THE IMPACT OF BLOCKCHAINS for Human Rights, Democracy, and the Rule of Law

Information Society Department

DGI(2022)06

Authors :
Florence G'sell
Florian Martin-Bariteau

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

French edition:
*L’impact des blockchains sur les droits de l’homme,
la démocratie et l’État de droit*

All requests concerning the reproduction or translation of all or part of this document should be addressed to the Directorate of Communication (F-67075 Strasbourg Cedex or publishing@coe.int). All other correspondence concerning this document should be addressed to the Directorate General Human Rights and Rule of Law.

Layouts and Cover Page:
Information Society Department
Council of Europe

Images: Shutterstock

This publication has not been copy-edited by the SPDP Editorial Unit to correct typographical and grammatical errors

THE IMPACT OF BLOCKCHAINS for Human Rights, Democracy, and the Rule of Law

An Overview Report

Report to the Council of Europe by

Prof. Florence G'sell
Professor of Private Law, Université de Lorraine

Prof. Florian Martin-Bariteau
Associate Professor of Law and University Research Chair in Technology and Society, University of Ottawa

Council of Europe

Table of Contents

Executive Summary

Blockchain technology presents an opportunity for government, international organizations, non-governmental organizations, industry stakeholders, and, more generally, members of the public to engage in the recognition of and respect for human rights as well as to resolve current human rights issues.

Building on years of research by cryptographers and network engineers, the technology was introduced by Satoshi Nakamoto on October 31, 2008, in a whitepaper presenting the Bitcoin cryptocurrency and a whole financial system. Inspired by Bitcoin, there are today more than 18,000 cryptocurrencies in existence. Although the technology is most often associated with cryptocurrencies and other financial instruments or assets, some coins were developed for specific use cases and functions, and the development of decentralized applications and "smart contracts" allowed for the deployment of systems to manage anything from digital identities, to medical records, land titles and zoning registries, intellectual property rights, digital identity, voting systems, supply chain and aid.

This report explores the risks and potential benefits of blockchain technology for democracy, human rights and the rule of law. It aims to showcase use cases and flag potential issues, as well as to provide initial recommendations to the Council of Europe for additional research and prospective programming regarding blockchain technologies.

The report highlights some of the promising features of blockchain technology and various types of implementation, from cryptocurrencies, to smart contracts, to distributed autonomous organizations (DAOs) and non-fungible tokens (NFTs). It also presents some of the important limitations that may impede fundamental rights.

As the technology has numerous applications including democratic tools and support for human rights, the report presents different use opportunities in line with the Council of Europe's global democratic agenda to advance democratic functions and ensure accountability and transparency, from digital identity and information self-determination, to supporting refugees and vulnerable populations, responsible supply chain, immutable land titles and voting systems, as well as efficient dispute resolution mechanisms.

Finally, the report discusses some of the legal issues that may arise from the use of this technology, with emphasis on matters that may welcome leadership from the Council of Europe in regards to the protection of anonymity and privacy rights; the legal status of automated contracts and decentralized autonomous organizations; and the conflict of law and jurisdiction due to the distributed and global nature. In the appendix, the report includes a table presenting the interface of blockchain technologies with the *European Convention on Human Rights*.

Introduction

It is not often that a technology is meant to solve old social, economic and political challenges. This is, however, the ambition of blockchain technology, which, from the outset, has been developed with a view to finally overcoming the problems of cooperation and coordination that arise within human communities. The idea is to replace established institutions such as states and banks with technological and impartial tools that can generate trust outside of traditional institutions—removing the need for such trusted third parties. The founding idea of blockchain is to give to all those who wish to do so the possibility of interacting online on a code-driven platform that is not controlled or administered by any human authority. The possibility for users to carry out peer-to-peer transactions online without intermediaries or the intervention of a trusted third party limits the risks of human error or corruption.

The technology builds on an ideology best illustrated in Timothy C. May's 1992 *Crypto-Anarchist Manifesto*. Consolidating years of online conversation within the cryptography community, this manifesto predicted and called for new cryptographic techniques allowing individuals and groups to communicate and interact online anonymously. Above all, crypto-anarchists aimed to allow individuals to live, communicate and exchange without being monitored, controlled or taxed by governments. The crypto-anarchist project of a totally decentralized platform could make it possible to reconnect with the initial architecture of the Internet, which was buried by the appearance of huge centralized corporate platforms.

Years later, the libertarian belief that encryption and cryptographic tools could liberate the masses is still very much alive. By combining cryptography and distributed architecture, blockchains are designed to provide the technological infrastructure for human interaction at the social, political and economic levels without third-party intervention. At the same time, the primacy given to computer code over any other type of constraint may lead one to think that human communities interacting on blockchain platforms no longer need the law. No doubt this explains why jurists who study blockchain start by wondering whether the legal rules they know are valid in an environment precisely designed to favor programming at the expense of human rules. This will also be the perspective of this report, which is devoted to the question of whether and to what extent the fundamental rights of people who interact on blockchain platforms are threatened or guaranteed.

To this day, blockchain is most often associated with cryptocurrencies and other financial instruments or assets. Its first implementation, Bitcoin, created a virtual currency and a whole financial system. Since then, news outlets continuously reprise stories about the economic craze around crypto-assets, or their use by nefarious actors.

However, beyond cryptocurrencies, the blockchain technology has numerous applications including democratic tools and support for human rights. In fact, blockchain technology builds on years of computer science research and creates secure and immutable systems. The purpose of this report is to explore the risks and potential benefits of blockchain technology for democracy, human rights and the rule of law, beyond the financial craze.

The report first provides a technical primer on blockchain technology and various types of implementation, from cryptocurrencies, to smart contracts, to distributed autonomous organizations (DAOs) and non-fungible tokens (NFTs). The report then presents different use opportunities in line with the Council of Europe's global democratic agenda, before discussing some of the legal issues that may arise from the use of this technology with emphasis on matters that may welcome leadership from the Council of Europe. Finally, as this is an initial report that aims to showcase use cases and flag potential issues, the paper concludes with initial recommendations for additional research and prospective programming regarding blockchain technologies for the Council of Europe. A table presenting the interface of blockchain technologies with the *Convention for the Protection of Human Rights and Fundamental Freedoms* (*European Convention on Human Rights*) is also provided as an appendix.

It should be noted that legal issues regarding cryptocurrencies and crypto-assets, *i.e.* when tokens are used as means of payment, securities or other kinds of assets, are out of scope of the present report and have been subject to other studies. The Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism have extensively and proactively considered the cryptocurrency-specific issues of money laundering and the financingal of illicit activities.

Similarly, the report will not discuss criminal activities involving blockchain-powered solutions. Certainly, the blockchain craze has led to an increase of such cases, notably through the use of cryptocurrencies for ransoms and payments. However, from the legal perspective the crimes are the same, and not unique to the technology. Most countries have now updated their legal frameworks to ensure the processing of such transactions, and "Know Your Customer/Client" (KYC) compliance schemes. Moreover, the full transparency of the ledgers can be leveraged by law enforcement. Nonetheless, the initial pseudo-anonymity, as well as the global and distributed nature of the technology may present important challenges for law enforcement and will be discussed.

References

Cheng, Evelyn (2017). "Dark web finds bitcoin increasingly more of a problem that a help, tries other digital currencies."

Crumpler, William (2021). The Human Rights Risks and Opportunities in Blockchain, CSIS.

De Filippi, Primavera & Aaron Wright (2018). *Blockchain and the Law: The Rule of Code*, Harvard University Press.

May, Timothy (1988). "The Crypto Anarchist Manifesto."

Rueckert, Christian (2019). "Cryptocurrencies and fundamental rights," Journal of Cybersecurity, 5:1.

Weinstein, Jason (2021). "Why Bitcoin is Better for Crime Fighters than Criminals."

Werbach, Kevin (2018), *The Blockchain and the New Architecture of Trust*, MIT Press.

1. A Primer on Blockchains

This section presents the inner workings of blockchain technology, including how it works, its limitations, and its possible implementations. For the sake of this non-technical report, the presentation may be simplistic at times by explaining key complex technical aspects in an accessible language, both to unpack the hype and clarify the technology's limits for future research and programming.

What is a blockchain?

Building on years of research by cryptographers and network engineers, the technology was introduced by Satoshi Nakamoto on October 31, 2008, in the whitepaper for the Bitcoin cryptocurrency. Under the pseudonym Satoshi Nakamoto, one or more anonymous researchers proposed a secured solution to allow a certain number of operations to be carried out—such as a transfer and storage of value and data—without any intervention from a trusted third party.

Blockchains are distributed and secure ledger systems that can operate autonomously without the need for a central controlling or coordinating authority, eliminating the need for trust and intermediaries in the operations. These systems can allow certain operations to be carried out, such as a transfer of value or information, without any intervention from a trusted third party. This aspect of the blockchain technology, which renders the information secure and quasi-immutable without the need for a trusted third party, is of key interest in humanitarian and democracy-seeking contexts where governmental and non-governmental organizations may be lacking public trust, or trust in each other.

Blockchains store data in a sequential record, in a network of nodes said to be secured by several layers of security, from the way the blocks of data are interlinked, to the redundancy and synchronization of the network. Transparency is a key feature of blockchains that are fully public ledgers: any interested party is able to read the information in the ledger, as well as write new information into it subject to respecting the consensus protocol.

While not bullet-proof, the technology presents significant security mechanisms for data integrity, and recordkeeping to make sure no party can tamper with the information in the ledger. Every time a block of data is added to the blockchain ledger, it includes a unique fingerprint (called a hash) of the previous data contained in the previous block. As such, it forms a chain of blocks that is reinforced by each new addition. This is a first layer of immutability for blockchains as any given block cannot be altered without tampering with all subsequent blocks. If a data block is tampered with, the hash of this block changes, and will not match the hash stored in the subsequent block. As a result, all subsequent blocks will be discarded.

The stored data is further protected by distribution through a **peer-to-peer network** to eliminate the risks inherent with centralized databases. If any party tries to tamper with information stored on the blockchain, the protocol of the distributed network can detect and prevent it. In addition, in a distributed network, if any node is down, the network continues to function with no loss of data or integrity. As every node of the peer-to-peer network has a full copy of the ledger, if one peer node is tampered with, only its copy of the ledger will be affected. This provides resistance to failures and attacks, as if one peer node fails, the rest of the network and the copy of the ledgers are not compromised. It is possible that the rest of the network will not even be aware of the anomaly.

This distributed network is securely updated and synchronized according to the procedures set out in the consensus algorithm, which is aimed at avoiding a situation where the tampering of a node contaminates the rest of the network. Peer nodes of the distributed network need to reach consensus on the validity of all transactions and hold a copy of the full ledger of data. Node operators, called miners, have the responsibility to validate and certify all data operations and blocks on the blockchain. Once a block is validated and broadcasted, the nodes verify it and append or discard it. This is how new blocks are added to the ledger. Different blockchains have different methods of validation. The most common, found in the Bitcoin blockchain, is the method of "proof of work," which involves performing complex cryptographic calculations to solve a mathematical problem that requires substantial computing power. This method can be costly in terms of energy. It leads to a competition between the network's nodes to solve the calculations faster than another, as they are then rewarded with the network's native token upon block confirmation. This competition continuously increases the need for more computing power and more energy.

In response, other consensus mechanisms have been developed, with the primary alternative being "proof of stake." This method does away with confirming blocks through energy intensive computations in favour of either allocating mining power according to the number of tokens held, or randomly between potential miners holding a minimal stake. This is therefore more energy-efficient. Another method uses "proof of space," which allocates mining power according to the computing or storage capacity available to each miner. This method is, however, less energy-efficient as it still rewards the computational or storage power of a miner.

Sometimes, there can be discrepancies in the network. Where this is the case, the version that is found in the majority of nodes will take precedence and the whole network will update accordingly. The minority version is discarded in a side-chain. This additional layer of security, achieved through the majority rule of the distributed network of nodes, is also one of its points of failure. A blockchain is only secure if the power is evenly distributed between node operators. Any concentration in power is a security threat to the whole network. Once an actor or a group of actors retains 51% of the network control, they have the power to take over the whole network and intentionally exclude or modify transactions. This security threat—called the "51% Attack"—is why the operators keep a close eye on node coalitions and regroupings, including the geolocation of operations. This security risk is nonetheless minimal for established networks with a large number of nodes, as the costs involved for a third party actor to engage in such an attack would be astronomical.

Another advantage of the blockchain technology is its **transparency and pseudo-anonymity**. Blockchains are public and transparent ledgers. Each node has a full copy of the ledger, and it is possible for any interested party to read all the information recorded and to trace all transactions and operations within it. It is not possible to hide or redact information on a blockchain—except if the stored information is encrypted by the users.

Despite this transparency, however, the identity of parties is hidden in plain sight through pseudo-anonymization. Nodes and users do not need to provide names or personal details to be part of the network. Each user is given a public and a private key. The public key is an address known to everyone, and the private key is only known to its owner for authentication, to sign their messages and decrypt messages addressed to their public address. Rather than their name, users are known under their public address. It is therefore impossible to know who is behind a given public address when no information was requested at the time of the address's creation—it could be anyone, and users can have more than one address.

However, contrary to popular belief, blockchains do not achieve full anonymity. It remains possible to re-identify the owner of an address since it is possible to trace all transactions, which may infer the identity of the user. Some transactions may be linked to off-chain assets known to be owned by the user, or patterns of transactions may unveil off-chain communities or behaviours. In some cases, the user may have provided their public address to a third party who knows their identity. Forensic analysis of the transactions on and off the chain may take time, but they can unveil the identity of a user, as well as the full history of their operations. Law enforcement agencies have famously leveraged those techniques to reveal the identity of criminals and track their activities on and off blockchains.

