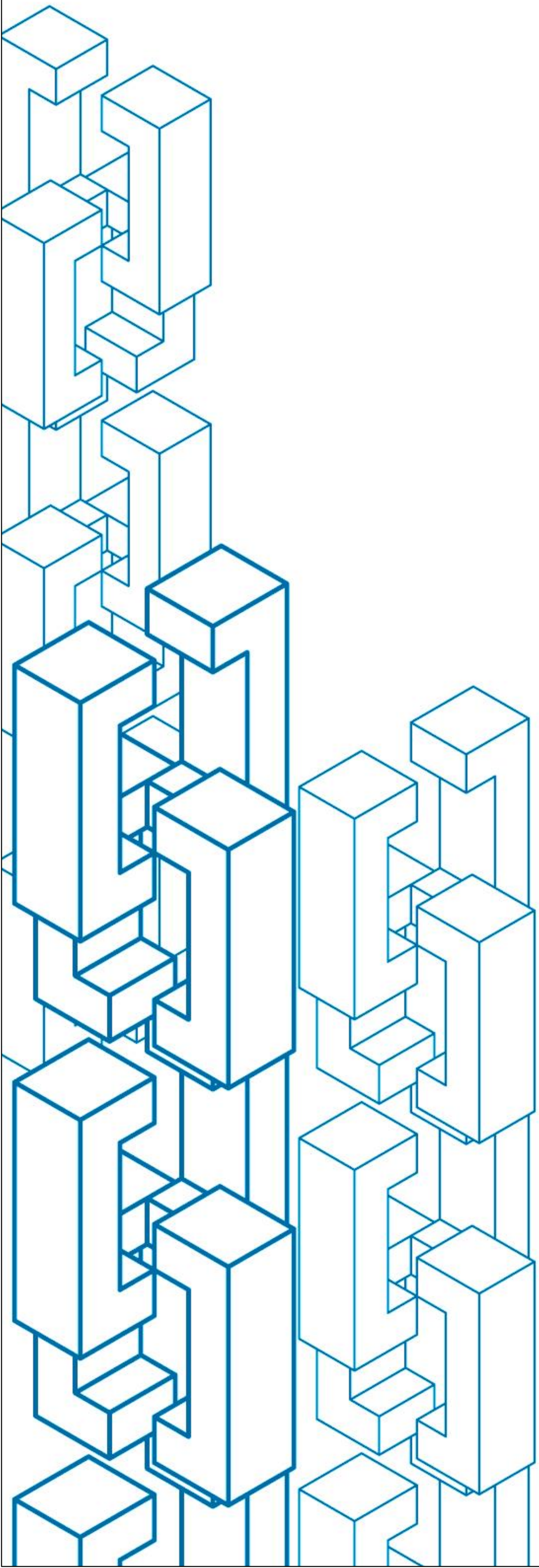
United Nations
Educational, Scientific and
Cultural Organization

Canadian
Commission
for UNESCO



Beyond Bitcoin:
Blockchain technology's hidden potential

Prepared for the Canadian Commission for UNESCO
By Ryan J. A. Murphy
Ottawa, Canada, February 2021

To cite this article:

MURPHY Ryan J. A., “Beyond Bitcoin: Blockchain technology’s hidden potential”, Canadian Commission for UNESCO, Ottawa, Canada, February 2021.

The views and opinions expressed in this article are those of the author and do not necessarily reflect the official policy or position of the Canadian Commission for UNESCO.

Table of Contents

Introduction

Asking how blockchain will be useful is a difficult question to answer. It might be like asking the folks who built the Internet in the 1980s to describe ridesharing platforms, social networks, and smart homes while they were still ironing out the details of how the Internet's protocols would work. As you shall see, blockchain is a technology whose principles upend and subvert many conventional ideas of how technology and society must operate. We are (still) in the very early days of blockchain research and development. Predicting exactly how the ideas underpinning blockchain will interact with these actors and existing systems is impossible.

So, instead of making predictions, it is my intention to provide a primer on blockchain for a non-technical audience that explores its potential applications beyond finance. Section one begins by explaining what a blockchain is, emphasizing the problems of trust and the potential of trustlessness. In section two, I provide a simple explanation of how a blockchain works by way of an analogy. In section three I summarize seven fundamental principles of blockchain technologies, adapted from Tapscott and Tapscott's 2018 book *Blockchain Revolution*. In section four I explore four exemplary areas that illustrate blockchain's potential beyond finance—specifically in advancing digital dignity, creating digital value, empowering digital governance, and facilitating digital collaboration.

Before we begin, though, here are a few caveats. First, this is not a technical paper. You should not need a background in computer science or even technology—nor one in the social sciences or the humanities—to understand and enjoy it. I will also take advantage of this non-technical approach to avoid some of the most controversial and confusing topics around blockchain: the nuanced, technical constraints and possible faults in the technology. Let's make an assumption that the technology works, as Bitcoin has demonstrated, and focus on why it is transformational.

In addition, it should be noted that the blockchain ecosystem is rife with speculative investing. Many conversations about blockchain technologies go hand-in-hand with how much the participants have invested in different blockchain tools. By way of disclosure, I hold a small amount in several blockchain tokens: Stellar (XLM), an "open network for storing and moving money"; Smartlands (SLT), a token that facilitates fractional investment in institutional-grade assets; Augur (REP), a prediction market and forecasting token; Ripple (XRP), a commerce and payments-focused token; Ethereum (ETH), a blockchain providing distributed computing capabilities; and Bitcoin (commonly BTC, or XBT according to the International Standards Organization). None of these projects are mentioned in the following text except for Bitcoin and Ethereum, which are both fundamental in blockchain discussions.

