockchain has triggered speculations on whether China will launch its own cryptocurrency, the e-Yuan. An article covering this issue discusses the implications this move would have in China, especially in terms of monitoring financial flows and preventing money laundering and tax evasion. If a digital currency replaces cash, the government would theoretically be able to monitor all payments made with the e-Yuan.

The Swedish central bank has, since 2017, been investigating the need for, and the effects of, a state-backed digital currency. In February 2020, the bank announced a collaboration with Accenture on a pilot project aimed at finding technical solutions that would back a Swedish sovereign cryptocurrency. The technical requirements guiding the pilot project note that: "The solution is based on digital tokens (e-kronor) that are portable, cannot be forged or copied (doublespent) and enable instantaneous, peer-to-peer payments as easily as sending a text." The recent sharp decrease in the use of cash in Sweden and the need for a digital alternative may explain the push behind the e-krona project. The project is currently in a testing phase which may last one year. Once this phase is over, political discussions and decisions will follow.

The European Central Bank (ECB) is also experimenting with an electronic Euro. But while in Sweden the use of cash is rapidly declining, 79% of sales in Europe are still based on cash. Because Europe has a very efficient banking system, the ECB struggles to find incentives that are strong enough to justify the introduction of an e-Euro. Still it “has established a proof of concept for anonymity in digital cash, referred to ... as ‘central bank digital currency’.”

The four major types of blockchain

Blockchains have over time developed into several different types. Whether they are open or closed, centralised or distributed, their qualities determine functionality and energy consumption levels as well as consensus mechanisms. There are four major types of blockchains. Each fulfils different purposes.

- The **public, permissionless** blockchain is open for anyone to sign into. It is typical of cryptocurrencies such as the Ether or Bitcoin. The security measures it requires demand significant computing resources, leading to high energy consumption and scalability challenges.
- The **public, permissioned** blockchain is open for all to read, but only a permissioned group has the ability to write records. This type of blockchain may be used for supply chain management or provenance registries. Security measures are simpler, transaction rates higher and energy consumption low.
- The **closed, permissioned** blockchain, where only authorised participants are granted access, typically serves companies collaboratively sharing a distributed ledger.
- The **private blockchain** is controlled by one entity. Access to this type of blockchain is strictly supervised. It is often used for distribution of cryptocurrencies and tokens in humanitarian aid initiatives. The functions of private blockchains resemble those of a traditional database in that control is centralised. Their unique feature is that records are stored in an “unbreakable” chain.

The Ethereum blockchain, with its currency “Ether,” entered the stage in 2015. Although Ethereum is a decentralised network, the Ethereum foundation has some form of oversight of its blockchain and currency. The Ethereum blockchain can hold any kind of text and code, not just a ledger of timestamped transactions. The software therefore enables so called “smart contracts.” Smart contracts are small applications governed by agreements. They can execute automatically when given conditions are met, for example by fulfilling escrow agreements in a real estate transaction.

In late 2015, the Linux community, joined by IBM and Intel, founded the Hyperledger project. This is a private blockchain governed by one or more entities. The Hyperledger consists of several specialised frameworks. One of them, the Hyperledger Fabric, is the most frequently applied framework and promises to be a tool for financial applications or for provenance and supply chain traceability. It is well known as the platform used to track the provenance of diamonds.

Confusing definitions

The definition of a blockchain as a decentralised database distributed on a network of nodes and updated through a consensus protocol is limiting. Several projects fall outside this definition. The World Food Programme’s (WFP) pilot project Building Blocks has been criticised for claiming to use blockchain technology, when all it really does is use the database element of the technology. There is no consensus mechanism at play and until recently the network consisted only of WFP hosting the database on a few servers simulating a blockchain.

As an example of existing confusion on definitions, the Estonian Government data-sharing system, the X-Road, is often classified as a blockchain, but, *stricto sensu*, it isn’t. Some argue that a “blockchain is a decentralised and distributed database which is updated through a consensus protocol,” and that “the common factor between blockchain and X-Road is that they both use cryptographic hash functions for linking data items to each other.”

Sometimes the words “blockchain” and “distributed ledger technology” (DLT) are used interchangeably. A report discussing these terms notes that the word “blockchain” has lost its meaning and lacks a “universal definition.” There is also concern surrounding the use of these “problematic definitions” by regulators or lawmakers as a way “to pass some sort of legislation to demonstrate how crypto-friendly or tech-savvy they are.” When proper definitions are not in place, it becomes challenging to develop clear frameworks and precise legislation to regulate the sector.

A benchmarking study on blockchain affairs across the financial services industry tries to sort out the confusion by clarifying the various terms. The study describes a growing industry with new actors from various backgrounds and shows how the development of the technology is about to enter its production phase, which, especially in the finance sector, is generating a natural push towards establishing working concepts. In the study, the terms “blockchain” and “DLT” are used interchangeably, still presenting precise properties of a distributed ledger technology. DLT is a “multi-party consensus system

that enables multiple distrusting entities to reach agreement over the ordering of transactions in an adversarial environment without relying on a central trusted party.” They specify five criteria to support the definition:

1. Multiple entities (computers) need to be able to create new records.
2. Entities need to reach agreement on the ordering of records.
3. Each entity needs to independently be able to validate records.
4. Each entity needs to be able to detect unauthorised changes to the records.
5. Entities must also be able to detect changes in consensus over records.

Only a few functioning systems today comply with these criteria. The authors of the study recommend against using the term “blockchain” for systems only applying parts of the technology. Yet, 77% of current projects use the terms “blockchain” or “DLT” without being neither decentralised nor dependent on multiparty consensus.

A working paper series on blockchain economics explains the Blockchain Trilemma. **Correctness, decentralization, and cost efficiency** are three qualities that should ideally be found in any record-keeping system. The paper suggests that no blockchain ledger can satisfy all three qualities at the same time and points to the computational challenge in verification and consensus in a fully decentralised blockchain. On the one side, this process leads to high costs. On the other side, leaving verification of records to a few trusted nodes saves cost, but loses the idea of a fully distributed power of decisions.