In some contexts, the transparency of the ledger may be problematic. Indeed, public access to the information and ability to track the data and users can present privacy or confidentiality risks. To overcome the risk, privacy-enhancing protocols and solutions are being developed. (Those privacy considerations will be discussed in detail below in Section 3.) Similarly, the permissionless feature of the technology might not be best suited to some uses.

In response, variations of the public and permissionless blockchains technology have been proposed with hybrid permissioned ledgers where users are allocated select permissions to perform only certain activities on the network, from a public read-only and controlled write access, to more complex permission schemes. Some have also proposed wholly private ledgers within an organization or a consortium of organizations where the operation of the ledger and access to data can be restricted to a small number of vetted users.

Finally, one of the key features of blockchains is their autonomous execution and trustworthiness. The operations and verification processes execute autonomously through the networks every time that a node reads it, all the while verifying the integrity of the chain. There is no discretion for parties; when information, a transaction, an order is included in the ledger, it will be transmitted and executed across the network in an autonomous way. This generates a series of major advantages where there is a lack of trust between parties, as it reduces the need for intermediaries to execute or enforce operations and rules.

References

Bacon, Jean, Johan David Michels, Christopher Millard & Jatinder Singh (2018). "Blockchain Demystefied: A Technical and Legal Introduction to Distributed and Centralised Ledgers," Richmond Journal of Law & Technology 25:1.

Narayanan, Arvin, Joseph Bonneau, Edward Felten, Andrew Miller & Steven Goldfeder (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press.

Nakamoto, Satoshi (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System."

Walch, Angela (2015). "The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk," NYU Journal of Legislation and Public Policy 18:837.

Cryptocurrencies

Cryptocurrencies are a type of virtual currency powered by the blockchain technology. The first fully functioning cryptocurrency, Bitcoin, was proposed in 2008 and launched in 2009 amid a global financial crisis that diminished public trust in the existing financial system's checks and balances, as well as the capacity of governments to provide appropriate oversight. In the seminal *Bitcoin: A Peer-to-Peer Electronic Cash System*, the mysterious Satoshi Nakamoto exposed the Bitcoin platform project which was meant to power an entire disintermediated and distributed peer-to-peer payment system. Bitcoin was designed to facilitate the online transfer of funds directly from one party to another without intermediaries and to eliminate the need for central authority and trusted third parties and their associated costs.

The decentralized nature of blockchain, and by extension Bitcoin, is a core element of the system. The development of a distributed consensus was the key technical problem to solve to build a distributed financial system. Users have their cryptographic wallets that act as accounts, and they can directly order the transfer of funds and receive funds themselves, subject to validation by the operators. The entire record of transactions is available on the public ledger, even if the wallet holder's identity remains pseudonymous.

When A wants to transfer Bitcoins to B, the transaction from A's wallet to B's is signed and broadcasted to all the nodes on the blockchain. As part of the broadcast, miners confirm the availability of funds, and come to a consensus throughout the blockchain that this transfer occurred and that the intended amount of Bitcoins has changed owners. B can review the transaction on the ledger and confirm that the transfer to their wallet was successful. The open ledger is meant to provide transparency and make sure that coins are not spent twice.

In addition to creating a virtual currency and a payment system, the Bitcoin blockchain includes its own monetary policy. New units of cryptocurrency are created during the mining process to reward the miners that validate and add blocks to the ledgers. Bitcoin has inspired an ever-growing legion of followers and spinoffs, but it is far from the only cryptocurrency in circulation today. There are more than 18,000 cryptocurrencies in existence. Several of them follow in the footsteps of Bitcoin and are intended for payments and transmitting money amongst their users, like Litecoin or the privacy-friendly Monero. Each cryptocurrency has its own monetary policy. For some, their value is linked to market demand, while others are tied to fiat currencies or other assets to create a stable coin, such as Tether. Some have even been developed as a joke, like DogeCoin, which spawned from a meme image of a Shiba Inu dog and was developed as a critical commentary on the wildly speculative nature of cryptocurrencies.

As well, some coins were developed for specific use cases and functions. It is worth noting that, despite their names, not all cryptocurrencies are used as a currency. While some are still used as financial instruments or assets, the coins or tokens may be adapted for many other purposes. For example, the Namecoin blockchain provides a decentralized domain name system (DNS) service for Internet addresses under the extension .bit, which is safe from censorship. Likewise, the Storj token allows people to share files across its decentralized network.

More than a decade later, the technology serves many other uses, notably through blockchains like Ethereum or Cardano, which support decentralized applications and their so-called "smart contracts." On these platforms, developers can deploy systems to manage anything from digital identities, to medical records, land titles and zoning registries, intellectual property rights, digital identities, voting systems, supply chains and international aid.

References

Nakamoto, Satoshi (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System."

Narayanan, Arvin, Joseph Bonneau, Edward Felten, Andrew Miller & Steven Goldfeder (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press.

“Smart” Contracts

In 2014, Ethereum launched a new blockchain aimed at not only transferring cryptocurrency tokens (called ethers) but also at developing decentralized applications deceptively called “smart contracts.” Despite their name, it must be noted that these are not necessarily contracts in the legal sense of the term.

A smart contract is a computerized transaction protocol that automates a set of predefined and agreed upon conditional actions. Codified clauses are automatically enforced once the pre-programmed conditions are satisfied without any human intervention. The coded instructions are triggered by events. Behind the scenes, a series of “if” and “then” conditions trigger actions: if “this” condition is fulfilled, then “that” executes a predefined action. It is very simple, yet powerful. As with any other computer software, the possibilities are unlimited, provided that the stipulations can be expressed in computer code, and that a computer can realize the intended action. One of smart contracts’ main advantages is they remove the need for third parties, and risks of reliance on parties’ discretion. Smart contracts are both defined by the computer code and executed and enforced by the code itself automatically, without discretion.

Smart contracts today are increasingly being developed to leverage blockchain technology. As a result, the term has become synonymous with blockchain-enabled auto-executable contracts. However, the existence of self-executed actions with little or no human intervention predates blockchains. Indeed, Nick Szabo theorized the idea of smart contracts through his published papers in the mid-to-late 1990s. He proposed developing a clear coding language to allow more complex smart contracts to be run by computers. These computerized contracts were considered “smart” as they could self-execute and enforce their conditions—at least they were “smarter” than traditional contracts, which could only express the commitment of the parties without enforcing the contract’s conditions. Smart contracts would then reduce fraud, loss, arbitration and enforcement costs and other transactional costs. In essence, smart contracts are behind coffee and snack vending machines: the machine will deliver the chosen product when you insert the expected money, without discretion on the part of the seller, or negotiation on the part of the buyer. Nick Szabo’s idea was revolutionary at the time but seems elementary today considering modern developments in technology. Since then, so-called “crude” smart contracts have embedded themselves into our society.

Smart contracts are increasingly developed on blockchain-powered platforms in order to leverage the technical advantages of the secured distributed ledger technology. Their decentralized systems allow for the elimination of intermediaries in some transactions, saving time, and limiting conflict related to negotiation processes, conditions or performance of contracts.

Using blockchains to power smart contracts provides enhanced security since the ledgers cannot be altered, modified or destroyed. Blockchain technology renders the information secure and immutable, including the content of the scripted and agreed upon conditions. Parties cannot intervene or change the terms of the agreement. If any party tries to change a contract, term or transaction on the blockchain, the protocols of the distributed network can detect and prevent it. However, the inability to change the script also presents challenges. Since information stored on the blockchain is permanent, it is not possible to change the initial terms of the smart contract as is the usual practice of contractual amendments—except when such a possibility is provided for in the initial code. As a result, amending smart contracts that are not pre-programmed for modifications could be significantly more challenging and costly, if even possible, than it currently is through paper amendments.

Other high-level benefits of using blockchain for smart contracts include their autonomous execution, the verifiability of execution and trust reduction. The smart contract's script will execute autonomously through the network every time that a node reads it, all the while verifying the integrity of the chain. However, as there is no discretion for parties. Once the terms are agreed upon, scripted, and entered in the chain, the obligations will be executed without any action from any parties to the contract, sometimes with terms that reinforce the operational security, such as placing funds in a virtual escrow account (*escrow wallet*) before automatically releasing them when the operation is unwound (*e.g.* the goods are delivered). In most smart contracts, the contracting parties are offered a way to enforce contractual obligations and ensure performance without relying on the state (or a third party) to intervene.

In addition to cost reduction and faster execution, automation and lack of party discretion generate a series of major advantages where there is a lack of trust in a contractual relationship. Automation also reduces the need for intermediaries to execute or enforce obligations. However, it brings some risks as it is impossible to prevent the execution as it has been designed. If there is a transaction, it will be repeated in a loop. If there is an error, it will be repeated in a loop as well.

Finally, smart contracts are confronted with some technical limitations—one due to blockchain, and others inherent in digitalization. A "smart" contract can only be as smart as its developer and the computers running it. In addition, the program cannot do more than what is allowed by the current state of computing, which renders only certain types of smart contracts and uses viable. As natural language cannot be directly executed by a computer, smart contracts require that contractual obligations be translated into computer-readable and computer-executable terms.

In addition, a major limitation for smart contracts is the inability of blockchains to interact with external resources and data that a user stores in their ledger. This problem was solved with the development of blockchain middlewares called "oracles." Oracles bridge smart contracts to key off-chain resources like data feeds (*e.g.* the weather, the time of arrival of a plane, the arrival of a good at its destination), legally binding e-signatures or bank payments. As such, oracles can deliver information to trigger the execution of the smart contract, or make smart contracts trigger off-chain actions (*e.g.* order a financial institution to execute a payment). Although oracles provide endless opportunities for smart contracts, they also bring new security challenges. Indeed, blockchain's appeal is the removal of third parties and the need for trust in a contractual relationship; however, oracles bring these aspects back into the equation.

Oracles can also help mitigate another key limitation of smart contracts by connecting them to the physical world. The development of the Internet of Things and "smart properties" has allowed smart contracts to connect to everyday tools, such as cars, door locks, lights and more, thereby expanding the realm of digital enforcement. Still, beyond the digital world, traditional methods of enforcement—with their limitations—still need to be employed.

There are many applications for smart contracts. However, for the time being, smart contracts are mainly found in two types of transactions: transferring funds in cryptocurrencies when certain conditions are met, and imposing financial penalties when certain circumstances occur. They can provide efficiencies in executing basic commercial contracts, or even facilitate alternative dispute resolution processes. In the real estate industry, they can facilitate transactions by using commercial smart leases, and eliminate the "middleman" by using the smart contract as the escrow agent rather than a third party, thereby reducing costs. In the insurance industry, smart contracts can reduce delays for the compensation of insured victims by automatically crediting an insured traveller when an oracle detects a delay in a plane's scheduled departure or arrival. In the logistics sector, smart contracts can ensure that senders receive payments only after the actual delivery of the package to the recipient.

The development of blockchain-based smart contracts is, however, limited by concerns of confidentiality arising from the transparency of the technology. As smart contracts and transactions are recorded and visible to all, in addition to the potential reidentification of the users, it excludes for the time being the execution of sensitive or confidential transactions (e.g. payment of employees or suppliers) on public blockchains such as Ethereum as long as cryptographic solutions remedying this problem are not implemented.

In addition, the more complex the smart contract is, the more costly it will be to execute. For example, smart contracts executed on the Ethereum platform require paying a fee, known as "gas," for the contract to run on the blockchain and the relevant transactions to be added to the blocks. The more complex the transactions in the smart contract, the higher the price of "gas." Due to this cost, smart contracts remain relatively simple for now. Yet, new standards and new platforms are regularly proposed to alleviate those costs and offer more opportunities for smart contracts.

As a result, in the near future, smart contracts are expected to automate numerous operations, whether to transfer funds, increase development of the Internet of Things or create a fully automated online marketplace. Today's smart contracts provide relatively simple and precise parameters and execution methods. Yet, in the likely future, smart contracts will become increasingly complex and allow elaborate transactions.

References

G'sell, Florence (2019), "Intelligence artificielle et blockchain", in Alexandra Bensamoun & Grégoire Loiseau, *Droit de l'intelligence artificielle*, Dalloz.

Martin-Bariteau, Florian & Marco Pontello (2020), *Hashing Out Agreements: An Overview of Smart Contracts under Canadian Law*.

Mik, Eliza (2017). "Smart Contracts: Terminology, Technical Limitations and Real World Complexity," Law, Innovation & Technology.

Raskin, Max (2016). "The Law and Legality of Smart Contracts," Georgetown Law Technology Review 1:2 306.

Surden, Harry (2012). "Computable Contracts," UC Davis Law Review 46:629.

Szabo, Nick (1994). "Smart Contracts," Nick Szabo's Essays, Papers, and Concise Tutorials.

Szabo, Nick (1996). "Smart Contracts: Building Blocks for Digital Markets."

Szabo, Nick (1997). "The Idea of Smart Contracts," Nick Szabo's Papers and Concise Tutorials.

Szabo, Nick (1997). "Formalizing and Securing Relationships on Public Networks," First Monday.

Werbach, Kevin & Nicolas Cornell (2017). "Contracts Ex Machina," Duke Law Journal 67:313.

Decentralized Autonomous Organizations (DAOs)

A decentralized autonomous organization (DAO) is a blockchain-based organization that enables collective action and decision-making. Those computerized organizations leverage a multitude of smart contracts connected together to autonomously operate their governance scheme without the need for central leadership, or any human intervention, on a peer-to-peer network involving all stakeholders.

DAOs can have different types of architectures and objectives. All the usual governance, membership and operational rules and actions are encoded in smart contracts. While each smart contract is designed to perform specific tasks, they can collectively perform relatively elaborate tasks when connected together and interacting. If the first DAOs functioned by involving human intervention, the latest advancements allow for fully automated decentralized organizations which can be fully functioning corporations or cooperatives. By integrating more elaborate artificial intelligence tools into these DAOs, it will be possible in the future to create intelligent organizations, programmed to act autonomously and capable of adapting to changing circumstances.