In the next section, I explain the core problem blockchains aim to solve—trust—and describe what a blockchain is.

Trustlessness

What requires trust?

Everything. We can't make any agreements without trusting:

(a) the contents of the agreement,
(b) the systems and environment in which the agreements take place,
(c) the information forming the basis of the agreement, and
(d) whoever we're making the agreements with.

We can’t form new knowledge without trusting both the information on which the knowledge is based and the source from which we’re receiving it.

Imagine a friend invites you to dinner at a restaurant. Such a mundane thing doesn’t seem to require anything as dramatic as trust. And yet, for dinner to be what you hope, you need to trust:

(a) that the invite is actually a dinner (and not an ambush, like a surprise party),
(b) that the restaurant will be open,
(c) that you’re accurately remembering how much you enjoy that friend’s company, and
(d) that the friend is not going to forget their wallet again.

You’ll also need to trust your calendar (are you actually free that evening?), the mode of transportation you’ll use to get there (did your mechanic actually fix your brakes?), the whole line of food production (from whether the sauce is authentic to whether the ingredients were contaminated), and a host of other factors that can influence whether your dinner goes well.

If that’s just dinner, imagine the kind of trust it takes to make sure major cross-border shipments get from origin to destination, or to ensure that the tips received by a journalist come from reputable sources, or to guarantee the results of a medical breakthrough based on thousands of data points across thousands of patients.

Because trust is so important, we—as individuals, organizations, and society as a whole—put a lot of time and effort into enabling trust. But if so many things require trust, what does trust itself require? Conventionally, trust in *something* requires trust in *someone*. It implies a judgement that someone else will perform the actions you expect them to, allowing you to act accordingly.[1] You trust your bank to keep your money safe, and so you trust the transactions you make based on the values you can see in your bank account. You believe a rumour because the person who reported it is vouched for by other people you believe in. Or you find that others trust a shipping company (e.g., it has a good reputation), and so you trust it to ship valuables to a family member. This kind of triangulation helps us act with certainty about our agreements.

It also requires deferring power. In other words, we deem something else to be an authority over the conditions of our agreements (e.g., a bank, a confidant, or a business). And our economies function because we trust that contracts are enforceable by the rule of law.

This deference has a cost. It is costly to maintain and sustain these institutions and relationships. It is also risky: if our trust is misplaced and error or malice causes a problem with our agreements, the agreements will fail, and we are usually stuck with the consequences. One of the most valuable aspects of blockchain technologies are their *trustlessness*. As I will discuss in the next section, blockchains minimize the work required to develop trust. Blockchains shift the trust that we have to build and maintain in people and institutions to trust in the design and engineering of blockchain technology.[2]

While much media attention has been paid to the disruptive force of blockchain in the world of finance, the focus of this paper is not blockchain’s financial uses. Instead, I aim to emphasize the many other ways people are reimagining the fundamentals of communications, governance, education, healthcare, and beyond through the unique features of blockchain.

Of course, in order to trust a technology, you should know how it works. In the next section I explain how a blockchain operates by way of analogy.

A brief, non-technical explanation of the blockchain

A blockchain is essentially a chain of blocks of information. Different blockchain technologies create public or private ledgers of information. Public blockchains use networks to validate the contents of these ledgers and make them available to others—decentralized transparency. They allow participants to record an interaction—say, a payment transaction from one person to another. And they do all of this without requiring a centralized authority to verify, record, and maintain the ledger of cumulative transactions.[3]

The ledger is a fundamental technology used for centuries to, well, track things—usually money. Bookkeepers maintain ledgers so that the current state of accounts can be summarized. They help us know who took what, and what it was for, and when. Ledgers help us see patterns of transactions in our activities. They are also tools to help us make sure our accounts stay balanced; that we do not promise to spend more money than we have received.

Of course, the conventional ledger has its weaknesses. Paper is easily lost or damaged, and handwriting can fade.[4] Of course, that's what computers and spreadsheets are for. Surely all the issues of the traditional ledger are resolved by putting it on a computer and saving it to the cloud. Electronic ledgers even add features: we can make fancy charts and run computational analysis without a calculator, for example.

Unfortunately, there's still another potential problem with traditional ledgers: the people who maintain them. Even automatic systems—like commonplace Interac machines and the networks and software they run on—are manually designed, developed, and maintained. Whether through error or malice, these ledgers can be manipulated. For this reason, we turn to third-party intermediaries to assure the integrity of our ledgers. Banks and other financial services, for instance, tie your identity to the loan you're taking out to pay for a new vehicle; they check whether you are likely capable of paying off that loan over time, and they confirm the necessary details with the seller. This way, you can't show up at a car dealership and promise to pay for the car the next day, only to never reappear.

That system works well enough. We've used it for decades to do business and keep our world in order. But there are challenges. We depend on intermediaries to avoid error and malice when it comes to our records. These intermediaries also come at a cost. Thus, we may spend money on an intermediary, trusting that they will maintain their records effectively, only to sometimes have them fail and to lose property, identity, or data in the process.

Imagine, for instance, that you attend a small college, racking up student debt in the hopes that your degree will net you a successful career. A month after graduation, however, the college announces bankruptcy and all staff disappear. The college had a ledger of its students and their degrees, but the ledger doesn't mean much if it can't be accessed.