Prerequisites for blockchain technologies

While there is enthusiasm surrounding the potential applications of blockchain technology, not all contexts have the right conditions for it. In the last five years, digital land registries have emerged as a popular field of application.

A review of several projects that are incorporating blockchain technology into public registries offers an understanding of the prerequisites that may need to be in place for the technology to be successful. Records need to be digital, which in many cases entails a cumbersome process to digitise paper documents. When disputes over conflicting information, such as rights to ownership or use of land are solved, information should be as correct as possible.

A secure, digital identity needs to be in place to establish a strong connection between a person and their assets. A system enabling multiple signatures and allowing alterations

by entities other than the owner is preferable for property registries. If the sole owner of an asset dies, a trusted entity should be able to transfer ownership. For digital registries to be functional and transparent, users need access through an internet connection or mobile broadband. Finally, the owners of the assets, just as much as anyone engaging with regulations or conflict solving, are helpless without the digital literacy necessary to access and manage registries.

The need for digital literacy, laws and regulations, or political decisions might be more challenging for a digitalisation process than the technology itself. According to a working paper on blockchain and property: “Blockchain is unusual in that it is a social technology, designed to govern the behaviour of groups of people through social and financial incentives. It is therefore inherently political in a way that few other technologies are.”

Properties of blockchain relevant for anti-corruption

Corruption in the public sector leads to a lack of trust between citizens and government institutions. Transparency of government decisions and open public registries can facilitate the monitoring of registries and reduce the risk for corruption.

The blockchain promises tamper-proof records that corrupt clerks or bureaucrats cannot modify. The distribution of a ledger and the consensus mechanisms also make it difficult for one entity to falsify entries. An article featured in the World Economic Forum states that, “while the scalability of those solutions remains challenging, blockchain has emerged as the most promising disruptive technology in the fight against corruption... It possesses important features that can help anchor integrity in bureaucracies, by securing identity, tracking funds, registering assets, and procuring contracts.”

When corruption represents a breach of trust, a technology that strengthens trust becomes an attractive solution in public projects.

When corruption represents a breach of trust, a technology that strengthens trust becomes an attractive solution in public projects.

Trust in people and trust in code

The continuous decline in confidence towards governments and policymakers in many western societies has raised concerns for the health of our democracies.

In the online commerce arena, online trust became a key asset for transactions between strangers. With the advent of the sharing economy, trust was mediated by online platforms. Not only was trust a necessary element of online transactions, but it also became part of in-person interactions: booking a room in the house of a complete stranger, couchsurfing, riding in somebody else’s car. Trust has even been dubbed the “currency” of the sharing economy.

Artificial intelligence systems, blockchain technologies, or smart, self- executing contracts represent yet another test for people’s trust in technology. When analysing digital tools, trust is highly dependent on the quality of the code underlying each specific tool. Experts recommend a cautious approach towards online, digital tools, especially in complex and sensitive contexts, as shown in the recent Iowa Democratic Party caucuses in February 2020.

Trust is now dependent on the quality of the code. Those with the competence to alter the code are in control. Poorly written code, insufficient testing, security breaches, or hacker attacks challenge the confidence people have in decision-making systems. Researchers are developing mechanisms to study and evaluate the trustworthiness of code.

Trust in gatekeepers

The bitcoin blockchain was designed to reduce the dependency on institutions. Trust lies in the algorithms managing consensus between the nodes of the blockchain network. Code is the law and the enabler of trust. The technology has been called a “trust-machine.” However, some experts add nuance to this definition. Without trust in the technical devices that host them, or in the programmers and code, the whole blockchain loses credibility.

The natural habitat of a cryptocurrency is cyberspace. It’s within those digital boundaries that trust is secured. If Bitcoins were to leave cyberspace and were to be converted into fiat currencies, there would need to be an oversight entity to supervise transactions. Similarly, if the blockchain is securing physical records (for example for land, diamonds or human beings) trust in those who enter the records in the blockchain

becomes critical. The incentives for good behaviour reside outside the blockchain and its codes. Trust in governance bodies is a must.

An immutable record



For blockchain data to have any value, it must be entered by a trusted person or operator. Whether it is for precious minerals, land title, or a refugee status – the person or office who creates the record is equally important. As with a Babylonian clay tablet, a blockchain record may never change (Photo: Wikipedia, Public domain).

When blockchain records represent values or objects from the physical world, trust needs to go beyond the digital sphere. The person or operator entering data must be trusted for the data on the blockchain to have any value, as does the person or office creating a record (whether it's for precious minerals, a land title or a refugee status). If this system fails, what remains is a false, immutable record. Just like the clay tablet above, a record on a blockchain may never change.

Without trust, the ledger itself is worthless. Radio-frequency identification (RFID) tags or biometric data are meant to secure the link between a physical entity and its digital representation. But there still needs to be an individual doing the iris scan or attaching the RFID tag to the object and making sure it stays there. When the blockchain record describes a piece of land, it can only be trusted if the information matches reality. As stated in a working paper series on blockchain economics: “While blockchains can keep track of ownership transfers, enforcement of possession rights is still needed in many blockchain applications.”

Transparency vs privacy

Transparency is frequently referred to as one of the advantages of blockchains. It is an essential element of both a blockchain and any anti-corruption effort. All transactions in an open blockchain are searchable. Every coin mined in a cryptocurrency and put in circulation is accounted for. The verification mechanism is preventing they are spent twice. Consensus among the nodes in the network ensures that the registered transactions are correct.

Transparency is an essential element of both a blockchain and any anti-corruption effort. Because of their transparent nature, blockchains hold a lot of promise.