In the absence of centralized management, the organization is fully managed and operated by computer code. Stakeholders interact with each other according to a protocol programmed by the code: voting and providing input on decisions to be made. Similar to shareholders of a corporation or members of a cooperative, a DAO's governance is coordinated using governance tokens. Interested parties must procure tokens to participate. Each token grants voting powers, but also the right to collect dividends or acquire benefits from goods or services managed by the DAO. In some cases, more governance tokens translates into greater voting power.

In addition, DAOs may allow for more secure, transparent and accountable governance. The security features of blockchain technology provide greater certainty to stakeholders regarding the governance scheme and voting rights and may reduce potential abuses. Similarly, everything is recorded in a blockchain, from the code to the decision, which allows for better accountability and auditing processes. Should the DAO be run on a public blockchain, any interested party could audit the organization's operation. This can be useful when public trust has been lost or is at stake. However, as previously highlighted for smart contracts, this transparency could also limit the adoption of the technology by industry.

The first DAO, called "The DAO," was launched in 2016 on the Ethereum platform to facilitate the crowdfunding of diverse projects. Investors contributed cryptocurrencies and received tokens granting them voting rights on the funding proposals brought before the organization. Investors would then receive profits from the funded projects based on their token rights. Since then, many more DAOs have formed. The MolochDAO aims to organize members willing to contribute capital to fund Ethereum as an essential public good and infrastructure. The Finnish investment cooperative Robin Hood Coop uses a DAO to manage the assets of the cooperative's members. In Germany, Koina uses a proprietary blockchain to provide a monetary system that allows producers to obtain credit to independently finance their future activities. Beyond the crowd-finance industry, Arcade City proposed a ride-sharing DAO that offers shared transportation services to the public in exchange for a fee in cryptocurrency. More recently, the ConstitutionDAO formed with a single purpose: to raise funds to buy a non-fungible token of the Constitution of the United States of America; but they lost the auction.

References

Buterin, Vitalik (2014). "DAOs, DACs, Das and More: An Incomplete Terminology Guide."

G'sell, Florence (2019), "Intelligence artificielle et blockchain," in Bensamoun, Alexandra & Loiseau, Grégoire (2019). *Droit de l'intelligence artificielle*, Dalloz.

Metjahic, Laila (2018). "Deconstructing the DAO: The need for legal recognition and the application of securities laws to decentralized organizations," Cardozo Law Review 39:1533.

Szabo, Nick (1994). "Smart Contracts."

Wright, Aaron & Primavera De Filippi (2015). "Decentralized Blockchain Technology and the Rise of Lex Cryptographia."

Non-Fungible Tokens (NFTs)

A non-fungible token (NTF) is a non-fungible unit of data stored on a blockchain that can be transferred between users. Contrary to cryptocurrencies such as Bitcoin, which are composed of fungible tokens where each unit of Bitcoin is interchangeable with any other unit of Bitcoin, NFTs are not mutually interchangeable. Building on the idea of Nick Szabo's smart properties, NFTs allow for the commodification and trading of either tangible or intangible (digital) assets—from an animated flying cat to houses, concert and lottery tickets and loans.

NFTs gained popularity in 2021, most notably in the art world in an effort to support digital artists. The technology made headlines when Christie's auction house facilitated the unprecedented sale of an NFT by the digital artist Beeple for US $69 million. Most digital art in the NFT space depicts 8-bit nostalgia of the early Internet era. But as it becomes more accessible, artists are tackling more socially critical subjects. For example, dissident Chinese artist Badiucao released an Olympic-themed NFT collection critiquing China's human rights record. Badiucao's NFT platform allows citizens to contribute and mint their own critical work in the collection.

NFTs create scarcity of digital goods, and support the management of rights, from copyright in the work, to ownership of the work itself. They build on the recordkeeping of blockchains to provide secured certificates of authenticity or of ownership. In addition, smart contracts facilitate direct sales and payment from one party to another and provide the opportunity to incorporate automated royalty payments to artists. This financial compensation from secondary market sales of the goods represented by the token is an attractive component for both digital artists and speculative investors—which explains, in part, the success of NFTs.

There are various types of NFTs, but the most common is a metadata file containing information encoded with a digital version of the tokenized thing (title, artwork, etc.). Alternatively, the entire work is uploaded to the blockchain. This option comes at a significant cost and is therefore less popular. Most NFTs are developed under the ERC-721 standard on the Ethereum blockchain platform. At its core, an NFT includes two elements: the Token ID, a number generated upon the creation of the token, and the Contract Address, that refers to the location of the smart contract managing the ownership and logic of the NFT. This combination makes the NFT unique, meaning only one token in the world exists with that combination of Token ID and Contract Address. In addition, the NFT could include the wallet address of its creator, which, in connection with the EIP-2981 standard, allows the creator to require and automate royalty payments on subsequent sales.

NFTs often include a link to the original tokenized work. The NFT is not, in fact, the work itself, but rather a unique digital representation linked in some way to an original work. Notably, while NFTs can signify the digital representation of rights in a tangible or intangible asset, they do not necessarily grant ownership rights of the asset. For example, the sale of a work of art represented by an NFT may transfer the ownership of the token but does not necessarily transfer the copyright vested in the artwork. Likewise, the recordkeeping capacity of the blockchain does not protect against copies and infringements outside the blockchain hosting the NFT.

Recently, a group known as SpiceDAO purchased the NFT containing the intended cinematic interpretation of film-maker Alejandro Jodorowsky's novel *Dune*. Unbeknownst to SpiceDAO, the $3 million token did not include copyright, nor did it include the right to reproduce the work in the book.

References

Angeleti, Gabriella (2022). "Crypto group shamed for spending $3m on 'Dune' book, mistakenly believing it had acquired copyright to produce NFTs."

Burks, Zach, James Morgan, Blaine Malone & James Seibel (2020). "EIP-2981: NFT Royalty Standard."

Christie's Auction House (2021). "Beeple's opus."

Cooper, James & Peter Grazul (2021). "NFTs for freedom: Nonfungible tokens and the right to self-determination."

Entriken, William, Shirley Dieter, Jacob Evans & Nastassia Sachs (2018). "EIP-721: Non-Fungible Token Standard".

Griffith, Erin (2021). "Why an Animated Flying Cat with a Pop-Tart Body Sold for Almost $600,000."

Guadamuz, Andres (2021). "Non-fungible tokens (NFTs) and copyright."

Harris, Gareth (2022). "Badiucao launches NFT collection to protest against China's human rights record on even of Beijing Winter Olympics".

Mediapedia (2018). "The Various types of Crypto Tokens".

Reyburn, Scott (2021). "JPG File Sells for $69 Million, as 'NFT Mania' Gathers Pace".

Criticism of Blockchains

The blockchain technology and its ecosystem are surrounded by hype and craze. Nevertheless, this enthusiasm ought to be curbed. It is certainly a powerful technology with many applications, and is often presented by its advocates as a panacea. However, as previously highlighted, this is quite removed from reality. The technology is not the solution to all problems, nor is it suited to all needs. The transparency and immutability features can be counterproductive and incur new risks in some cases. Moreover, despite popular belief, the security of the blockchain is not bullet-proof. It relies on the absence of coalitions of nodes, and the need for users to keep their credentials safe. In addition, errors in the code or governance protocol of the blockchain can allow for malicious actors to take control of certain assets or transactions. In the last year, these supposedly theoretical scenarios have actually happened.

Despite the craze, blockchain technologies have been highly criticized for their impact on society. Cryptocurrencies, such as Bitcoins, have often been associated with criminal activities. Certainly, at first, criminals have leveraged these tools, and developed new scams owing to the financial craze of crypto-assets. Nefarious actors and heinous groups have used crypto-assets to fund themselves. However, such behaviours are not new or unique to the blockchain ecosystem. In addition, law enforcement agencies and courts have now caught on, and anti-money laundering frameworks have been updated accordingly. Major illicit platforms—such as the infamous Silk Road—have been dismantled, and new frameworks are cracking down on criminal activities.

The use of blockchains also generates environmental concerns and criticism. The adoption of crypto-assets, smart contracts, DAOs and NFTs are enmeshed in controversy for their high energy use and the ensuing greenhouse gas emissions associated with blockchain transactions. Indeed, blockchains—notably those relying on proof-of-work protocols—require a significant amount of computational power, and thus of energy, generating large carbon emissions. In June 2018, the Bank for International Settlements criticized the use of public proof-of-work blockchains for this high energy consumption.

A recent study from Cambridge University estimated that by 2022, the Bitcoin and the Ethereum blockchains together will release up to 120 million tonnes of CO^2 each year. In November 2021, the Swedish Financial Supervisory Authority and the Swedish Environmental Protection Agency called for a European Union-wide ban on energy-intensive cryptocurrency mining, stating that crypto-assets are a threat to the climate transition. The agencies considered the potential benefits and found they were outweighed by the "enormous" energy consumption and carbon footprint. They consider that, without an EU-wide ban of energy-intensive mining, the EU will not be able to meet its climate targets. While contested, a ban of the "proof of work" consensus has also been advocated for by the vice-Chair of the European Securities and Markets Authority. It should be noted that the environmental impact of mining could be considered as infringing on the right to a healthy environment as protected by the European Court of Human Rights under its constructive interpretation of Articles 2, 5 and 8 of the European Convention on Human Rights.

In light of these criticisms, developers are turning towards less energy-intensive mining protocols like "proof of stake." Indeed, the Ethereum platform will be moving to a "proof of stake" protocol in 2023. Other options include looking into moving some operations off-chain to keep only the key elements that need to be automated or that are at risk of being tampered with.

In addition, crypto-asset miners are keen to use more renewable energy, and some initiatives look at recycling the heat generated by the mining activities. In British Columbia, MintGreen partnered with the city of North Vancouver to heat a hundred houses and industrial buildings. In France, WiseMining developed mining boilers with which users can heat their homes by mining bitcoins.

Crypto-asset miners are also increasing their presence in cold climate regions that naturally cool computers and reduce energy bills and consumption. They are moving to countries that have low or subsidized energy fees. Yet, these energy-based considerations may include governance and geopolitical risks for blockchain platforms. Indeed, they could lead to a concentration of groups of miners in specific regions that could threaten the governance of the distributed system. If 51% of the miners of a blockchain are within a single jurisdiction, the network risks being controlled or tampered with by the government.

References

Association pour le développement des actifs numériques (2022). "Ban of Proof-of-Work protocols: wrong answer to real global environmental challenges".

Cambridge Centre for Alternative Finance (2022), "Comparisons," Cambridge Bitcoin Electricity Consumption Index.

de Vries, Alex, Ulrich Gallersdörfer, Lena Klaaßen & Christian Stoll (2002). "Revisiting Bitcoin's carbon footprint," Joule.

Shin, Hyun Song (2018). "Chapter V. Cryptocurrencies: looking beyond the hype," *BIS Annual Economic Report*, Bank for International Settlements.

The Economist (2022). "The charm of cryptocurrencies for white supremacists."

Thedéen, Erik & Björn Risinger (2021). "Crypto-assets are a threat to the climate transition—energy-intensive mining should be banned," Finansinspektionen—Swedish Financial Supervisory Authority.

Weinstein, Jason (2021). "Why Bitcoin is Better for Crime Fighters than Criminals."

2. Opportunities for Human Rights and Democracy

Blockchain technology presents an opportunity for government, international organizations, non-governmental organizations, industry stakeholders, and, more generally, members of the public to engage in the recognition of and respect for human rights as well as to resolve current human rights issues.

First and foremost, blockchains can support fundamental freedoms by facilitating the pseudo-anonymity of users on the Internet. At the same time, blockchains are proposed as platforms to develop secured digital identities, and notably self-sovereign identities that can provide documentation to refugees and migrants. The technology could also enable personal autonomy by facilitating information self-determination for citizens.

Building on those capacities, blockchain features have been leveraged in the humanitarian context to bring transparency, support aid distribution, provide financial services to the unbanked and ensure fair wages for workers. Blockchains can also help combat human rights abuses in supply chains and to secure land titles. The technology has been proposed to support democratic functions, such as enabling secured voting platforms and collaborative law making. Moreover, blockchains and smart contracts have been deployed to support dispute resolution mechanisms, and have been suggested to support state courts and evidence chains of custody.

Those are just some examples of how the technology can be used to advance democratic functions and ensure accountability and transparency. This section describes some of those current and potential applications of blockchain technology to support human rights and democratic functions, as well as to empower individuals and marginalized communities. As blockchain technology develops, its applications in resolving human rights issues will expand. Over the next few years, it will be important for industry stakeholders, governments and members of the public alike to familiarize themselves with blockchain as an invaluable resource, which will allow them to accelerate humanitarian responses around the globe.

Fostering Freedom Through Pseudo-Anonymity

On public blockchains, the pseudo-anonymity of users prevails. As previously mentioned, only their public address is visible and it is, in principle, impossible to know who is behind a public address. It could hide a company, an institution or an individual.

Certainly, the pseudo-anonymity that prevails on blockchains involves risks that are often highlighted. Transactions in crypto-currencies could facilitate tax fraud, allow massive money laundering and finance terrorism. However, this pseudo-anonymity concurrently offers guarantees in terms of freedom and privacy. Indeed, even if all transactions are theoretically transparent on open blockchains, these transactions are not explicitly linked to individuals or organizations in the physical world. This makes it possible to protect the identity of the parties, to guarantee them full freedom of action and to protect their personal data.