But you aren't going to give up. You went to school and earned your degree. So you call everyone you can—instructors, college staff, the government department of education—and eventually find two independent copies of an up-to-date record held by other institutions of the college's graduates with your name on the list. This **decentralized distribution** of the college's graduate ledger helps verify its authenticity, and the day is saved.

Unfortunately, it is highly inconvenient for potential employers to call two separate authorities to verify the claims on your resume. So, you put some more effort in, and you get the department of education to reconcile the two lists and upload the verified result to an online system for all to see. This **transparency** affords convenience and trust in the record, and the problem is solved—until a second scandal strikes.

A journalist covering this story makes a disastrous discovery: many of the students on the graduate list never even enrolled in a course. A scheme of bribery and a corrupt registrar led to a system in which "students" could buy degrees for quadruple the cost of the tuition fees. Your degree is now virtually worthless because no one can trust the entries on the ledger.

Luckily, your degree was in computer science, and you actually *did* take classes in that degree. You discover several different sets of encrypted records of all student enrolments and grades held separately by various government departments. So, you develop a system that **automatically** checks whether a graduate has enrolled in and completed a sufficient number of courses in their supposed program at your old college. To guard against further corruption, you convince each department to run this system locally on their data. A record of a graduate will only be generated if each system verifies the same records for that student.

But you are worried that the public will question your legitimacy as an individual. So, you develop a **consensus** mechanism to validate this record. As every student is verified, they become a stakeholder in the list's validity. Whenever the system adds a new record, every already-validated student must check if that record represents a valid student. Since each student knows at least a few other students, but students who bribed their way through do not, it is easy for the network you've established to refute invalid records. Last, each record is published automatically to a public feed, with details about each graduate's degree, such that anyone can review the ledger as it develops.

This system automatically chains together blocks of independently verified, consensus-driven, distributed proofs of students' work. This is a contrived example of a blockchain.

Blockchains provide a resilient record by distributing every new piece of information added to them to every participant in a network. Through cryptography or consensus, each addition has built-in proof that it is a valid addition to the blockchain. Through transparency, all participants can see the details of the protocols that led to each new record and what those additions contained. Lastly, these protocols are fulfilled continually as the blockchain participants actively verify that new transactions are true and accurate—without the need for costly intermediaries. Through this unique design, decentralized blockchain computing has proved to be remarkably secure.

Note that there is not only one blockchain; rather, blockchain is a technology that can be implemented through a number of different approaches and for a variety of applications. Some blockchain technologies operate using their own custom blockchain infrastructure, while others are built on top of previously-established blockchains.

In the next section, I discuss seven principles fundamental to blockchain's potential.

Seven design principles

If a blockchain is a transparent, secure, distributed ledger, then what are the common traits of blockchain applications?

In their book, *Blockchain Revolution*, Don and Alex Tapscott describe seven "design principles" for blockchain applications.[5] They write (p. 219):

> *[T]hese seven principles can serve as a guide to designing the next generation of high-performance and innovative companies, organizations, and institutions. If we design for integrity, power, value, privacy, security, rights, and inclusion, then we will be redesigning our economy and social institutions to be worthy of trust.*

Adherence to these principles is not a requirement of any project, per se, but they are features common to most applications. Their original description is worth reading in full, but because these principles are core to blockchain's uses, I summarize each below.

But first, I want to re-emphasize something in the paragraph above, and this is crucial: these features do not function the same way in any given blockchain. If you choose to engage in a blockchain project, please be diligent and review how that project implements these principles.

1. Networked integrity[6]

The integrity of blockchain systems is intrinsic to every step of the process and every component of the system. Expectations about the system and its participants are hard-coded in its rules, structures, and operations. As a result, blockchains are trustless. No one can act in a way that subverts these encoded expectations; in turn, no one has to worry about whether others will betray them or fail to fulfill their commitments.

As discussed earlier, in a blockchain system the power to verify any activity's authenticity is distributed across the whole network. Every recorded agreement and transaction is logged and validated by the entire network. There's no one point of weakness, as there is in systems that rely on a central authority.

2. Distributed power[7]

On a blockchain, the entire network of participants holds authority over the activity of the blockchain. This power is governed in a variety of ways, but one thing is always true: no one participant can take control. Hard-coded physical restrictions guarantee the impossibility of takeover.[8]

In general, anyone can participate in the mechanisms that sustain the blockchains they participate in. In fact, conventionally, a blockchain's entire network of participants is collectively responsible for ensuring its integrity. Without centralized power or intermediaries, it's impossible to freeze or seize assets, and no one can wield total control over the blockchain's rules and operations. This feature is also used in the development of systems of distributed governance, where anyone participating can propose new directions for the blockchain that are then reviewed, debated, and voted on by every other participant.

3. Value as incentive[9]

Participants in blockchain networks each contribute to the advancement of the chain, reviewing new additions and coming to consensus about the addition's legitimacy through a variety of possible consensus algorithms. Blockchains conventionally reward this participation with value in the form of the blockchain's asset. These assets, often called coins or tokens, incentivize the behaviour of participants to act as good stewards of the blockchain.

This has three implications:

1. The value of these tokens, outside of the system, is directly related to the value of the system itself. Therefore, it is in the best interest of anyone who holds value within a blockchain to ensure that the blockchain is healthy and active.
2. The transparent nature of blockchain transactions protects them from counterfeiting, theft, and often even inflation. For instance, the exact source and every expenditure of BTC in existence has been tracked, and that transaction history can be reviewed by anyone.
3. Tokens may be held by devices and organizations. Blockchain's automaticity and trustlessness therefore affords the possibility of independence for machine-to-machine (and therefore organization-to-organization) interactions. For instance, via blockchains, an autonomous vehicle could be incentivized to provide services and coordinate with autonomous charging stations and roadways, exchanging value independent of human interaction to coordinate resources on the

Internet of Things.[10] Similarly, an organization may be responsible for its own resources and act of its own accord in interactions with other organizations or individuals. Imagine a store that maintains its inventory, updates schedules, pays staff, and changes prices automatically in coordination with a network of stores and customers.