Bitcoin exchanges in some countries need to comply with Know Your Customer (KYC) regulations. This does not mean that the asset holder is revealed to all other users, but that the exchange may have to identify customers for inspecting authorities or alert authorities about suspicious transactions.

In government procurement systems, a blockchain ledger could record and secure key events in a procurement process. This would prevent tampering and allow for audits of the process, extending what already is available in open procurement systems. Property and company registers, procurement data, or provenance records are areas considering the use of blockchain technologies because of their transparent nature.

But the EU General Data Protection Regulation (GDPR) may prevent certain information from being recorded in a transparent blockchain. Revealing identifying data, such as information of an individual farmer in a transparent supply chain system, may conflict with privacy regulations. In a competitive market, companies might also prefer to protect information about their providers, clients, and other business relations. A KPMG report for the OECD analyses the tension between transparency and privacy and urges for some form of negotiation when choosing between open and closed blockchains. In principle, a blockchain never forgets – as the records in a chain cannot be removed without breaking the chain. Because of this immutable trait, the “right to be forgotten,” also covered by GDPR regulations, may have implications for blockchain projects that include personal identity information.

Ernst & Young claims to be able to meet these needs by enabling privacy even on public blockchains. Their recent transaction protocol, [zero-knowledge-proof \(ZKP\)](#), promises private transactions on a public blockchain.

Distributed or re-centralised power?

On September 15, 2008, just before the Bitcoin white paper first emerged, Lehman Brothers filed for bankruptcy. The global financial crisis unfolded and trust in central, financial institutions crumbled. The libertarian idea behind blockchain technology and distributed ledgers is closely linked to the declining trust in these institutions.

Redistribution of power and the exclusion of central, controlling companies from the financial system seemed to be a viable alternative to influential but unreliable players.

Fully distributed ledgers can, among other benefits, prevent powerful actors, such as large corporations, from exclusively controlling a certain market or sector. This in turn, can help prevent corruption. The Bitcoin blockchain was meant to create these conditions. But after a decade, Bitcoin's number of verifying nodes is decreasing, clustering the power of the network in fewer entities. [Some argue](#) that “political power on the blockchain is not truly distributed, but rather re-centralized in a ‘tech elite’ – creating a new avenue for corruption through the abuse of their powers.”

Hash power, or the capacity to calculate cryptographic hashes, is a measure of power on the Bitcoin network. [According to a report about hash power in China](#), about 65% of the global hash power resides in China due to affordable electricity and access to the latest generation of hardware. Indeed, a major fear in the Bitcoin community is the threat of a so-called [51% attack](#), where 51% of nodes collude in order to rewrite the chain and re-distribute assets. This is not a realistic threat at the moment but might become one if the number of nodes drops and gets concentrated in one particular country or is controlled by a few companies.

Blockchain applications

Land rights

An article on a blockchain-based land titling project in the Republic of Georgia notes that: “The challenge for countries without adequate land management is not simply to build a land registry system but to create a system that is trustworthy, efficient, and free

of corruption.” Land and property rights are a combination of legislation and local, historical customs. A register details who owns a particular piece of land, but also who may access it at particular times of the year or under particular conditions. Seasonal land rights, as those described in a [study of Northern Kenya](#), are only one example of how access and rights to land, water, pastures, hunting grounds, minerals, or forests are a highly complex matter. Describing this intricate set of traditional rules and including them in a modern registry is, according to the Food and Agriculture Organization (FAO), a power game in which poor, rural communities are more likely to lose. Governments may grant access to land for commercial or development purposes, ignoring unwritten rights of rural communities. The 2010 FAO report on [statutory recognition of customary land rights](#) investigates best practices on how to formalise century-old informal rights.

Once there is agreement on laws and regulations and trustworthy institutions to execute them, once disputes over land rights are settled, once maps and agreements are entered into the ledger, only then a timestamped proof of rights may be suitable to be registered in an immutable, distributed ledger such as the blockchain.

The land register of Georgia

Georgia is frequently mentioned as a country with a land registry residing on a blockchain. This is slightly misleading. When the company Bitfury approached the government of Georgia offering a test to adopt blockchain technology as a security measure for its registry, the land-management system was already far developed.

As shown in an [Openaid graphic](#), international donors contributed significantly to support the development of government and civil society in Georgia in the last decade. This included creating strong, non-corrupt institutions. In 2004, the National Agency of Public Registry (NAPR) was established under the Ministry of Justice to reform and digitise the system for land management. Legislative, institutional, administrative, and technological sectors were modernised and digitised. What was known to be a slow, bureaucratic, and corruption-prone country has now become a model for many. Georgia is seventh on the World Bank Doing Business Ranking and has climbed significantly on the UN E-Government Development Index as well as on the Transparency International (TI) CPI index. And the climb started long before blockchain arrived in the country.

In 2014, ten years after the modernisation of land management started, the San Francisco-based company BitFury [established a Bitcoin mining facility](#) in Georgia, betting on cheap electricity and favourable tax regulations. The company established similar bitcoin mining operations in [Norway](#), Iceland, and Canada for the same reasons. As described in a [New York Times article](#), Bitcoin mining turned into a valued activity

in Georgia and thousands became familiar with the technology – for a while there was more money in bitcoin mining than farming.

In 2016, BitFury signed a contract with NAPR to design and manage a public, permissioned blockchain residing on the Bitcoin blockchain, which would secure and timestamp notarised documents and contracts. Land and property owners would thereby have immutable proof of ownership and transactions, and constant access to their records through an encrypted (hashed) entry on the blockchain. Later on, BitFury developed a new blockchain with a modified security protocol. In doing so, they also lowered the consumption of electricity to run the system. The Exonum blockchain is in fact able to handle far more transactions per second than the Bitcoin blockchain. Exonum is now applied for securing proof of ownership to land in Georgia.

The transition from a paper-based to a digital land rights registry would not have been possible had it not been for the high quality of data developed over more than a decade. According to the previously cited [article on blockchain-based projects in the country](#), “the high quality of the NAPR data was a consequence of the political reforms pursued by the Republic of Georgia before the project.”