Benefits of Pseudo-Anonymity for Fundamental Freedoms

The pseudo-anonymity promised by blockchain technology ensures that freedoms are respected. For example, being anonymous online may condition the freedom of expression of some people. It is indisputable that anonymity protects the freedom of individuals to communicate information and ideas that they would otherwise be prevented from expressing. Similarly, anonymity guarantees the freedom of individuals to live private lives. These considerations explain why the “right to anonymity” is for many an essential guarantee, so much that the organization ARTICLE 19 considers anonymity a fundamental right, which includes the right to anonymous speech, the right to read anonymously and the right to browse online anonymously. From that perspective, encryption is seen as a basic requirement for the protection of the confidentiality of information and its security, which is essential to the protection of the right to freedom of expression online. Guaranteeing an effective anonymity on blockchain platforms is not only necessary to preserve privacy in general, but also to ensure personal data protection. Data protection is indeed achieved if the data subjects are not identifiable. As such, the pseudo-anonymity of blockchain technology supports the objectives of the European Union’s *General Data Protection Regulation* and the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention 108).

Limits of Pseudo-Anonymity

The scope of the pseudo-anonymity guaranteed by blockchain must be qualified. Indeed, as explained in Part 1, it is often possible to discover the real identity of users. On private and permissioned blockchains for which access is restricted to a small number of people, the identity of the users is *a priori* known to the person who administers the platform. On public and open blockchains, users are often forced to reveal their identity. To store and transfer crypto-assets, users generally create an online wallet with a service provider, which usually involves revealing one’s identity. Anti-money laundering regulations impose obligations on providers similar to those imposed on traditional financial services, such as the identification of their customers under the “Know Your Customer” (KYC) obligation, the monitoring of customer activities and the reporting to national financial intelligence units. Platforms perform checks and require proof of identity, such as a copy of a driver’s license, a passport or an invoice. In addition, in practice, many wallets on those platforms may be linked to real bank accounts or credit or debit cards.

It is still possible for users to forgo creating an online wallet and store their private key in an offline wallet—whether hardware wallet or paper wallet—that is completely disconnected from the Internet and does not require them to disclose their identity. It is also possible to store their private key directly on their computer. But even in these last hypotheses, the risks of re-identification are real; insofar as it is possible on a public blockchain to trace all transactions coming from a given public address, re-identification of the owner of the address from known elements is possible with the help of machine-learning tools.

Strengthening Anonymity on Blockchain Platforms

A number of techniques have been developed to enhance anonymity on blockchain platforms. New crypto-currencies called “privacy coins” have emerged in an effort to guarantee true anonymity and privacy. Newer coins such as Monero, Zcash and Dash, were specifically designed to guarantee the anonymity of their users. These privacy coins use anonymity-enhancing technologies to prevent revealing transactions’ details, or to make it very difficult to track transactions. These include Zero-Knowledge Proof (ZKP) techniques, stealth addresses and circular signatures.

The ZKP techniques are one of the most promising developments for privacy. It makes it possible to answer a binary question (true/false) without ever having to reveal the information supporting their assertion. This allows, for example, someone who claims to be over 18 years old to attest to this without disclosing their date of birth. All they have to do is scan a QR code and have an algorithm perform an operation that simply returns a “yes” or “no” answer to the question of whether the person is over 18. At no point does the person have to reveal any other information, thus preserving their privacy. This technique can also be used to prove other information, such as the fact that a person is authorized to work in a country without having to disclose their marital status or nationality. It is also possible, thanks to this technique, to publish transactions on the Zcash platform without giving any details about the transaction amounts or the public addresses involved. Additionally, the ZKP protocols allow for the removal of the historical links between transactions. Users prove that they own the tokens at the time of the exchange and then the tokens are destroyed ("burned") to make room for new, blank tokens (with no history) to be used in the transaction. As there is no relation between the new tokens and the destroyed tokens, it is impossible to make a link between a token and a user.

Other techniques are used to avoid re-identification. For example, a new pair of keys can be used for each transaction. Transactions can also be grouped together in such a way that it is impossible to discern the parties to the transaction, or so their identity can be hidden within other transactions by linking a single transaction to multiple public keys, even though the transaction came from only one of the public keys. Sometimes the techniques are combined for greater effectiveness. In this manner, on the Monero platform, it is possible to hide the amount of the transaction and the public address (key) of the sender and receiver through a combination of techniques, since, for each transaction, a new public address and corresponding private key are generated.

In parallel to "privacy coins," some initiatives simply aim to create privacy-friendly environments such as Oasis Network and Secret Network, which are designed to run smart contracts in a privacy-by-default environment to protect user data as well as the confidentiality of the operations. For example, the Secret Network's nodes process and store data in secure environments that operate like a "black box" that cannot be tampered with. Since data is encrypted and private by default, users have "viewing keys" to view their sensitive data. They allow users to maintain control over their data and decide what is shared and with whom.

Advances in anonymization techniques can rightly cause concern for authorities who fear the proliferation of fraudulent and illegal activities. It is therefore important to find the right balance between the imperative of privacy and data protection, and the objective of combating illegal activities. It should also not be forgotten that the prevention of criminal offenses often takes precedence over data protection requirements, even under the GDPR (Recital 19).

References

ARTICLE 19 (2015). "Right to Online Anonymity: Policy Brief."

ARTICLE 19 (2019). "Blockchain and freedom of expression."

Ferdous, Md Sadek, Farida Chowdhury, & Madini Alassafi (2019). "In Search of Self-Sovereign Identity, Leveraging Blockchain Technology," IEEE.

Fink, Michèle (2019). "Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?", European Parliamentary Research Service.

Zyskind, Guy, Oz Nathan & Alex "Sandy" Pentland (2015). "Enigma: Decentralized Computation Platform with Guaranteed Privacy."

Zyskind, Guy (2021). Introducing SCRT Labs—An Evolution of Enigma.

Supporting Digital Identity

Traditionally, the authority entitled to establish the identity of individuals is the state, which does so on the basis of its own identification methods. The state establishes the official identity of individuals from various information provided (name, gender, date of birth, place of residence, etc.) and issues official identity documents on this basis. Things are different in the virtual world. The question of the identification of individuals online arose along with the first computer networks. From the outset, the equipment used by Internet users has included means of identifying users to some degree through, *e.g.*, their IP address. However, as the number of online exchanges and transactions increased, more in-depth identification methods became necessary and were gradually offered by digital service providers. These providers have developed centralized online identity management systems. Based on certain information provided by users, these systems assign users an “identifier,” which may correspond to the user’s official identity or to a pseudonym, depending on the case, and may be attached to a certain amount of information. For example, to make online purchases, the user must register on an e-commerce site and provide their name, address, e-mail, telephone, bank details, etc.

Online, there are “trusted third parties” who have the power to define the methods of identification of a person, to attribute an “identifier” to that person and to secure their identification with the help of credentials (*e.g.* passwords, code). These “trusted third parties” are private entities. Some even delegate authentication to other trusted third parties, such as when users are prompted to log in with their e-mail address or with their social media identity. Often, such identification services are offered by large technology companies (*e.g.* Apple, Google, Facebook) that provide reliable and secure identification services. In 2008, the creation of Facebook Connect allowed Facebook (now Meta) to occupy an increasingly important place in the digital identity market.

However, relying on “trusted third parties” is very problematic because it makes users dependent on large platforms that control accounts and always have the ability to arbitrarily cut off access. In addition, users have to share a large amount of personal information, without always knowing what use will be made of their data. Platforms use their identity management business to systematically collect user data, track users and engage in targeted advertising. In such an environment, individuals’ data is held by a number of private entities, which possess information that users have been forced to share with them in order to conduct online transactions. The security of this data is not always guaranteed, since data leaks and identity theft remain frequent in the virtual world.

In such a context, blockchain technology could allow users to free themselves from the controlling practices of these large technology companies. Decentralized structures allow the development of new models of digital identity management in which users control their digital identity: “self-sovereign identity” (SSI). It is believed that SSI could even compete with the current monopoly of state-assigned identities. While this may seem exaggerated, an SSI system can compensate for the absence of state-issued identity documents, either because they have been lost or destroyed, or, quite simply, because the state in question failed to provide them. It could also help in cases where the identity document is not recognized by a state, *e.g.* in the case of diplomatic conflicts.

Controlling Identification: The Concept of “Self-Sovereign Identity” (SSI)

The development of “self-sovereign identity” (SSI) aims to place users at the center of their digital identity by allowing them to control their own virtual identity. Since the early 2000s, new methods of creating digital identities have been centred on the user’s consent and the objective of interoperability. The goal is for users to no longer need to divulge personal information every time they log onto websites. However, it is not possible to truly relinquish control to users within the framework of centralized networks where a few private entities manage identities. This is how the concept of decentralized identity emerged to allow users to manage their own identity and to control the information they share in the form of certificates. Simply put, a decentralized identity allows for the full, clean and complete ownership of all information related to the user. Decentralized identities are not determined and held by each platform, but are part of a decentralized network designed in such a way that users retain control of their identity, while being able to authenticate themselves everywhere with the same digital identity. Decentralization also supports data minimization goals by providing only the necessary information to the platform itself. If a minimum age is required, the system can confirm that the threshold is met without disclosing the exact age; or if the age is required, the system can confirm it without disclosing the exact date of birth.

Blockchain technology enables the development of such decentralized identity systems in which identifiers and information are owned and controlled by users rather than by centralized entities. In fact, blockchain users are already identified by a public key visible to all and a private key that is personal to them and guarantees their control. Only the person who holds the private key has access to the account and the assets associated with it. The idea is to leverage this technical infrastructure to uniquely identify and authenticate a person or organization without the need to rely on a government authority or centralized registry.

The creation of a blockchain-based SSI involves a digital wallet application that allows the creation of SSI digital identifiers. When the wallet is created, one or more decentralized identifiers (DID) are generated and assigned. A decentralized identifier is a URL associated with a single identity, which can be in the form of a QR code. The DID links the individual to the DID Document which contains all public information about the identified person, starting with a public key designating the document’s controller. The DID Document is public, accessible to everyone, and can only be modified by its official controller thanks to the controller’s private key.

While the DID Document contains public information, the information to be shared is stored as “Verifiable Claims” (VCs). Once the digital identity wallet is created, it is possible for its holder to collect credentials from various organizations authorized to digitally deliver such credentials. These VCs, established and signed by trusted third parties, attest to the veracity of certain information. They can be issued by organizations such as governments (e.g. identity), universities (e.g. diplomas) and insurance companies (e.g. health coverage). Each VC credential is digitally signed by the private key of the issuing organization, which makes it possible to verify the reliability of the credential by consulting the DID Document’s issuer. The digital wallet can also include links to data stored in the cloud, such as encrypted medical records. The decentralized identity holder may, if necessary, decide to give permission to access this information to those who wish to view it.

SSI systems have many advantages. They allow users to create multiple digital identities, to browse discreetly online by presenting their credentials without being tracked and to limit the volume of data collected on users. They also provide the security guarantees offered by decentralization, as data is not stored by a single centralized authority. They greatly reduce the risk of identity theft and, more broadly, fraud. Finally, they can manage all kinds of official information: birth or marriage certificates, passports, visas, residence permits, diplomas, social security documents, etc.

Currently, solutions are developed on public and permissionless blockchains such as uPort (now Veramo), Jolocom or Sovrin, while others are developed on consortium blockchains such as KYC Chain or ID2020. The Civic project has proposed a unified identity verification system for the decentralized ecosystem where the Civic Pass allows users to download an application and configure it with various personal identity information (name, address, social security number, passport number, driver's license, etc.). The application encrypts this data using a private key issued by a third party, which ensures that Civic does not access personal identity information without user consent. Multi-factor biometrics (*e.g.* fingerprint scanning) secures the application and allows users to keep control of their data. The application only stores credentials, not the user's data itself. Users can then use their Civic Pass to be authenticated on various platforms without providing their personal information to those platforms.

It is unlikely that decentralized identity systems will make it possible to dispense entirely with states' role in attesting people's identity. Indeed, SSI systems require credentials to be issued by trusted issuers, and government authorities will always be needed to provide reliable information. However, the use of blockchain-based digital identity solutions can help all those who do not have official documents, either because they have never had any, because they have been provided with forged documents (as is often the case for migrants) or because these official documents have been destroyed or lost.

References

Allen, Christopher (2016). "The path to self-sovereign identity."

Bajpai, Prableen (2017). "How Blockchain Can Help Humanitarian Causes".

Crumpler, William (2021). The Human Rights Risks and Opportunities in Blockchain, CSIS.

Desai, Vyjayanti, Anna Diofasi & Jing Lu, (2018). "The global identification challenge: Who are the 1 billion people without proof of identity?", World Bank Blogs.

Der, Uwe, Stefan Jähnichen & Jan Sürmeli (2017). "Self-sovereign Identity—Opportunities and Challenges for the Digital Revolution."

Ferdous, Md Sadek, Farida Chowdhury, & Madini Alassafi (2019). "In Search of Self-Sovereign Identity, Leveraging Blockchain Technology," IEEE.

Lyons, Tom, Ludovic Courcelas & Ken Timsit (2019). "Blockchain and digital identity," European Union Blockchain Observatory and Forum.

W3C (2021). "Decentralized Identifies (DIDs), v1.0: Core architecture, data model and representation".

Wang, Fennie & Primavera De Filippi (2020). "Self-Sovereign Identity in a Globalized World: Credentials-Based Identify Systems as a Driver for Economic Inclusion," Frontiers in blockchain 2.

Enabling Informational Self-Determination

Blockchain technology can enable informational self-determination by offering alternative solutions for data management where users can regain control of their own data, and allow this data to be shared in a transparent and decentralized way. This ability is enhanced by the fact that platforms can run smart contracts to automate data sharing. Chiefly, blockchain technology can give users more control over the sharing of their personal data while ensuring data portability. In this respect, the technology can help guarantee "personal autonomy based on a person's right to control of his or her personal data and the processing of such data," as provided by the Preamble of the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention 108 Plus).