4. Security[11]

Cryptography is the science of secret-keeping—in particular, how to encode and decode data such that:

- confidentiality is maintained (e.g., no one can read the message except the intended receiver);
- data consumers are authenticated (e.g., proving your identity as the rightful recipient or verified creator of data);
- integrity is maintained (e.g., proving that data has not changed);
- verification that the sender/receiver did send/receive the data (also known as nonrepudiation); and
- keys to encrypted data can themselves be shared cryptographically. [12]

Every interaction with a blockchain features built-in asymmetric cryptography. This means that the cryptographic key that encodes the data is different from the key that decodes the data, and there is no way to backwards-decode encrypted data. Everyone who interacts with the blockchain must participate through these cryptographic functions.

Built-in asymmetric cryptography guarantees the security of transactions on blockchains. Without this kind of security, most people would never even consider transacting value without an intermediary—a real, trusted entity—working to determine the authenticity of the sender and the receiver. With it, the need for those intermediaries diminishes—as do their fees and infrastructure costs.

5. Privacy[13]

Blockchain's trustlessness affords privacy in a way that was previously impossible. In conventional transactions, you must trust that the other participants in a transaction are who they say they are. To do this, you must often know their identities. By providing a way to guarantee the terms and results of exchange without trust, blockchains also eliminate the need for exposing identity. Further, since cryptography is built directly into every interaction within a blockchain, the identity of participants cannot be revealed unless that's what the application is designed to do.

Breaches of personal data held in traditional databases are made possible by the design of the technology itself. Apps or devices often need to know who we are via a login or account. Interaction with a blockchain requires no such identity, only a cryptographically-generated key. By giving you, the blockchain user, the sole responsibility of maintaining your data, only you can leak it. To this end, blockchain users are encouraged not to share their private keys with anyone and not to store them on insecure services.

As we shall discuss, giving individuals trustless privacy and granular control over their data—what Tapscott and Tapscott call "little data"—can be beneficial in many ways.

6. Rights preserved[14]

Once completed, no transactions on a blockchain can be changed or revoked. Since blockchains record all public details about transactions on the distributed ledger, ownership of every token on the blockchain can be confirmed and traced, if only to a private address. It is therefore impossible to claim ownership over a token that isn't yours—and this impossibility translates to any other asset exchange implemented via a blockchain.

This feature can be used to develop an incorruptible proof of ownership system. Someone who holds a deed to property can log their ownership of that property on a blockchain, linking that deed to a public key and a timestamp. If proof of ownership is required later, the owner simply needs to use their private key to demonstrate that the record is theirs.

Another implementation of this feature is the “smart contract.” The terms of any agreement can be hard-coded—entered using programming language—as instructions on a blockchain.[15] Smart contracts automatically execute their instructions when the conditions are met. Tapscott and Tapscott use the example of a songwriter’s license over their music. A songwriter might license a song to a publisher for a specified duration and amount of royalties. With a blockchain-based smart contract, the fees would be paid as per the agreement entirely autonomously, and as soon as the duration elapses, the license would immediately transfer back to the songwriter. It is even easy to imagine a blockchain-based music service that used this information to pay composer and artist every time the song is played.

7. Inclusion[16]

For many people around the world, particularly in developing countries, access to financial services can be a significant barrier to their ability to participate in the economy. People typically need to provide citizenship, an address, and other parts of their identity to get a bank account, and a bank account is often required to participate in many financial transactions. Blockchain-based currencies subvert this expectation. You can create a blockchain address and send and receive money with only an Internet connection—it’s even possible to participate in blockchains built on basic text messaging.

Another barrier to economic participation for many is the value of their local currency. Blockchain-based currencies provide a potentially more stable alternative to volatile local currencies. By facilitating access to the economy, blockchain can, in turn, support the prosperity of people typically excluded from economic progress.

Beyond the financial world, there are many examples showing the usefulness of blockchain technology embedded in various types of platforms and tools, something we will explore in the next section.

Exemplary applications

Exploring blockchain’s potential beyond finance by examining four classes of application that are derived from the principles above gives an interesting overview of the uses of blockchain by online communities, whether through podcasts or news sites. The four classes are grouped into four categories, namely: digital dignity, digital scarcity, digital governance, and digital collaboration. These four areas don’t represent everything blockchain can do, but they represent exciting categories of blockchain’s potential.

Restoring ownership, control, and consent over your digital self.

Blockchain for digital dignity

Many of us are unaware of, ignore, or dismiss how the digital services we depend on work—for example, what exactly happens when your smartphone uploads all the photos you’ve taken to cloud services. For the most part, this is as it should be. We trust the technology we use in life and work in the same way that we trust our vehicle mechanics, and the mechanics of all the transportation infrastructure we use when we travel from place to place.

Yet, as with any complex system, not everything always works. And in technological, data-dependent systems, we’re not always aware that anything’s gone wrong—or what the consequences are—until much later.