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) and its [Blockchain Lab](#) are some of the supporters of the reform project in Georgia, and emphasise political will and adaptation of regulations as important elements for its success.

Blockchain-based pilot projects

The Swedish Mapping, Cadastre and Land Registration Authority has, together with private sector companies, experimented with blockchain and smart contracts to improve real estate transactions and mortgage deed processes. These processes are slow and involve multiple entities such as banks, brokers, and the notary office. Converting to smart contracts and a blockchain-secured process would save a significant amount of time and cost in a real estate transaction process. Sweden aspires to being at the [forefront of technological development](#). Their land registration system dates back to 1628 and has, for centuries, been considered a positive example of a system capable of innovating and improving services.

The Swedish land registry



Georgia's land registry resides on a blockchain. High quality data has made this possible, perhaps not dissimilar to the depicted 18th-century Swedish registry page (Photo: Swedish National Archives).

Full implementation of a blockchain test performed in 2018 will demand further developments. The blockchain technology will have to match the need for a functioning real estate transaction system and align with other government databases and with EU regulations, such as those outlined in the GDPR. There are legal considerations and a need for new legislation to be in place for digital contracts, digital signatures, and other aspects of a totally digital real estate trade system. The project is now in preparation for political considerations and decisions.

Blockchain-based land registries have been suggested for several countries, including Honduras, Brazil and Ghana. In 2015, USAID supported a project in Honduras, aiming to solve conflicts, disputes, and fraudulent appropriation of land. But the prerequisites for implementing a blockchain were not in place. Presidential elections in the country put the project on hold only a couple of years after its initiation.

The government-run tech company SERPRO investigated the use of blockchain to replace Brazil's partly paper-based and fragmented land records, but an internet search could not even locate updated information on the project.

Similarly, blockchain was proposed as a solution for the land registry of Ghana, but not much came from the project "besides the fact that the Ghanaian government signed the MoU in 2018," as reported during the 2019 OECD Global Anti-Corruption & Integrity Forum.

Digital Identities

Estonia's X-Road

Estonia was among the first countries to issue a digital identity authenticated by the government. With the mandatory ID card, citizens can access government services and personal data residing in both private and government databases. The X-road software links up with and gives access to the e-services. The project started in the 1990s, during the rebuild of government institutions after the liberation from the Soviet Union. The intention was to design a cost-efficient governance system, giving digital access to government services to all citizens. Another objective was to provide increased transparency and accountability. There are separate databases for separate sectors, such as law, policing, health, voting, and education. Citizens are given access through the X-road, which is the “digital highway” providing interoperability between connected services. The connections are end-to-end encrypted, and hashes are used as identifiers for accessed information. The Nordic Institute for Interoperability Solutions (NIIS) clarifies that the X-Road is not based on blockchain technology, rectifying statements made in a New Yorker article. Encryption and cryptographic hashing to link data elements predates Bitcoin and the blockchain.

Estonia is also the first country to issue an e-residency, where anyone who wants to register a business in the country can apply for a digital citizenship. Since the late 1990s, the country has climbed steadily in international rankings, such as the Ease of doing business ranking or the Corruption Perception Index (CPI). With a 2018 score of 73 on the CPI, Estonia is among the twenty least corrupt countries in the world.

India's digital ID

The largest biometric ID project of its kind is the Aadhaar digital ID project in India. Officially, registration is voluntary. However, certain programmes, like the kerosene subsidy or education services, are not accessible without it. Aadhaar is a 12-digit number issued at random by the Unique Identification Authority of India (UIDAI). To obtain the number, individuals need to submit demographic information (such as name, age, and gender), as well as biometric data (ten fingerprints, two iris scans, and facial photography). The private company IndiaStack is powering most Aadhaar applications and wants to spread the technology globally. Some question the close connection between government entities and private interests. Others fear that access to these registries may become a powerful tool for surveillance. Another Indian entity, resembling the Estonian X-road, is OnGrid. It gives users secure access to their records, such as educational certificates or employment verifications.

Self-sovereign identity

The Sustainable Development Goal [SDG 16.9](#) aims to provide a legal identity for all, including birth registration. Several pilots and initiatives have been launched to contribute to this goal, and blockchain technologies are being considered as a tool to provide a digital ID.

[ID2020](#) is an alliance that includes companies like Accenture, Microsoft, Gavi, and IDEO and is supported by the Rockefeller Foundation. The alliance works towards providing a digital ID for the 1,1 billion people who lack proof of identity. The ID2020 manifesto states that “... Individuals need a trusted, verifiable way to prove who they are, both in the physical world and online.” ID2020 explores if “cryptographically secure, decentralized systems — could provide greater privacy protection for users, while also allowing for portability and verifiability.” In early 2020, the first version of their technical requirements was published online, with an invite for stakeholders to comment and give input. The project stresses that “individuals must have control over their own digital identities, including how personal data is collected, used, and shared.”

Self-Sovereign Identity (SSI) is the idea behind ID2020. Its genesis are the challenges a citizen of the modern, connected world has in maintaining a myriad of online identities. In contrast to the centrally stored identities in the Indian Adhaar system, SSI is based on concepts derived from the structure of the internet – where any single machine can connect with any other. To be truly global, such a system has to be based on agreed upon identification standards. The most current one is the [Decentralized Identifier \(DID\)](#) developed by the World Wide Web consortium and supported by major companies and organisations, including the ID2020 alliance.

Blockchains for humanitarian aid

The UN Refugee Agency (UNHCR) has compiled a full set of tools for collecting biographic and biometric information for identity systems aimed at providing refugees with access to assistance. The [PRIMES](#) ecosystem is interoperable and covers a whole chain of services, from registration of refugees to cash-based assistance.