Blockchain is already used to share data between partners. One of many examples is the Blockchain Insurance Industry Initiative (B3i), which enables the world's largest insurers to share data on natural catastrophe insurance contracts. This data sharing platform allows participants (*e.g.* insurers, reinsurers, brokers) to manage all administrative exchanges, from underwriting to premium and claim settlement. This is a permissioned consortium blockchain in that the data processed is related to a common activity (*e.g.* natural disaster insurance) and access to the data is restricted to a small number of people. B3i has recently been appointed by a coalition of European nuclear pools to develop a distributed ledger technology—based solution for the management of inter-pool reinsurance contracts.

It is also possible to create open architectures that protect individuals' personal data. As previously explained in relation to decentralized identities, blockchain makes it possible to conceptualize methods of managing and sharing data while allowing users to control their own data. Users can use their private key to authorize or deny third parties access to their data. A blockchain connected to an off-chain database storing the user's real data in encrypted form (using encryption keys belonging to the user) simply stores a hash of the data. The conditions of data sharing between the different actors is provided for in smart contracts, and each access remains subject to the user's agreement. Such a system guarantees total transparency and ensures that the data has not been modified, either by the user or by anyone else. Users would then have effective control over the use of their data.

Many initiatives have built on these functionalities, notably in the health sector. In Estonia, blockchain technology is being used to give patients more control over their health data. Every time healthcare records are accessed or changed, the occurrence is verifiable through blockchain's guaranteeing system, process and operational integrity. Patients can control and authorize access to their health data, even by medical professionals. Likewise, the MyHealthMyData project leverages a blockchain structure in which data subjects can authorize, deny and withdraw access to their data according to different use cases. The objective is to create a European-wide registry capable of anonymously collecting consents and allowing access to data anytime, anywhere and by anyone. Individuals, researchers, laboratories and health professionals could easily search and mobilize a large volume of data while ensuring the informed consent of patients, regardless of their location, the complexity of the data and the laws governing data protection. In the United States, Patientory uses blockchain to organize the consultation of medical records, and Medrec:M offers decentralized solutions for managing health data through an authentication log that governs access to medical records. All this could lead to large-scale sharing possibilities where medical records could be made accessible and interoperable to all hospitals belonging to the same network or region.

Beyond the health sector, the same approach could be extended to all areas where personal data sharing is necessary. For example, a consortium of fourteen European organizations have launched the Decode project, which aims to provide tools for individuals to control the use of their personal and non-personal data. Finally, Project Liberty aims to leverage blockchain to enable the creation of decentralized and interoperable social networks in which the user has sole control over his data, thanks to the DSNP protocol.

References

DECODE (2020). "DECODE: Giving people ownership of their personal data."

Fink, Michèle (2019). "Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?", European Parliamentary Research Service.

MyHealthMyData (2020). "A New Paradigm in Healthcare Data Privacy and Security."

Supporting Refugees and Vulnerable Populations

Blockchain technology could help trace and report on all stages of migration and asylum policy interventions, including asylum procedures, missing migrants, remittances and the administration of major databases.

Building on the mentioned identity capabilities, blockchain technology is increasingly promoted by governments, corporations and human rights advocates as a cutting-edge tool for addressing even the most intractable humanitarian and human rights issues, including those that acutely affect refugees, such as food insecurity.

Providing Identity to Refugees

According to the World Bank, more than one billion people, 80% of whom are in Sub-Saharan Africa and South Asia, face difficulties in obtaining an official identity document. In particular, most of today's 26 million refugees have lost their original identity documents. Without proof of identification, these individuals cannot access basic services such as education, healthcare or financial services, or even find housing or work. They remain disenfranchised and marginalized in society.

Blockchain-based SSI could resolve issues caused by lack of identification for vulnerable populations exposed to the risk of discrimination or exploitation, and allow them to effectively benefit from their most essential rights. Even without official documents, asylum seekers can reference the attestations and certificates they collect throughout the asylum seeking process in the host country. Blockchains can enable different organizations (*e.g.* NGOs, governments) to communicate with one another with certainty. Blockchain could therefore enable faster and more secure identification in case of massive migration flows.

For this reason, many projects aim to provide a digital identity to migrants, refugees and displaced persons. The United Nations-supported ID2020 alliance led by Microsoft, Accenture and several UN agencies has proposed a collaborative blockchain-based digital identification network to provide legal identification to 1.1 billion people with no official documents worldwide. In Kenya, the blockchain platform BanQu has helped Somali refugees establish a permanent and verifiable digital identity. Such blockchain platforms can provide digital identification and digital proof of birth or education credentials on a single system. Furthermore, using blockchain technology to manage these identification pieces would allow different organizations, governments and institutions to communicate with each other with certainty. It would also allow for quicker identification in case of migratory flow or separation of families. The technology has indeed been proposed to support and track the reunification of children with their parents.

Combating Child and Human Trafficking

The implementation of open records of identification can help prevent trafficking. The United Nations Office for Project Services (UNOPS) is currently partnering with the World Identity Network and the United Nations Office of Information and Communications Technology to pilot a blockchain project that helps identify those who have lost legal identification and, in doing so, aids in combating child trafficking. This project is part of "Blockchain for Humanity," announced during the Humanitarian Blockchain Summit in New York on November 10, 2017. According to United Nations statistics, nearly half of the world's children under the age of five do not possess a birth certificate. These children are "invisible" to governments or development agencies that design and deliver social programs.

Undocumented children are easy prey for human traffickers, who often use fake identification documents to transport them across borders. Blockchain could not only help catch traffickers, as the children's digital identities would be tracked and stored, but it could also help secure data on an immutable ledger, making trafficking attempts more traceable and preventable. Similarly, U.S.-based Consensys won the bid to launch a digital identity pilot that would require children attempting to cross the border to scan their eyes or fingerprints, which would automatically notify their legal guardians by phone.

Managing and Distributing Aid and Resources

Blockchain systems could allow governments and international organizations to efficiently manage and distribute aid and resources, and help increase transparency and accountability when channeling and spending funds in third countries. It is not always clear how aid organizations are spending collected funds. Funds can too easily be discontinued or unaccounted for. The benefits, entitlements and aid processes of today often involve a significant amount of overhead and checks for compliance. Government programs such as social security and pension payments, medical care benefits, and domestic and international aid could benefit tremendously from blockchains. An open and centralized ledger could allow refugees, stakeholders and the public who provide such organizations with funds to monitor expenses, to see whether and how refugee recipients are actually helped. It could also automate processes for eligibility verification and disbursement of funds, such as distribution of funds for those affected by a major natural disaster. In addition, blockchains could help to ensure that benefits reach their intended beneficiaries and are not diverted.

Some platforms have successfully supported aid distribution to refugees. The United Nations' World Food Program has supported the development of the "Building Blocks" project, a blockchain-based platform to address challenges in distributing aid to refugees. The platform facilitates cash transfers and delivery of food assistance for Syrian refugees in Jordan. It allows agencies to create virtual accounts for refugees and upload monthly cash deposits, and makes sure that the funds are only redeemable by the intended individual. People scan their iris to pay for their purchases in a supermarket, and this data is compared to a United Nations database. The programme has been able to reduce costs of administration and provide greater security and transparency for refugees who collect assistance.

Supporting the Unbanked Population

Blockchain-based implementations could also support unbanked populations. The non-profit Stellar Development Foundation currently provides access to financial resources to the world's unbanked population. Its decentralized blockchain includes partners from around the globe, and allows individuals to move money quickly, reliably and at almost no cost. In Venezuela, BitGive, a blockchain-based donation tracking platform, has been leveraged by organizations to collect and distribute humanitarian aid to struggling orphans, hospitals and animal rescue centres. In Uganda, the Humanity First Token, a virtual currency pegged to the national fiat currency, provides funds and means of payment to refugees for food, solar panels and other essential items at local vendors. In Sierra Leone, the nonprofit microfinance organization Kiva, working in collaboration with the United Nations as well as the Sierra Leonean government, has the ambition to provide every Sierra Leonean citizen with a decentralized blockchain-based identity to access financial services. Kiva is deploying a blockchain-based identity platform that will allow individuals to build a credit file based on their past interactions with banks and micro-credit organizations. Each individual can thus collect in their wallet certificates issued by the institutions with which they have already interacted. Then they can give access to these certificates to the credit organizations to which they apply for financing.

Supporting Labour Rights

Blockchain could also support fair and equitable labour rights for refugees. Smart contracts could create transparent records of employment and other agreements between refugees, workers who are often subject to human rights abuses, multinational organizations and exploitative local employers. Smart contracts could be used to resolve such issues and ensure refugee rights are respected in employment. Beyond lower rates for labour, employers may not always fulfill the initially agreed upon contract and the parties may not be able to seek legal recourse, as there is no physical employment contract. Smart contracts could help ensure that workers receive their fair and due pay. An oracle could automatically provide clocking time of the worker to a smart contract that would trigger immediate payment of the worker's wage.

Adverse Effects

While bringing transparency and accountability, the use of blockchain technologies can also have negative effects. Their overall benefit must be put into perspective when the technology is used to help vulnerable populations. Using blockchain for identification purposes implies that the people concerned are properly equipped, notably with smartphones and an Internet connection. This is not always the case for the most vulnerable populations. These problems with access to devices and the Internet have already led some aid groups to abandon SSI pilot projects because of the difficulties encountered. Therefore, some experts have downplayed SSI's usefulness and put into perspective it benefit as a tool to empower marginalized groups. Furthermore, the storage of users' private keys remains a sensitive issue, as these must be properly and individually secured, and it is nearly impossible to recover lost keys. Given these limitations, it should not be concluded that blockchain technology will be able to fully compensate for the absence or loss of official identification documents in the immediate future.

Moreover, as with any technological solutions used to manage data, breach of privacy is a risk, as the data can track the actions and movement of the individuals and the technology often relies on corporate or privately-owned solutions. When using public blockchains, even if personal details such as names are encrypted, the record of transactions is viewable to anyone with access to the blockchain. This might be quite delicate and sensitive for vulnerable populations such as stateless refugees. In the case of aid distribution, the fact that transactions can be verified to ensure the money is used for productive purposes such as shelter or food, rather than alcohol or drugs, implies a lack of trust that can be degrading for the receiver. In the case of wage distribution, such systems and records could, at the same time, be used by governments as evidence of illegal activity against refugees and migrants who do not have legal immigration status.

References

Arditti, Salon (2018). "How Blockchain Could Make Refugee Programs More Transparent."

Bajpai, Prableen (2017). "How Blockchain Can Help Humanitarian Causes."

Cheesman, Margie (2022). "Self-Sovereignty for Refugee? The Contested Horizons of Digital Identity," Geopolitics 27:1, 134–159.

Crumpler, William (2021). The Human Rights Risks and Opportunities in Blockchain, Center for Strategic and International Studies.

Gramatikov, Martin (2017). "Unchaining Access to Justice: The Potential of Blockchain."

Irrera, Anna (2017). "Accenture, Microsoft team up on blockchain-based digital ID network."

Orcutt, Mike (2017). How Blockchain is Kickstarting the Financial Lives of Refugees, MIT Technology Review.

Rueckert, Christian (2019). "Cryptocurrencies and fundamental rights," Journal of Cybersecurity, 5:1.

Stellar Development Foundation (2018). "Finance with a Mission."

Schrepel, Thibault (2019). “Blockchain and human rights: utopia, or dystopia, or both?”.

Talhouk, Reem, Kyle Montague & Andy Garbette (2018). “Blockchain for Refugees: Current Uses, Opportunities and Considerations”.

Wojno, Marc (2021). “Binance calls for global regulatory frameworks for crypto markets: Released 10 Fundamental Rights”.

United Nations Office for Project Services (2017). “World Identify Network and United Nations team up to launch innovation blockchain pilot to help prevent child trafficking.”

World Food Program (2018). “Building Blocks: Blockchain network for humanitarian assistance—Graduated Project.”

Reducing Human Rights Abuses in Supply Chain

When buying from large companies, customers are often completely unaware of human rights abuses and crimes committed by distributors of these large companies. This is seen in a variety of industries, from food production to diamond mining. In addition to human rights abuses, customers are unaware of product supply chains or whether their food has been harvested ethically.

Blockchain platforms could allow customers and stakeholders in supply chains to monitor distributor practices. Indeed, they offer unique opportunities to address both transparency and traceability issues for supply chains with the creation of a common, trusted record for the provenance of goods and the conditions of their production at all stages of procurement. This would improve the transparency both for the customer and for all the supply chain actors by helping them carry out due diligence and remedy human rights abuses in the supply chain. It would also increase accountability by recording third-party certifications, and facilitate audits both with respect to human rights, worker conditions and environmental concerns.

For example, to answer calls for transparency by customers Everledger has collaborated with jewellers to launch a blockchain platform to track every detail surrounding the production of diamonds. When purchasing a diamond, customers can verify that it was sustainably produced. Provenance, a company based in the United Kingdom, uses blockchain to trace the origins and histories of products. Individuals across the globe can download the Provenance mobile application and view the journey of their purchased products. In France, the agrifood industry developed a blockchain to ensure the traceability of chicken production. Similarly, the World Wildlife Fund for Nature has collaborated with fishing companies to develop a blockchain tracking platform for tuna fisheries.

While blockchain cannot eradicate unfair practices in the global market, it does provide the public with access to information. As members of the public become more aware of the context surrounding their purchases, they will be better able to make informed choices.

References

Commandré, Ysé, Catherine Macombe & Sophie Mignon (2021). Implications for Agricultural Producers of Using Blockchain for Food Transparency *Sustainability* 2021,*13*,9843.