Take, for example, the Valentine's Day text messages of November 7, 2019. Early on the morning of November 7, people across the U.S. received odd messages, originally sent on February 14, 2019. The messages were sent on February 14th only to be received months later, when the server they had become stuck on was finally repaired. While many of the erred messages might have simply caused a funny conversation when received on November 7, some were unfortunately devastating—imagine receiving a message of love from an ex-partner with whom the separation wasn't smooth, or from a relative who had since died.[17]

Syniverse, a telecommunications infrastructure company, owned the problematic server. When a customer on one consumer wireless carrier company sends a message to someone on another, infrastructure owned and maintained by third-party companies like Syniverse rout them between carriers.

On the surface, this story is about a failure of service delivery. The consequences of failure in this system were messages that failed to be received as intended. This is a significant lesson on its own. However, wrapped in this service failure is another lesson: even our day-to-day tasks have become immensely complex. When we sign up for text messaging with our mobile service provider, we don't know that our data is being handled by dozens of other companies. We have become numb to signing terms of service agreements that grant wide-ranging permissions over the use of our data,[18] no matter how unthinkable and wide-ranging the use (or abuse) of our data may be.[19]

In a decade that has seen some of the biggest betrayals of trust in technology in human history, blockchain applications promise to restore data ownership and control to people and to restore confidence in the tools we use. Blockchain applications provide a framework to secure our data, give us more control over its use, provide records of its existence, and indicate whether it has been tampered with. In doing so, they facilitate digital dignity, restoring your individual agency, identity, and control over your own data and privacy.

This application of blockchain is made possible primarily because of the technology's built-in asymmetric cryptography. Similarly, a blockchain's distributed ledger means that a verified record of data saved to a blockchain is always available, has not been tampered with, and can only be accessed by those given explicit consent (via the sharing of private keys). With standardized data formats, a variety of services can be authorized to contribute data from different sources in a cohesive way, and a range of services can then access different parts of a person's data according to their wishes.

The benefits of trustless, blockchain-based digital identity are manifold. Take, for instance, what might be core to most people's identity: their citizenship. Conventional citizenship systems rely on complicated documentation and the central authority of the governments that authorize them—documentation that can be lost, damaged, and stolen and authorities that can be disrupted or corrupted. Refugees are some of the most vulnerable people who suffer from these issues. Blockchain-based identity systems could remove the need for both paperwork and for a stable authority that supports that paperwork. Documentation—and the assets, services, or transactions you make, such as land deeds or border crossings—can be digitally stored on a secure, distributed ledger, accessible via your private key, linked to your relatives, and granularly shareable. Taqanu is one such blockchain identity system striving to be a "catalyst for global inclusion," serving as a self-sovereign identity platform.[20] Instead of depending on a fragile piece of paper and the machinations of bureaucracy to protect who you are, tools like Taqanu could help people maintain their own identities.

Credentials for migrants are another issue. Blockchain identity systems can make credentials and related records more transparent and accessible. Hashed Health is a firm aiming to do just that with their Professional Credentials Exchange. This Exchange provides members with the ability to verify and check healthcare credentials and the various artifacts associated with practice. Consider the all-too common story of immigrants or refugees with extensive experience and credentials who must give up their profession because of the cost of becoming re-certified.[21] A blockchain-based Professional Credentials Exchange could minimize the amount of effort required for these newcomers to provide proof of their expertise and, in turn, allow them to pick up where they left off in their new home.

Other examples of blockchain's identity benefits exist in healthcare. Healthcare data is a major area of change in recent years, especially with the development of Electronic Health Records (EHRs, sometimes also called Electronic Medical Records). When kept updated and consolidated, EHRs provide healthcare providers with their patients' comprehensive history and link to tools such as referrals that facilitate healthcare services across organizational boundaries. However, EHR systems have shortcomings. For instance, EHRs tend to be managed by healthcare providers and institutions and patients are rarely in control of their information. Moreover, EHR standards are not well-established, so patients transferring from one provider or jurisdiction to another may not be able to convert their EHR data easily.[22] Blockchain-based EHR systems provide an obvious alternative to this scenario. Through services like Patientory, patients themselves could have ownership over their EMR data, providing keys to the requisite information to their providers and relatives.[23]

These healthcare examples demonstrate the difference between data privacy—the rules around how your data is used and saved—and the concept of data confidentiality, sharing data only with the intended party and no one else.[24] Conventional "big data" applications depend on the consent given by many of us when signing a Terms of Service for a newly-purchased product. Big data's consumption of your personal information has several implications. First, it betrays your confidence, as demonstrated by Spotify's data-based advertising campaigns.[25] Second, your data is valuable—but you are never compensated for that value.

In contrast, blockchain tools are fostering new approaches to data confidentiality. These tools can facilitate the sharing of data without the disclosure of data. Blockchain-based big data applications may be able to be deployed locally. It is possible to analyze your data solely on your devices and record the results to a collective, helping organizations use our data to train models and agree on collective decisions without disclosing individual details.[26] In turn, because blockchains can keep meticulous—but private and secure—records, it should be possible to reward people when their data has been useful. MediBloc, for example, is a blockchain-based personal health record service that gives patients control of their health data. Patients can control third-party access to their health records, allowing them to make per-use decisions about when their data is used by their providers, their insurance companies, or research centres, and enabling them to be directly rewarded when their data is used.[27]

For a final example, let us return to the messaging scenario described at the outset of this discussion on digital dignity. The centralized nature of our current text messaging infrastructure is ultimately at fault for the weird and sometimes upsetting messages received by thousands in November 2019. However, missing messages are not the only potential consequence of this central-point-of-failure architecture; it also exposes these messages to mass surveillance.[28] Blockchain offers an alternative. Messengers built on blockchain technologies like Session[29] and Status[30] do not store messages in any central location; instead, encrypted messages are routed through a network of blockchain nodes, ensuring they remain private while eliminating the risk of the kind of single-server failure experienced at Syniverse.