The World Food Programme (WFP) included the ID part of the toolbox in a project known as [WFP Building Blocks](#), serving Syrian refugees in Jordan camps. Building Blocks is built on a private, permissioned blockchain and tied to the UNHCR identification system. Moving the “cash for food” programme over to their own system saved WFP close to [one billion US\\$](#) in fees previously paid to credit card companies for ATM cash transfers. In addition, WFP now has a record of every single transaction,

although not linked to the individual. The project has passed the pilot study phase and is in production for more than 100,000 refugees in Jordan.

Blockchains for financial inclusion

Kiva, a crowdfunding non-profit organisation, has signed a contract with the government of Sierra Leone to provide its citizens with access to Kiva's micro-finance platform. The organisation will provide a digital ID based on the voter registration database created for the 2018 elections. Each individual will carry a physical ID card in addition to a digital wallet, preferably installed on a smart phone giving access to micro loans. This ID will connect to a distributed ledger, the Kiva protocol, used for documentation of the user's credit history. The Kiva protocol can normally be accessed via a smart phone app. In Sierra Leone, the plan is to make the Kiva protocol available at service points and in banks, since it is unlikely that all users will own a smartphone. The UN has injected a total of 15 million US\$ into the project.

Sierra Leone has a population of 7,9 million and as many as 6,9 million mobile connections. According to GSMA intelligence, 54% of the population has access to a mobile broadband, but only 9% uses the internet, which tells us something about digital literacy. Two-thirds of individuals over 15 are illiterate according to the Human Development Index and 52% are living below the poverty line of 1,9 US\$ per day.

An article published by frontiers in Blockchain takes a close look at both the Kiva project in Sierra Leone and the WFP Building Blocks project for Syrian refugees, stating that “as demonstrated by the Kiva and WFP case studies, identity is inherently use case dependent. Interoperability and standardization will be important for scale, but the success of a particular identity application will depend on how its deployment is tailored to the use cases and local conditions.”

The article provides an in-depth discussion of digital identities, self-sovereign identities and blockchain technologies and notes that “a true self-sovereign identity system would require a certain level of infrastructure, primarily high penetration of affordable smartphones that can securely store private keys and reliable connectivity.” The phones needed for the system are definitely not affordable, and in fact cost approximately 250 US\$.

A farmer in Sierra Leone would ideally own a smartphone to accomplish the task of borrowing money to buy seeds. Without it, the farmer would have to rely on the Kiva office, the service point, or a bank to obtain digital credentials and eventually access funds or loans. Having to rely on others for help in this scenario could create opportunities for corrupt mechanisms such as bribery.

Grassroots Economics in Kenya has a slightly different strategy. Based on cooperatives in local communities, microloans and a local “currency” are available for interactions between small-scale industries. Since 2010, the concept has developed into seven different currencies in different locations in Kenya.

Remittances and global transactions

The SDGs also cover remittances and their positive impacts on families, communities and countries. Transfers using cryptocurrencies may reduce transaction fees charged by traditional brokers. According to the International Labour Organization (ILO), there are 160 million migrant workers in the world. Most of them regularly send money home. Borderless cryptocurrencies would suit their needs perfectly. In Hong Kong, migrant workers can convert their funds into a cryptocurrency when sending money to their home country, where it then converts into the currency of the receiving country. Regulatory uncertainties and liquidity issues are obstacles in what could become a large industry. In the example above, crypto exchanges eventually would require transferring fiat currency between countries to balance their cash stock.

The Monetary Authority of Singapore (MAS), in collaboration with J.P. Morgan and Temasek, is looking into similar challenges, not for migrant workers, but for the business market. Project Ubin is a pilot in which blockchain technologies were used for financial transactions. The first step was to migrate a certain volume of tokenised Singapore Dollars (SGD) onto a distributed ledger. Backed by an equivalent amount of SGD in custody, the digitised dollars were used to verify how digital currencies can be utilised in international transactions. As a result of the project, there is now a blockchain-based prototype “that enables payments to be carried out in different currencies on the same network.”

The strategy of Ripple is also to work with governments and regulations attempting to modernise the global flow of finances which has “more in common with the outdated postal system than this generation’s internet.” Established in 2012, Ripple is based on “the idea of using blockchain technology and digital assets to enable financial institutions to send money across borders, instantly, reliably and for fractions of a penny.” Their blockchain platform and digital asset, XRP, promise to facilitate faster and cheaper international transactions. The financial industry wants to rationalise international transactions by employing blockchain-based solutions, but without letting go of their role as mediators.

A thorough analysis of the remittance market and blockchain observes that: “As existing and incumbent financial players are flocking toward blockchain technologies for clearing and settlement of payments, existing power structures can be challenged but also reinvented and reinforced.”

Regulating the flow of crypto assets

According to the crypto-investigators at Chainalysis, illicit financing and money laundering transfers added up to billions in 2019. The company tracks flows of funds, and due to the transparency of cryptocurrency networks they are able to get an overview of the flow. While they are not able to get details of the sender or recipient, they can detect directions and flows of potentially illegal transactions by following crypto-exchanges with a dodgy reputation. “The need to launder funds is the common thread among all the forms of crypto crime we analyze.”

That said, anonymous transactions are not necessarily illegal. Wikileaks, which was blocked by banks after the exposure of diplomatic cables (Cablegate) in 2011, invites donors to use cryptocurrencies or use a proxy organisation for donations. Exactly the same is done by militant Palestinian groups asking for financial support to “circumvent international laws and sanctions.” An FDD Long War Journal article documents how militant groups instruct their donors to use Bitcoins through social media campaigns.