Crumpler, William (2021). The Human Rights Risks and Opportunities in Blockchain, CSIS.

Project Provenance Ltd. (2018). “Create and publish engaging, trustworthy sustainability content.”

Tholen, Jerwin, Dennis de Vries, Audrey Daluz, Claudiu-Cristi Antonovici & Wietse Van Brug (2019). “Is there a role for blockchain in responsible supply chains?”, OECD Centre for Responsible Business Conduct.

Walport, Mark (2015). “Distributed Ledger Technology: beyond block chain,” UK Government Office for Science.

Protecting Land Titles and Real Estate Ownership

Land registries are an essential tool to ensure the right to private property on real estate, from zoning to recording changes of ownership. Such registries could be destroyed in the event of a natural disaster or a cyber-attack. As a result, the owners would be deprived of legal means to claim their rights, given that the government would have no record of land titles and prior ownership. This also means that property owners would have no way to prove they are entitled to compensation in case of damages. Even without disasters, land registries are very precarious in certain regions of the world, either due to the lack of administration, poor record-keeping or authorities' corruption. Some marginalized groups are subject to inequitable or discriminatory allocation of land, while some communities have issues asserting their rights over ancestral lands.

The blockchain technology could be leveraged to provide a secure and transparent record for land titles that would be protected against tampering, disasters and abuses. It could improve the resilience of registries and ensure the rights of private owners, including by making sure that lands owned by marginalized groups are not transferred without their consent. It may also bring efficiencies and reduce costs associated with land transactions and record keeping.

The start-up Bitland has proposed blockchain for land title protection in Ghana by keeping property deeds on a public ledger. By doing so, land disputes can be resolved by viewing the record kept on the blockchain. This prevents human errors and lost land records. India, Georgia, Ukraine and Sweden have also begun to implement similar structures to facilitate land title management and the sale of real estate, where a blockchain application records detailed information on the properties being sold as well as each step in the sales transaction.

References

Center for Social Innovation (2019). "Blockchain for Social Impact: Moving Beyond the Hype," Stanford Business.

Crumpler, William (2021). The Human Rights Risks and Opportunities in Blockchain, CSIS.

Eder, Georg (2019). "Digital Transformation: Blockchain and Land Titles," OECD Global Anti-Corruption & Integrity Forum.

Kim, Christine (2021). "Sweden's Land Registry Demos Live Transaction on a Blockchain."

Nimfuehr, Marcell (2017). "Blockchain application land register: Georgia and Sweden leading."

Oprunenco, Alexandru & Chami Akmeemana (2018). "Using blockchain to make land registry more reliable in India".

Supporting Voting and Democratic Transparency

Blockchain technologies have the potential to enable new methods of voting by transforming what often remains a paper-based process in countries, or an electronic process with limited validation and auditability capacities. This can enhance the convenience and confidence for citizens. By ensuring that individual votes are eligible and counted correctly, the reliance on blockchains could potentially help prevent voting issues such as ballot rigging, which persists in many countries. These issues, if not overcome, can result in a lack of trust in democratic processes and can enable election results that do not reflect the wishes of the public.

The central features of blockchain technology can democratically empower individuals because they can decentralize and diffuse authority. This empowerment can be accomplished through blockchain networks, where members take part in decision-making processes as a new form of direct democracy.

Blockchain and accompanying software tools can offer services to states to help run elections in a secure and transparent way, guaranteeing the authenticity of every vote cast and making sure the vote count is accurate. The outcome of an election can be heavily influenced by the absence of a credible voter registry at the outset. Moving a voting system onto a blockchain could help prevent voter fraud because blockchains are encrypted, decentralized, and incorruptible. Such a voting network could not be corrupted by a single party, essentially because it would not exist in a single place. Furthermore, on a blockchain, signatures could be digitally collected and registered. As an immutable record of signatures is created, the possibility of fraud is further decreased. Such a secure digital ballot box could be adopted by communities, political parties and corporations worldwide, increasing public participation in the democratic process by making voting more accessible.

Blockchain platforms would not only support voting for political parties, but they could also allow for greater participation in the law-making process. Digital signatures could be used to allow a new bill to be introduced into a legislative house. In 2016, the Institute for Technology and Society of Rio de Janeiro (ITS Rio) built a blockchain-based application called Mudamos that establishes the identity of voters based on a unique identification number that each voter and taxpayer receives from the Brazilian government. It then allows them to formally express their support for socially-driven draft bills. In the first two months after launch, 600,000 people downloaded Mudamos and 7,000 law proposals have been received so far. Blockchain could help resolve the high demand for effective civic participation.

Blockchain open platforms could also increase transparency and accountability of financial aspects of political parties and political campaigns. Nevertheless, there is regulatory risk to blockchain technology being outlawed or regulated by governments, particularly corrupt ones. These concerns make the need for action by those with an interest in preventing human rights and other abuses even more important.

While blockchains are good at providing security, accuracy and transparency for e-voting and democratic activities, some factors may hinder mainstream public acceptability or effective deployment within communities, such as connectivity and digital literacy, especially depending on how the system is designed.

References

Biehl, Zoe (2018). "6 Ways Blockchain is Radically Improving Global Human Rights."

Boucher, Philip, Susana Nascimento & Mihalis Kritikos (2017), *How blockchain technology could change our lives*, European Parliamentary Research Science.

Chaum, David, et al. (2016). *The Scantegrity Voting System and its Use in the Takoma Park Elections*, Auerback Publications.

Hughes, Kobina (2017). "Blockchain, the Greater Good, and Human and Civil Rights," Metaphilosophy 48:5 654-665.

ITS Rio. "Mudamos."

Ledger Insight (2020), "Russia's blockchain voting site crashes soon after it went live."

Ledger Insights (2021), "Korea to trial blockchain in large scale online voting."

Lemos, Ronaldo (2016). "Using the Blockchain for the Public Interest."

Nasser, Yomna, Chidinma Okoye, Jeremy Clark & Peter Y A Ryan (2018). *Blockchains and Voting: Somewhere between hype and a panacea (A Position Paper)*.

Zambrano, Raul, Ruhiya Kris Seward & Phet Sayo (2017). *Unpacking the disruptive potential technology for human development*, International Development Research Centre.

Powering Dispute Resolution and Justice Systems

There have been several solutions aimed at providing dispute resolution solutions via arbitration procedures encoded in smart contracts. Employing smart contracts for the purposes of dispute resolution might provide a solution for the enforcement of online dispute resolution decisions. These platforms offer "decentralized justice" services through mechanisms coded in smart contracts. Disputes arising out of or in connection with an agreement are resolved by private adjudicators through self-enforcing decisions. The procedure followed is automated and not controlled by anyone.

The main platforms are Kleros, Aragon and Jur. The Aragon platform has set up a particularly original dispute resolution system that involves "guardians." Anyone wishing to bring a dispute to the platform pays a deposit—which is returned if the case is won—and presents their arguments. Users wishing to act as "guardians" in the resolution of the dispute must activate their tokens in Aragon Court's smart contract. The more tokens a guardian has activated, the higher the probability of being selected. When a "guardian" is "drafted" for a dispute, a portion of their activated tokens is locked until the dispute is finalized. Unlike traditional courts, Aragon Court "guardians" are not supposed to rule impartially on disputes but instead are asked to rule the way the plurality of guardians is expected to rule. To incentivize consensus, "guardians" who do not vote in favor of the final ruling have their locked tokens slashed. "Guardians" who vote in favor of the final ruling are rewarded with dispute fees and tokens from "guardians" who voted with the minority

There is potential for further automation of dispute resolution and enforcement, but there is also the fundamental question of how to safeguard fairness and due process within such decentralized networks outside of state control. Still, there is no reason why blockchain-based solutions could not work within public dispute resolution as well. Traditional courts are not adapted to small transnational disputes. As technology develops, these issues of access to justice are becoming increasingly urgent.

Vitalik Buterin, the co-founder of Ethereum, is unsurprisingly an advocate of using blockchain-based arbitration for smart contracts. However, he does not think this solution is a worthy competitor to traditional courts. He stated that "it arguably competes with existing private arbitration more than anything else. Traditional courts serve the very important function[] of figuring out what the appropriate remedy is when the parties to a dispute have no prior relationship, and so they did not agree to any arbitration between themselves." Similarly, although the lodging of a court claim is likely to be seen as disproportionately costly considering the low value of the majority of the disputes, it must be noted that automated enforcement is only possible on online assets and operations. States maintain a monopoly over the use of force over digital assets that are out of reach of smart contracts, and over non-digital ones. They also are responsible for dealing with non-compliance of a decision. This holds true not only for judgments issued by a state court, but also for arbitral awards.

Still, blockchain could also be leveraged by the justice system. In most countries, justice has an enormous information management issue. Justice systems have an issue with the quality of their data, and often rely on legacy systems and processes for their data management. As blockchain-based proposals have successfully addressed these challenges for corporations and financial activities, blockchain technologies could present a unique opportunity for public systems to increase accuracy and transparency through secure, auditable, distributed records.

In all countries, but especially in those where corruption is a concern or where law enforcement and the justice systems have lost public confidence, blockchain technology could be leveraged to secure the chain of custody for evidence. Some countries, such as China, announced they were looking into developing blockchain records to track forensic evidence. Similarly, some companies have proposed tools to law enforcement agencies such as the Kinesense video investigation platform, which leverage blockchain to secure digital evidence from the point of ingestion to the creation of reports. Hashes of the digital evidence can then confirm the authenticity of any exported evidential report and prove the chain of custody.

References

Koulu, Riikka (2016). "Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement," SCRIPTed 13:1 40.

Redman, Jamie (2016). "Vitalik Buterin: Blockchain and the Future of Courts."

3. Legal Issues Regarding Distributed Technologies

In the libertarian crypto-anarchist perspective that has inspired blockchains since their inception, the technology is intended to develop outside of any centralized control, and therefore outside of any state regulation. In other words, for its promoters, blockchain aims to constitute an "order without law," regulated solely by computer code. Some of the systems implemented today may create a sentiment of lawless order. Others integrate or implement private, automated, coded regulation systems. It has been argued that widespread deployment of this technology would create the expansion of a new subset of law called *lex cryptographia*. Some die-hard advocates believe that these cryptographic systems are harder, if not impossible, to regulate. According to them, blockchain networks would be the ultimate version of "code as law," which would result in society moving from the "rule of law" to the "rule of code."

However, this perspective is *not* tenable for the jurist or the regulator, and it has been proven wrong across the world. While we have powerful algorithms, behind those algorithms are humans who create them. The algorithms are not left to make all of the decisions by themselves. Therefore, as a society, we must refrain from oversimplifying our thinking about technology and tackle current issues surrounding innovation instead.

Yet, the technology raises complex legal questions, whether in regards to the protection of anonymity and privacy rights; the legal status of automated contracts and decentralized autonomous organizations; or the conflict of law and jurisdiction due to the distributed and global nature of most implementations.

Personal Data Protection Concerns

As previously mentioned, despite the protection afforded by pseudonymity on blockchain platforms, the transparency feature of the technology can raise data protection concerns for users. From a legal perspective, it certainly raises the question of its compatibility with applicable data protection rules where personal data are concerned, to the extent that technology does not always prevent the identification of users.

The first blockchain projects were designed for the indefinite storage of data, in order to facilitate data integrity and auditability. The idea was that every transaction going back to the first block (the "genesis block") would remain in the registry indefinitely. In this respect, the blockchain allows users to store, authenticate and secure data, giving the data an intangible and immutable character. However, these features conflict with the current objectives of personal data protection in that they run counter to key data protection requirements, such as data minimization, storage limitation, the right to rectify personal data, the right to object to processing and the right to erasure of data.

In 2019, Michèle Fink highlighted the many points of tension between blockchain technology and the principles arising from the European Unions' *General Data Protection Regulation* (GDPR). The GDPR is based on the assumption that there is always a "data controller" that data subjects can turn to in order to enforce their data protection rights. However, the decentralized nature of blockchains makes it very difficult to identify such "data controllers." In addition, the GDPR requires that data may be modified or deleted. Yet, the characteristics of blockchain technology make deletion or modification impossible, or at least very difficult. Admittedly, the GDPR's legal concepts present an uncertainty that does not always allow for precise conclusions about the compatibility of blockchain technology with the principles of personal data protection.

The points of tension identified with regards to the GDPR are also problematic and concerning under other data protection frameworks, and most notably conflict with the principles derived from the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention 108). Two key features of blockchain technology appear to be particularly problematic: the transparency and immutability associated with blockchains. As previously mentioned, many blockchain platforms are designed with transparency in mind, so that transactions can be seen by anyone and those who conduct them are eventually identifiable. This presents risks for users, and a potential liability for platform operators. In addition the principle of immutability which guarantees the integrity of the blockchain and avoids contradictions goes against the rights of accuracy and deletions. In principle, any attempt by a user to erase or overwrite existing data will be detected by others and corrected. However, even if an existing block cannot be modified, alternatives exist and are used today, such as adding a new transaction to rectify the information. While the initial information will still exist, people will first see the updated data. In addition, when the data is encrypted, it is always possible for the person who wishes to erase the data to destroy the encryption key. Once the key is destroyed, the data becomes indecipherable for everyone, which is almost the same as erasing it—assuming that the encryption cannot be broken.

On the whole, the incompatibilities with the rules organizing the protection of personal data ought to be nuanced given the great variety of existing blockchain platforms and their distinct technical characteristics. For example, techniques are being developed to reinforce confidentiality and anonymity and to give users more control over their data. Some platforms only allow authorized users to access the information stored on the blockchain, and others are designed to ensure the secrecy of transactions, preserve anonymity and keep transparency to a minimum. It should be noted that off-chain storage of personal data could be part of the solution, since only transaction data would be on the blockchain. Personal data could be securely stored in a cloud held by a third party under the control of the user, which would then also allow for its deletion or modification. Such a system would be desirable to ensure that users who have lost their private keys can still retrieve their data. This, however, presents security risks as a third party could take control of the keys.