In sum, unlike their conventional counterparts, blockchain applications for digital dignity provide a new way for citizens and consumers to control their identities and their data. You need not trust that your identity is being maintained, used, or shared responsibly. You don't need to give up your personal information by default. Instead, these systems preserve your privacy intrinsically, they reward your participation, and you are free to participate in whatever way you choose.

Owning the intangible.

Blockchain for digital value

The digital era has made it extraordinarily easy to share content and be published, and very difficult to assert or monetize copyright. In the face of these tensions of Internet-scale, conventional business models are under pressure. News publications have shut down. Instead of selling albums, music is streamed for cents per track. Visual artists fight for Instagram brand sponsors while sharing their art for free. At the same time, content is seemingly free to consumers. Yet, as the adage goes, "if you aren't paying for the product, you *are* the product." Free apps and services require you to sign terms that give up your personal data such that it can be used to target advertisements (or political campaigns) with microscopic precision. That precision advertising accompanies content that appears free—along with sponsored product placement.

Blockchains make it possible for content creators to record a claim of ownership over property—physical or digital. With the technology's automaticity, cryptography, transparency, and decentralization, it becomes possible to generate and transact exclusive, unique digital products. Proof of ownership of these projects is transparent and traceable. As Sebastian Posth puts it:

> *Adding a layer of trustless transactions to the internet will result in a fundamental, structural change of how digital and physical media content will be created, discovered, distributed and traded online. It will shake up established structures and business models of centralized platforms and give way to new and unexpected ways of selling and licensing content or addressing a global audience.*[31]

Blockchain tokens can be used to convert digital items—artwork, intellectual property, music, in-game items, etc.—into a digital, time-stamped asset that can be traded, but cannot be forged, stolen, changed, or copied.

An obvious use of this application is artwork. Conventionally, it is easy to reproduce—and duplicate—digital artwork. It is hard, if not impossible, to verify the "original" version of a file representing a digital artwork. The introduction of digital value facilitates the creation of online galleries and art markets such as SuperRare, in which buyers can purchase digital artworks in the same way that art buyers can purchase a real-world painting or sculpture.

Sebastian Posth's own Content Blockchain Project aims to simplify the ownership of digital content. He points out that in purchasing conventional digital content, there is vagueness about whether the customer actually owns the content. In many cases, we instead license the content to be able to use it in a certain way. The Content Blockchain aims to provide smart licenses, represented by tokens, that facilitate the actual ownership and trading of digital content like books and music.

In addition to helping consumers deal with the ownership of digital products, blockchain tools also promise to help creators themselves. In the music industry, for instance, blockchain platforms support automated tracking of ownership and licensing of songs and samples so that artists retain their rights. What's more, the smart contracts deployed by these platforms can help artists get paid. For example, Ujo is a blockchain-based artist payment platform that promises artists a fee-free service to share their music while automatically collecting payments. The platform automatically splits payments between collaborators as per their blockchain smart contract-based agreement.

With blockchain applications for digital value, you need not merely trust in the preservation of your right to ownership—whether you're a creator sharing their works with others or a consumer purchasing the latest release from their favourite artist. Trust is also not required to guarantee that you're being paid for your work appropriately. Instead, the mechanisms that protect your claims and the contracts that pay you are built directly into these blockchain systems. By enabling digital value while maintaining ownership rights and collaboration agreements, blockchain tools stand to facilitate a new era of online creativity and consumption.

From microgovernance to borderless organizations.

Blockchain for digital governance

> *For my generation and the world we live in, it sometimes feels that there are no values at all anymore—that's almost something of the past. There is no common hope of building a future together as a species. But I think with this technology we can give a little bit of the hope back to all of us.* - Luis Cuende[32]

Democracy has not yet reconciled with the realities of our faster, flatter world. Blockchain technologies offer new approaches to organizing large-scale decision-making worth exploring in the face of this modern uncertainty.

Perhaps the most prominent example of blockchain-based governance is the DAO model: Decentralized Autonomous Organizations. DAOs, or sometimes Decentralized Autonomous Corporations (DACs), are organizations governed by programmed rules rather than a central executive. DAOs use blockchains to record their operations and rules transparently to the participants—those holding the relevant tokens—of the blockchain. Changes to the rules governing a DAO are essentially changes to the organization's smart contract encoded on the blockchain. Changes may be proposed and voted on by participants entirely transparently. These rules are then executed autonomously by the blockchain.[33]

DAOs hold great promise for for-profit companies, but the potential benefits of DAOs go beyond the business world. Governments around the world could leverage the blockchain for the benefit of citizens. In their 2019 report to the Joint Research Centre of the European Commission, David Allessie, Maciej Sobolewski, and Lorenzino Vaccari [34] write (p. 10) that "blockchain technology has a potential of facilitating direct interactions between public institutions, citizens and economic agents." They continue (p. 11):

> *… blockchain technology can disrupt the status quo in the public sector. Blockchain can bring efficiency by spanning siloes, flattening tiers and inspiring new service delivery models for governments. The architectural set-up of blockchain can also reduce operational risk and transactional costs, increase compliance and increase trust in government institutions.*[35]

We may learn about other features of blockchain-based governance by examining the consultancies offering to help set these services up. ConsenSys is one such consultancy building blockchain applications on Ethereum infrastructure. They provide identity management services (allowing government staff to securely manage identities, permissions, and assets). Another service they offer is smart regulation (allowing the creation of legal documents and regulations that are tamper-proof). They also provide asset and process management for both physical and digital assets. Finally, they provide support for budgeting and financial management, enabling government financial record-keeping for immediate and transparent reconciliation. ConsenSys also publishes a continually-updated record of government blockchain implementations around the world on their website.[36]

Blockchain tools can also support governance on smaller scales. Aragon provides blockchain-based collaboration tools to help people create what they call "global, bureaucracy-free organizations, companies, and communities." These organizations can conduct fundraising and transparently facilitate open decision-making processes.

Many have lost their trust in the governance systems that decide so much about how we live and work together. Blockchain-based governance systems go beyond the need for trust in leadership. Political promises can be implemented as smart contracts that revoke funding or permission if they are unfulfilled. Democratic systems can operate at faster and more granular scales. Spending and decision-making can be truly transparent and incorruptible. Perhaps, through these tools, organizations can be led without any hierarchy at all.

Working together at new scales.

Blockchain for digital collaboration

One clear advancement enabled by the Internet is the ability to work together at greater scales than ever before. Collaborative tools like Google Docs help students half a province apart keep simultaneous class notes for the lecture being streamed from yet another town. Cloud-based collaboration is now possible in engineering and manufacturing. Crowdsourcing tools enable thousands of people to contribute to a single initiative in myriad ways, and all on their smartphone while sitting on their couch.

Blockchain promises to advance this capacity to collaborate even further. Let's start with an obvious example: social media. While social media create an appealing environment for sharing information, they are also highly profitable avenues for advertising sales—usually without any payment to the content creators.

With blockchain, however, a different business model is possible. For example, Steemit is a social network that aims to build a social economy. With STEEM tokens, Steemit rewards users who publish, vote, and comment on content for their contributions to the community. From their official documentation:

> *While most social media sites extract this value for the benefit of their shareholders, Steemit believes that the users of the platform should receive the benefits and rewards for their attention and the contributions they make to the platform.*[37]

By creating these microeconomies and designing the mechanisms they run on, blockchain-based platforms like Steemit look to incentivize healthy communities that are immune to the kinds of problems described above.

Other blockchain technologies have implemented different kinds of behavioural incentives for collaboration. Medibloc's Real World Data encourages patients to provide anonymized data to healthcare services and researchers to advance medical innovation. Similarly, blockchain facilitates participation in citizen science projects—such as the EU-funded Decentralised Citizen-Owned Data Ecosystem (DECODE)—by making it easier and more secure for participants to contribute their data.[38]

Perhaps the most imaginative use of blockchain-facilitated collaboration, however, goes beyond human collaborators. The Internet of Things (IoT) is the colloquial term for Internet-enabled tools and devices, such as autonomous vehicles and smart homes. Conventionally, IoT devices can only work together in the ways that we tell them to. In other words, collaboration between IoT devices must be pre-programmed. Blockchain smart contracts, however, allow IoT designers to establish economic principles for IoT collaboration. Machines can have, spend, and earn their own currency. As discussed previously, imagine a self-driving car that can earn tokens by providing transport to riders, then spend those tokens on recharging and maintenance.[39] Melanie Swan argues that this enables not just self-driving but *self-owning* cars. From there, it is not difficult to see how networks of interacting, intelligent IoT machines can behave independently of direct management to provide entire service ecosystems to people.[40]

The efficient and effective coordination of resources between a set of actors is a significant challenge. Systems that can coordinate effectively are likely to be more capable of achieving their goals while being more sustainable with the resources they consume. In any given system, we entrust many aspects of coordination to centralized coordinators: people or organizations who are fallible, and whose mistakes or malice cause unfair distribution and cost the system as a whole. Still other kinds of contributions are undervalued (or completely unvalued) because we have never before had the ability to quantify or record them. In applications of blockchain for digital collaboration, however, we can place our trust in the intrinsic economy of the system itself.

Conclusion

As a relatively novel technology, it is difficult to predict blockchain's future applications and effects. Just as we continue to see societal transformations as a result of the Internet, blockchain services, apps, platforms, and infrastructure will lead to emergent, yet-unimaginable phenomena.

Underlying all of blockchain's potential, however, is a core concept: the deferral of trust. Blockchains may eliminate the bottlenecks and single points-of-failure that exist in conventional systems, instead distributing both risk and reward for the betterment of entire networks. The promise of blockchain lies in the processes, products, platforms, and systems we can build if we do not need to rely on third parties for manual coordination and maintenance. Instead, we may defer the trust we would conventionally place in these third parties, placing that trust in blockchain networks and infrastructure. It's like crossing a river: it may be possible to move cargo and people across even the harshest rapids by placing our trust in a ferry and its crew, but it is generally safer, faster, and more reliable to simply use a bridge.

[1] See Diego Gambetta's discussions on "Can We Trust Trust?", p. 4. http://www.sociology.ox.ac.uk/papers/gambetta213-237.pdf

[2] This shift in trust is vulnerable to two significant critiques. First, like all data-driven technologies, the data that goes into a blockchain must be generated by someone or something, commonly called an "oracle." For a blockchain to be effective, this data must be good quality—in other words, even if the blockchain technology is perfect, the data itself may not be. This means that blockchains minimize the trust required to process its transactions, but users of the blockchain must still trust the third-party oracles generating the data that drive it. This is known as the "oracle problem." Second—and again, like all technologies—the integrity of a blockchain depends on the integrity of the software, hardware, and networks that run it, and the designers and engineers who build and maintain these technologies. Ergo, trustless blockchains require trusting their infrastructure. Bruce Schneier details these critiques for *Wired*. https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/

[3] The introduction to Melanie Swan's 2015 textbook *Blockchain* provides an excellent, accessible explanation for blockchain's history and how it works. https://www.oreilly.com/library/view/blockchain/9781491920480/

[4] Handwriting can also be illegible to begin with, if you're me!

[5] http://blockchain-revolution.com

[6] *Blockchain Revolution*, pp. 178-185.

[7] *Blockchain Revolution*, pp. 185-188.

[8] While it is technically possible to assert absolute control over most blockchains, the literal cost in processing power to do so is always vastly greater than any potential financial gains.

[9] *Blockchain Revolution*, pp. 188-194.

[10] For a review of implementations working on this idea, see Bailey Reutzel's May 26, 2017 article on CoinDesk. https://www.coindesk.com/blockchain-move-self-driving-cars-fast-lane

[11] *Blockchain Revolution*, pp. 194-199

[12] Gary Kessler maintains an excellent overview of cryptography for free online, https://www.garykessler.net/library/crypto.html#intro

[13] *Blockchain Revolution*, pp. 199-206

[14] *Blockchain Revolution*, pp. 206-214.

[15] Some call this "dry code", as opposed to the "wet code" of human language agreements. Nick Szabo discusses this distinction on a blog post. http://unenumerated.blogspot.com/2006/11/wet-code-and-dry.html

[16] *Blockchain Revolution*, pp. 214-218.

[17] The Verge's Jacob Kastrenakes provided a comprehensive overview of this event on November 21, 2019. https://www.theverge.com/2019/11/21/20974692/valentines-day-text-message-delay-explanation-sms-syniverse-carriers

[18] Natasha Lomas and Romain Dillet outline the issues with modern Terms and Conditions for *TechCrunch*. https://techcrunch.com/2015/08/21/agree-to-disagree/

[19] Reporting for *The Guardian*, Carole Cadwalladr uncovered how Facebook personality quiz data was used to engage in psychological and political warfare, leading to the election of Donald Trump in the USA and the referendum decision for the United Kingdom to leave the European Union. https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy

[20] Taqanu's founder, Balázs Némethi, provides an excellent argument for the need for blockchain solutions to the refugee crisis for Prospect Magazine: https://www.prospectmagazine.co.uk/science-and-technology/how-blockchain-technology-could-help-refugees-get-citizenship

[21] See https://www.cbc.ca/news/canada/new-brunswick/immigrant-crediential s-not-recognized-1.4128960

[22] In fact, a common approach to this transfer of information might be to have the data printed and faxed to the destination—inconvenient and insecure at best and delaying care in an emergency at worst!

[23] Roger Pearl, M.D., wrote an excellent overview of the role of blockchain in EHRs for Forbes on April 10, 2018. https://www.forbes.com/sites/robertpearl/2018/04/10/blockchain-bitcoin-ehr/#1726a03779e7

[24] For an excellent and wide-ranging interview on these topics, The Verge's Editor-in-Chief interviews Amber Baldet on The Vergecast podcast, published on October 29, 2019. https://www.theverge.com/2019/10/29/20936216/amber-baldet-interview-blockchain-facebook-libra-vergecast

[25] See http://musebycl.io/music/spotifys–2018-holiday-ads-are-out-and-they-know-just-what-playlists-you-made-year and https://www.adweek.com/creativity/spotify-unearths-more-hilarious-user-habits-in-global-outdoor-ads-for-the-holidays/

[26] cf. Baldet and Patel's discussion. https://www.theverge.com/2019/10/29/20936216/amber-baldet-interview-blockchain-facebook-libra-vergecast

[27] See http://www.biospectator.com/view/news_view.php?varAtcId=6509

[28] See e.g., the USA's PRISM program; https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

[29] https://getsession.org

[30] https://status.im/features/#secure-messenger

[31] Posth wrote a useful overview of blockchain's impact on cultural industries In Medium on May 11, 2019. https://link.medium.com/6ToEKKe5P1

[32] Co-Founder of Aragon, a blockchain platform for building Decentralized Autonomous Organizations, in an article from Andrew Leonard in BREAKERMAG published February 20, 2019. https://breakermag.com/can-aragon-make-decentralized-autonomous-governance-work/

[33] Ethereum's founder, Vitalik Buterin, provides an overview of this concept and others on Ethereum's blog, published May 6, 2014. https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

[34] "Blockchain for Digital Government" was edited by Francesco Pignatelli. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC115049/blockchain_for_digital_government_online.pdf

[35] Charlie Towers-Clark lays out the Estonian case for Forbes on May 13, 2019. https://www.forbes.com/sites/charlestowersclark/2019/05/13/why-governments-should-be-using-blockchain/#1eb984967c3d

[36] https://consensys.net/blockchain-use-cases/government-and-the-public-sector/

[37] See "How does Steemit differ from other social media websites" https://steemit.com/faq.html#How_does_Steemit_differ_from_other_social_media_websites

[38] Writing for New Scientist, Matt Reynolds covers DECODE And some other blockchain crowdsourcing projects on May 22, 2017. https://www.newscientist.com/article/2131950-citizens-give-up-data-in-blockchain-project-to-improve-cities/

[39] I first encountered this idea in Melanie Swan's *Blockchain* on page 26. On May 26, 2017, Bailey Reutzel published an article for CoinDesk covering several projects that are implementing these ideas. https://www.coindesk.com/blockchain-move-self-driving-cars-fast-lane

[40] p. 26