The EU Fifth Anti Money Laundering Directive (5AMLD) came into force in January 2020. According to the compliance company, ComplyAdvantage, the new directive now treats cryptocurrencies and providers of wallets and exchanges as it does the ordinary financial market, including the obligation to submit reports on suspicious activity. Financial Intelligence Units have the authority to obtain the identity of cryptocurrency owners, since they have to declare assets for tax purposes. The Financial Action Task Force (FATF) is developing procedures and tools for supervision of Virtual Assets Service Providers (VASPs) and monitoring how they comply with KYC/AML regulations. Since virtual assets, such as a cryptocurrency, are inherently global, international collaboration on standards, regulations, and supervision is needed. The OECD is creating awareness among tax auditors on how to discover possible money laundering, tax evasion, or terrorist financing involving cryptocurrencies. Transactions of cryptocurrencies are still possible without revealing your identity in some countries. As KYC and AML regulations force gatekeepers and crypto exchanges to register the real identities of account holders, the hope is to detect some of the illegal funds and prevent cryptocurrencies from furthering their reputation as a tool to finance crime.

Blockchain, provenance, and logistics tracking

Immutable blockchain records should hold correct data. When they represent physical goods, the relation between the record and the physical object should be immutable as well.

The Gübelin Gem Lab has developed a technique to invisibly tag gemstones with nano-sized particles at the mine. The particles penetrate the stone and traces of this “DNA” are identifiable also after cutting and polishing. The information on origin and ownership of the stone is logged on the Provenance Proof Blockchain, an initiative for documentation of gemstones. The ledger is built on the Everledger blockchain which also holds projects on minerals, luxury articles, and art. De Beers has a similar project with the [Boston Consulting Group](#). Provenance, authenticity, and traceability of millions of diamonds reside on the customised platform Tracr. The project is credited with combatting blood diamonds and restricting illegitimate stones used for terrorist financing.

[Bait to plate](#) is a pilot project residing on the Ethereum platform to investigate how trust and traceability can be achieved in the tuna fish supply chain. The pilot performed in 2018 by Consensys and supported by WWF in New Zealand, Australia, and Fiji aimed to demonstrate traceability of the valuable Yellowfin Tuna. Each fish was tagged with a radio-frequency identification (RFID) tag and could be followed on its journey to the restaurant by a journalist from [Wired](#).

According to IBM, food fraud is increasing due to lack of transparency, accountability, and effective regulations. But customers are increasingly focused on the source and production processes of their food. Through the Food Trust blockchain, IBM teamed up with the food retail chains to track products such as shrimp from India and lettuce from Arizona. According to [Coindesk](#), more than 80 brands have joined the experiment, including giants like Nestlé, Unilever, Carrefour, and Dole Food. Producers delivering to these chains are encouraged to register their shipments on the blockchain. Walmart is one of the first companies to demand registration for fresh leaf products.

But supply chain management still suffers from lack of standards to support interoperability. [A Gartner press release](#) predicts that most blockchain-based supply chain initiatives will suffer from fatigue. “A combination of technology immaturity, lack of standards, overly ambitious scope and a misunderstanding of how blockchain could, or should, actually help the supply chain” will inevitably cause the market to experience blockchain fatigue.

“Agreeing to standards” is at the basis of the TradeLens project initiated by IBM and the shipping company Maersk to log and share shipping transaction and event data. Maersk alone controls about 25% of the container traffic across the oceans and is able by itself to create an ecosystem of data. Other major ocean carriers hesitated to partner with a blockchain initiated by their main competitor. But eventually six of the world’s largest carriers joined the consortium, followed now by port authorities who are signing in on the same platform. TradeLens may become a standard tool for tracking shipping containers.

Digital literacy as a prerequisite to harness the blockchain’s potential

Blockchain technologies and cryptocurrencies can be deployed as helpful tools in anti-corruption projects. The technology can redistribute power from centralised institutions to individuals. Its code is a catalyst for trust among participants, who are fully responsible for their own assets. In an open cryptocurrency blockchain there is no “password reset” function, no central entity to go to. There needs to be a discussion outside the tech community on fundamental features of the technology as they relate to trust, immutability, and the possible shifts of power.

The success and failure of blockchain-based projects depend on the surrounding infrastructure and the social or political context rather than on the technology itself. Still in its early days, blockchain technologies lack stringent standards and an agreed upon terminology. Decision makers should therefore fully understand this emerging technology to gauge its applicability in different contexts.

Particularly in developing countries, it is important to understand if the prerequisites of connectivity, digitised data, and digital literacy exist before launching blockchain-based projects.

Methodology

Close to three hundred articles, reports, and media posts helped identify key features of the technology, which may support decision makers and anti-corruption practitioners. The identification of core elements of the technology enabled reflections around trust, immutability, and transparency, which are key features of the blockchain. A few case

studies highlight in which contexts the technology is likely to be most valuable. These questions guided the research:

- What are the key aspects of the technologies that will enable decision makers and stakeholders to have a qualified opinion on the possible application of blockchain technologies?
- To what extent are blockchain technologies applicable to anti-corruption initiatives?
- Are there examples of best practices in developing countries?

References

- Abadi, J., and Brunnermeier, M. 2018. Blockchain Economics. National Bureau of Economic Research, 1–53.
- Aggarwal, N., and Floridi, L. 2019. The Opportunities and Challenges of Blockchain in the Fight against Government Corruption. 19th General Activity Report, GRECO 82 (March): 22–25.
- Alderman, L. 2019. Despite Bitcoin’s Dive, a Former Soviet Republic Is Still Betting Big on It. New York Times.
- Allison, I. 2019. World’s Second-Largest Grocer Joins IBM Food Trust Blockchain. Coindesk.
- Araujo, F. 2019. Bitcoin v bolivar: Can cryptos save Venezuela. Raconteur.
- Associate French Press (AFP). 2020. Maduro bids to revive Venezuela’s ‘petro’ cryptocurrency. France 24.
- BBC News. 2019. Facebook’s Libra should be blocked in Europe, France Says. BBC News.
- Benbunan-Finch, R., and Castellanos, A. 2018. Digitization of Land Records: From Paper to Blockchain. Association for Information Systems.
- Binance. 2020. The World’s Leading Cryptocurrency Exchange. Website
- Binance Academy. 2020. Proof of Authority Explained. Website.
- Blockgenic. 2018. Different Blockchain Consensus Mechanisms. Hackernoon.
- Bloomberg. 2019. Xi’s Blockchain Push Triggers Frenzy in China Technology Stocks. Bnn Bloomberg.
- Brody, Paul. 2020. How Public Blockchains Are Making Private Blockchains Obsolete. EY Global.

Chainalysis. 2020. Money Laundering in Cryptocurrency: How Criminals Moved Billions in 2019. Insights.

Chen, J. 2019. Fiat Money. Investopedia.

———. 2020. Escrow Agreement. Investopedia.

———. 2019. Know Your Client (KYC). Investopedia.

Coinbase. 2020. Top 50 Cryptocurrency Prices. Website.

Cointelegraph. 2020. What is Ethereum: Guide for beginners. Website.

———. 2020. What are smart contracts: Guide for beginners. Website.

Corasaniti, N., Frenkel, S., and Perloth, N. 2020. App Used to Tabulate Votes Is Said to Have Been Inadequately Tested. The New York Times.

Cuckier, K. 2019. The meaning of the blockchain. The Economist.

De, N., and Dale, B. 2019. Visa, Mastercard, eBay, Stripe Follow PayPal in Quitting Facebook's Libra Project. Coindesk.

Digiconosmist. 2020. Bitcoin Energy Consumption Index. Website.

Eder, G. 2019. Digital Transformation: Blockchain and Land Titles. 2019 OECD Global Anti-Corruption & Integrity Forum.

e-estonia. 2020. What is e-Residency. Website.

———. 2020. X-road. Website.

———. 2020. X-road not to be confused with blockchain. Website.

Eriksson, F. 2017. The Rapid Economic Liberalisation and Ruthless Fight against Corruption in Georgia. U4 Practitioner Experience Note.

Ethereum. 2020. Ethereum. Website.

European Central Bank. 2019. Exploring anonymity in central bank digital currencies. In Focus, Issue no 4.

European Commission. 2020. Anti-money laundering and counter terrorist financing. Website.

Fairley, P. 2019. Ethereum plans to cut its absurd energy consumption by 99 percent. IEEE Spectrum.

FATF. 2019. Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers.

Frankenfield, J. 2018. Proof of Work. Investopedia.

———. 2019. Proof of Stake. Investopedia.

———. 2019. 51% Attack. Investopedia.

Ganeriwalla, A., Casey, M., Shrikrishna, P., Bender, J.P., and Gstettner, S. 2018. DOES YOUR SUPPLY CHAIN NEED A BLOCKCHAIN?.

Gefen, D., Karahanna, E., and Straub, D. W. 2003. Trust and TAM in Online Shopping: An Integrated Model. MIS Q. 27 (1): 51–90.

General Data Protection Regulation (GDPR). 2016. Regulations. Official Journal of the European Union.

Gerard, D. 2017. The World Food Programme’s much-publicised “blockchain” has one participant — i.e., it’s a database. Attack of the 50 Foot Blockchain.

Godbole, O. 2019. Highest in 2 Years: 65% of Bitcoin Hash Power is in China, Report Finds. Coindesk.

Graglia, J.M., and Mellon, C. 2018. Blockchain and property in 2018: At the end of the beginning. Innovations: Technology, Governance, Globalization, 12(1-2), pp.90-116.

Graglia, J. M., Mellon, C., and Akin, E. 2017. Prerequisites for Incorporating Blockchain into a Registry. New America Blog. 2017.

Haber, S., and Stornetta, W.S. 1990. How to time-stamp a digital document. In Conference on the Theory and Application of Cryptography (pp. 437-455). Springer, Berlin, Heidelberg.

Hayes, A. 2019. Stablecoin. Investopedia.

Heller, N. 2017. Estonia, The Digital Republic. The New Yorker.

Higginson, M., Nadeau, M., and Rajgopal, K. 2018. Blockchains-Occam-Problem. McKinsey Insights, 41–47.

Hyperledger. 2020. Hyperledger Fabric. Website.

ID2020. 2019. ID2020 Launches technical certification mark. Medium.

———. 2019. ID2020 Technical Requirements. Website.

———. 2020. We need to get digital ID right. Website.

IndiaStack. 2020. What is India Stack. Website.

International Labour Organization (ILO). 2018. New ILO figures show 164 million people are migrant workers. Website.

Jeffries, A. 2018. 'Blockchain' Is Meaningless. The Verge.

Jospe, C. 2019. When It Comes to Blockchains and Energy Usage. Nori Blog.

Kagan, J. 2020. Digital Wallet. Investopedia.

Kempe, M. 2016. The Land Registry in the Blockchain. Kairos Future.

Kempe, M. 2018. Blockchain tested live – can save billions for house purchasers and mortgage borrowers. Kairos Future.

Kim, C. 2019. From Cardano to Ethereum, 2020 Could Be Deciding Year for Proof-of-Stake. Coindesk.

Kiva. 2020. The journey of a Kiva Loan. Website.

Kivimäki, P. 2018. There Is No Blockchain Technology in the X-Road. Nordic Institute for Interoperability Solutions.

Knight, R. S. 2010. Statutory Recognition of Customary Land Rights in Africa An Investigation into Best Practices for Lawmaking and Implementation. FAO Legislative Study.

Kuhn, D. 2019. European Competition Watchdog Fears Libra's 'Closed Economy.' Coindesk.

Lengoiboni, M. 2011. Pastoralists Seasonal Land Rights in Land Administration: A Study of Northern Kenya. Wageningen University.

Li, K. 2019. The Blockchain Scalability Problem and the Race for Visa-Like Transaction Speed. Hackernoon.

Libra. The Libra mission. 2019. Website.

Lucian, A. 2019. The Top Cryptocurrency Exchanges That Don't Require KYC Verification. Beincrypto.

Mak, R., Sweeney, P. 2019. Breakingviews – China's e-yuan will be more cryptic than crypto. Reuters.

Marinoff, N. 2018. Bitfury Expands To Norway With 35\$ Million Bitcoin Data Center. Bitcoin Magazine.

Matsakis, L. 2019. Following a Tuna from Fiji to Brooklyn—on the Blockchain. Wired.

Mercy Corps. 2020. A Revolution in Trust: Distributed Ledger Technology in Relief and Development. Website.

Monetary Authority of Singapore. 2019. Project Ubin: Central Bank Digital Money using Distributed Ledger Technology. Website.

Möhlmann, M., and Geissinger, A. 2018. Trust in the Sharing Economy: Platform-Mediated Peer Trust. Cambridge Handbook of the Law of the Sharing Economy, Cambridge University Press, Cambridge.

Nakamoto, S. 2019. Bitcoin: A peer-to-peer electronic cash system. Manubot.

OECD. 2018. OECD Blockchain Primer. OECD.

———. 2019. The Policy Environment for Blockchain Innovation and Adoption: 2019 OECD Global Blockchain Policy Forum Summary Report. OECD Blockchain Policy Series.

OECD and KPMG. 2019. Is There a Role for Blockchain in Responsible Supply Chains?

Omale, G. 2019. Gartner Predicts 90% of Blockchain-Based Supply Chain Initiatives Will Suffer 'Blockchain Fatigue' by 2023. Gartner Press Release.

Openaid. 2020. Openaid aid to Georgia graphic. Website.

Palmer, D. 2019. IBM, Maersk's Blockchain Platform TradeLens Is Shipping to Russia. Coindesk.

———. 2020. Oman's Largest Port Joins Blockchain Shipping Platform TradeLens. Coindesk.

Rauchs, M., Blandin, A., Bear, K., and Mckee, S. 2019. 2nd Global Enterprise Blockchain Benchmarking Study. Cambridge Centre for Alternative Finance.

Ray, S. 2017. Cryptographic Hashing. Hackernoon.

Reiff, N. 2020. Blockchain Explained. Investopedia.

Rella, L. 2019. Blockchain Technologies and Remittances: From Financial Inclusion to Correspondent Banking. Frontiers in Blockchain 2.

Rinne, A. 2019. 4 Big Trends for the Sharing Economy in 2019. World Economic Forum. 2019.

Ripple. 2020. Instantly Move Money to All Corners of the World. Website.

Santiso, C. 2019. Here's How Technology Is Changing the Corruption Game. World Economic Forum.

Sathe, G. 2018. After Beta-Testing On A Billion Indians, The Tech Behind Aadhaar Is Going Global. Huffington Post.

- Schneier, B. 2019. There's no good reason to trust blockchain technology. Wired.
- Senou, O. 2019. Tracking Fiji's tuna with blockchain technology. CTA Blog.
- Shang, Q., and Price, A. 2019. A Blockchain-Based Land Titling Project in the Republic of Georgia: Rebuilding Public Trust and Lessons for Future Pilot Projects. *Innovations: Technology, Governance, Globalization* 12 (3–4): 72–78.
- Shrier, D., Wu, W., and Pentland, A. 2016. Blockchain & infrastructure (identity, data security). *Massachusetts Institute of Technology-Connection Science*, 1(3), pp.1-19.
- Sloane, R. 2020. Conflict Minerals and Child Labour: Enabling Better Business with Blockchain Traceability. Hyperledger Blog.
- Smartmatic. 2019. Civil and voter registration Sierra Leone 2017. Website.
- Sveriges Riksbank. 2020. The Riksbank's e-krona pilot. Sveriges Riksbank.
- Thaker, A. 2018. The New Oil. Caravan Magazine.
- The Economic Times. 2017. Aadhaar mandatory for kerosene subsidy, Atal Pension Yojana.
- Tobin, A., and Reed, D. 2016. The Inevitable Rise of Self-Sovereign Identity. Sovrin Foundation.
- Transparency International. 2018. Estonia. Website.
- Truzman, J. 2020. Gaza-based militant group Mujahidin Brigades publishes series "The Beating Heart of a Nation." Long War Journal.
- . 2020. Palestinian militant groups appeal for Bitcoin donations to promote jihad. Long War Journal.
- UN Development Programme. 2020. Human Development Reports. Website.
- UN Sustainable Development Goals. 2019. SDG 16. United Nations.
- UN Refugee Agency (UNHCR). 2020. Registration and Identity Management. Website.

Unique Identification Authority of India. 2019. What is Aadhaar. Government of India.

Uslaner, E. M. 2015. Trust, Political. International Encyclopedia of the Social & Behavioral Sciences: Second Edition. Second Edi. Vol. 24. Elsevier.

W3C. 2020. Decentralized Identifiers. Website.

Walch, A. 2017. The Path of the Blockchain Lexicon (and the Law). Review of Banking & Financial Law 36: 713–66.

Walter, C., Gamble, R., Alarcon, G., Jessup, S., and Calhoun, C. 2017. Developing a mechanism to study code trustworthiness.

Wang, F., and De Filippi, P. 2020. Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. Frontiers in Blockchain 2 (January): 1–22.

Weizsäcker, F. v., Eggler, S., and Atarim, E. 2019. Land Registries on a Distributed Ledger. GIZ. Berlin: Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ).

Wood, M. 2019. European Central Bank confirms exploring digital Euro as retail, wholesale CBDC. Ledger Insights.

World Bank Group. 2019. Doing Business 2019. The World Bank.

World Food Programme (WFP). 2020. Building Blocks Blockchain for Zero Hunger. Website.

Yu, X. 2018. China to stamp out cryptocurrency trading completely with ban on foreign platforms. South China Morning Post.

Zaharia, M., and Kim, D. 2018. Bitcoin start-ups in Asia take aim at remittances market. Reuters.