Ultimately, it appears that the objective of protecting personal data must, above all, be taken into account by the developers designing the architecture of blockchain platforms. They will have to ensure that the modes of governance and the operations on the blockchains are determined in such a way that data protection is guaranteed.

References

Commission Nationale Informatique & Liberté (2018). “ Solutions for a responsible use of the blockchain in the context of personal data, ”.

Fink, Michèle (2019). “Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?”, European Parliamentary Research Service.

Rueckert, Christian (2019). “Cryptocurrencies and fundamental rights”, Journal of Cybersecurity, 5:1.

Conflict of Laws and Jurisdictions

One of the biggest legal challenges for blockchain-based systems is the determination of the applicable law and competent jurisdiction due to the technology’s distributed nature. Though the challenge of jurisdiction and applicable law for global networks, such as the Internet, is not new, the distributed ledgers further elevate the issue. While for a website the location of the parties, the servers, or the accessibility of a service can be established, the same cannot be as easily achieved for blockchain-based applications. On a blockchain, the content and actions can run through nodes and operators performing operations all over the globe and across many jurisdictions. Those nodes can be in any jurisdiction at any time, and new actors can join or leave the network at any time from any jurisdiction.

In an entirely distributed environment, there is no precise substantial link to determine the applicable law. Even if the applicable law can eventually be determined, it is coupled with uncertainty as to the competent jurisdictions if nothing was agreed upon at the beginning. Of course, it may happen that the parties have taken care to include provisions for the governing law, as well as the choice of forum for litigation—*e.g.* comments in the code of the smart contract, DAO or NFT that include actual contractual provisions. Some jurisdictions allow parties to elect a jurisdiction and a governing law if there is a substantial link to the jurisdiction. Due to the distribution of the ledger, it would theoretically be possible for a party to elect a forum in another jurisdiction where a node is run. In the matter of dispute resolution, the contract could also include an arbitration clause. But when one is not provided, the difficulty is all the greater as it can be complex to locate the nodes, or identify either the server or the natural or legal person responsible for administering the platform. Moreover, even when the parties are identified, traditional litigation is not necessarily easy if they are geographically distant.

As previously pointed out, it may happen that, even where the parties have not entered into any legal contract in the formal sense of the term, the methods of settling disputes are provided for in smart contracts by the platform's computer code. The use of "decentralized justice" can be very effective and adapted to the platform economy. However, these very unique methods of dispute resolution must be used with respect for the rights of the parties and for due process. It is, for example, necessary that the online dispute resolution method proposed by the previously discussed Aragon platform truly respect the procedural rights of the parties.

In any other case, determining the applicable and appropriate rules can be quite a headache. Considering so many competing norms and jurisdictions, one could argue that none should apply. Blockchain-based solutions would be systems, contracts and organizations without law, and out of any governmental purview. By design, this is certainly what crypto-anarchists were looking for. However, this is not a tenable position for the rule of law—nor is having competing jurisdictions. It could be appropriate to develop a body of general principles—such as the UNCITRAL or Unidroit principles—to govern the determination of the applicable law and competent jurisdiction for distributed systems platforms. Such principles would also propose a uniform framework to regulate blockchain platforms with a certain number of common rules considered essential (*e.g.* consumer information, amendments, recourses, etc.).

References

Guillaume, Florence (2019). "Chapter 3: Aspects of private international law related to blockchain transactions", in Kraus, Daniel, Thierry Obrist & Olivier Hari (2019). *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law*, Edward Elgar Publishing.

Wright, Aaron & Primavera De Filippi (2015). "Decentralized Blockchain Technology and the Rise of Lex Cryptographia".

Werbach, Kevin (2018). "Trust, but Verify: Why the Blockchain Needs the Law", Berkeley Technology Law Journal 33:2 487.

Werbach, Kevin (2018). *The Blockchain and the New Architecture of Trust*, MIT Press.

Smart "Contracts"

The introduction of smart contracts has raised questions about how this latest technological development conforms to traditional contractual doctrine. Smarts contracts may not always be contracts at law, either because they lack foundational requirements or do not meet formalist requirements of specific frameworks. However, smart contracts could revolutionize the practice of contract law and they do not appear to shake the foundations of contract law. Indeed, scholars, legislators and courts have discussed the digitalization of contracts for decades. States have subsequently amended paper-based provisions and allowed adaptive measures for agreements contracted in the digital world, notably based on UNCITRAL principles. As a result, smart contracts can easily interface with the law of contracts, either under common or civil law, even though their practice may raise issues related to enforcement and jurisdiction. Nonetheless, such issues are not exclusive to smart contracts, and are rather the product of the ubiquity of the digital context.

Legal Status

If we keep in mind that the smart contract is only a simple computer program, it may be logical to dissociate it from the agreement of the parties, and therefore from the contract in the legal sense of the term. Even if the smart contract were to result in the concluded agreement, it might not be able to replace the actual contract. It is, however, easy to distinguish the contract from the smart contract when an agreement has been expressly concluded between the parties before the implementation and/or execution of the smart contract. In this case, the smart contract does not correspond to the agreement itself, nor to the expression of this agreement, which was concluded verbally or in writing, even if it was in electronic form. It is simply a means of execution.

Often, smart contracts may not be executing a more traditional contract but may be the only expression of the will of the parties. In these cases, while they share the same name, could such smart contracts be considered contracts at law? It is tempting to see the smart contracts as the expression of the contract binding the parties: this is the "code-only smart contract" hypothesis. The smart contract could represent and materialize the agreement concluded and could, in this respect, serve as evidence of the existence of the contract. However, for a smart contract to be considered as an enforceable contract under law, it needs to satisfy all of the requirements of a valid contract.

At law, a contract is an agreement between two or more persons which gives rise to an obligation that may be enforced in the courts. In order to have a valid contract, there must be a "meeting of the minds" of the parties on all essential matters relating to it.

For the meeting of the minds to be realized and a contract to be binding, contract principles require formal offer and acceptance, as well as proper consideration, cause and object. Meeting these required contractual elements in the digital context, and especially with respect to automated and disintermediated situations, can present some challenges. However, these principles can today be realized through computerized actions. As such, if the smart contract includes all those elements, it could be considered a valid contract at law. While traditional contract doctrine has defined the requirements needed to form a contract, legally binding contractual effects for smart contracts will depend on a number of variables. Until this is addressed by courts, it is unforeseen how parties to a smart contract will demonstrate that each legal contract formation requirement has been satisfied.

The question of whether smart contracts are "contracts" is even more at play when considering legal requirements for contract formation under the different restrictive frameworks, notably those designed to protect weaker contractual parties (*e.g.* consumers or borrowers) or for which a statute provides for specific form (*e.g.* notarized contracts).

The absence of a traditional contract prior to the implementation of the smart contract may be an issue as a matter of evidence. The smart contract may be legally insufficient in cases where specific form is required for evidence purposes, and where the applicable law requires a written contract. In this case, the computer code alone, even if the parties have clearly consented to its application, cannot be legally considered equivalent to a written contract and will only be valid—if at all—as a simple beginning of proof. The same will apply in cases where a specific form is required as a substantive condition. In all these cases, it will be necessary to draw up a classic contract beforehand, either with a paper document or with forms provided for concluding a contract in electronic form.

Automation and Immutability

Beyond the mere question of legal status, the smart contracts' immutability and automation with lack of party discretion may introduce some risks. Indeed, it is impossible to prevent the automatic execution of the smart contract. Since the contract may be executed on a continuous basis, it is important to be extremely careful when scripting it. If there is a transaction, it will be repeated in a loop. If there is an error, it will be repeated in loop.

In addition, the immutability of the blockchain prevents any modification and any adaptation of the terms of the contract in the event of, for example, a change in circumstances. From this point of view, the smart contract technique pushes the famous maxim *pacta sunt servanda* ("agreements must be kept") to the extreme. However, the inability to change the script can also present challenges. Since the blockchain is permanent, amending smart contracts that are not programmed for pre-established modifications could be significantly more challenging and costly than it currently is through paper amendments. Contrary to the usual practices of contractual amendments, it is not possible to change anything in the initial smart contract terms—unless such a possibility is included in the initial script. The more amendments required, the more coding and testing necessary, which results in greater costs. At the same time, a smart contract that cannot be amended may be deemed void in some jurisdictions or areas of practice.

The only solution is to provide from the outset, in the programming, for the possibility of amending the contract, granting a grace period or even waiving the execution of the smart contract. This is not easy, however, because any programming requires extremely precise clauses. If the possibility of amending the contract is programmed, the conditions under which the modification can take place and the possible changes must all be detailed. Otherwise, modifying the smart contract is almost impossible. It is true that sometimes the parties agree on a new smart contract that corrects the effect of the first one—for example, if the new smart contract allows the defaulting debtor to access the connected objects again. However, this solution is difficult to implement in the presence of smart contracts that address multiple users who are not always identifiable due to pseudonymization.

This immutability of smart contracts may also conflict with some essential principles of contract law that nullify or terminate contracts, such as public order directives or the duty of good faith. Under civil law and in some common law jurisdictions, parties should enter into agreement and perform contracts in good faith—under pain of nullity. Since the duty of good faith applies to all contracts, it should apply to smart contracts if they are, indeed, contracts. However, it has yet to be explored how the duty of good faith might be engaged in the execution of smart contracts. How could a party "nullify" a smart contract when it can't be altered? Beyond the public order and the duty of good faith, the issue is found with all other causes of termination or nullity of contract. This is not so much a legal issue as an implementation issue.

Certainly, one could provide for such situations *ab initio* in the code and rely on oracles, though as previously discussed, the introduction of oracles brings its own challenges.

Scripting Legal Terms and Interpreting Computer Code

Despite the promise of smart contracts, one major issue arises: the viability of smart contracts requires the ability to express contractual obligations in code. As natural language cannot be directly executed by a computer, smart contracts require that contractual obligations be translated into computer-readable and computer-executable terms. However, this conversion and the code's resulting execution cannot always be achieved. In addition, translating legal contracts into self-executing code means losing much of the functionality and flexibility of traditional legal language. The words "reasonably," "to the seller's best efforts," "act of God," or "good faith," for example, are difficult to code in the current "if this, then that" format. Moreover, as it stands, computer code does not operate well with qualitative or subjective provisions. Many contractual obligations in current contracts are drafted with the intention of being generic enough to be applicable to a variety of different situations, some of which could not have been foreseen at the time of drafting.

In addition, refraining from drawing up a contract in the traditional sense and relying exclusively on the smart contract creates a difficulty in that in order to consent to the application of the smart contract, the terms and conditions must be understood. If no presentation of the terms of the smart contract is made in everyday language, then the party without computer skills might not be able to understand their commitment. The problem is all the more acute as, in most cases, smart contracts are standard-form contracts where a service provider offers services (*e.g.* insurance coverage) within the framework of a smart contract that is already in place. It is therefore desirable that the use of a smart contract be accompanied by the prior distribution of all the necessary explanations and details so that users can give their informed consent.

This is also a professional liability issue for legal practitioners who might not understand the characteristics and limitations of computer software. Equally, those trained in computer science are not generally familiar with the scope and subtleties of legal terms. As a result, neither group is sufficiently knowledgeable to anticipate the problems that may arise in more advanced smart contracts. Furthermore, they may not be well positioned to appreciate what it is that they do not know. There are important implications to this limitation with regards to the script of a smart contract, as, similar to how a comma in a contract can cost millions, a typo in a script could lead a transaction to crash or to be executed in error—or cost millions.

Enforcement and Execution

If a smart contract is found to be legally binding, the question of its enforceability raises new issues. Given smart contracts' automation features, academics have touted the ability of smart contracts to eliminate legal disputes over issues of specific performance. Specific performance issues arise when parties commence legal action over one party's failure to carry out contractual obligations and where the remedy sought is a court order requiring the performance of the disputed contractual obligation.

The whole point of the smart contract is that it settles the question of contract execution from the outset, since execution takes place automatically once the conditions laid down by the program are fulfilled. Smart contracts could eradicate specific performance issues, as human intervention is removed or limited. A notable flaw in this argument is that the blockchain cannot physically enforce a contract, or compel a person or entity to perform any obligations, meaning courts will likely have to grapple with performance issues in a new, modern context.

The more complex the smart contract, the more disputes may arise because of coding issues, erroneous performance, failure of a third party (*e.g.* an oracle providing data or executing a performance), parties' intent, and other non-technical questions. One solution is for the smart contract to include a dispute resolution mechanism that allows parties to defer problems to a court or an arbitration tribunal. Then, the court or tribunal could provide instructions on how to resolve the dispute.

The absence of such an embedded mechanism or oracle does not deny parties their right to justice, since they can always file a complaint before a judicial court. Certainly, since a script cannot be rewritten, a court will not be able to compel orders over a blockchain, nor will it be able to order that the code be undone. However, the court retains the ability to order parties to mitigate the contract's consequences (*e.g.* to write a new smart contract that would undo erroneous performance, execute the performance or compensate other parties when specific performance is not possible).

Necessary Limits

Although some consider smart contracts to be superior instruments to traditional contracts, smart contract technology undoubtedly has its limits and raises significant legal difficulties. It is likely that, in the future, these difficulties will diminish thanks to the evolution of the technology. Current projects aim to develop smart contracts that can be amended or resolved. In addition, the integration of artificial intelligence layers will make smart contracts even more "intelligent" by allowing the code to adapt based on less precise conditions and by leaving a margin of appreciation to the machine.

It would not be realistic to give up the possibilities that smart contracts offer in terms of automation and cost reduction, especially as organizations are using them more frequently. However, neither does it seem acceptable to allow smart contracts to be implemented and offered to users outside of any rules, guarantees and recourse, especially for customers, marginalized groups and people with low digital literacy.

References

Abrahams, Nick, Zein El Hassan & Sean Murphy (2016). "Can Smart Contracts be Legally Binding Contracts? An R3 and Norton Rose Fulbright White Paper."

G'sell, Florence (2019), "Intelligence artificielle et blockchain," in Bensamoun, Alexandra & Loiseau, Grégoire (2019). *Droit de l'intelligence artificielle*, Dalloz.

Kolber, Adam (2018). "Not-So-Smart Blockchain Contracts and Artificial Responsibility," Stanford Technology Law Review 21:2 199.

Lipshaw, Jeffrey (2018). "The Persistence of 'Dumb' Contracts," Stanford Journal of Blockchain Law & Policy 2:1.

Martin-Bariteau, Florian & Marina Pavlović (2020). "AI and Contract Law," in Florian Martin-Bariteau & Teresa Scassa (eds.), *Artificial Intelligence and the Law in Canada*, LexisNexis.

Martin-Bariteau, Florian & Marco Pontello (2020), *Hashing Out Agreements: An Overview of Smart Contracts under Canadian Law*.

Mik, Eliza (2017). "Smart Contracts: Terminology, Technical Limitations and Real World Complexity."

Raskin, Max (2016). "The Law and Legality of Smart Contracts," Georgetown Law Technology Review 1:2 305.

Sherborne, Andreas (2017). "Blockchain, Smart Contracts and Lawyers," International Bar Association.

Tjong Tjin Tai, Eric (2017). "Formalizing Contract Law for Smart Contracts," Tilburg Private Law Working Paper Series 06:2017.

Legal Status of Distributed Automated Organizations

As computer programs, the ability of decentralized autonomous organizations (DAOs) to emulate fully functioning and autonomous organizations raises the question of their legal status. Should a DAO be only considered, formalistically, as lines of code, or should the legal framework functionally recognize them as legal persons, or something in between? The question of recognizing a true legal personality for DAOs is nowadays being raised by increasingly intelligent organizations with the possibility of carrying out transactions—and therefore legal acts—in a purely automated manner. In light of UNCITRAL uniform laws, most countries have recognized the potential for contracting with an electronic agent through the agency or mandate frameworks. However, DAOs invite us to revisit those questions as they feature not a single legal person, but a group.

The contractual nature of DAOs is indisputable: by deciding to acquire DAO tokens and to participate in its functioning, tokenholders express their wish to collaborate within the framework established by the computer protocol. As such, a DAO could be considered a "contract organization," where the governance rules set up in the code could be considered similar to the articles or statutes of an organization. A body of scholarship invites to consider such organizations as *de facto* corporations, as the code mandates cooperation and compliance with the governance scheme of the organization, as well as acting as the agent of the tokenholders. Both common law and civil law have learned to recognize de facto corporations, with, in some cases, a limited liability framework for tokenholders. If we consider DAOs as contractual organizations, they could be recognized as general partnership or silent partnership at common law, *société en participation* in civil law, or tokumei kumiai in Japan. The entity would be recognized as a venture in itself wherein all stakeholders are fully liable, but they usually do not receive legal personhood.

In light of those conversations, Malta has developed a framework allowing for registration and recognition of DAOs, without, however, granting them a full legal personality. On the other hand, Wyoming, Vermont and Delaware, and the Republic of the Marshall Islands, have provided new corporation registration schemes recognizing DAOs as a new limited liability corporate model under which DAOs are granted legal personality and their tokenholders are protected. In general, these regulations require that one or more natural persons, acting as a member or representative of the DAO, disclose their identity and place of residence. The situation is, however, much more complicated when the DAO's creators and participants do not disclose their identity. It seems difficult, in such a case, to recognize the legal personality of purely virtual organizations created or animated by unknown people. Third parties carrying out transactions with such an entity would have no recourse in case of difficulty.

Where the legal personality of DAOs is not recognized by the applicable regulations, tokenholders could also decide to avoid the general partnership framework and to incorporate the DAO, while providing in the articles of incorporation that rules and decisions will be made by the DAO. However, not only does this require that a natural person act as the agent of the corporation but the organization and operation of the DAO will have to be in accordance with the law applicable to corporations. While it would bring some legal certainty, this would represent a very strong constraint for tokenholders.

It is important to note that, when provided for by the applicable regulation, DAOs' legal personhood is limited in the same way as other legal personhoods, in contrast to the legal personality of natural persons. Such limitations are essential, especially in a human rights perspective, to ensure accountability against abuses and to protect potential victims. As is the case of corporations, the liability of the actors behind the legal person could still be engaged for some serious or criminal matters.

The legal difficulties around the legal status of DAOs are best illustrated with what happened to *The DAO*, the first organization of this kind which launched in April 2016. Within its first weeks of existence, *The DAO* managed to raise considerable sums of money, which immediately aroused attention. On June 17, 2016, an "attacker" exploited a flaw in the programming that allowed them to appropriate nearly US $55 million. While the action seemed unethical and against the goal of the group, some dispute that the misappropriation was legally reprehensible and amounted to theft. Indeed, the documentation of *The DAO* clearly stated that the terms and conditions were set out in the code of the smart contract, and the attacker had only exploited the code for his own benefit.

The attack did not lead to judicial intervention, but to a solution decided collectively on the Ethereum platform. The entire Ethereum community, not just the members of *The DAO*, voted in favor of a hard fork consisting of modifying the history of past transactions to delete them from the blockchain, in order to return to the state of the chain before the embezzlement. This solution of rewriting the transactions was in direct contradiction with the blockchain's principle of immutability, drawing intense criticism.

While the solution offered remedies to The DAO's tokenholders, this outcome did not provide an answer to the legal questions raised by the case, which went beyond the simple legal qualification of the behavior of "the attacker." If it had not been possible to reverse the past entries, would *The DAO*'s investors have had to forfeit the $50 million embezzled without any recourse? Having invested at their own risk, could they have filed a claim against the authors of the code for faulty programming? Furthermore, what liability could they have had to third parties of *The DAO*? Even assuming that *The DAO* was considered a joint venture, should all the tokenholders be considered equally liable or should curators and contractors be given greater liability? And how could each tokenholder even be identified since they acted anonymously? This case shows the difficulty of defining these new online organizations with respect to the existing frameworks.

References

G'sell, Florence (2019), "Intelligence artificielle et blockchain," in Bensamoun, Alexandra & Loiseau, Grégoire (2019). *Droit de l'intelligence artificielle*, Dalloz.

Martin-Bariteau, Florian & Marina Pavlović (2020). "AI and Contract Law," in Florian Martin-Bariteau & Scassa, Teresa (eds.), *Artificial Intelligence and the Law in Canada*, LexisNexis.

Metjahic, Laila (2018). "Deconstructing the DAO: The need for legal recognition and the application of securities laws to decentralized organizations," Cardozo Law Review 39:1533.

Reyes, Carla L., Nizan Geslevich Packin & Ben Edwards (2017). "Distributed Governance," William & Mary Law Review Online 59:1.

Conclusion

As blockchain technology develops, its applications to resolve human rights issues will expand. It can be adapted to advance democratic functions and ensure accountability and transparency. Over the next few years, industry stakeholders, governments and members of the public should familiarize themselves with this invaluable resource and cultivate its use to accelerate humanitarian responses around the globe. It is in the best interest of the Council of Europe to delve into the technology's ability to promote its democratic and human rights agenda in the field. However, as discussed, the deployment of blockchain technologies comes with a plethora of legal issues including risks to the fundamental rights and liberties protected under the European Convention on Human Rights and other international instruments. Despite the crypto-anarchist's will, distributed systems need to be regulated to mitigate risks and injustices.

It appears essential for the Council of Europe to develop a research and policy agenda that allows it to be fully aware of the opportunities and risks presented by blockchain, and to propose the appropriate legal instruments in order to benefit from what the technology can bring while limiting its potential negative effects. In this respect, while this report aims to provide a general overview on the subject, several particularly important points merit further specific reflection.

First, blockchain technology shows interesting opportunities for dispute resolution and arbitration that should be further investigated. At the same time, it is necessary to ensure that blockchain-based dispute resolution solutions guarantee the respect of procedural rights, and in particular the right to a fair trial.

Second, decentralized identities and data governance solutions have the potential to give control back to users over their data, and enhance their privacy. Yet, appropriate frameworks are needed to ensure those solutions effectively guarantee data subjects' rights and do not constitute a recommodification of their personal information. Therefore, such solutions should be further studied by the Council.

Third, it seems essential that the Council reflect on the complex interface between encryption and fundamental freedoms. This is particularly necessary at a time when some democratic states are considering banning encryption for reasons related to the fight against terrorism and illicit activities. While encryption may obfuscate some nefarious activities, it also allows for the protection of our privacy, of our institutions and our fundamental liberties, notably the freedom of expression and the freedom of the press. The right balance must be found between respect for freedoms and the need for the states to ensure public order.

Finally, the Council of Europe could address various difficulties that have an impact on the fundamental rights of individuals and should be resolved. For example, the Council may advance standards and instruments to mitigate issues related to the applicable law and competent jurisdiction for distributed systems. The Council could also provide guidance as to how much automatic enforcement is acceptable from a fundamental rights perspective.

Overall, the Council of Europe should continue to support research and opportunities for conversations regarding the impact of blockchains on human rights, democracy and the rule of law. Looking at the Council's successful endeavour with respect to artificial intelligence, it would be interesting to launch a similar multi-stakeholder initiative on blockchain and distributed technologies to share good practices and develop guidelines and policy recommendations—if not to recommend new legal instruments to promote the responsible development of this technology.

Appendix - Blockchains and the European Convention on Human Rights

Fundamental Rights	Opportunities	Risks
Right to liberty and security (Article 5)	➔ Pseudo-anonymity on the blockchain guarantees freedom and privacy. ➔ The identification techniques provided by the blockchain support citizens' empowerment. ➔ The identification techniques provided by the blockchain will allow vulnerable people to be identified in a secure way, so that they can claim their rights to access essential services (*e.g.* food, health, education).	➔ Pseudo-anonymity on the blockchain does not completely prevent the identification of individuals interacting on blockchains. ➔ Automation through smart contracts makes people prisoners of a computer program.
Right to a fair trial (Article 6)	➔ Dispute resolution solutions offered on the blockchain are confidential, fast and efficient.	➔ Jurisdiction and applicable law are very difficult to determine for transactions on public blockchains. ➔ Alternative dispute resolution solutions offered on the blockchain may not respect the most essential procedural rights. ➔ Uncertainty about the legal nature of DAOs and the pseudonymity of participants is an obstacle to ensuring the rights of token holders.

Fundamental Rights	Opportunities	Risks
Right to respect for family and private life (Article 8)	➔ Pseudo-anonymity on the blockchain protects privacy and personal data. ➔ Fully encrypted platforms (“privacy coins” platforms) and blockchains with data privacy by default guarantee a quasi-anonymity respecting the right to privacy.	➔ Pseudonymity is relative on many blockchains in that re-identification is possible and users are generally required to disclose their identity when creating their digital wallet.
Freedom of expression (Article 10)	➔ Pseudo-anonymity on the blockchain is a guarantee of the right to freedom of expression.	➔ Pseudo-anonymity on the blockchain can be lifted, especially for users who have created digital wallets with KYC-compliant providers.
Freedom of peaceful assembly and association (Article 11)	➔ The cooperation of multiple users on blockchains is an exercise of freedom of association in the broadest sense.	
Right to protection of property (Protocol No. 1, Article 1)	➔ NFTs can support digital goods management, licensing ➔ Smart contracts can support property management through smart properties and smart leases. ➔ Where land ownership management systems are failing, blockchain can enable reliable land ownership records and prevent fraud.	➔ Attacks and security breaches, such as in *The DAO* case, can lead to misappropriation and loss of property.

Fundamental Rights	Opportunities	Risks
Right to participate in free elections (Protocol No. 1, Article 3)	➔ Blockchain allows the deployment of reliable online voting systems, in which voters post their encrypted ballots on a publicly accessible blockchain and can verify whether their vote has been counted correctly. It is also possible to imagine a situation where the platform is not managed by the government alone but by different stakeholders (*e.g.* municipalities, regions, political parties, civil society organizations).	
Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)	➔ Fully encrypted platforms and blockchains with data privacy by default guarantee that users are not identifiable. ➔ The recent "off-chain" data storage solutions in which data can only be consulted after validation by the user can be a very secure way to give the user control and to share sensitive data in compliance with data protection frameworks.	➔ Pseudo-anonymity is relative on the blockchain in that re-identification is possible and users are generally required to disclose their identity when creating their digital wallet. ➔ The immutability of the blockchain does not allow the deletion of sensitive personal data. This immutability is in contradiction with the right to deletion and modification.

Fundamental Rights	Opportunities	Risks
Right to a Healthy Environment (CoE Parliament Resolution, *Combating inequalities in the right to a safe, healthy and clean environment*, September 2021; as well as Article 2 [right to life], 5 [liberty and security] and 8 [respect for private and family life] as interpreted by the European Court of Human Rights)		➔ The energy consumption of the Blockchain and in particular of certain technical protocols (such as the proof of work) leads to a problematic environmental record.

This report explores the risks and potential benefits of blockchain technology for democracy, human rights and the rule of law.

It aims to showcase use cases and flag potential issues, as well as to provide initial recommendations to the Council of Europe for additional research and prospective programming regarding blockchain technologies.

The report highlights some of the promising features of blockchain technology and various types of implementation, from cryptocurrencies, to smart contracts, to distributed autonomous organizations (DAOs) and non-fungible tokens (NFTs).

It also presents some of the important limitations that may impede fundamental rights.

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 46 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE