DECEMBER 2021

The Human Rights Risks and Opportunities in Blockchain

AUTHOR
William Crumpler

CONTRIBUTORS
Marti Flacks
Amith Mandavilli

A Joint Report of the CSIS Strategic Technologies Program and Human Rights Initiative

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

DECEMBER 2021

The Human Rights Risks and Opportunities in Blockchain

AUTHOR

William Crumpler

CONTRIBUTORS

Marti Flacks

Amith Mandavilli

A Joint Report of the CSIS Strategic Technologies Program and Human Rights Initiative

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Acknowledgments

CSIS thanks Amy Lehr, James A. Lewis, and William Carter for their leadership support during this project, and Mariefaye Bechrakis, Faraz Ansari, Molly Naylor-Komyatte, and Ricardo Rendon Cepeda for their research and administrative assistance during the drafting of this report. CSIS also thanks the more than 50 individuals who participated in interviews and workshops over the course of this project.

This report was made possible through a grant from the U.S. State Department Bureau of Democracy, Human Rights, and Labor.

Contents

Executive Summary

A blockchain is a form of distributed ledger technology that allows a group of users to cooperatively maintain a record of transactions. By virtue of the way blockchain organizes the process of recording and validating transactions, this record is both tamper resistant and tamper evident, helping to protect the integrity of information stored by the network. Because of blockchain's distributed governance mechanism, these systems are also able to minimize or even eliminate the role of central authorities, improving transparency and resilience and minimizing the risk of corruption or abuse. Thanks to these properties, blockchain has been proposed as a potential solution to a wide range of problems in the human rights and international development space.

However, questions remain as to the true value of the technology in solving these issues, including whether it may introduce new human rights risks or distract from addressing current risks. To address this question, this report considers the human rights opportunities, risks, and challenges associated with the adoption of blockchain solutions in four prominent use cases—supply chain transparency, voting, digital identity, and land rights management. The report summarizes the advantages and risks of blockchain technologies and details the human rights challenges in each area that cannot be solved by blockchain alone. The analysis closes with recommendations for companies to help ensure that the blockchain products and services they develop and deploy will help to strengthen human rights around the world.

Supply Chain Traceability

Bottom Line: Blockchain technologies offer unique opportunities for achieving supply chain traceability and should continue to be explored as a way to help companies improve their due diligence processes and more comprehensively map their supply chain. However, this work should not take precedence over the more important task of building tools and institutions for collecting and verifying information about labor conditions—an issue which blockchain cannot solve.

More than 24 million people around the world are subjected to forced labor, and tens of millions more work under other abusive labor conditions. As governments increasingly move to mandate human rights due diligence by end-user companies, and some leading companies seek to improve respect for human rights in their own supply chains, blockchain has been proposed as a means to support more robust supply chain traceability and transparency. Specifically, blockchain has been advanced as a way for companies to track physical goods as they move through a supply chain and establish a common, trusted record for the provenance of those goods and the conditions of their production.

The transparency and distributed coordination allowed by blockchain could allow the technology to be uniquely beneficial as the basis for supply chain traceability initiatives. Blockchain can facilitate the recording of supply chain data such as date and location of harvest or manufacture, which can be valuable in identifying high-risk products or components, and in tracing a product through its life cycle to help companies more comprehensively map their supply chains. However, blockchain cannot verify the accuracy of data input into the chain, leaving the system vulnerable to abuse. This is particularly the case regarding claims made about working conditions, which are relatively easy to falsify when entered into a blockchain.

The most important potential advantage of blockchain for supply chain initiatives would come from the real-time traceability enabled by the network, which would lower the administrative burden of due diligence programs and enable the continuous monitoring of suppliers. The distributed nature of blockchain systems may also provide unique advantages that could lower the cost of implementing traceability programs, improve their ability to scale, and cultivate trust among participating firms. Even with the introduction of blockchain, however, traceability initiatives will continue to face significant obstacles, such as encouraging adoption throughout the supply chain, ensuring producers have access to the necessary technical infrastructure, and coordinating both companies as well as government regulators on adopting common data reporting standards and interoperable platforms.

The primary limitation of blockchain traceability systems is that they would not automatically improve visibility into whether a given supplier is engaging in illegal or abusive behavior. While the technology may provide some limited benefit as a means of immutably linking data to actors and making any derived insights more accessible to downstream providers, this is only valuable if the underlying challenges of collecting accurate, reliable data about labor conditions can be resolved. Thus, while blockchain may be valuable in supply chain traceability, its direct value for preventing labor abuses in supply chains is limited without additional tools, including stronger regulatory and market pressure for more sustainable business models and a stronger-worker-led system of accountability. Investment in blockchain technologies should therefore not supplant an emphasis on developing solutions to these more fundamental problems.

Voting

Bottom Line: Blockchain cannot solve the fundamental insecurity of online voting. While blockchain may prevent some forms of ballot tampering if implemented properly, these platforms will always be reliant on other forms of hardware and software that make them vulnerable to large-scale, undetectable exploitation. For this reason, blockchain-based voting platforms should not be used to conduct online voting, though there may be an opportunity for the technology to help secure voter registration or the reporting of election results.

The right to vote is frequently undermined by electoral mismanagement, either as a result of intentional manipulation by authorities or by a lack of electoral administration capacity that allows for outside manipulation by third parties. Advocates of blockchain voting believe the technology could help ensure access to free, fair, and peaceful elections by enabling forms of online voting that would help improve voter access and protect ballots from manipulation by electoral authorities. Specifically, blockchain has been proposed as a way of operationalizing end-to-end verifiable internet voting, whereby voters can verify for themselves whether their vote was counted properly without having to rely on any other party or system.

Advocates argue that blockchain may improve election administration in two ways. The first is by enabling online and mobile voting systems that may be easier for voters to use, resulting in improved turnout and a reduction in ballot errors. Studies so far have shown some evidence of small turnout improvements from the use of online and blockchain voting, though the magnitude of this effect remains a matter of debate. Online voting may also eliminate some opportunities for voter intimidation at in-person polling locations by giving voters the option to submit their ballots remotely—though remote voting may introduce new risks for coercion that occurs in voters' homes or workplaces, where ballot secrecy cannot be assured.

Blockchain has also been proposed as a solution to the manipulation of votes by corrupt authorities. If encrypted ballots were logged on a blockchain system managed by a diverse pool of actors, it would theoretically make it much more difficult for any actor to delete or tamper with those votes. However, this advantage is dependent on election administrators agreeing to open their voting process to a radical level of transparency by observers—something that is highly unlikely to occur in jurisdictions where election integrity is most under threat.

Blockchain-based systems are also limited in that they cannot provide assurance that votes have not been tampered with before being logged on the blockchain. Just as in the supply chain traceability use case, Blockchain would only serve to protect ballots once they are submitted to the network and can do nothing to prevent tampering by government authorities or outside actors that occur at other points in the voting process. Election security researchers have consistently found that the hardware and software used by online voting systems for submitting, receiving, and counting ballots are highly vulnerable to attacks, even when blockchain is used to store the votes. These vulnerabilities could allow both internal and external actors to carry out large-scale disruption or manipulation for a very low cost.

These issues could be overcome if an online voting system were able to achieve end-to-end verifiability by allowing voters to check their votes after the election concluded to determine for themselves whether tampering had occurred. However, while blockchain is one way of operationalizing end-to-end verifiable internet voting, election security experts have repeatedly emphasized that blockchain is not only unnecessary for realizing this goal but in many ways actually inferior to traditional information systems due to its added complexity. While blockchain-enabled voting, like other internet-based voting systems, currently poses severe risks to election integrity, blockchain may still be able to play a useful role in improving election administration if used to store voter registration data in a way that was more transparent and less vulnerable to tampering or used by polling locations to submit their vote tallies in a way that would make disruption and misinformation around election results less likely. These areas have received comparatively little attention relative to systems focused on the collection and tallying of ballots, and further work in this area should be encouraged.

Digital Identity

Bottom Line: Blockchain could help enable self-sovereign identity (SSI), a system of identity management that allows individuals to manage their own identity information instead of relying on centralized third parties. SSI could give individuals greater control over their personal data and help individuals without official documentation build a record of identity. However, SSI will not lead to better data governance practices without strong legal and regulatory pressure and could lead to significant privacy risks if deployed inappropriately. For this reason, deployments involving vulnerable populations or in places that lack strong legal protections should not be pursued until strong governance frameworks can be developed.

An estimated 1 billion individuals lack access to official identification. Obstacles to obtaining legal identity are particularly high for many of the over 26 million refugees in the world today, especially those who may have lost their original identity documentation as a result of conflict or natural disasters. Individuals excluded from official identity systems face enormous barriers to participating fully in economic and social systems. Proponents of blockchain believe that the technology may offer the potential to address many of these issues by serving as the technical infrastructure for a new kind of identity system termed "self-sovereign identity," where identifiers and credentials are held and controlled by users rather than by central authorities.One potential benefit of SSI is that it would allow individuals to build a portable record of identity from unofficial sources. For example, SSI may make it easier for residents of refugee camps to take the health records, educational credentials, and professional certificates accrued through their interactions with humanitarian organizations and use them after leaving the camp. Importantly, however, the value of these credentials is determined primarily by whether the receiving party agrees to honor them. While SSI may make it easier for individuals to establish a trusted link between themselves and these functional credentials, political and legal reform would be necessary before populations could utilize these credentials in place of more foundational identity documentation.

SSI also promises improvements to privacy by making the aggregation of personal information by centralized controllers unnecessary and empowering users to control their own identity information. The privacy benefits of SSI are undermined, however, if any personal information is stored directly on the blockchain, because this information can never be deleted and thus would create a permanent risk to the individual's privacy. Further, because some vulnerable populations may not have access to the smartphones required to store digital credentials, these individuals will likely end up relying on third parties to host their identity wallets. This relationship creates a number of potential risks depending on the policies and practices of the custodian and the level of control the user is able to exert. Finally, while SSI may enable better data governance practices by minimizing the need for third parties to collect information about users when verifying their identity, absent strong legal protections, there is nothing stopping governments, companies, and even civil society organizations from continuing to collect and utilize information about individuals in ways that violate their rights.

In the humanitarian sector, the use of SSI may help to improve the administration of aid programs by allowing organizations to collaborate more efficiently and reducing the amount of data each group collects about the individuals it serves. However, these benefits require overcoming a number of technical, operational, and political barriers to coordination and would have to be carefully structured to avoid excluding any individuals while managing the challenges of custodianship.

Blockchain-based SSI systems may help improve access to identity documentation and address the privacy risks of centralized digital identity systems, but only if individuals are granted true control over their information and have the tools to access it. Absent significant improvements in technology access, digital literacy, and legal protections, this will be unlikely in many settings. Responsible deployments would require careful attention to the significant risks involved and would require that both the technical architecture and especially the system's governance process be carefully constructed to resist abuse and prioritize the needs and interests of the users. For this reason, while work toward building SSI systems may be worthwhile, plans to apply this technology in places without adequate legal and regulatory infrastructure, or for vulnerable populations in humanitarian settings, should be approached with extreme skepticism.

Land Rights Management

Bottom Line: Blockchain technologies could help reduce some risks of mismanagement and corruption in land administration and may reduce the costs associated with participating in formal land management systems. However, blockchain does not help ensure that the details of land records are properly recorded and risks legitimizing unfair land distributions. Therefore, blockchain systems should continue to be explored in this area but should not distract from the more important initial steps of building high-quality, digitized records of property ownership.

Many countries around the world remain reliant on paper-based systems of land administration. These systems lead to substantial risks of mismanagement, loss of documentation, and conflict or property loss caused by incomplete or inconsistent records. Further, women and other disadvantaged groups often face barriers to claiming land or property rights regardless of the administrative system in question, and communities that hold collective ownership over land are often excluded from formal recognition. The primary advantages of blockchain lay in its ability to create a shared, trusted record of land records that can protect against forgery, tampering, and other forms of abuse by authorities. The use of smart contracts on the blockchain may also help to reduce the costs associated with land transactions, increasing the likelihood that landowners would participate in formal land management systems rather than rely on informal ones. Blockchain-based systems would also be more resilient than centralized systems in the face of conflict or natural disaster as long as the network had sufficient geographic diversity.

Blockchain land management systems have two primary drawbacks. The first major drawback is that the benefits of blockchain systems to disadvantaged groups rely on the willingness of the government to protect and enforce the rights that are codified on the network. In the case of women, for example, while blockchain may provide a means of more immutably recording women's property rights, this would not matter if women do not have the legal right to own land. Similarly, groups that have collective ownership over the land would receive no benefit if the country's legal system does not recognize collective ownership rights.

The second is that blockchain systems cannot guarantee the integrity of data when it is entered on the network. A primary challenge in advancing land rights is ensuring that populations that previously relied on informal mechanisms to record and pass down property rights can have those rights officially codified. This can often be a fraught process, as multiple individuals or families may simultaneously claim the right to a particular piece of land and neighbors may disagree over where boundaries lie. A blockchain would not help officials manage this process and could not provide any guarantees that errors would not be made. If land rights are distributed unfairly as a result, blockchain land management systems may end up reinforcing an unjust status quo.

The primary risk of blockchain initiatives lies in their potential to distract jurisdictions from investing in the initial process of developing more rights-respecting and inclusive land ownership systems and codifying them through high-quality, digitized records of property ownership. Without this work, blockchain systems risk reinforcing an unjust status quo. Therefore, while blockchain may have a role to play as part of a longer-term strategy for improving land rights management, the technology should only be considered if it is paired with or built on top of more systematic and comprehensive rights-based land allocation and management system.

Addressing the Human Rights Impacts of Blockchain Technologies

Depending on the use case and the details of implementation, some blockchain systems may exacerbate or pose new risks to universal human rights. Drawing from the UN Guiding Principles on Business and Human Rights as a framework, this report suggests a set of recommendations for how the groups involved in building and deploying these systems can take steps to reduce these risks. Though these recommendations are primarily targeted at corporations, they are also relevant to any civil society or government agency that is considering whether to deploy or participate in a blockchain system.

The first set of recommendations concerns the identification of human rights impacts. All organizations involved in developing or deploying a blockchain system should conduct due diligence to identify any potential human rights risks associated with the proposed use of blockchain technology. For blockchain, this should also include an assessment of whether the technology is fit-for-purpose to achieve any positive human rights impacts that may be claimed from its deployment, as well as assessing any potential human rights harms that may result from its use. After this initial assessment, organizations should adopt an ongoing review of risks and impacts to account for changes in the technology and in the context of its use. This process should be supported both by internal structures and procedures as well as by external advisory bodies that can help identify potential risks before they arise. All developers of blockchain technology should also conduct due diligence of potential buyers and partners before moving forward with sales or deployments in order to assess the risk that deployments may lead to human rights abuses.

The second set of recommendations concerns the mitigation of risks. Developers of blockchain technology should leverage contractual or other mechanisms to continuously review how their technology is being used by buyers in order to ensure that any abuses can be quickly identified and addressed. This should include an ongoing assessment of whether claimed human rights benefits are being realized. Developers should also ensure that the technical architecture of both the blockchain system and all supporting digital infrastructure is designed to minimize privacy and security risks. To reduce the risks of inappropriate use, developers should provide training to buyers to educate their employees on proper use of the system and how to avoid situations that may lead to risks of abuse. All responses the company takes to mitigate risks should be tracked to provide information on the effectiveness of their measures.

The third set of recommendations concerns transparency. Organizations involved in developing or deploying blockchain technology should institute a policy statement outlining their human rights commitments, which should be informed through consultation with relevant internal and external expertise. Organizations should also actively communicate information about how they are managing any potential and actual human rights impacts, including the outcomes of the responses they take. Developers working on blockchain technologies should, where possible and practical, utilize open-source software and allow for third-party audits in order to allow outside parties to identify any potential risks in the system. Furthermore, the administrators of permissioned blockchain systems should allow and encourage the participation of a diversity of parties as part of the network in order to ensure that the technology's transparency benefits can be attained.

Finally, organizations should ensure that remedy is available to anyone whose rights are impacted by the deployment of blockchain systems. Blockchain poses a number of unique challenges to the remedy process due to the immutability of data logged on the blockchain. Developers and practitioners must be aware of these risks and ensure that users are never at risk of harms for which no remedy is possible. Organizations should also consider how the distributed nature of blockchain systems may impact their ability to provide remedy in the case of any harms that come to light. Any deployments that include or focus on vulnerable populations must also consider how access to remedy may be impacted by a lack of technical infrastructure or digital literacy and strive to ensure that remedy is not only available but also accessible for these groups.

1

Introduction

First popularized in 2008 as the basis for the cryptocurrency Bitcoin, blockchain has grown over the past decade to become one of the most often discussed but poorly understood innovations of the modern digital economy. The promise of blockchain—to create systems of information sharing and storage that are secure, transparent, and decentralized—has sparked widespread excitement among technologists, entrepreneurs, activists, and policymakers. Many see the technology as a potential answer to a variety of human rights challenges, from ease of access to voting and identity-based service delivery to land rights protections and supply chain transparency. This excitement has been particularly strong among the human rights and international development communities, which nurture hopes that blockchain can help bypass corrupt or ineffectual institutions around the world to provide badly needed services that reinforce human rights norms more transparently and efficiently.

However, it is not clear that blockchain alone will provide a solution to these human rights challenges. Blockchain systems are never deployed in isolation but are embedded in existing technical and political systems that create challenges blockchain cannot always solve. In addition, there are very real technical and governance challenges that can complicate blockchain implementation and potentially limit its effectiveness as a human rights tool. Organizations hoping to tap into this new technology must understand these issues before they can decide whether it is the most appropriate solution, as well as whether its use may create new human rights risks. Similarly, as in all industries, companies that build and deploy these systems have a responsibility to ensure that their products and services do not cause or contribute to human rights harms and instead are designed and implemented to reinforce human rights norms.

Blockchain systems are never deployed in isolation but are embedded in existing technical and political systems that create challenges blockchain cannot always solve.

This report begins with an overview of how blockchain works and how decisions over protocols and access management can affect the advantages and disadvantages of deploying blockchain technology. The report then proceeds to examine four use cases that help illustrate the impact blockchain may have on important human rights issues. The analysis closes with recommendations for companies to help ensure that the blockchain products and services they develop and deploy will help to strengthen human rights around the world.

2

What Is Blockchain, and How Does It Work?

To understand both the potential and limits of blockchain systems, it is first necessary to understand how the technology works.[1] To begin, one should imagine a simple ledger. A ledger is nothing more than a book where each page is filled with a list of recorded transactions: on Monday, Alice gave Bob $10, on Tuesday, Carol gave Dan $15, and so on. Updating a traditional ledger is simple. The person in control of the book writes down the latest transaction on the most recent page. Modern systems utilize computer databases instead of physical books, but the essence is the same.

In most situations, nothing more complicated than a database is necessary for organizations seeking to keep electronic records of transactions. But when there is fear that the person in control of the ledger may not be trustworthy, a single point of failure can become dangerous. There may be nothing stopping the ledger's owner from falsifying the newest record or changing past records to suit their interests. These risks are compounded by a lack of transparency. If the ledger is controlled by a single entity that will not let others review the details of recorded transactions, it becomes difficult to determine if manipulation has occurred. These threats exist not just for ledgers used to record financial transactions but also for similar systems used to record votes, land titles, credentials, or almost anything else.

Blockchain systems attempt to solve this problem by distributing the power to make decisions about what transactions to record and legitimize. In contrast to a traditional ledger, which is held by a single authority, a blockchain is shared among multiple participants. Every user or "node" on the network has a full copy of the entire ledger, which is formatted as a sequence of cryptographically linked blocks (equivalent to the pages of a traditional ledger). These blocks are strung together into a "chain" to provide a complete history of transactions that have taken place over the network.

In a blockchain system, the nodes on the network must come together to agree on all new transactions. If someone wants to initiate a transaction over the blockchain, they first broadcast the intended transaction out to the rest of the network. These transactions are digitally signed using public key cryptography to prevent malicious users from being able to impersonate others. Periodically, all the computers on the network will gather up the new transactions awaiting approval into a single group (called a block) and check to ensure that the transactions have a valid signature and adhere to the blockchain's rules. Once a majority of nodes reaches a consensus on the validity of a block, it is added to the chain. The updated blockchain is then broadcast back out to all the nodes, which begin the process all over again.

The question of who is able to become part of a blockchain network is one of the key distinguishing factors between different types of blockchain systems. Because of Bitcoin's famously open governance system, many incorrectly assume that all blockchain systems must necessarily allow for the participation of anyone and everyone. In reality, many blockchain implementations are managed by central authorities or groups that restrict who may be a part of the network. These systems are referred to as closed or permissioned. The benefits of these permissioned systems are improved privacy, greater efficiency, and—depending on the nature of the users involved—potentially greater resilience to malicious disruptions. However, permissioned systems are often less transparent and reintroduce many of the same risks of abuse by administrators that blockchain was originally meant to solve.

Systems can fall along a spectrum between fully open and fully closed, allowing participation by the public in some activities but not others. Most systems aiming to address issues such as supply chain traceability, voting, digital identity, and land rights are at least partially closed to improve the network's efficiency. These kinds of deployments vary widely. Some are fully private blockchains maintained by industry consortia to manage supply chain processes. Others are hybrid models that restrict validation and publishing to approved users but still allow the public to see the history of transactions on the network. Most of the networks considered as part of this report fall into the latter category of hybrid blockchains, which are often termed "public-permissioned" blockchains.

Immutability

A primary benefit of blockchain systems is their ability to take advantage of encryption and consensus validation to make the network resistant to tampering. Entries in a traditional database can be overwritten, manipulated, or erased. However, with blockchain, the full detail of every transaction is immutably logged in a way that both resists tampering and ensures that any changes that do get made are evident to the other actors on the network.

This is possible because the blocks that make up a blockchain contain not only a list of transactions made over the network but also a cryptographic fingerprint, called a hash, that uniquely represents the contents of each block as well as all the blocks that came before it. Changing even a single character in a block will result in a completely different hash, making these functions useful for determining whether a given piece of data has been tampered with. Hashes can be calculated easily by anyone on the network, allowing every node to verify for themselves whether a particular block actually hashes to the value it purports. This means that nodes cannot try to pass off a tampered block as being equivalent to the original. Because the data contained in past blocks is used to calculate the hash, the manipulation of any historical records can also be easily identified.

Hashes make it easy to determine when blocks have been altered but on their own are not enough to allow a group of strangers who do not know or trust one another to work together to maintain the network. After all, a malicious node could always change a few transaction details in a block, recalculate all of the hashes, and then send their new fraudulent chain out to the other users. At that point, there would be two competing chains on the network which would each appear at first glance to be legitimate. As long as this were possible, a blockchain network could never sustain trust. The solution to this problem comes from the consensus protocol of the network, which creates a set of rules for how nodes cooperate when validating transactions. In a public blockchain such as Bitcoin or Ethereum, consensus protocols help solve the trust problem by forcing nodes to expend large amounts of computational resources to calculate the hashes, making it more difficult for malicious actors to tamper with the blockchain record.

In permissioned systems, such as most blockchains in the use cases studied in this report, trust is instead maintained by only allowing known and approved actors to participate in validating transactions. This allows these systems to avoid the high computational and environmental costs of permissionless systems. Malicious behavior is disincentivized by ensuring that any node that approves fraudulent transactions suffers damage to their reputations or even legal action.

Though the immutability of blockchain records is beneficial in most cases, there are some instances where this can also increase risks. Because information cannot be deleted from a blockchain, any data placed onto the network will be there forever. This does not mean that records cannot be updated, but rather that past versions of that record will still remain logged on the network even after an update. Blockchain systems thus pose an extraordinarily high risk to privacy whenever they are used to record sensitive personal information. Even if fully encrypted, the fact that these records will be logged forever means that they will always be vulnerable to hacks or future decryption by more powerful computer systems. In jurisdictions such as the European Union, privacy and data protection regulations do not allow for sensitive information to be stored in such an immutable way.[2] For these reasons, no blockchain system should ever be used to directly store personal or other sensitive information.

The risks related to immutability are compounded when considering that blockchains do not control the integrity of data introduced into the system. While blockchain systems can guarantee the integrity of data once it has been entered on the blockchain, they cannot guarantee that the data is correct when entered. A blockchain system for supply chain transparency, for instance, can guarantee that no one will erase or tamper with records once they have been logged, but they cannot stop a farmer from falsely claiming that their products were organically grown. Blockchain systems still rely on traditional institutions for certification and oversight to guarantee that the data being entered is true. This may be the most important limitation of blockchain technologies and will be discussed in detail in each of the case studies below.

While blockchain systems can guarantee the integrity of data once it has been entered on the blockchain, they cannot guarantee that the data is correct when entered. . . . Blockchain systems still rely on traditional institutions for certification and oversight to guarantee that the data being entered is true.

Transparency

Another notable benefit of a blockchain compared to traditional database systems is its transparency. In contrast to a centrally controlled database where only one party controls access, a blockchain system allows every node on the network real-time access to all transactions occurring over the network as well as to a full history of past transactions. This degree of transparency can be useful in situations where users do not trust one another and need a means of monitoring or auditing transactions. But as with any other system, taking advantage of this transparency requires users and institutions to have the knowledge, technical capacity, and resources to provide oversight and accountability.

While this radical transparency can have obvious benefits, it is not always desirable. In some applications, such as voting or identity management, perfect visibility would pose an unacceptable risk to privacy. In these cases, it is necessary to limit who can access certain pieces of information encoded on the blockchain. Encryption is one option, though this increases the complexity by requiring a parallel system of storage and distribution for encryption keys. Another option is to build the platform as a private blockchain rather than a public one and restrict access to only those users approved by a central entity. At this point, however, the difference between the blockchain and a traditional database becomes narrower.

Another solution to the privacy problem is to simply avoid encoding sensitive information onto the blockchain. For example, instead of storing the information itself, a blockchain could instead be used to store hashes of files that are kept off-chain in a traditional database. This would allow users to ensure that their records had not been tampered with by comparing the current hash of their records with the hash that had been stored on the blockchain. This comparison would immediately reveal if tampering had taken place, providing an additional layer of security without ever requiring the contents of the file to be made public. An example of this is in land rights management, where property titles can be kept in a centralized database and hashed copies can be distributed to landowners so that they can always check to see whether the official record matches their own. In these cases, blockchain may not eliminate the role of centralized institutions but may be able to provide additional security and trust to help those institutions function better.

Resilience

Blockchain's distributed nature makes the system more resilient to disruption by conflict, natural disasters, or malicious activity. In contrast to centralized systems, blockchain's peer-to-peer operation means that the network can never be taken offline by an attack on a single node. Public blockchain systems are more resilient than private ones due to the larger size of the network, but in general all blockchain systems have this advantage. Importantly, this resilience depends on the diversity of the network. In the case of natural disasters and conflict, a blockchain network must have sufficient geographical diversity to continue operating despite disruptions to a particular region. In the case of hackers, the network must have sufficient technological diversity in the kinds of infrastructure hosting nodes in order to be resistant to malicious activity targeting specific computer vulnerabilities.

For reasons already covered, blockchain systems are also resilient to attacks or mistakes that could erase or change data thanks to the use of encryption and consensus validation. However, blockchain systems are not impenetrable. The frequency with which major cryptocurrency exchanges have been breached provides clear evidence that even if the blockchain itself is resistant to attacks, the applications and infrastructure surrounding it are not similarly secure.[3] For example, even if a blockchain were used to store ballots submitted online, this would not prevent someone from hacking a user's device and using it to submit a tampered ballot. Institutions cannot assume that a blockchain will remove the need to think carefully about cybersecurity risks in the same way as any other digital system.

Efficiency

Compared to traditional databases, blockchains are inefficient. For a blockchain system to function, it is necessary for every single node to store a full copy of the network's transaction history. This storage requirement greatly increases the financial, material, and energy costs of implementing a blockchain solution, as hundreds or thousands of copies of a full transaction log must be stored instead of just one.

> ***Institutions cannot assume that a blockchain will remove the need to think carefully about cybersecurity risks in the same way as any other digital system.***

The requirement that each node be able to store the entire blockchain also puts a limit on the size of the data that can be stored. Most blockchains only allow for the storage of encoded files on the order of kilobytes or less.[4] While some types of small files may be stored this way, larger files must still be kept on physical devices or on the cloud. Though it is possible to store hashes of these larger files on a blockchain to allow for verification that they have not been altered, the files themselves are almost always housed elsewhere.

The consensus process also greatly slows down transaction speeds of blockchain systems compared to a database. The redundancy of having a majority of nodes confirm every block significantly slows the rate of validation. The Visa network, for example, is able to clear almost 400 times as many transactions per second as Bitcoin.[5] Not only are Bitcoin transactions slower to clear, but they also require enormous amounts of computational power. A single bitcoin transaction requires as much energy as 770,000 Visa transactions, or approximately as much as the daily energy consumption of 42 U.S. homes.[6]

Importantly, however, these costs are primarily associated with public cryptocurrencies. The efficiency of blockchain systems is heavily dependent on the governance model and consensus protocol used by the network. The kinds of permissioned (closed) blockchain networks that make up the majority of cases discussed in this report tend to have transaction rates and energy costs far closer to traditional information systems. However, by virtue of blockchain's distributed nature, even permissioned systems will inevitably face scalability concerns above and beyond that faced by centralized alternatives.

Smart Contracts

Smart contracts refer to the use of code to automatically execute the terms of a contract.[7] Smart contracts can be used to automatically execute transactions on a blockchain network once a certain set of conditions is met, such as releasing funds from an escrow account, transferring ownership of a property title, or publicly updating the details of a shipment as it moves through a supply chain. In all of these cases, the calculation and its results are stored on the blockchain in a transparent and tamper-resistant way.

Smart contracts can allow parties that do not trust one another to enter into agreements based on their mutual trust for the code being used. This allows organizations to avoid the need for third parties, improving the speed of transactions, eliminating opportunities for manipulation, and reducing reconciliation costs. In more advanced blockchain implementations, smart contracts can also enable a greater degree of process automation than ever before, since a far wider range of operations can be preprogrammed and trusted to run in line with all parties' expectations. The use of smart contracts introduces risks, however, due to the possibility that false or incomplete information uploaded to a blockchain may trigger the execution of contracts in ways that would be difficult to control.

3

Supply Chain Traceability

Bottom Line: Blockchain technologies offer unique opportunities for achieving supply chain traceability and should continue to be explored as a way to help companies improve their due diligence processes and more comprehensively map their supply chain. However, this work should not take precedence over the more important task of building tools and institutions for collecting and verifying information about labor conditions—an issue which blockchain cannot solve.

Human Rights Context

Free trade agreements that lower barriers to trade and technological improvements in manufacturing and transportation have driven supply chains to become global. A single product is often produced with components sourced or manufactured from many countries, assembled in multiple locations, and sold to end users all around the world. The resulting supply chains rely on multiple tiers of suppliers in potentially dozens of countries.

The relentless drive to continually reduce costs creates business models that incentivize exploitation of workers, especially at the bottom of the value chain. Article 4 of the Universal Declaration of Human Rights (UDHR) and Article 8 of the International Covenant on Civil and Political Rights (ICCPR) prohibit forced or compulsory labor, and more than 170 countries have signed the International Labour Organization's conventions on forced labor.[8] Yet, more than 24 million people around the world are subjected to forced labor, and tens of millions more work under other abusive labor conditions.[9] As governments increasingly move to mandate human rights due diligence by end-user companies, and some leading companies seek to improve respect for human rights in their own supply chains, blockchain has been proposed as a means to support more robust supply chain traceability and transparency[10]:

- **Traceability:** A traceable supply chain is one where it is possible to identify every key upstream actor that contributed to the production of any given product. Traceability enables corporate and government actors to systematically identify and map risk across a given supply chain. Absent accurate traceability, the origin of raw material inputs can be fabricated or lost in a web of off-the-book subsidiary suppliers, making it more difficult for end-user companies to hold suppliers to human rights standards. For example, following horrific revelations about abusive conditions on fishing vessels, Humanity United surveyed 23 Thai-based seafood corporations and found that 82 percent of them had acquired some measure of traceability back to fishing vessel origin.[11]
- **Transparency:** A transparent supply chain is one where there is accurate and reliable information available for every known actor in that chain, allowing an observer to know what is being produced and what the relevant conditions of that production are, including labor practices. Transparency enables interested parties to assess potential or existing human rights impacts at each step of a given supply chain. Absent transparency, details such as transaction data, sourcing standards, and provenance verification remain unknown, impeding assessment of labor right impacts.

Blockchain for Supply Chain Traceability

For any company to conduct supply chain due diligence and effectively address forced labor, both traceability and transparency must be present. The aim of blockchain supply chain efforts is to address both transparency and traceability by using the technology to create a common, trusted record for the provenance of physical goods and the conditions of their production. This would be accomplished by creating a digital token on the blockchain for each resource, material, or component of a product and using those tokens to publicly track those goods as they flowed from actor to actor.[12] Every product or batch of products would be labeled with a QR code, NFC/RFID tag, or other sensor device that links to their associated record on the blockchain.

These records could hold a variety of data, from the date of production to the identity of the producer. It could also contain information about the labor conditions impacting its production. As the items move between companies, these codes or tags would be scanned by workers to update the information contained on the blockchain. As materials are combined and processed to create new products, those inputs would be linked to any new outputs to provide a full and transparent record of the item's supply chain journey. This information could then be accessed by downstream buyers to help them understand the product's complete provenance.

The aim of blockchain supply chain efforts is to address both transparency and traceability by using the technology to create a common, trusted record for the provenance of physical goods and the conditions of their production.

In the context of labor rights, the key question of blockchain traceability systems is how this system could provide accurate information about the labor conditions of a given producer. In general, there are three approaches to this problem: (1) using the blockchain to record the results of third-party audits or certifications; (2) using the blockchain to record worker-reported data about labor conditions; or (3) using the blockchain to automatically record information about a company's business practices—such as the movements of fishing vessels, the payment records of workers, or their interactions with regulatory and enforcement authorities—that can be analyzed to produce insights about how workers are being treated. By linking this information to producers on the blockchain, downstream buyers would be able to more easily access a broader range of data to help inform their due diligence processes.

Recording third-party certifications and audit results is the most straightforward way to provide information about worker conditions. This approach would take advantage of the fact that some firms already undergo regular assessment for the purposes of regulatory compliance or as part of their participation in voluntary certification schemes. In a blockchain system, the results of these assessments could be uploaded to the cloud by auditors and linked to the producer as part of their blockchain record. Because this profile would then be linked to the tokens of every good or material produced by that entity, this arrangement would allow any downstream actor to easily check the certifications or audit the results of any producer they are tied to.[13]

However, recording worker-reported data directly on the blockchain is also an option. Levi Strauss, for example, has piloted a blockchain-based system for recording the results of worker well-being surveys at factories in Mexico and Poland.[14] Blockchain's role in the system is to ensure that the survey results are logged publicly and immutably and to help reassure workers that their responses are recorded correctly without revealing their identity.[15] Blockchain may also be able to support other initiatives such as the Libertas app developed by slavefreetrade, which supports self-reporting by workers about their labor conditions as a way of calculating a risk score for producers.[16] Once logged immutably on the blockchain, information derived from these tools would be more easily accessible to downstream providers and could be used to inform due diligence processes.

Finally, insight into labor conditions could also be gained by analyzing the operational data produced by a company.[17] By establishing a record of a company's business practices, auditors, NGOs, and downstream buyers can establish systems for automatically flagging potentially risky behavior. For example, in the seafood industry, the use of vessel monitoring systems can allow outside parties to track a ship's movements, revealing when the vessel may be engaging in high-risk practices such as staying out at sea for over a year—a possible indicator of forced labor.[18] Other high-risk behaviors such as inconsistent worker payment records, high labor turnover rates, or incomplete legal documentation could also be flagged. The results of this monitoring could help flag suppliers that may be at high risk for illegal of abusive practices, helping to inform follow-up due diligence and mitigation efforts by regulators and downstream buyers.[19]

In some cases, end-user companies may be able to perform this kind of analysis on data uploaded directly to the blockchain. In other cases, especially where large quantities of data are involved, the information would have to be stored separately off the blockchain. In these cases, blockchain would serve to store either pointers to that off-chain data, so that other actors could find and analyze it themselves, or simply the findings of firms which had analyzed the data.

Case Study: Sea Quest Fiji

In 2017, the World Wildlife Fund for Nature (WWF), blockchain developer Viant, internet and communications technology (ICT) provider TraSeable, and tuna fishing company Sea Quest Fiji engaged in a project to institute blockchain-based tracking for tuna fisheries.[20] The project involved tagging tuna caught by Sea Quest's fishing vessels and uploading information about each fish to a blockchain. As each fish advances through the supply chain, its tag is scanned at regular points to record information such as the date, time, and GPS coordinates of the fish at each step in the process. After processing and packaging, QR codes allow the fish to continue to be tracked all the way to the final consumer, with all information being logged publicly.[21] In addition to provenance data, this blockchain also records the certifications earned by the producer as evidence of responsible production.

According to interviews with Sea Quest, the fishing company found the blockchain system to be more effective and secure than alternative technologies such as barcoding, which is more susceptible to manipulation and cannot represent the same volume or diversity of data.[22] In addition, Sea Quest emphasized that the ability to log data automatically helps reduce the risk of tampering by eliminating opportunities for humans to control what data is being entered. In interviews, WWF reported that blockchain-based solutions are highly attractive for traceability initiatives due to their immutability and their potential to make it more difficult to hide information by breaking down information silos.[23]

Sea Quest also reported that the blockchain system makes it easy for outside entities such as Fiji's labor department to validate production records, helping to build trust in the integrity of captured data. Sea Quest noted that their traceability system has the capacity to expand to also include information about crew lists, vessel tracking, and any other data that may be required by regulatory authorities.

The experience of Sea Quest also serves to highlight some of the challenges that come with blockchain traceability systems. Sea Quest reported struggling with the RFID tags they initially used for their pilot, as there was little local expertise in sourcing, installing, and maintaining the RFID equipment. Eventually, Sea Quest ended up abandoning RFID tags altogether, moving to QR codes instead while also evaluating NFC tags as a possible alternative.[24]

In addition, the project highlighted the importance of cooperation for actors throughout the entire supply chain.[25] Without downstream actors willing to cooperate in extending the traceability project, it would have been impossible to achieve the attained level of end-to-end transparency. As a vertically integrated company that owned its own processing facilities, this traceability integration was easier for Sea Quest to achieve than it likely would be for most other seafood actors.

Advantages of Blockchain for Supply Chain Traceability

1. **Blockchain could improve the visibility firms have into the supply chain actors they are involved with, helping to carry out due diligence and remedy human rights abuses in its supply chain.**

Modern global supply chains are incredibly complex and fragmented, often involving hundreds of suppliers across multiple countries. This makes achieving traceability more than one or two levels down challenging. By providing a trusted, decentralized mechanism for recording product information throughout a full supply chain network, blockchain could help companies achieve greater visibility into the actors they are entwined with and allow them to identify high-risk suppliers more easily. Once these actors are identified, buyers would then have the opportunity to work with that producer to remedy their behavior, alert relevant government authorities to ensure that the actor's behavior was investigated, and, if necessary, cut that actor out of their supply chain altogether.

The greatest advantage of blockchain compared to alternative database systems that would record information from tier three and below suppliers is the way that blockchain networks support real-time traceability. Because every entity has a copy of the full blockchain record and sees all incoming transactions, the administrative burden of traceability can be dramatically reduced. Relevant information can be made instantly available in real time on a single platform. This benefit can also extend to auditors, regulators, NGOs, and any other actors with an interest in monitoring the activities occurring on the network. Further, because this information is constantly being updated, it could allow companies to build systems to continuously monitor their suppliers for red flags, making it easier for due diligence to become more than a one-off or periodic exercise.

2. **Blockchain may help improve the transparency of supply chains by allowing data to be stored in an immutable way, which would protect against manipulation and make it easier for observers to discover discrepancies.**

Because data stored on a blockchain is highly resistant to tampering, downstream supply chain actors and third-party observers can have greater trust that information logged by a producer cannot be manipulated. When combined with automatic data-collection processes utilizing sensors or tags, this feature may allow an increasing amount of information about supply chain processes to be immediately and immutably logged. This information would be much harder to tamper with compared to paper-based or traditional electronic records, which may remain in the producer's control for months before being passed along to an outside party.

Importantly, blockchain only assures the integrity of data after it has already been uploaded. It does not prevent false data from being added by entities hoping to avoid scrutiny or cover up for illegal or abusive behavior. However, blockchain may make it easier to identify and investigate such information. Thanks to the transparent, immutable nature of records logged on the blockchain, outside parties can easily conduct audits to verify the integrity of data reported by producers. This makes it more likely that producers that routinely submit false information will eventually be discovered and held accountable.

Open and distributed blockchain systems could also make it easier for outside parties to attest to the truth of claims logged on the blockchain. This may include worker attestations uploaded through mobile platforms or verification provided by NGOs, auditors, or regulators. Further, if operational data is made available, downstream companies can conduct their own checks for patterns of behavior that may indicate human rights risks. By making these sources of information more readily available to downstream actors and other observers, blockchain may make it easier for companies to leverage multiple sources of data and strengthen their due diligence processes.

3. **Blockchain may lower the costs of operationalizing supply chain traceability initiatives and improve scalability, making it more likely for a broad array of actors to participate.**

Cost is a major barrier hindering the uptake of better supply chain tracking technologies. Particularly for first-mile producers, implementing traceability initiatives can be prohibitively expensive, leading to reduced adoption. Because the value of traceability schemes is dependent on tracking materials through the full chain of suppliers, gaps in uptake among small-scale producers—which are often at the highest risk for illegal or abusive practices—can dramatically undermine the value of the entire network.

Blockchain may help to reduce the costs borne by producers in several ways.[26] First, its adoption may lead to cost savings due to the improved efficiency of electronic record-keeping compared to paper records, such as in the case of Sea Quest described above. Blockchain traceability systems may also help eliminate redundancy in data recording by providing a single platform for uploading data and by standardizing the information that producers are expected to record. Smart contracts may further reduce costs by allowing firms to automate certain transactions and processes without having to rely on legal intermediaries.[27] Finally, blockchain may help reduce the audit burden felt by producers if the data they upload is able to allow buyers, regulators, and certification bodies to institute more effective remote-monitoring schemes and better target in-person audits for high-risk entities.

Because of its distributed nature, blockchain may also allow traceability efforts to scale more rapidly than systems based on other technologies. Once data reporting requirements and a network consensus mechanism have been established, new users can be quickly and easily onboarded onto blockchain platforms and integrated into ongoing operations.

Importantly, however, both the cost and scalability of a blockchain system is heavily dependent on how it is set up. Any traceability solution making use of a public blockchain would quickly face barriers due to high transaction costs and slow transaction speeds. Permissioned blockchains, in contrast, may allow for greater volumes of data to be transacted at lower costs, though with potentially fewer third parties able to verify the data.

Risks of Blockchain for Supply Chain Traceability

1. **Depending on what information is recorded, workers may face risks to privacy and may be subject to employer retaliation.**

If a blockchain traceability system records information collected by or about workers, it could create risks that these workers' private information may be exposed or that they may become vulnerable to retaliation by employers for reporting on abusive practices.

Risks to worker privacy would primarily emerge if details about workers were logged as part of tracking programs meant to ensure their well-being. For example, the nonprofit iRespond has worked with the Thai government to establish a system of using iris scans to log fishermen as they board and exit their vessels. These logs help create a record that allows observers and regulators to identify when a worker does not return from a journey or when a worker is being kept aboard a vessel for an extended period of time. This system is not currently linked to any blockchain but is an example of the kind of data that could be uploaded to a blockchain to expand its utility in supply chain due diligence.

However, the capture of individuals' biometrics and work details presents obvious privacy risks. These blockchain-related risks may be mitigated by ensuring that no biometric data is directly logged on the blockchain and instead guaranteeing that only the result of crew checks are visible to outside parties.

Even if no biometrics are logged, system designs must still take care to ensure that any pseudonymous identifiers are unable to be linked back to workers in a way that may reveal information about them.

Threats of employer retaliation against workers arise if producers are able to link critical reports of the supplier's business practices back to the individual workers or factories. All systems that rely on worker-reported data, therefore, must ensure that the identities of these workers are protected and that information they log cannot be traced back to them. This is challenging, however, as these systems must simultaneously be able to verify and attest to the fact that these workers are, in fact, tied to the workplaces they are submitting information about. Likewise, even anonymity does not prevent retaliation against workers at a particular factory or business unit—a risk that is true in non-blockchain-based worker reporting systems as well.

The blockchain pilot carried out by Levi Strauss to log worker well-being surveys on the blockchain addressed this issue by providing each worker with a pseudonymous ID that was not linked to any personal information.[28] In addition, the researchers uploaded the surveys in batches, preventing employers from correlating answers to worker identities based on their submission time.[29] The project team managed to get around the problem of worker verification by being present while the survey was taking place, allowing the group to attest to the validity of the surveys being logged. These practices would be extremely difficult to replicate in most workplaces, however, due to resistance by employers.

Supply Chain Traceability Issues Blockchain Does Not Solve

1. **Blockchain cannot prevent producers from reporting false data about their products or practices, a key barrier to improving supply chain transparency.**

While blockchain systems can help ensure that data is not manipulated after it has been recorded on the ledger, it cannot ensure that the data is accurate when it is uploaded. This creates risks that blockchain traceability systems could legitimize fraudulent claims made by supply chain actors about their labor practices.[30]

As addressed in the section's introduction, one of the primary ways of providing attestation for labor conditions is through third-party audits and certifications, and upstream supplier attestations. Such social audits and attestations, however, often provide limited credible information to reliably assess labor conditions.[31] Interviews conducted for this project have revealed a broad skepticism among labor rights and supply chain transparency experts about the ability of audit results and certifications to provide authoritative information about whether an entity is engaging in illegal or abusive business practices. Therefore, traceability solutions that are limited to logging third-party certifications will be insufficient to provide full transparency into an actor's labor conditions.

The use of worker-reported data for verifying claims also comes with challenges. In some cases, workers may be hesitant to contribute due to concerns over retaliation or lack of faith in the utility of reporting. In other cases, the information reported by workers may not be representative. Experts interviewed for this report pointed out that business owners have used designated attestors among their workers who are compensated for providing false information or verifying fraudulent claims to regulators. In addition, there are significant logistical difficulties involved in regularly obtaining a broad and representative sample of information from workers. Language barriers may make it difficult for workers to make use of tools developed by researchers, and organizing space and time for workers to regularly engage with reporting tools can be difficult in many of the workplaces most at risk of abusive practices.

The final source of data for verifying labor conditions is the operational data collected from and about producers. Depending on what data is used, there are a broad array of challenges in ensuring this data is both available and reliable. For example, one labor rights expert interviewed for this project described a project that required fishing vessel owners to use monitored electronic payment systems to identify when owners may be withholding wages from their workers. This system was able to be subverted by captains who would collect the ATM cards from workers and withdraw the cash themselves to prove that the money was transferred on time, without handing the cash over to the workers. Similarly, monitoring the terms of worker contracts, for instance, does not reveal whether those terms are actually being honored on the ground. Blockchain may be used, however, to track business practices that may be indicators of abuse rather than the abuse itself.

Without robust, authoritative third-party verifiability of the claims made by producers, the information logged as part of a blockchain traceability system may have only limited value to buyers conducting risk assessments of their supplier base. The use of these systems may in some cases be actively counterproductive if blockchain ends up legitimizing actors that take advantage of this uncertainty to misrepresent their own business practices.

An additional issue with this approach is that the necessary data may be extremely difficult to access. While in some cases information may be gleaned from public sources, in many others the only actors who would hold this data would be government regulators or the companies themselves. Both of these groups will likely be resistant to opening an increasing amount of their information to wider scrutiny. Thus, both data quality and availability can pose a key barrier to transparency efforts.

> ***Without robust, authoritative third-party verifiability of the claims made by producers, the information logged as part of a blockchain traceability system may have only limited value to buyers conducting risk assessments of their supplier base.***

2. **Blockchain traceability solutions may rely on the availability of technological infrastructure that may not exist for small-scale producers.**

In order to participate in traceability initiatives, producers must have access to the tools, devices, and connectivity required to connect their processes to a global blockchain network. For many small-scale producers at the end of supply chains, this access does not currently exist.[32] Many of these producers still rely on paper-based systems of recording information. The products they create may not lend themselves to RFID tags or other tracing tools, and their operations may also not be designed to accommodate them. Onboarding these actors onto a blockchain platform would require significant investment in technological infrastructure and digital training that could slow and complicate uptake among the actors that are the most important targets for traceability efforts. The experience of Sea Quest in struggling to support the implementation of RFID tags for tuna traceability foreshadows the problems that many of other small-scale producers may have if asked to adopt new technological systems. The availability of devices and infrastructure would also affect any plans to empower workers to directly report information about working conditions.

3. **The value of blockchain traceability systems is dependent on broad uptake within a supplier ecosystem, which may be limited due to concerns over cost, confidentiality, and disagreements over reporting standards**

The success of traceability initiatives is dependent on buy-in from actors throughout the full supply chain of a particular product. If some actors refuse to participate in tracking programs, critical information about supplier linkages would be unavailable to downstream buyers and outside observers.

Some actors may be wary of the costs of purchasing the equipment necessary to participate in traceability initiatives and the resources required to train and maintain a workforce capable of logging the information required. Though blockchain may lower some of the costs of traceability systems, as described previously, it will not eliminate them.

Some producers may have concerns that participation could expose sensitive business information such as price, production capacity, or supplier relationships. In order to address this, blockchain traceability systems could allow for selective disclosure, where entities can control who can access the information they upload to the traceability platform. However, providing producers with the ability to control the visibility of their information presents an obvious conflict with the goal of full transparency. Traceability programs must also contend with the fact that some producers may resist participation simply because they do not want their abusive practices to be revealed.

Workers may also resist the adoption of traceability systems. As addressed previously, this may be due to general privacy concerns related to the collection of their data or specific fears of reprisal from employers. Additionally, in industries where asset tracking is currently accomplished manually, workers may fear for the loss of their jobs or wages if automated systems were seen as replacing their role. Some workers linked to small-scale producers may also not want to participate because they may have fled from law enforcement and would see integration into any kind of formal identity and tracking system as a possible threat. Ultimately, downstream buyers and regulators will largely influence whether producers adopt such systems.

Finally, the difficulty of coordination on data-reporting standards and platform interoperability may create practical barriers to bringing a diverse array of actors onto a shared platform. If suppliers cannot agree on common standards for what data is to be recorded and how it is to be represented in digital form, traceability systems will not be able to take shape. Suppliers often provide goods to multiple intermediate and end users, raising the possibility of needing to incorporate multiple tracing systems. While progress is already being made in some industries to articulate common standards for data reporting, the sheer diversity of potential data points and the difficulty of achieving consensus in the context of competing supplier priorities will create ongoing challenges for traceability initiatives.[33] Finally, as there is not likely to ever be a single global platform for recording supply chain data, the interoperability of different blockchain platforms will be a key requirement for traceability platforms to achieve the necessary scale to fully represent a diverse array of supplier networks. If traceability systems were to end up being siloed, it would greatly diminish their potential benefits.

Conclusion

Corporations have both an opportunity and a responsibility to address labor abuses in their supply chains by conducting due diligence of their suppliers and assessing the risk that they may cause, contribute to, or be linked to these abuses through their business operations. In order to undertake this work, however, companies must understand their supplier relationships and have access to trusted information about worker conditions for those producers. Blockchain has been proposed as a solution to both of these problems due to its potential to serve as a trusted repository for information about products, suppliers, and the relationships that exist between different groups of actors in a supply chain network.

By allowing firms to track the journey of products through a supply chain, blockchain may make it easier for firms to map their supplier relationships and improve their due diligence processes. While other technologies may also be used to achieve product traceability, the distributed nature of blockchain systems provides several unique advantages that could lower the cost of implementing these programs, improve their ability to scale, and cultivate trust among participating firms. There continue to be many difficult and unsolved problems in this space that exist independent of whether blockchain is used, including access to technical infrastructure, coordination on reporting standards, and adoption hesitancy among producers. Nonetheless, blockchain has the potential to serve as the basis for future traceability programs if these barriers can be addressed.

Blockchain's benefits for transparency, however, are far more limited. Better awareness of labor conditions will require addressing the current gaps that exist in certification and audit regimes, worker reporting, and the analysis of operational data. Blockchain will not help to solve any of these problems. While the technology may provide some limited benefit as a means of immutably linking data to actors and making any derived insights more accessible to downstream providers, this is only valuable if the underlying challenges of collecting accurate, reliable data can be resolved. This emphasizes that blockchain should not be viewed as a panacea to the problem of labor rights abuses, but rather as one tool among many that would have to be used in concert to address systemic risks.

4

Voting

Bottom Line: Blockchain cannot solve the fundamental insecurity of online voting. While blockchain may prevent some forms of ballot tampering if implemented properly, these platforms will always be reliant on other forms of hardware and software that make them vulnerable to large-scale, undetectable exploitation. For this reason, blockchain-based voting platforms should not be used to conduct online voting, though there may be an opportunity for the technology to help secure voter registration or the reporting of election results.

Human Rights Context

Voting is a universal human right owed by states to all citizens. Article 25 of the International Covenant on Civil Rights (ICCPR) provides that states owe its citizens the right to take part in the government of their country, directly or through freely chosen representatives. Free, fair, and peaceful elections are the vehicle by which governments deliver on this obligation.

The right to vote, however, is frequently undermined by electoral mismanagement, either as a result of intentional manipulation by authorities or by a lack of electoral administration capacity that allows for outside manipulation by third parties. While there are many forms of electoral interference that undermine free and fair elections, blockchain technology has the potential to impact two high-risk aspects of electoral administration:

- **Fidelity of Vote Counting:** The right to vote is undermined by electoral administration that cannot guarantee the security and accuracy of vote counting. Government authorities frequently manipulate vote-counting systems for the purpose of fixing official electoral results. In other cases, political parties, both in and out of power, seize opportunities created by insecure systems to manipulate results themselves. A 2010 study of elections that took place between 1978 and 2004 found manipulation in 61 percent of cases.[34] Freedom House's *Freedom in the World 2021* report finds that 70 percent of countries and territories it surveyed hold elections using some degree of unfair electoral laws or with partisan election management.[35]

- **Voting Access:** Voter turnout rates vary widely around the world, from highs above 80 percent to lows in the 30 percent range.[36] Turnout can be attributed to numerous factors, including compulsory voting laws, automatic voter registration, and aggregate levels of national education.[37] Challenges in physically reaching polling places and in filling out paper ballots can be additional barriers to participation in some cases.

Blockchain Voting

Proposals for applying blockchain technologies to election systems are usually presented in the context of broader, more ambitious plans to replace paper-based voting with online voting. Notably, proposals for internet voting have existed since long before blockchain networks were first devised, and most examples of e-voting today do not use blockchain at all. This includes Estonia, which, despite the use of blockchain for other e-governance purposes, does not use blockchain in its widely referenced internet voting system.[38]

However, these systems have attracted intense criticism from election security experts. While such systems may include a number of technical and procedural controls to prevent tampering and manipulation, they ultimately still require voters to trust the integrity of election officials, network infrastructure, and their own computers.[39] A failure at any of these points could lead to undetectable manipulation of voting results, which not only creates a risk of election tampering but also could undermine public trust in the election process and cast doubt upon even legitimate elections.

Blockchain has been advanced as a potential solution to this problem by serving as one way for internet voting systems to achieve end-to-end verifiability, whereby voters can verify for themselves whether their vote was counted properly without having to rely on any other party or system.[40] When voting with paper ballots, voters can easily confirm that the marks they make on their ballot correspond to their preferences. Online systems, in contrast, represent votes as pieces of code that voters have no way to see or verify. Errors or malicious attacks could manipulate this code without the voter realizing it, leading to a different ballot being submitted than what the voter had intended. In an end-to-end verifiable system, however, a voter can confirm for themselves whether their ballot was both cast as intended (their selections were correctly recorded) and counted as cast (their ballot was included in the final tally).

Blockchain voting systems propose to achieve this by having voters post their encrypted ballots to a publicly accessible blockchain rather than sending them directly to election officials. The nodes on the blockchain network then work together to check the validity of each ballot before adding them to the chain, which acts as a complete record of votes in that election. In blockchain voting schemes, all nodes in the network may be run by a single government entity, but ideally the responsibility for validating ballots would be shared between a wide range of actors, including election administrators, political parties, and civil society organizations. Some proposals would allow members of the public to also participate in the validation process, though this may create additional privacy and security challenges.

Election officials would collect the encrypted ballots from this public blockchain in order to tally the results. Ballot secrecy could be preserved either by using homomorphic encryption to combine votes while still in encrypted form or by using mix networks to shuffle the ballots so that they cannot be traced back to the voter.[41] After the election, voters could use a receipt generated by their voting application to look up their ballot on the public blockchain and confirm that it conforms to their expectations. This verification process would allow manipulation to be identified even if only a very small portion of voters actually went through the process of verifying their ballots.

Though blockchain voting has been piloted for a number of small-scale organizational elections, its use in political elections has been extremely limited so far. The most notable deployments to date have occurred in conjunction with elections held in the United States, Russia, and Venezuela (see text boxes below).

Case Study: Voatz

Voatz is a blockchain-based election platform that allows voters to submit their ballots remotely through their mobile phone. Voatz has been used in more than 75 elections, including in West Virginia for the 2018 U.S. midterm elections, in Denver for the city's 2019 municipal elections, and in Venezuela for a national referendum organized by interim president Juan Guaidó.[42]

Voatz begins by verifying the voter's identity and eligibility. In the United States, this has required voters to submit a picture of their official ID, which is compared with a video selfie taken by the voter to confirm their identity. A biometric such as a fingerprint or smartphone facial recognition feature is then used to link the voter to their device, preventing them from using other devices to submit multiple votes.[43] In settings such as Venezuela where few have access to phones with biometric authentication, Voatz compares the credentials to records from an official voter ID database.[44]

Once voters are registered, they receive a ballot which they fill out within the Voatz app. Upon submitting the ballot through the app, the app generates an anonymous ID that is added to the ballot as well as to a pair of ballot receipts sent to the voter and the election authority.[45] This ID is meant to enable vote spoiling, post-election audits, and voter verifiability without the risk of revealing the voter's identity. The encrypted ballot is then submitted to the blockchain, where a network of servers collaborates to verify the ballot's integrity.[46] Election authorities have the opportunity to decide which organizations can participate as verifiers, and every election so far has had at least Voatz, the election authority, and a third-party auditor participating on the network.[47]

After polls close, election officials can access votes stored on the network and print them as paper ballots, which are scanned and tallied in the same way as any other ballot. Voters and election officials can use the anonymous ID attached to the ballot and receipt to confirm whether any given ballot has been properly recorded.[48]

After pilots of the system, election officials reported being pleased with the ease and simplicity of the process.[49] One study estimated that the availability of Voatz mobile voting led to a 3 to 5 percent increase in remote turnout.[50]

However, Voatz has also drawn heavy criticism from security experts.[51] In August 2020, three MIT researchers published a study demonstrating that Voatz was susceptible to a range of malicious attacks that could expose voters' choices to outside parties and even lead to votes being altered.[52] The authors found that malicious actors could break into voters' mobile devices to read and alter votes, take control of the server used to receive votes before they are posted to the blockchain, or listen in over the network and use leaked data to infer how a user voted.[53] With respect to Voatz' use of blockchain, the researchers found that "the system's use of the blockchain is unlikely to protect against server-side attacks."[54]

Voatz disputed these results.[55] However, a third-party security assessment commissioned by Voatz confirmed the MIT team's findings and identified 16 additional "high-severity" technical vulnerabilities.[56] With respect to Voatz' use of blockchain, that assessment concluded: "Storing voting data on a blockchain maintains an auditable record to prevent fraud, but this comes at the expense of both privacy and increased attack surface. . . . Anyone with administrative access to the Voatz backend servers will have enough information to fully reconstruct the entire election, deanonymize votes, deny votes, alter votes, and invalidate audit trails."[57]

Despite this risk, Voatz has stated that there have been no known instances of hacking or interference in its trials thus far.[58]

Case Study: Russia

Since 2019, Russia has been experimenting with blockchain voting as a way to enable internet voting for its citizens. In September 2019, the city of Moscow used a blockchain-based voting system to allow citizens in three districts to vote in local elections.[59] Blockchain voting was used twice in 2020 in State Duma pre-elections and for a national referendum on amendments to the Russian constitution. In 2021, Russia allowed citizens in six regions to use the platform when voting in the State Duma election, recording more than 30,000 votes using a blockchain.[60] According to the study team's interviews with Russian election monitor Golos, some information about the system used in Moscow's city elections has been made available to civil society, but the system used for federal elections remains entirely opaque.[61]

When a voter submits their ballot on Moscow's remote voting platform, their vote is anonymized and posted to a blockchain in encrypted form.[62] Election officials reportedly tally the votes posted to this blockchain using homomorphic encryption and collect anonymous paper ballots from each blockchain voter to fulfil legal requirements for paper confirmation.[63] At the end of the election, voters are able to check the public blockchain to verify that their vote was recorded as intended.[64] The information posted to the blockchain is also meant to allow journalists and independent researchers to conduct independent verifications of the integrity of recorded votes.

However, researchers, journalists, and election monitors have identified several issues with the way these systems have been deployed so far. Ahead of the 2019 Moscow elections, for example, a security researcher showed that it was possible to break the encryption scheme used by the platform within 20 minutes using a standard personal computer.[65] This would potentially allow an attacker to reveal the identity of voters on the platform and tie them to their ballots. During the 2020 national referendum, Russian media outlet Meduza found that the keys provided by election officials to allow observers to check the vote count could also be used to decode the votes published by election authorities.[66]

Meduza was also able to derive the passport numbers of almost 1.2 million Russian voters who had registered to vote online based on information made available by officials.[67] After the election, many of these same passport numbers were found to have been put up for sale on the dark web by unknown hackers for $1.50 each.[68] In 2021, the blockchain system was heavily criticized by opposition members after it led to significant delays in the posting of vote totals, raising concerns that Russia's ruling party may have leveraged the system to log fraudulent votes.[69]

Actions by Russian officials have amplified these issues with the blockchain. For example, in 2019, after the flaw in the Moscow platform's encryption was discovered, the city stopped sharing information necessary for researchers to verify their security checks.[70] Election officials also failed to publish vote decryption keys after tests in 2019 and 2020 and refused to allow outside entities to host nodes on the network.[71] Election observers were also shut out from observing the most recent 2021 elections.[72] These actions made it impossible to independently verify the integrity of the votes, nullifying the potential transparency benefits of blockchain.[73]

Advantages of Blockchain Voting

1. **Blockchain-based voting systems with a diverse pool of validators may reduce certain risks of election tampering by requiring the collusion of multiple groups to alter recorded ballots.**

Compared to centralized voting systems, blockchain may reduce some risks of election tampering by making it more difficult for any single individual or organization to tamper with votes after they have been recorded. So long as the blockchain is operated by a sufficiently diverse set of actors (for most private blockchains, this means that no single organization controls one-third or more of the nodes on the network), the records logged on the blockchain should be resilient to attempts by malicious actors to delete ballots, alter ballots, or add new and fraudulent ballots to the results pool. This can help improve the security of vote records and potentially bolster public confidence in the integrity of associated elections.

2. **A blockchain-driven move to mobile and internet voting may lead to greater turnout and reduce voter error.**

Few studies have been conducted on the turnout effects of blockchain voting systems due to the limited number of pilots that have been held to date. The most thorough examination analyzed the use of Voatz' mobile blockchain voting system during the 2018 elections in West Virginia and estimated that the platform increased voter turnout by 3 to 5 percent.[74] This aligns with findings in Canada, where non-blockchain internet voting in local elections in Ontario was estimated to have increased turnout by 3.5 percent.[75] However, studies have found that internet voting (without blockchain) had no impact on turnout for elections in Switzerland, Estonia, or Norway and a slightly negative effect in Belgium, making it difficult to draw strong conclusions.[76]

Internet voting may also help to enfranchise less-educated voters who may make mistakes on paper ballots that lead to those votes being discarded. In Brazil, for example, one study found that a large number of ballots were discarded due to errors relating to voters' lack of understanding of the instructions.[77] The introduction of electronic voting machines at polling locations, including a system that gives an error message if a voter is about to submit a ballot that is invalid, is estimated to have led to millions fewer rejected ballots.[78] If blockchain were to help catalyze a move toward systems that were also easier for citizens to understand and less likely to result in rejected ballots, this could lead to the enfranchisement of millions more around the world.

3. **A blockchain-driven move to mobile and internet voting may help reduce the risk of voter coercion in areas where voters fear harassment or where in-person voting does not provide sufficient guarantees for voter secrecy.**

In some countries, voters may face the threat of extortion or physical danger when venturing out to the polls during elections. To cite just one example, the 2020 elections in Burundi were characterized by multiple reports of opposition members being threatened and beaten on their way to the polls and instances of groups taking individuals' voter cards and voting in their place.[79] Internet voting provides an alternative method of casting a ballot in instances where security concerns may prevent citizens from physically traveling to a polling place. Blockchain-based internet voting systems may help voters avoid these risks and help ensure that election outcomes reflect the free will of voters.

4. **Blockchain may help improve election transparency if civil society groups are allowed to participate on the blockchain network.**

If civil society groups were allowed to participate as nodes on the blockchain, they would be able to directly observe how votes are collected, processed, and tallied. Even for those not included on the network, the information available through the public blockchain records could lead to greater transparency compared to other forms of internet voting. For instance, Russian journalists with Meduza were able to reconstruct a timeline of votes cast during the 2019 Moscow City Duma elections, allowing them to check for anomalies in voting patterns that could be used to identify possible instances of forced voting.[80]

Just as governments control the ability of in-person election monitors to observe voting and counting, the majority of transparency benefits from blockchain are contingent on civil society groups being allowed to participate on the network. Further, the transparency offered by participation on the network would be limited to the collection and tallying of votes. If ballot manipulation occurred before votes reached the blockchain, civil society groups would not necessarily be able to detect the tampering from their position on the network. A blockchain-based internet voting system may therefore significantly alter civil society's approach to parallel vote tabulation.

> ***Just as governments control the ability of in-person election monitors to observe voting and counting, the majority of transparency benefits from blockchain are contingent on civil society groups being allowed to participate on the network.***

5. **Compared to other internet voting schemes, blockchain voting systems may be more resilient to some forms of network disruption.**

A key benefit of blockchain technology is that its distributed nature grants a natural resilience to disruption. In contrast to centralized information systems, blockchains lack any single point of failure that can be targeted to bring the network down. If a node on a blockchain network is taken offline, the other nodes can simply route around it. This property could be valuable in the context of voting, as it may reduce the risk that election systems could fall victim to disruptions such as denial-of-service (DoS) attacks, where malicious actors flood servers with an overwhelming volume of traffic that makes it impossible to service legitimate users. Importantly, even if the only result of such an attack was to delay the receipt of votes, voters experiencing those delays may interpret any problems as evidence that a more serious hack had occurred and lose trust in the reported outcome of the election.

However, blockchain only confers these benefits if voters are able to connect directly to the blockchain network. A system that requires voters to use a web interface to connect with the blockchain is just as vulnerable as a fully centralized voting system, as its reliance on a web interface constitutes a single point of failure that can be targeted by any actors looking to disrupt the voting process.

6. **Blockchain may be useful as a way of securing voter registries, election night reporting systems, and other election processes unrelated to vote tallying.**

Election security efforts are often focused on the technologies used to collect and tally votes. However, attacks on other complementary systems such as voter registries and election reporting processes can also carry significant risks.[81] For example, changes to voter registries by malicious actors or by governments looking to disenfranchise certain segments of the population can lead to disruptions and confusion on election day if they cause voters to be unable to verify their eligibility at polling places. Alternatively, malicious additions to voter rolls could be used to support ballot-stuffing schemes.

Similarly, disruptions to election night reporting—the systems that jurisdictions use to report their unofficial vote counts to media and the public after polls have closed—can create the perception that tampering may have occurred even if no votes were manipulated. For example, some polling locations may be prevented from submitting their results due to DoS attacks or other disruptive techniques, which may lead some to interpret the delays as evidence of government manipulation. A similar effect could be achieved by hacking into the websites used by jurisdictions to publish vote tallies as they are reported on election night, leading to confusing and inconsistent reports that may cause the public to doubt the integrity of the election.[82]

Blockchain may be able to help reduce the risk of attacks on these processes. For instance, if voter registration data were stored on a blockchain operated by a diverse group of actors, it would be much more difficult for any government or malicious actor to remove or alter records. Furthermore, so long as the blockchain were made public, any manipulation would be publicly logged, allowing individuals to find out when tampering had occurred and seek remedy. In the same way, if election night reporting processes were to adopt blockchain as a way for individual jurisdictions to publicly and immutably submit their tallies, it could reduce the risk that the reporting process could be disrupted and help guard against misinformation.

Risks of Blockchain Voting

1. **Blockchain voting systems would require voters to rely on digital systems that are vulnerable to compromise by malicious actors.**

Moving to an internet-based voting system, even one that utilizes blockchain, does not eliminate the risk that electoral results can be compromised—and in many cases would make it easier to do so. Attacks on internet voting systems do not require physical access, can affect a large number of votes in a single attack, and cost little more than an attack on a single user.[83] Due to the complexity of these software systems, there is also a substantial risk that the attack would go undetected by voters, election officials, and observers. These risks are not merely theoretical. Security researchers have found vulnerabilities in internet voting systems used in Estonia, Switzerland, and Washington, D.C.[84]

Blockchain does not eliminate these risks, which is the primary reason why blockchain voting proposals have met with severe and near unanimous criticism by election security experts.[85] Introducing blockchain addresses only a relatively minor component of the online security equation. While blockchain helps to ensure the integrity of data once it has already been logged to the network, it cannot help to prevent attacks targeting other elements of election infrastructure, such as:

- Spreading malware to voters' phones that can alter or delete the ballots they submit;
- Manipulating the code used by election authorities to tally votes;
- Compromising intermediary servers or web interfaces used to submit votes, connect voters to the blockchain network, or examine information on the blockchain;
- Listening in on the voter's network to detect ballot choices; and
- Compromising voters' phones, tablets, or computer chips through supply chain attacks.

The providers of internet voting systems can take some measures to reduce these risks. The Voatz app, for example, only works on updated mobile devices that have not been jailbroken and uses antivirus software to scan devices for indications of compromise. The app also will not function on unsecured wireless networks. Notably, however, these protections would not have prevented the kinds of attacks demonstrated by Trail of Bits and MIT researchers.[86] Ultimately, any internet voting system will face a serious risk of compromise given the current state of cybersecurity, regardless of whether blockchain is used.

> ***While blockchain helps to ensure the integrity of data once it has already been logged to the network, it cannot help to prevent attacks targeting other elements of election infrastructure.***

2. **The incorporation of blockchain into electronic voting systems would increase software complexity and complicate security management, leading to greater vulnerability to attacks.**

Introducing blockchain into an electronic voting system increases the overall complexity of the software environment. This can lead to new security risks due to the potential introduction of new software vulnerabilities. Blockchain also complicates the process of fixing vulnerabilities once they are identified. In contrast to a centralized system where a single organization can quickly act to deploy security fixes, blockchain networks require the coordination of a large number of actors to respond to security problems.[87] This lack of centralized authority would also make it more difficult to hold any single entity responsible in the event that an attack or malfunction were to occur.

3. The complexity of blockchain and internet-based voting systems could reduce voter confidence in the integrity of the election process

Proponents often argue that the greater security offered by blockchain voting platforms could improve public trust in the election process. However, there are risks that the reverse may occur if voters do not trust the integrity of blockchain-based voting schemes or internet voting schemes in general. The simplicity of paper-based voting can be an advantage in terms of public confidence, as it is easy for the average voter to understand the process by which paper votes are recorded and tallied. Understanding the systems behind online voting, including blockchain, is much more difficult. One survey conducted in the United States found that 43 percent of potential voters were "not at all" or "not very" confident that votes cast online would be counted correctly, compared to just 11 percent who were similarly skeptical about the counting of a scanned paper ballot.[88]

Further, the specifics of blockchain voting systems may introduce new doubts for voters. For example, the Russian election monitor Golos reported that Russian voters were frequently confused by the country's blockchain voting system and were uncomfortable using a system that would allow them to look up their ballot after the election had finished.[89] The availability of this option made some voters believe that others would also be able to see their ballot after the election was over, reducing their trust in the system and their willingness to participate.

4. The process of authenticating voters may introduce privacy risks depending on what information is collected from voters, how it is processed, and whether it is placed on the blockchain.

In order for mobile voting to be secure, there must be a way to reliably authenticate the voter's identity before they submit their ballot. Some internet voting schemes, such as Estonia's, allow citizens to use their national ID card to digitally sign their electronic ballot. Most nations, however, lack electronic IDs. In their absence, it is likely that many schemes will instead rely on alternative authentication methods such as biometrics. Voatz is an example of a platform that utilizes this approach. As described previously, Voatz requires voters to submit a picture of their official ID and a video selfie to authenticate their identity, in addition to other non-biometric personal information such as location, address, and date of birth. Some of this information is also shared with a third-party contractor responsible for the authentication process. Depending on how this information is handled, whether it is deleted immediately after registering the user, and what visibility and control users have over the data collected about them, Voatz and other similar platforms could constitute privacy risks for their users.

Further, some blockchain voting implementations write some form of personal information about voters directly onto the blockchain. This constitutes a substantial privacy risk, as this information cannot be deleted. Even if the information is encrypted, the fact that it is immutable means that it will continue to be accessible even after technology has advanced to a point where that encryption can be defeated. Given the sensitivity of voting and the importance of preserving ballot secrecy, any blockchain implementation that would store voter information on-chain would constitute a severe and unjustifiable privacy risk.

Voting Rights Issues Blockchain Does Not Solve

1. **Blockchain would not make it easier to implement end-to-end voter verifiability.**

As addressed in the opening of this chapter, end-to-end verifiability is a highly attractive property for an internet voting system, allowing voters to verify whether their vote was counted correctly without needing to trust the election infrastructure involved or the administrators overseeing the process. Blockchain has been proposed as a way of operationalizing end-to-end verifiability by serving as the public bulletin board that voters can reference when checking their vote. Notably, however, blockchain does not add any additional security to this process compared to a bulletin board hosted centrally by an election authority.[90]

While it may seem that blockchain would offer a more secure format for this bulletin board due to its tamper resistance, in reality it makes no difference. End-to-end voting schemes would be able to identify tampering either way. Indeed, this is exactly why end-to-end voting is so attractive to security researchers in the first place. A government that deletes or changes a voter's publicly posted ballot would be exposed as soon as the voter pulls up the system to check. So long as this is true, there is no need for complicated systems that make it more difficult to tamper with ballots. Security is assured not by making it impossible to alter the vote count but by making it impossible for votes to be altered without being discovered. Further, the encryption necessary to ensure that these public ballots are only accessible to their owner can be implemented just as easily using traditional technologies. Therefore, while blockchain may be used as a way to operationalize an end-to-end voting scheme, it is not strictly necessary for these benefits to be gained and may serve to complicate potential deployments by adding unnecessary complexity.

2. **Blockchain would not protect voters from attacks that cut off their connectivity.**

While blockchain may reduce some risks of election disruption, it does not protect against attacks that target the connectivity of the voters themselves. During the Venezuelan referendum supported by Voatz, for example, the Maduro-controlled state internet service provider CANTV blocked internet service for a large portion of the population during the voting period, preventing them from accessing the service.[91] While some forms of disruption may be addressed through the use of virtual private networks (VPNs) or alternate platforms such as Telegram, so long as voters must rely on third-party infrastructure to access voting systems, there will always be the potential for outside disruption of the voting process. Blockchain cannot address these risks.

3. **Remote voters may still be vulnerable to certain forms of coercion due to their relative lack of vote secrecy.**

While remote voting may reduce some risks of voter coercion, it may also create new and unique risks for those who lack privacy when filling out their remote ballots. For example, voters may be forced to fill out their ballots in the presence of their employers, spouses, or supporters of certain political groups, who may threaten retaliation for not submitting votes for particular candidates. Remote voting also carries the risk of vote-selling schemes, where voters obtain compensation for voting in a certain way. Blockchain does not eliminate these risks for electronic voting schemes.

Some voting systems may combat these risks by supporting vote spoiling, where voters are able to submit multiple ballots up until the close of an election, with each overriding the last. This can help reduce some of the risks of coercion and vote selling by allowing voters to go back and change any votes that may have been submitted under pressure. However, vote spoiling is still not a perfect solution. For example, in households that only have a single shared device controlled by the head of that household, other members of the family may not have the opportunity to later go back and resubmit their votes.

Further, there is a risk that voters' anonymity can be violated or that voters can be intimidated or induced into sharing their ballot receipts with third parties, allowing those third parties to access the voters' ballot and determine who they voted for. The ballot receipts generated in end-to-end systems are intended to allow individuals to check after the election is over to determine whether their vote was recorded properly. However, a third party may gain access to those receipts, creating new risks of voter intimidation, vote selling, or the elimination of voter anonymity.

Conclusion

The attraction of internet and mobile voting is clear. Beyond the obvious benefits to convenience and efficiency, the accessibility of a simple, reliable method of remote voting may help improve voter turnout, enfranchise low-income voters, reduce the impact of voter intimidation, and standardize election processes. Blockchain advocates argue that decentralized election systems powered by blockchain networks could help bring this dream closer to reality by addressing many of the security concerns that have long plagued internet voting schemes, providing a new mechanism for improving the transparency of elections, and warding against tampering by election officials.

However, even with the addition of blockchain, internet voting is highly vulnerable to large-scale, undetectable manipulation and in many cases would be even more vulnerable to manipulation than in-person voting.[92]

Secure internet-based elections are not possible without end-to-end verifiable voting, where voters are able to verify whether their ballots were received and tallied correctly without having to trust the software or election administrators involved in the process. While blockchain is one way of operationalizing end-to-end verifiable internet voting, election security experts have repeatedly emphasized—both in the published literature as well as in interviews conducted for this report—that blockchain is not only unnecessary for realizing this goal but is in many ways actually inferior to traditional information systems in this regard due to its added complexity.

Realizing many of the benefits of blockchain voting would also depend on election administrators opening their systems to a radical level of transparency by observers, something the authors feel is highly unlikely to occur in practice in areas where election integrity is most under threat. This study's conclusion is therefore that blockchain-enabled voting, like other internet-based voting systems, would currently pose severe risks to election integrity that would outweigh its potential benefits and should not be considered for political elections until strong assurances are in place that these systems can be implemented in a secure and responsible way.

Notably, however, blockchain may still be able to play an important role in improving election security by helping to secure complementary election processes such as voter registration and election night reporting. These stages of the voting process receive less attention than the collection and tallying of votes, yet their failure can do almost as much damage to public confidence in the integrity of election results. Further work exploring the role of cryptography and blockchain to secure these processes could potentially have an important impact on improving election security around the world.

5

Digital Identity

Bottom Line: Blockchain could help enable SSI, a system of identity management that could give individuals greater control over their personal data and help individuals without official documentation build a record of identity. However, SSI will not lead to better data governance practices without strong legal and regulatory pressure and could lead to significant privacy risks if deployed inappropriately. For this reason, deployments involving vulnerable populations or in places that lack strong legal protections should not be pursued until strong governance frameworks can be developed.

Human Rights Context

Digital identity solutions aim to increase access to and improve the fidelity of identification credentials, which are almost universally required to access basic public goods and government services. The World Bank reports that over 1 billion people face challenges in acquiring official identification.[93] Of this billion, 80 percent live in sub-Saharan Africa and South Asia and 90 percent live in low- and lower-middle-income countries. Obstacles to obtaining legal identity are particularly high for many of the over 26 million refugees in the world today, especially those who may have lost their original identity documentation as a result of conflict or natural disasters.

Individuals excluded from official identity systems face enormous barriers to participating fully in economic and social systems. For example, individuals without IDs may find it impossible to open a bank account. Without a bank account, they may find it difficult to be approved to rent an apartment. And without a lease to demonstrate proof of residency, they may find it difficult to find a job. In this way, the lack of foundational identity can create a cascading series of challenges, restricting rights and preventing individuals from accessing essential benefits and services.

Obstacles to obtaining legal identity are particularly high for many of the over 26 million refugees in the world today, especially those who may have lost their original identity documentation as a result of conflict or natural disasters.

Credentialed identity acts as the basis for numerous rights. Blockchain technology as a platform for digital identity can impact several rights, particularly in the context of the rights of refugees and migrants:

- **Right to Privacy:** Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Convention on Civil and Political Rights (ICCPR) provide for the right to privacy. The protection of personal data is fundamental to privacy. Migrants and refugees face challenges in securing their privacy when working with state border authorities and international organizations that cooperate with governments. Such authorities seek information, including biometrics, social media content, and other data points, from migrants and refugees in order to determine eligibility for admission and to track their activities upon arrival. Such collection may be done without consent or used outside of the accepted scope. Digital ID systems, which also utilize personal data, may likewise be abused to violate migrants and refugees' privacy rights.
- **Right to Asylum:** UDHR Article 14, along with the Convention Relating to the Status of Refugees, provides for the right to asylum as well as the prohibition on forcible return to a country where one's life or freedom would be threatened.[94] Underlying drivers of asylum claims—forced displacement, persecution, and armed conflict—frequently render migrants and refugees bereft of credentialed documentation. The absence of global consensus on how to establish identity in undocumented asylum seekers undermines the verification of asylum seekers' claims for protection.
- **Right to Equality:** UDHR Article 2 and ICCPR Article 2 provide for the right to equal rights, or non-discrimination. ICCPR Article 26 stipulates equality before the law and equal protection by the law without discrimination. Migrants and refugees are frequently, and on the basis on uncredentialed status, denied equal protection under state law. For example, Greek border authorities are reported to illegally obstruct migrants from accessing legal services needed to claim asylum absent identification.[95] In the United States, border patrol agents are reported to refuse or fail to return physical identification documents, without which asylum seekers cannot access digital bank transfers or prove custody of their children.[96]

The lack of foundational identity can create a cascading series of challenges, restricting rights and preventing individuals from accessing essential benefits and services.

Blockchain for Digital Identity

The core problem of identity management is how to allow someone to prove a claim about themselves to a party that does not trust them. This could be anything from a job applicant wanting to prove to a prospective employer that they graduated from a certain university to a shopper wanting to prove to a store clerk that they are over a certain age. This problem can be resolved if the first party is able to show that a mutually trusted third party has attested to their claim. In the case of the job applicant, that might mean presenting the diploma given to them by their university. In the case of the shopper, it may mean presenting a government-issued ID card that shows the customer's date of birth. In these examples, both the diploma and ID card are a form of credential that allows their owner to prove that a trusted third party has confirmed certain attributes about them.

The value of a credential is determined by how much each party trusts the authority that issued the credential and how much they trust the credential itself. The information contained on a government-issued ID card, for example, is presumably far more trustworthy than the information found on a person's social media account. That is both because an ID card is more difficult to falsify and because it is issued by a more reliable and authoritative party.

Credentials are tied to individuals through the use of identity systems. A government-issued ID card, for instance, may be associated with the identity established for a person through a civil registry. This type of ID system—often referred to as a *foundational* ID system—provides a legal proof of identity that allows the individual in question to access a wide range of public and private services.[97] A social media account, in contrast, is a form of *functional* ID that serves to authenticate a user for a specific and narrow use case. In both of these cases, identity is provided in a centralized way, with a single authority generating and distributing identifiers to their citizens or users.

As noted above, approximately 1 billion people currently lack access to foundational legal identities, often preventing them from exercising their rights and cutting them off from a range of essential services. These obstacles to obtaining legal identity are particularly high for the over 26 million refugees and stateless persons in the world today who may face significant political barriers to recognition and have often lost their original identity documentation as a result of conflict or natural disasters.

Proponents of decentralized digital identity believe that the technology may offer the potential to eliminate many of these obstacles by serving as the technical infrastructure for a new kind of identity system termed SSI. The SSI identity model could leverage blockchain as the backbone for a fully decentralized identity system where identifiers and credentials are held and controlled by users rather than by central authorities.[98] In contrast to traditional identifiers such as national ID numbers that are distributed by a single government entity, decentralized identifiers (DIDs) could uniquely represent any person, organization, or object without needing to rely on any centralized registry, government authority, or private ID provider.

DIDs are generated and assigned when a user begins using an SSI digital identity wallet. DIDs can be thought of as a kind of URL that is uniquely associated with a single entity and which points to a digital document that contains instructions about how that DID can be used and how the owner can prove that the DID belongs to them.[99] The most common method of proving ownership over DIDs is public key cryptography, where a user generates a pair of cryptographic keys (essentially large numbers that serve as complex passwords) during the sign-up process. The keys are paired so that any information digitally signed by one can be verified by the other. One of these keys is referred to as the public key and is published on the blockchain as part of the DID document (or shared privately peer to peer). The second key, referred to as the private key, is stored in a wallet application that only the user has access to.

Any time an individual wants to prove that they are the person who corresponds to a DID, they can present an assertion digitally signed with a key that is derived from their private key. The verifying party can then authenticate the user by going to the public blockchain, finding the public key associated with the claimed DID, and performing a check using a cryptographic algorithm to see whether the two keys correspond. The fact that a derived key is used instead of the master private key allows a user to create a new key for each interaction they have, preserving their pseudonymity and preventing their activity from being correlated and traced back to them. DIDs can be linked to a user's wallet application to allow them to automatically authenticate themselves when online and can be represented in the real world by QR codes that can be scanned to confirm a person's identity.

Once an individual has a digital identity wallet, other organizations can digitally issue them credentials such as diplomas, driver's licenses, or work permits. These credentials can be stored by the user in the user's digital identity wallet on the device of their choice or in the cloud. Each credential is digitally signed by the issuing organization's own private key. The fact that they are signed by the issuer means that any party at any time can check the legitimacy of that credential by looking up the issuer's public key. This allows parties to quickly and easily determine whether a given credential is trustworthy.

DIDs can also hold references to data stores located off the blockchain that may hold information pertaining to the DID owner. For example, a DID could contain a pointer to encrypted health records that are stored at a separate location on the cloud. Entities wishing to access this information could request permission from the DID owner, who may then choose whether or not to grant access.[100]

Importantly, at no point would it be necessary for a person to store personal data directly on the blockchain. Identifying information would only be stored by the user in their wallet application or off-chain by third parties according to the nature of that relationship. Blockchain's role in SSI systems is not to store identity data itself but rather to act as a trusted public reference for DIDs and their associated public keys. The decentralized, immutable nature of blockchain is utilized here as a way of establishing a common source of truth that lets any party verify who a given DID belongs to and evaluate the authenticity of digital credentials.

Case Study: iRespond

iRespond is an international nonprofit focused on developing a biometric digital identity solution for healthcare providers, humanitarian groups, and government agencies. iRespond's platform uses biometrics (primarily iris scans, though fingerprint and facial recognition may also be considered in some circumstances) to establish a unique, 12-digit digital ID for each user. These IDs are stored on a cloud server and linked to the encrypted hash of the user's biometric template, allowing them to securely access any associated identity information while minimizing the collection of personal information.

iRespond's platform has already been deployed in seven countries across Southeast Asia and Africa.[101] Most notably, iRespond carried out a pilot with the International Rescue Committee in the Mae La refugee camp in Thailand, which houses around 40,000 refugees from Myanmar.[102] The purpose of this pilot was to improve the administration of health services to refugees. Instead of relying on paper IDs, iRespond's solution allowed refugees to authenticate themselves at health clinics in the camp by consenting to an iris scan. Once the systems are fully integrated, the scan would unlock the patient's electronic health records, giving the service provider an extremely high degree of certainty that the health records belong to that patient. The participation of other providers outside the camp could allow individuals to leave the refugee camp without having to worry about losing access to their health records.

One type of record that iRespond has looked to supply through this program are birth attestations. To help create a record of birth for babies born in the camp, iRespond piloted a project that would provide both paper and digital birth attestation credentials to the families of newborns.[103] These credentials—which are recorded on a blockchain—include the identifier of both the mother and the child, allowing them to prove to outside parties that they have a connection to that credential.[104] Further, this digital credential could be used to recover a physical copy of the birth attestation should it ever be lost.

At no point does iRespond collect or store any personally identifiable information or health data. The iris scans taken from users are deleted once they have successfully enrolled or authenticated themselves. Non-biometric personal information is never collected, as the unique ID renders this unnecessary. The pseudonymous ID is all that participating organizations need to track and record information about individuals. Perhaps the most important benefit of this arrangement is that iRespond cannot be pressured by governments to turn over information about the populations they serve.

The ultimate goal of iRespond is for their solution to be used not just for electronic health records but also as a way for refugees to accumulate other forms of credentials such as immunization records, professional training certifications, and education credentials.[105] For those with a smartphone, these credentials could be stored directly in their wallet application. For those without smartphones, a physical document with a QR code could be used as an analog backup, with the digital credentials being kept on a web-based wallet until the individual gets access to a mobile phone.[106] In either case, the issuer would store a copy of the credential in case the individual lost access to their wallet.

Advantages of Blockchain for Digital Identity

1. **Blockchain identity systems may help individuals who lack official documentation build a portable record of identity from unofficial sources.**

Lack of official, legal identity can prevent individuals from accessing a variety of public and private services by making it difficult for an individual to show that a trusted institution has attested to their identity and attributes. Without a government, bank, or other similarly authoritative entity to attest to the truth of a claim, many organizations simply choose not to trust the individuals involved, as the risk is deemed too high. SSI may offer the potential to change this by making it easier for individuals to accumulate trusted informal credentials that can be used to support identity claims.

One example of how SSI platforms could allow individuals to take advantage of informal credentials is the case of Kiva. Kiva is an identity provider that is working with the government of Sierra Leone to deploy a blockchain-based identity platform that would allow individuals to build a credit record based on their history of interactions with microfinance institutions and other informal sources of credit.[107] Kiva seeks to allow microlenders, banks, and other financial institutions to participate as nodes on a blockchain network and assigns credentials to an individual's wallet attesting to their loans and payments. Outside institutions could then access the person's credit record by requesting permission to view their profile. By leveraging the untapped value of functional identity relationships, this solution could help drive financial inclusion in a country where only 20 percent of the population is banked and less than 1 percent is covered by a credit bureau.[108]

SSI would also help ensure that the credentials accumulated by an individual in one location are portable to new settings. The residents of refugee camps, for example, may collect a long list of health records, financial records, professional certificates, and educational credentials as part of their interactions with aid providers and humanitarian organizations in that camp. All of this identifying information would be lost, however, as soon as they left the camp. With SSI platforms whose governance frameworks assure continuous access by the individuals and organizations using them, refugees could continue to reference this information even after they leave, making it easier for them to integrate themselves and their families into the economy.[109]

2. **Blockchain identity systems may help protect individuals' privacy by reducing the consolidation of personal information by data controllers and improving individuals' ability to control how their data is shared.**

The consolidation of personal information by centralized identity providers creates privacy risks for users in several ways. First, it creates an attractive target for hackers who may seek to steal identity information and then exploit it as part of identity fraud or other criminal schemes.[110] Second, the depth and variety of data available to the identity provider could allow that provider to extrapolate sensitive information about a person's life in ways that the data subject may never expect. This information may be used, sold, and shared in ways that are largely opaque to the user. This risk is particularly acute for vulnerable populations in humanitarian settings that may feel pressured to provide personal information in order to obtain needed benefits and services. Such populations may also face challenges in learning how that information is used and shared with other parties.[111]

Blockchain could reduce many of these risks by allowing information to be stored in a decentralized fashion while still allowing users to maintain control over how their information is disclosed and used. Without SSI, the only way to unify the disparate identities and credentials associated with a user is to bring them all under the control of a single identity provider. With SSI, however, credentials can be controlled by the users themselves, preventing the consolidation of personal data by third parties and granting individuals the opportunity to exert granular control over what information is disclosed when they authenticate themselves to an outside party.[112]

Additionally, these systems could also allow users to assert control over their data throughout the full lifetime of their relationship with an organization. This is possible because all of an individual's credentials and data would be stored either on their device or as an encrypted file in a web-based wallet maintained by a third party. Thus, an organization would have to ask a user's permission each time they wished to access their information or ask for consent for ongoing access. Users could then decide whether and under what conditions to grant access. The result would be a general improvement in users' ability to understand how and when their data was being accessed by other parties and to restrict access for processing they feel uncomfortable with.

An additional privacy benefit of SSI is that it could enable individuals to use a cryptographic technique called a zero-knowledge proof (ZKP) to prove claims about themselves without ever having to reveal the information supporting their claim. For example, consider a bar that requires its patrons to present an ID card with their date of birth to confirm that they are over the age of 21. Technically, the bar only needs to know that the person was born more than 21 years ago. It does not need to know the precise date of birth for that person. However, there is no traditional method that allows a person to confirm that they are of legal drinking age without turning over their full ID, which contains not only their complete date of birth but also unrelated personal data such as their name and address. With ZKPs, however, it would be possible to simply 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 21. At no point would the person have to reveal any other information to the bar, helping to preserve their privacy.

The benefits of ZKPs extend beyond protecting birthdays. They can also be used to prove that a person qualifies for a loan without disclosing their credit rating or income or that they are authorized to work in a country without disclosing their citizenship status. If SSI and its associated credentials were to become more common, an increasing portion of identity checks could shift to this model, yielding broad improvements to data privacy and empowering individuals to minimize the amount of information collected about them by outside parties.

3. **Blockchain identity systems may help protect against the loss of identity documentation as a result of natural disasters or conflict.**

One of the primary drawbacks of physical ID documents is the potential for them to be lost or destroyed. This can have a devastating impact on households, especially those dealing with natural disasters or conflict, because in addition to dealing with the direct impacts of a humanitarian crisis, these individuals may also suddenly become unable to access the benefits and services most important to helping them recover.

Digital identity systems allow individuals to store their identifiers and credentials in digital form. This would allow an individual to continue to be able to access their identity information even if they lost their original paper records. And while even digital credentials may be lost if an individual loses their phone or their wallet password, the key recovery mechanisms and encrypted cloud backup offered by SSI platforms and the digital credential copies kept by issuers would make it simple for an individual to quickly restore their identity access in the event that something did go wrong.

SSI would also help ensure that credentials can still be verified even if the original issuer no longer exists. For example, if an individual received a degree from a university that was later destroyed during a conflict, they may eventually run into difficulties trying to prove to an employer that their degree is authentic. However, with SSI, the history of the DIDs and public keys for that institution would be immutably logged on the blockchain. This would allow the recipient of a digital diploma, or any other kind of credential, to verify its authenticity no matter the current state of the issuing institution. So long as the issuer has not revoked the individual's credentials, it will always be publicly verifiable.

4. **Blockchain digital identity systems may help to improve the administration of humanitarian aid to vulnerable populations.**

In the wake of conflict, disaster, or other humanitarian crises, victims are often forced to rely on a large and complex network of aid groups for access to essential services. Each one of these organizations currently maintains separate records and credentials for the individuals who participate in their programs. The result is that each aid recipient may quickly become responsible for managing a cumbersome array of credentials, leading to confusion and frustration.[113] This situation also leads to inefficiencies in the delivery of aid, as each organization is wasting resources to separately collect the same information from each individual. Redundant data collection can also lead to privacy risks, as individuals may end up disclosing their personal information to many different organizations without clearly understanding how their data will be used or shared.

SSI could improve this situation by granting aid recipients with a secure digital identity wallet that could be used to coordinate access to humanitarian benefits and services. Beyond the convenience and privacy benefits afforded to beneficiaries, the use of trusted digital identities could also help humanitarian organizations by ensuring that individuals can be properly targeted with aid and support, reducing the risk of double registration and fraud, reducing the administrative burden of registering individuals and maintaining their identity information, and preventing delays in aid disbursement.[114] These benefits may be particularly beneficial in the context of direct cash assistance, where trusted identities may allow humanitarian organizations to avoid high administrative and transaction costs and coordinate payments with other actors running similar programs.[115]

Risks of Blockchain for Digital Identity

1. **A move to digital identities catalyzed by blockchain-based identity management could lead to some services becoming inaccessible to those without digital IDs.**

The aggressive embrace of digital identity systems in a country could lead to risks that certain groups may be excluded from essential services if technical, bureaucratic, or other kinds of barriers render them unable to participate in the new identity system.[116] This risk has been demonstrated most recently in the case of India's Aadhaar system, which was launched to provide a biometrically linked ID number to every individual in the country. Research from 2019, however, indicated that 30 percent of India's homeless population and more than a quarter of its third-gender citizens were not represented, putting them at risk of being excluded from public and private services that were evolving to rely on Aadhaar numbers.[117] Even for those who were registered, one study found that 20 percent of the households in one state had failed to receive their food rations due to errors in biometric authentication, pointing to the need to ensure that digital IDs allow for backup ways of authenticating citizens.[118] The use of biometric modalities such as facial recognition may also create discriminatory impacts if the underlying algorithms exhibit differences in their accuracy rates for members of different races.[119]

While in theory blockchain-based SSI systems should be more accessible than traditional, centralized digital identity programs such as Aadhaar, there are still substantial risks that a lack of access to technical infrastructure and connectivity may result in some individuals facing barriers to participation in SSI platforms. For this reason, ID2020, a public-private consortium focused on advancing access to digital IDs, has released a set of technical recommendations clarifying that digital identity providers should make registration and authentication available offline (such as through printed credentials with scannable QR codes), support manual override in case identity cannot be proven, and establish failure modes for when individuals cannot follow the normal procedure for identification.[120]

2. **Blockchain may create additional privacy risks if personal information is stored directly on the blockchain.**

Because data stored on blockchains is immutable, any data stored on the blockchain subsequently takes on a permanent risk of disclosure. While encryption helps to reduce this risk over the short term, there is no guarantee that information will not eventually be revealed if the encryption keys are stolen or if technologies such as quantum computing will allow that encryption to eventually be defeated. This creates an imperative for all designers of blockchain systems to ensure that personal information is never stored on the blockchain itself. Instead, any potentially sensitive data should be stored directly on a user's device or separately in the cloud, hosted by a third party but still under the user's control. Adherence to this recommendation is especially important given that many emerging data protection legal regimes require that data controllers be able to delete personal information either at regular intervals or upon the request of a data subject, something blockchain would not allow.

The risks of publicly logging identifying information are particularly severe in the case of refugees and persecuted individuals, whose status may be used as a way of deliberately discriminating against them or targeting them with violence. Digital identity experts were concerned, for example, at the news that the United Nations would be collecting biometric data from Rohingya refugees as part of a digital ID scheme and sharing that information with the Bangladesh government.[121] Such information carries a significant risk of abuse, as it could be repurposed to organize a campaign to send Rohingya refugees back to Myanmar, or even be used as a tool for persecution or ethnic cleansing.

These risks are generally well appreciated in the SSI space, and most blockchain identity projects reviewed as part of this report asserted that a prohibition against storing personal information on-chain was a core principle of their platform. However, there have been exceptions that demonstrate the risks when this guideline is not followed. For example, Finland started a project in 2015 to provide refugees with debit cards linked to blockchain-based digital IDs. The purpose of this project was to allow the refugees to participate in day-to-day tasks more easily until they were able to receive their official identity documents. However, researchers found that the software involved recorded the details of financial transactions made with the cards onto the blockchain itself, posing large and obvious privacy risks.[122]

3. **SSI systems may require users to rely on NGOs or private identity providers as custodians of IDs and credentials for individuals who cannot manage their own identity information. This reliance could create risks if systems are not designed carefully.**

One of the most challenging questions in SSI is how to organize custodianship models for individuals who for various reasons cannot manage their identity information themselves.[123] This may be because the person in question is a child, because they are elderly and may lack the requisite digital literacy, because they are medically incapacitated, or because they do not have access to a digital device capable of storing credentials. In these cases, control over a person's identity information and credentials must be held either by a family member or by an NGO or commercial service provider that can act as a trusted intermediary.

These custodianship frameworks may introduce significant risks depending on what information is held by the custodians and how that data is managed. For example, some custodians may collect biometric information from individuals to use as a way of authenticating them when they request access to their identity documents. While other forms of authentication such as passwords or security tokens are possible, biometrics are often preferred due to the greater assurance they provide that an individual is truly who they say they are. The collection of this biometric data presents serious privacy risks, however, if the information were to fall into the hands of malicious actors or government officials. The capture of Afghan biometric databases by the Taliban demonstrates the extreme risks that could occur if biometric databases linked to vulnerable populations fall into the wrong hands.[124]

In addition, the collection of sensitive identity information—including but not limited to biometric data—could violate individuals' privacy unless they are granted the opportunity for informed consent. For many vulnerable populations, this is difficult to achieve due to the limited information individuals may have about how their data will be used, a perception that they cannot refuse data collection without jeopardizing their access to essential services, and constraints on the ability of humanitarian agencies to help individuals understand the operation of digital identity systems during crises that involve serving high volumes of aid seekers. In fact, several humanitarian experts interviewed for this project expressed skepticism that informed consent was even possible in the case of digital identity systems.

Custodianship systems must also be carefully architected to ensure that intermediaries cannot abuse their access to identity information and that identity information can be transferred back to the user or to a new intermediary as individuals move locations or change their living situations. In some countries, relevant legislation may need to be updated in order to allow custodians to manage identity information on the ward's behalf. Similarly, enabling users to recover their credentials if they lose access to their devices or wallet passwords will require organizations to maintain local copies of individuals' information. Key recovery is a common feature of online platforms and is not difficult to implement, but thought must be put into how the organization will securely maintain their data backups, including whether individuals may be required to authenticate themselves through biometrics in order to complete the key recovery process.

Reliance on custodians may also present risks if those custodians disappear. Individuals may have to rely on custodians to maintain their credentials for years or even decades. If that custodian is an NGO that loses funding or a company that goes bankrupt, individuals could lose their identity information unless some other organization was able to take over the management of the affected wallets. This also emphasizes the importance of ensuring that the organizations involved in the space adopt open APIs and common standards that would support data portability.

Digital Identity Issues Blockchain Does Not Solve

1. **Many kinds of credentials are unlikely to be replaced by informal alternatives, meaning government authorities would still have to be relied upon to provide legal, foundational IDs for many benefits and services.**

As described at the beginning of this chapter, the value of a given credential is determined both by the trust a party has in the integrity of the credential itself and their trust in the authority of the issuer. Blockchain-based SSI systems can help resolve the former question by allowing any party to verify the authenticity of a credential by using the public keys stored on the blockchain. However, even if the credential itself is trusted, it matters little if the issuer is not seen as an authoritative source for the claim being made.

For example, a government agency is unlikely to ever trust any party other than itself to verify that an individual is entitled to citizenship or to social benefits such as a public pension or welfare. Similarly, private entities will likely continue to rely exclusively on official forms of identity in situations where there may be legal ramifications for misjudging the truth of a claim, such as whether a certain worker is legally authorized to work in the country. This means that even if SSI were broadly available, absent significant political and legal reform, populations will continue to have to rely on government agencies and other formal organizations for many of the most practically important aspects of their identity. Thus, while the ability to present trusted functional IDs may help open some doors to those without legal documentation, many of the credentials that are most important for accessing essential services will likely continue to be gatekept by traditional authorities.

However, SSI may still be able to play some role in helping individuals access foundational IDs and official credentials. Individuals with access to a store of verifiable credentials and attestations may be able to leverage these when applying for official IDs, making the process simpler and easier. SSI could also help reduce costs and improve the speed of issuing official credentials by allowing agencies to simply issue credentials to a wallet rather than delivering physical documentation. Importantly, both of these benefits rely on officials being willing to participate in the SSI network, which cannot be assumed. Similarly, attempts to integrate SSI into humanitarian aid programming may end up being futile unless prominent authorities such as the UN High Commissioner for Refugees can be brought onboard.[125]

2. **The availability of SSI would not necessarily prevent government agencies or other actors from continuing to require individuals to turn over data in ways that could create privacy risks.**

In theory, SSI should make many common, risky data collection practices unnecessary. Instead of having to turn over large amounts of private information to each organization an individual wants to authenticate themselves to, an SSI model of identity management would allow a person to use a single set of credentials in a digital identity wallet that only they controlled to selectively disclose only the minimum amount of information necessary for verification. This only works, however, if institutions agree to be limited to collecting the minimum necessary amount of information about a person.

Many governments, private organizations, and even civil society groups find value in overbroad data collection and deliberately collect data they have no immediate need for out of the knowledge that they may one day be able to repurpose it. This is particularly true for the most sensitive data types, such as biometrics. Self-sovereign identity can be achieved without ever requiring the collection of biometric data. Biometrics are simply one method of authenticating that a user is tied to a certain wallet. While biometrics have particular value due to being highly unique and difficult to forge, alternative mechanisms like passwords, pin codes, physical tokens, and SMS- or app-based codes can also serve this purpose if the collection of biometrics is deemed too risky. However, absent regulations mandating minimization in data collection, many organizations will likely resist options to voluntarily limit the data they collect from the individuals they interact with. This will be most true of governments, who may view the overbroad collection of data “just in case” as being a positive obligation due to their role in protecting the population and designing new social programs.

Because of this, even if SSI were to be adopted, many government agencies may still require that individuals turn over large amounts of private information when signing up or force them to register for and use the agency’s own biometric service instead of the SSI platform when authenticating themselves. Vulnerable populations such as refugees and stateless persons would be particularly vulnerable to these practices due to their relative lack of legal protection and their reduced capacity to learn how their data is being used and act against abusive practices. Governments may also require domestic storage of identity data due to localization laws, complicating the deployment of truly decentralized systems.

The simple availability of SSI will not lead to better data governance practices on its own. Legal reforms of both government administrative practices and private data governance rules are the only way to change the incentives for institutions so that they begin adopting data minimization by default. SSI can help this process by ensuring that trusted identities can still be verified and shared even in the context of these minimization restrictions, but it cannot change these incentives without other forms of external pressure.

3. **Users of SSI may face technical barriers, including a lack of access to smartphones, poor digital literacy, and irregular internet connectivity.**

In order to store and use credentials as part of an SSI system today, in most cases users must first have access to a smartphone capable of downloading the necessary wallet application. However, in many developing nations and humanitarian aid settings, smartphone penetration is very low. In these cases, individuals would have to rely on physical copies, web-based wallets maintained by custodians, or devices managed by a single family member to store their credentials, eliminating many of the benefits of having a digital identity solution at all. In addition to smartphones, SSI systems assume that parties will have reliable access to the internet in order to locate DIDs on the blockchain and verify a user's credentials. This is also often a poor assumption in many of the settings where SSI's benefits would otherwise be the greatest. Some functions of SSI can still be performed offline if certain details are cached locally, but a persistent lack of connectivity would greatly diminish the value of these identity systems. These challenges of device and internet access have already led to some aid groups such as Netherlands Red Cross to abandon SSI pilots due to the challenges involved.[126]

The availability of SSI will not lead to better data governance practices on its own. Legal reforms of both government administrative practices and private data governance rules are the only way to change the incentives for institutions so that they begin adopting data minimization by default.

Even if smartphones and internet connectivity could be assumed—or web wallet technologies and safeguards were significantly advanced—it would take significant work by aid agencies, governments, and other parties to improve digital literacy and ensure that users are comfortable with how SSI operates. This may have to include the use of guides to help enroll and train individuals when they sign up or telephone and mobile-messaging helplines for registration and support. The degree of digital literacy shown by these populations will also be a key determinant of whether these individuals are able to take full advantage of SSI's potential benefits and learn how to exert granular control over what information they disclose to outside parties.

Conclusion

Digital identity systems offer the potential to help those without official documentation gain access to the paperwork they need to exercise their rights and access essential public and private services. The potential value of digital identity systems is broadly recognized, but a number of important questions remain regarding how identity data should be managed, how individuals should be required to authenticate themselves, and how the improved legibility of populations may impact their relationship to systems of authority. Traditional, centralized systems of identity management provide significant risks due to the volume and sensitivity of information that data controllers can accumulate about individuals. SSI presents an alternate vision of digital identity which emphasizes the importance of empowering individuals to control their own identity information. However, challenges remain in realizing this vision.

While SSI expands the potential value of functional identities and informal credentials, it is not clear that this will be enough to make up for the lack of foundational IDs when accessing many of the most important benefits and services currently inaccessible to those lacking formal documentation. SSI's current requirement that users possess smartphones and enjoy consistent internet connectivity also limits its potential benefits in humanitarian settings. And while fully realized SSI may offer a number of improvements to privacy and individual data ownership, in practice individuals may still face risks if personal information is stored inappropriately on blockchain networks, if organizations continue to collect personal information despite the availability of more private SSI solutions, or if individuals are forced to rely on third parties to manage certain aspects of their identity.

Blockchain-based SSI systems may help improve access to identity documentation and address the privacy risks of centralized digital identity systems, but only if individuals are granted true control over their information and have the tools to access it. Absent significant improvements in technology access, digital literacy, and legal protections, this will be unlikely in many settings. Responsible deployments would require careful attention to the significant risks involved and would require that both the technical architecture and especially the system's governance process be carefully constructed to resist abuse and prioritize the needs and interests of the users. For this reason, while work toward building SSI systems may be worthwhile, plans to apply this technology in places without adequate legal and regulatory infrastructure, or for vulnerable populations in humanitarian settings, should be approached with extreme skepticism.

6

Land Rights Management

Bottom Line: Blockchain technologies could help reduce some risks of mismanagement and corruption in land administration and may reduce the costs associated with participating in formal land management systems. However, blockchain does not help ensure that the details of land records are properly recorded and risks legitimizing unfair land distributions. Therefore, blockchain systems should continue to be explored in this area but should not distract from the more important initial steps of building high-quality, digitized records of property ownership.

Human Rights Context

Article 17 of the Universal Declaration of Human Rights provides for the right to own property. Land ownership is often a source of livelihood.[127] Nearly 800 million people around the world, mainly in rural areas, rely on subsistence agriculture to survive.[128] In cities, population growth and climate change are contributing to more informal housing and higher rates of forced eviction, threatening both property rights and livelihoods. Organizations working to improve global respect for land rights seek to tackle at least three fundamental challenges:

- **Inequitable or Discriminatory Allocation of Land Rights:** Discrimination against women and other disadvantaged groups in allocating land ownership remains too common. As of 2019, women in half of all countries globally are legally barred from claiming land or property rights equivalent to those which men enjoy.[129] Worldwide, women comprise less than 20 percent of landowners.[130] Minorities and other vulnerable groups—such as Romas in Europe, Dalits in Nepal, Samis in Sweden, and Nubians in Kenya—have also faced deprivation of formal land rights on the basis of discrimination.[131]

- **Assertion of Private Ownership Rights Over Collective Ancestral Ownership Rights:** Land ownership systems are often designed to recognize individual ownership but not collective ownership, despite historical practice in some regions. More than 50 percent of the world's land is community land. Globally, however, national laws recognize only 10 percent of land as belonging to communities, with another 8 percent designated by governments for community use.[132] In Africa, 78 percent of land is estimated to be community land, yet only 26 percent of this community land is legally recognized as such.[133]

  Legal recognition of communal land rights, in both Africa and other regions, is treated separately from formalization procedures that register and title land to specific communities. Although governments reliably provide private sector entities with procedures to establish land ownership, they rarely prioritize the creation of accessible mechanisms for community land formalization. The World Resources Institute reports that ancestral landowners are required to engage in three more government interactions on average—16 compared to 13—to establish land ownership in places where such recognition is an option.[134]

- **Difficulty in Formalizing Official Land Ownership:** Many centralized land management systems are based on vague or outdated property laws that render systems susceptible to intentional manipulation or poor management practices. Such systems make it more difficult for individuals to benefit from their land ownership. Estimates show that one in every five people worldwide has paid a bribe to access land services such as formalization of ownership or title transfers.[135] Lengthy title transfer processes and high fees can prove prohibitive to official property acquisition or sales. World Bank reports show registering a property requires a median of 31 days and a median cost of 4.8 percent of the property's value.[136] Often, individuals will opt instead for informal transfers outside the jurisdiction of a formal land management system. Informal transfers are less legally enforceable by design, leaving both landowners and tenants with less protection in cases of abuse, dispute, or conflict. As a consequence, efforts to maintain uniform land registration and management and manage future ownership claims are undermined.

Blockchain and Land Rights Management

In order to address the challenges described above, some governments and private firms are beginning to experiment with the use of blockchain to help modernize land management systems. The goal of these projects is to take advantage of blockchain's immutability, transparency, and decentralized governance to build systems that provide a more accessible and reliable foundation for recording and transacting land rights.

Broadly speaking, there are two possible models for integrating blockchain into land management systems. The first, more conservative approach is to use blockchain as a complement to existing centralized registries rather than as a replacement for them. In this model, government registrars would continue to store land records in a centralized database much as they always have, but timestamped hashes of those records would be logged on a separate blockchain layer accessible to parties outside the registry. This can be a public blockchain such as Bitcoin or Ethereum or a public-permissioned blockchain managed by a combination of government agencies, civil society groups, banks, real estate firms, and other relevant businesses.

Because the hash of a file changes if even the smallest detail is altered, these blockchain records could serve as a trusted reference for the original files. At any time, property owners can take a hash of their own copy of a land record, compare it against the hash stored on the blockchain, and confirm that they match. Though control over record changes would remain in the hands of a central authority, the blockchain would establish an independent source of truth that would allow any party to verify that their records and the public record are aligned.

Allowing land records to be linked to a publicly accessible blockchain could also enable a number of efficiency improvements to the land conveyance process through the introduction of smart contracts. Smart contracts can be used to specify what documents, data, and signatures must be collected at each step in a land transaction and orchestrate how the different actors proceed through the transaction process. Smart contracts would allow every party to have full, real-time visibility into what information has already been submitted by each party and what actions are still required to advance the contract. Because the hashes of documents would be stored directly on the blockchain, every party would be able to easily verify that they were working off the same document versions, eliminating the need for costly and time-consuming verification checks. Certain aspects of the conveyance process, such as the use of escrow services to hold deeds or payments until certain requirements are met, can even be fully automated by the code contained by the smart contract. These improvements can improve the speed of land transactions and reduce the associated costs.

Case Study: Georgia

In 2016, Georgia began working with software provider Bitfury to pilot a blockchain-based system for the country's land registry. The project established a hybrid blockchain system where records logged to the country's central digitized database would be hashed and placed onto the Bitcoin blockchain to serve as a trusted reference. As of 2021, 3.5 million land titles had been published on the blockchain in this way.[137]

For landowners, this reform did not significantly change the process they had to go through to register or transact their property. The registration process is still managed by the Georgian National Agency of the Public Registry (NAPR), which is responsible for collecting the relevant information from registrants and approving ownership records. However, after the registration process is complete, NAPR issues the owner with a pdf copy of their land record. This record is hashed and stored by NAPR publicly on the blockchain. At any time, landowners can use a tool on NAPR's website to hash their own copy of the record and search for it on the blockchain to ensure they match. While the website clearly indicates that the system is powered by blockchain, and includes an explanation of the technology, the use of blockchain does not materially change the average user's experience on the website.

According to interviews with NAPR, the agency is currently in the process of considering whether to pursue deeper blockchain integration, which may provide additional benefits.[138] This could include switching to a different blockchain that could support smart contracts and other efficiency improvements. However, NAPR is currently working to resolve a number of legal obstacles that could complicate deeper integration of blockchain platforms, including uncertainty over responsibility when errors on the blockchain lead to information being lost or recorded incorrectly, questions of whether blockchain-verified documents are accepted in courts, concerns over the potential for coercion when accepting electronic transactions, and ambiguity around whether smart contracts could comply with legal requirements that contracts be written in reasonable, understandable language.

The second, more ambitious approach to using blockchain for land management is to store property titles directly on the blockchain. In this formulation, titles would be represented as tokens on a permissioned blockchain network, eliminating the need for a centralized registry. These kinds of tokens would represent parcels of land through the attachment of metadata detailing the size, GPS coordinates, and other details about a property.[139] Ownership of a property would be a matter of having the encryption key linked to that property's associated token, and property transactions could occur by using smart contracts to manage and facilitate the transfer of these tokens between users.

Importantly, under this arrangement, parties would still need to rely on third-party databases to house data that is too large to place directly on the blockchain, such as the maps and cadastral data related to land surveys and many of the raw documents associated with a land parcel or transaction. Landowners would still have to trust government authorities or some other third party to store, manage, and protect this information, though the storage of hashes or pointers to this off-chain data within a token's metadata may help to prevent tampering and improve transparency.

A fully blockchain-based registry could grant property owners even greater assurance and control over their rights but would involve a greater deal of complexity than a hybrid system. Redesigning land administration around a blockchain platform would require greater time, resources, expertise, and risk tolerance from the implementing party compared to hybrid systems. Blockchain registries would also create a number of legal and regulatory challenges, such as defining the legal status of tokenized property and any fractionalized rights and determining the appropriate remedy if mistaken or malicious transactions took place on a network not fully controlled by a government authority.

Advantages of Blockchain for Land Rights Management

1. **Blockchain may help provide a secure and transparent record of land ownership that protects against forgery, tampering, and other forms of abuse by authorities.**

Both hybrid and fully blockchain-based land registry systems could lead to more secure and transparent processes for managing property rights. Hybrid systems that log the hashes of land records on a public blockchain would achieve this by establishing an independent record of the land registry. Because this blockchain is not controlled by government authorities, all actors can trust the integrity of the information it contains. At any time, property owners, civil society organizations, or any other group could use the information stored on the blockchain as a way to verify the integrity of the records kept by government authorities. This transparency would help to both identify manipulation when it has occurred and disincentivize authorities from attempting to tamper with records in the first place.

Fully blockchain-based registries would provide further benefits by distributing the power to modify property records so that no single actor could make changes to the registry without the awareness and approval of everyone else on the network. The use of digital signatures and timestamps would help definitively link records to particular users in a way that all parties can trust, while the append-only nature of blockchain transactions would ensure that any attempts to change or tamper with files could be easily tracked back to the responsible party. These benefits could help to prevent corrupt authorities from withholding or manipulating property rights and would strengthen public trust in the land administration process.

Further, to the extent that blockchain would enable a transition to apps or other direct electronic interfaces for submitting and processing property information, it would make it more difficult for officials to demand bribes by removing the opportunity for face-to-face meetings with officials who can refuse service unless compensated.

It is important to note, however, that many of these benefits may also be achieved without needing to use blockchain technologies specifically. Many of the key features of blockchain systems that make records tamper resistant—digital signatures, hashing, timestamps, and the logging of change histories—can also be applied in non-blockchain information systems. What makes blockchain unique is the way it combines these features with a transparent and distributed verification mechanism that allows multiple groups who do not trust each other to nonetheless agree on a common, trusted record of land assets and transactions.

2. **Blockchain can help improve efficiency and reduce the costs associated with land transactions, increasing the likelihood that landowners would utilize the formal land management system.**

The use of smart contracts to help orchestrate the land conveyance process could help improve the speed and efficiency of property transactions while reducing the associated costs and complexity. Often, nations have embarked on ambitious land registration drives that, despite bringing thousands of property owners into the formal registry system for the first time, had little long-term effect because the official system was so full of additional costs and complexity that many landowners simply reverted back to transacting their land through informal agreements.[140] Reducing the costs and complexity of formal land management systems is therefore a key requirement for sustaining long-term progress in land rights reform in developing markets.

Smart contract systems have proven beneficial in this regard. For example, in 2016, the Lantmäteriet, the Swedish mapping and land registration authority, entered into a partnership with the blockchain provider ChromaWay and several other partners to develop a proof-of-concept blockchain system for managing land conveyance. The project was motivated by dissatisfaction with the current conveyance process, which involved 34 separate steps, sometimes took multiple months to complete, and demanded inefficient procedures such as physically mailing documents between the parties, manually checking IDs, and requiring the buyer and seller to meet in a room to call a bank and provide verification for payments. By using electronic processes centered around blockchain-based smart contracts, the project team was able to reduce the number of steps in this process from 34 to 13 while significantly improving speed and reducing associated costs.[141]

3. **Blockchain can help improve the resilience of land management systems to disruption by natural and man-made disasters, which can jeopardize the rights of property owners.**

Accidents, natural disasters, malfunctions, and cyberattacks are all capable of disrupting land registry systems. Centralized land registries—particularly those that have not been digitized—are particularly vulnerable to these risks, as they represent a single point of failure for land information systems. The 2010 earthquake in Haiti, for example, reportedly led to the destruction of an enormous number of title deeds, greatly impeding efforts to rebuild the country.[142] Such losses could lead to widespread damage to property rights if former landowners are left unable to back up their claims.

For some organizations, cloud backups may be sufficient to mitigate these risks. However, even cloud backups can be vulnerable to loss or destruction if the data centers of a cloud provider are disrupted.[143] In comparison, every node serves as a de facto backup in a blockchain network. With a fully blockchain-based registry, this would mean that even in the face of massive and widespread disruption, nodes located outside the affected area could easily restore the land registry. With a hybrid registry, this would not be possible, as only the hashes of records would be stored on the blockchain rather than the records themselves. However, even in these cases, the hash record could be used as a trusted reference that could be used to evaluate the validity of a reconstructed registry. This would both help protect against mistakes and abuse when reconstructing records and improve public trust in the integrity of the reconstruction process.

4. **Blockchain can help promote financial inclusion by making it easier for landowners to access credit.**

The lack of formalized property rights makes it more difficult for individuals in developing markets to gain access to credit. Without proof of ownership, landowners cannot use their property as collateral for loans, reducing their opportunities to make investments, such as in businesses or education.[144] If blockchain were to provide an easier and more reliable way for landowners to maintain formalized rights to property, it may help promote financial inclusion and spur economic development.

5. **Blockchain could help protect women's rights to property by helping formalize their ownership rights and making it more difficult for men to sell women's property without their consent.**

In some countries, women do not possess full and equal rights to own and inherit property. Blockchain systems may be able to help alleviate this issue by making it easier for women to enforce control over their assets. The use of blockchain systems could help prevent the sale of property without women's consent by tying ownership over parcels of land to particular digital identities and requiring multiple parties to sign off before a transfer is approved.[145] The transparency afforded by blockchain may also help women prove their claims to inherit land in areas where customary law may not recognize the land inheritance but national laws do. This could also help avoid unlawful modification of their property records to reassign parcels to family members.

It is important to note, however, that these benefits are entirely dependent on women having the right to own and inherit property in the first place and on there being some authority willing to enforce those rights once they have been recorded. Even when rights have been formally recorded on a blockchain, there is nothing stopping the relevant authorities from simply ignoring them if they feel they will face no consequences for doing so. Ensuring women's rights to own and inherit property is ultimately a matter of legal and political reform that cannot be solved by technical platforms alone.

Risks of Blockchain for Land Rights Management

1. **Vulnerabilities in wallet applications or smart contracts could lead to private information being compromised.**

While blockchain technologies have a number of security benefits that help prevent parties from tampering with stored records, there are still potential points of failure that are introduced when blockchain systems are linked to other software. For example, the wallet applications that allow blockchain users to store the encryption keys for their assets can be compromised in the same way that it is possible for cybercriminals to steal individuals' bank passwords or credit card numbers. In a fully tokenized registry, this could lead to the revelation of private information such as the details of financial instruments associated with a property. Smart contracts face similar risks. Mistakes or vulnerabilities in smart contract code could lead to assets being automatically transferred in a way that none of the parties intended. Mistakes in the code used to adjudicate land rights could lead to mistakes in the land conveyance process that would impose additional costs on property owners and potentially cause a loss of trust in formal systems.

Even when rights have been formally recorded on a blockchain, there is nothing stopping the relevant authorities from simply ignoring them if they feel they will face no consequences for doing so.

2. **Blockchain registries may make jurisdictions dependent on groups of users that are outside of their control, risking long-term instability.**

Some implementations of hybrid blockchain models have used public blockchains such as Bitcoin or Ethereum to log the hashes of land records.[146] This makes authorities dependent on the long-term health and continued operation of these blockchains in order to ensure the integrity of these hashes. Should one of these public blockchains fall into disuse or become the victim of an attack, the integrity of records stored on that chain could no longer be guaranteed. Because these public blockchains are outside the control of government authorities, their failure and abandonment would create significant disruptions and force users to start over from scratch on a different blockchain.

Even in the case of permissioned systems, there is a risk that distributing the responsibility for governing the platform would make it more challenging to respond to malfunctions or attacks on the system. Depending on how the governance of a hybrid or fully blockchain-based registry would be achieved, the result could be an inability to respond quickly and decisively if a malfunction or hack were to compromise the network or its records.[147]

Land Rights Management Issues Blockchain Does Not Solve

1. **If existing land rights have been distributed unfairly, blockchain registries may end up reinforcing an unjust status quo.**

As addressed above, there are significant difficulties in ensuring that the initial distribution of land rights is fair and just. If that initial system includes or enables denial of rights—either by accident or intentionally—those violations would be codified on the blockchain, providing legitimacy to those violations. This would subsequently make it much more difficult for the impacted individuals to seek remedy due to the financial and administrative complexity of challenging formally registered rights and the legal burden of proof placed on disputants.

2. **Blockchain does not make it easier to transition citizens and properties from informal to formal systems.**

A primary challenge in advancing land rights is ensuring that populations that previously relied on informal mechanisms to record and pass down property rights can have those rights officially codified. Doing so can improve their tenure security and give them access to legal remedies in the event of disputes. This process is notoriously difficult, as it demands that officials manually seek out property owners, verify their identities and their relationship to the parcels they occupy, and conduct surveys to demarcate the boundaries separating their land and adjacent properties. This can often be a fraught process, as multiple individuals or families may simultaneously claim the right to a particular piece of land and neighbors may disagree over where boundaries lie. The integrity of this initial distribution of rights is independent of the technology being used to store the records. Regardless of whether the title is stored on a blockchain, in a database, or on a piece of paper, it is equally possible for a registrar to incorrectly assess who a plot belongs to and what its boundaries are.

3. **Land reforms centered on individual titling may disadvantage some groups of landowners whose use of land may not easily conform to the idea of individual ownership.**

While individual property rights may help improve the tenure security of a large number of landowners, there are some groups, including Indigenous peoples, smallholders, and nomadic or pastoral communities, that own land communally or that rely on having access to land that they do not work intensively or occupy permanently.[148] Land reform based on individual titling jeopardizes the rights of these groups as well as associated rights to essential goods such as food and water. Blockchain-based land management systems would do little to alleviate the risk that reforms may pose to these groups.

Regardless of whether the title is stored on a blockchain, in a database, or on a piece of paper, it is equally possible for a registrar to incorrectly assess who a plot belongs to and what its boundaries are.

4. **Blockchain does not eliminate the need to place trust in third parties for management and enforcement activities, including maintaining off-chain data, authenticating network actors, conducting land surveys, and enforcing dispute resolution.**

Though blockchain-based land management systems may reduce the number of times individuals must trust potentially corruptible intermediaries, the land registration and conveyance process will never be fully free from the need to involve third parties.[149] Licensed surveyors will still be needed to create maps of land plots and store the cadastral data that cannot be kept on the blockchain. Identity providers must be trusted to accurately verify the individuals and organizations participating on the network. Hybrid blockchain systems will still rely on central authorities to maintain and approve land titles, and even in fully blockchain-based registries, these authorities will likely still play a role in approving the format and legitimacy of transactions and new land records. Finally, as addressed above, third parties will still have to be trusted to accurately formalize the ownership of unregistered properties.

Most importantly, in the event of a dispute, landowners must trust that authorities will respect their rights in the resolution of that dispute. The need for trust in enforcement authorities becomes particularly important given that even if land registries were to become fully tokenized, officials would retain the ability to reassign property records away from their owners.[150]

Conclusion

Many countries around the world remain reliant on paper-based systems of land administration. These systems lead to substantial risks of corruption, loss of documentation, and conflict or property loss caused by incomplete or inconsistent records. Blockchain has been proposed as one possible technical infrastructure on which to build a more resilient, trustworthy, and transparent system for land administration. Most current uses of blockchain have leveraged the technology to complement existing, centralized registries in a way that helps guard against tampering and improves the efficiency of land administration. However, more ambitious proposals would see blockchain replace centralized registries as a distributed alternative for recording property details.

In the long term, blockchain may have value as part of a larger strategy of strengthening and modernizing land rights protections in developed and developing countries alike. Many of the benefits of digitizing and modernizing land records can be achieved without using blockchain, but the technology may provide several unique benefits that would not be possible otherwise. In particular, hybrid blockchain systems seem to offer an opportunity to strengthen and improve centralized registries in useful ways without accruing significant risks, while fully tokenized registries may eventually make it easier for individuals to engage with the formal land management system.

At the same time, blockchain does little to address the most fundamental issues impacting the rights of property owners, which are largely the result of unjust or unequal allocation of land rights and difficulties in formalizing existing rights. Therefore, efforts to protect property rights must first ensure that these informal rights can be accurately recorded as part of a high-quality, digitized land registry. While blockchain may help improve the security and transparency of land administration, its benefits will be limited to protecting the integrity of property rights that have already been recorded. Blockchain can do little to support the precursor requirements of providing the right to land ownership and to formalization of land rights. In some cases, a focus on adopting blockchain-based systems may in fact distract from these important initial steps. Although it is possible for governments to build emerging administrative systems around blockchain in anticipation of its eventual benefits, it is not necessary to do so in an initial phase to modernize land management systems.

To the extent that blockchain may become a part of future land administration systems, it is likely to do so in a progressive fashion. Thus, a country that decided to focus on a centralized registry of high-quality, digitized records would still be able to easily pivot toward blockchain adoption later on without significant challenges.

For governments that do decide to pursue a blockchain land management system, there are a number of prerequisites that must exist before such a system would be viable. First, governments must have a functional digital identity solution to allow for the authentication of users on the network. Second, the government must already maintain high-quality, digitized records that can be converted into hashes or tokens. Third, the parties that will be responsible for interacting with and administering the blockchain system must have access to and be knowledgeable about the technology and have bought into its success. Fourth, the government must ensure it has adequate internet connectivity to support the operation of the network. Finally, governments must clarify how existing laws and regulations apply to these new systems and pass new legislation where necessary to enable these systems within the context of their legal framework.

If these prerequisites are met, nations should carefully consider the architecture and governance of their blockchain solutions. While fully blockchain-based registries may have some advantages over hybrid systems, the technical, legal, and administrative challenges of switching to storing land records directly on the blockchain will likely render this option impractical for most jurisdictions in the near term. In the absence of a strong digital identity infrastructure, clear laws, extensive testing, and a broadly trusted governance framework, fully blockchain-based management of land rights is not practical. Hybrid systems represent a more attainable goal for nations looking to improve the transparency and security of their management systems and do not preclude the possibility of later switching to a fully blockchain-based model when the option becomes more viable.

7

Addressing the Human Rights Impacts of Blockchain Technologies

As highlighted above, blockchain deployments carry risks to universal human rights. This section considers how blockchain developers and implementers can take steps to reduce these risks, drawing on the UN Guiding Principles on Business and Human Rights (UNGPs) as a framework.[151]

While these recommendations are primarily targeted at corporations involved in developing and deploying blockchain technologies, the policies and practices listed here would also be highly relevant to any civil society group or government agency that is considering whether to deploy or participate in a blockchain system. According to the UNGPs, companies have a responsibility to respect internationally recognized human rights. They do so by exercising human rights due diligence—having in place effective policies and procedures to identify and address potential and actual human rights impacts throughout their value chain. Due diligence steps include assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed.

How companies are expected to respond to impacts will vary depending on their relationship to the impact. If they cause an impact, they are expected to cease or prevent it. If they contribute to an impact, they should cease or prevent their contribution and use their leverage to mitigate its effects to the greatest extent possible. Businesses should also seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products, or services by their business relationships even if they have not contributed to those impacts. They should use their leverage with their business partners to accomplish this. If they lack the leverage to prevent or mitigate adverse impacts and cannot increase their leverage, they should consider ending the relationship. Businesses also have a responsibility to provide effective remedies for human rights harms associated with their products and services.

The corporate responsibility to respect human rights is independent of whether governments are enforcing human rights–compliant laws and may in some cases require companies to adhere to higher standards than those set by national law. The relationship between the corporate responsibility to respect human rights and the existing human rights obligations of governments is closely interwoven. The UNGPs reiterate long-standing international law, noting that governments have a duty to protect human rights from adverse impacts by third parties, including companies. This means they should have in place laws, regulations, enforcement, and remedy mechanisms dealing with those private sector actors involved in blockchain development.

The UNGPs are a useful tool for considering the human rights responsibilities of companies that develop and sell blockchain technologies, as well as those who deploy them, and the policies and procedures they should have in place. The technology sector faces particular challenges related to how end users deploy their products. This challenge is why both human rights by design and evaluation of customers and context are vital tools for the sector, as discussed below. In addition, many of the use cases described in this report attempt to utilize blockchain for the purposes of facilitating or increasing respect for human rights in the sector in which it works; those who deploy these technologies—whether they be companies, governments, or even NGOs—should also undertake human rights due diligence that includes evaluating whether this technology can deliver the positive human rights results it claims.

Identifying Human Rights Impacts and Risks

1. **Conduct an assessment to determine the human rights impacts of the company's products and services.**

Companies that develop and sell blockchain technology should assess the actual and potential human rights impacts of their products and services prior to bringing them to market. Companies that plan to deploy blockchain technology in one of the four use cases covered in this report, or in another sector, should do the same. This assessment process should consider not only the actor's own impacts but also how the company could contribute or be directly linked to the impacts of others. To aid the company in creating safeguards, assessments should focus on identifying who will be impacted by the technology, what the actual and potential impacts could be in both the near and long term, and what mechanisms exist. In the case of the proposed use of blockchain to potentially solve human rights challenges, this assessment should specifically include an analysis of whether the proposed blockchain use will actually address the identified human rights issue, whether it will exacerbate it, or whether it will have no impact (but could distract from more appropriate solutions).

Typically, companies start this process with a high-level assessment of potential impacts. They then become more granular in their analyses, for example, by examining issues related to particular product use cases, the rule of law in countries of deployment, and the reputations of customers and how they will use the technology.

For example, companies may consider: the privacy risks associated with data collection related to their service (including not only the information posted on-chain but also the data collected for customer sign-up and verification); the security vulnerabilities of applications and information infrastructure connected to the blockchain network; the risks associated with key recovery and custodianship frameworks; the potential for the technology to expand or legitimize harmful practices by implementing partners; and the risks of transferring governance responsibilities of critical processes to a distributed network of actors.[152]

The assessment process should include technical, legal, and human rights experts from within the company as well as outside stakeholder groups and representatives from the communities that may be impacted by the product. Importantly, the assessment of human rights risks should not be seen as a one-time exercise. Risks to human rights may shift over time due to changes in the technology or the context of its use. Developers and implementers must therefore ensure that risk assessment is an ongoing process that is baked into the operations of their organization.

If through this process an organization determines that they cannot decisively prevent or mitigate the human rights risks associated with a blockchain deployment, they should halt implementation and not pursue deployment further until such a time as those risks can be addressed. They should also provide effective remedy to anyone harmed by the deployment.

Developers and implementers must ensure that risk assessment is an ongoing process that is baked into the operations of their organization.

2. **Institute internal structures and processes for identifying and escalating the potential human rights concerns posed by the firm's products and services.**

Developers and implementers should institute internal mechanisms for reviewing the development and deployment process for new products and services to identify potential risks to human rights. These structures should allow and encourage employees to voice concerns that come up during their work and escalate those concerns as necessary to a specialized body with the authority to set company policy. This body should be made up of a diverse group, including representatives from product development and customer support as well as human rights and legal staff.

3. **Establish external advisory bodies with representatives from a wide range of disciplines to provide outside assessment of the potential risk of the firm's products or services and how to maximize the potential benefits.**

Developers and implementers should consider establishing external advisory bodies to provide independent accountability and advice on issues relating to whether and how to utilize blockchain in real-world applications, including the human rights implications. These advisory bodies should be composed of experts from a range of disciplines, including human rights, consumer protection, accessibility, and data protection. Businesses should particularly seek out experts in the issue areas touched by their services, which for the issue areas covered in this report could include land rights, labor rights, election monitoring, and refugee service provision.

Firms should develop a structured process for bringing issues to this body for consultation, and all deliberations should be made publicly accessible, possibly with a time lag to manage any commercial sensitivities.

4. **Conduct due diligence of potential buyers and partners to assess the risk of deployments leading to human rights abuses.**

Before deploying blockchain platforms or services, developers should conduct due diligence on implementing partners to determine whether the actor or actors are likely to be involved in any activities that could create human rights risks, as well as whether their proposed application can deliver any claimed human rights benefits. For example, developers focusing on land rights management solutions may consider whether their blockchain services may be used as a way to legitimize unjust land registration practices by local authorities. Firms focusing on improving labor rights through supply chain transparency may consider the information their partners plan to store on the blockchain about workers and whether their plans may create privacy risks. And developers working on blockchain voting systems may consider whether potential customers have a history of vote tampering and whether they intend to centralize control over the blockchain network in ways that could enable further abuse.

These principles should be made publicly available and be incorporated into an internal process of reviewing potential new customers to determine whether a sale will lead to risk of abuse. Senior-level oversight is necessary to overcome the urge to make sales regardless of the consequences.

Mitigating Human Rights Risks

1. **Leverage contractual or other mechanisms to establish processes for controlling or regularly reviewing how customers are using the tools being provided to them.**

Developers should insert terms into their contracts and licensing agreements that prohibit operators from using their products or services in ways that could violate the rights of others or create unjustifiable risks for users. Oversight and enforcement of these terms can be accomplished through regular audits by the developer—which could be tied to licensing sunsets—or through observation of the operator's deployment by customer support, professional service, and sales teams as part of an ongoing relationship between the organizations. Companies should also look to use their contracts as a way of putting mechanisms in place that would help them track the effectiveness of their efforts to address or mitigate rights impacts.

Firms may encounter difficulties in finding out when contract provisions have been breached and enforcing the terms of their agreements. This should not, however, be taken as a reason for companies not to fulfill their responsibility to prevent or mitigate negative impacts stemming from blockchain deployments.

2. **Ensure the technical architecture of the blockchain network and surrounding digital infrastructure minimize privacy and security risks.**

Companies developing and deploying blockchain technology and applications should incorporate technical controls into the design and architecture of their systems to enforce privacy and data protection principles, including transparency, security, integrity, access control, accountability, and minimization, throughout the full life cycle of the data being collected and processed. Software developers should proactively consider the potential for privacy violations arising from errors or intentional misuse and design safeguards to guard against these risks. Implementers should carefully consider who will have access to data on permissioned networks and what type of data will be stored on chain. Examples of relevant practices could include designing systems to:

- Never store personal information directly on a public blockchain;
- Delete any personal identifiable information gathered for user verification after the process is complete;
- Support key recovery and custodianship (where appropriate) while strictly limiting access to approved parties;
- Only work on devices with certain minimum-security protections; and
- Implement differential privacy so that access to sensitive data can be restricted to only approved network nodes.

For use cases such as digital identity, firms should reference established guidance and standards for building secure and privacy-protecting solutions, especially when building systems that will be deployed in humanitarian contexts.[153]

Developers should implement organizational practices to ensure privacy by design is followed and enforced, such as conducting regular internal reviews, assigning dedicated personnel to oversee privacy issues, and training employees on privacy.

3. **Provide rigorous and accessible training for customers to help operators understand how to use the technology in ways that respect human rights.**

Prior to use, developers should work with their partners to ensure they are familiar with the risks involved in the systems and processes they are responsible for administering. In addition to technical training to familiarize partners with the software, developers should strive to educate their partners about non-technical risks and failures that could arise during operation and advise them on how to address them. For example, for providers of platforms for land rights management, training could include information on dispute scenarios that are likely to arise as new properties are logged in the system and on how to ensure that the results of any dispute processes are properly recorded in the system. Similarly, developers of blockchain voting systems should be responsible for working with election officials to understand how to address any errors transparently without compromising public confidence in the election process. Providers of supply chain management platforms could work with buyers to ensure they understand how to properly log data without inadvertently creating privacy risks through the information they contribute. Providers of digital identity solutions should work to ensure that their platforms are easily understandable, allow for informed consent, and are accessible to populations with low digital skills or intermittent connectivity.

Transparency

1. **Institute a policy statement outlining the company's human rights commitments.**

The statement of commitment should clearly set out the business's expectations for its personnel, business partners, suppliers, customers, and other linked parties. These expectations and commitments should be informed through consultation with relevant internal or external expertise and should be approved at the most senior level of the firm. The plan should be made public and circulated both internally to personnel in the firm and externally to partners and other relevant parties.

2. **Where possible and practical, developers should implement their solutions using open-source software and support third-party auditing.**

To reduce security vulnerabilities, developers should strive whenever possible to adopt open-source software and open standards for implementation. For use cases such as voting, where failures could lead to severe and potentially irreversible harms, there should be an expectation that systems be fully available to investigation by third parties to determine potential risks. While this does not necessarily require full source-code disclosure in every case, it should include, at a minimum, cooperation by developers with third-party assessments and the development of application programming interfaces (APIs) and technical tool kits to support robust and regular assessments of privacy and security.

3. **Communicate how impacts are addressed.**

Blockchain developers and implementers should identify how they are managing potential and actual human rights impacts through public reporting and report on how they address and remedy any human rights impacts that are identified. Increased transparency on outcomes and use cases would help companies in this sector differentiate themselves from less-responsible competitors.

4. **Allow and encourage the participation of a diversity of parties in deployed blockchain systems**

While blockchain systems carry the promise of radical transparency, for permissioned systems this transparency can be undermined if the party administering the blockchain does not allow records to be publicly viewable or if they too strictly limit the number or diversity of parties that participate in its operation. For example, supply chain traceability systems that limit visibility to a small consortium of companies have much more limited transparency benefits compared to a system that is publicly visible and allows NGOs and government actors to participate as nodes. All parties responsible for deploying and administering a permissioned system should ensure that a diverse range of parties is invited to participate in the operation of the network so that these systems may achieve their potential transparency benefits.

Remedy

1. **Provide remedy for those whose rights are adversely impacted.**

So that grievances can be addressed early and remediated directly, business enterprises should establish or participate in effective operational-level grievance mechanisms for individuals and communities that may be adversely affected by impacts that the company caused or to which it contributed. Companies are encouraged to support remedy for impacts to which they are directly linked.[154]

The question of remedy is particularly important to consider in the context of blockchain solutions due to the technology's unique properties and limitations. Because of the immutable nature of blockchain records, some forms of remedy—such as deleting data that is false or which could lead to privacy risks—could be impossible. Developers and implementers should understand how blockchain may shape the opportunities they have to provide remedy and ensure that steps are taken to avoid situations where these types of failures may take place. The most important consideration in this regard is personal information, which for these reasons should never be logged directly onto a blockchain, even in encrypted form.

Developers and practitioners should also understand the risks of smart contracts and other automated transaction mechanisms that may be built on top of blockchain networks. These systems automatically execute transactions without human intervention, and failures can lead to impacts that, depending on the network's governance mechanism, may be impossible to reverse. Among the use cases examined in this report, this risk is particularly salient for land rights management systems.

Because of the immutable nature of blockchain records, some forms of remedy—such as deleting data that is false or which could lead to privacy risks—could be impossible.

The ability to provide remedy is also affected by the governance setup of the network. Because blockchain decentralizes the power to make and record changes to the underlying data, institutions may not have the power to remedy certain kinds of failures. This is a particular risk for any system relying on a public permissionless blockchain such as Ethereum, which cannot be controlled by any single authority.

Finally, there must be an awareness not only of whether remedy is technically possible but also of whether it is practically accessible for affected populations. For example, in humanitarian contexts, vulnerable populations may lack an awareness of how their information is being used as a part of digital identity systems and may lack accessible mechanisms for taking actions in the circumstance when they do discover harms or risks. Developers and implementers must ensure that remedy is not only available but also accessible for these groups.

About the Author and Contributors

William Crumpler is a researcher with the Strategic Technologies Program at CSIS, where his work focuses on cybersecurity policy and the governance of artificial intelligence, 5G telecommunications, blockchain, and other emerging technologies. He holds a BS in materials science and engineering from North Carolina State University.

Marti Flacks is a senior fellow and director of the Human Rights Initiative at CSIS, which seeks to bring innovative thinking and a multi-disciplinary approach to tackle pressing global human rights challenges and better integrate human rights across foreign policy priorities. Ms. Flacks spent more than a decade in the U.S. government, most recently serving at the National Security Council (NSC) as director of African Affairs from 2015-17, where she coordinated U.S. policy across East and Southern Africa and on continent-wide trade and economic issues. Prior to the NSC, Ms. Flacks spent three years as deputy director of the Office of Energy Programs at the U.S. State Department, leading the department's work on energy transparency and good governance, and four years working for the U.S. special envoy for Sudan on implementation of the Comprehensive Peace Agreement and the independence of South Sudan. She joined the U.S. government through the President Management Fellowship program at the Department of Homeland Security. Prior to joining CSIS, Ms. Flacks served as deputy director and head of the North America office at the Business & Human Rights Resource Centre, a human rights organization focused on the role of business in respecting human rights. Ms. Flacks received a BS in foreign service from Georgetown University, a master's degree from the Fletcher School at Tufts University, and a JD from Columbia Law School. She is originally from Solon, Ohio.

Amith Mandavilli is a program manager with the Human Rights Initiative at CSIS. Before joining CSIS, Amith interned with the U.S. Mission to the United Nations, where he worked alongside U.S. diplomats who staffed the U.S. ambassador to the United Nations at the United Nations Security Council, and with the U.S. Department of State's Bureau of Democracy, Human Rights, and Labor. Amith received degrees in political science and biological sciences from North Carolina State University.

Appendix A

Project Methodology

Below, we have provided a brief outline of our research methodology for this project. It is our hope that other organizations may be able to use this approach to aid in the investigation of how other technologies impact human rights.

Determining Project Scope

Blockchain has been proposed as a solution to a wide range of problems, and the scope of this research project limited how many of these applications we were able to cover. To determine the specific applications we would investigate through this project, we leveraged desk research and consultations with stakeholders in the human rights community and abroad to understand which blockchain applications have the greatest implications for human rights development. We made this determination based on following criteria:

- Whether a particular application is currently being deployed;
- The number of individuals who are or will be impacted by the technology;
- The severity of potential negative human rights impacts from current or future implementations;
- The potential benefits of the technology in promoting and protecting human rights;
- The degree to which the technology would disproportionately impact vulnerable populations;
- The impact of the technology on civil society organizations and their operations;
- The irremediability of potential impacts from the technology; and
- The human rights impact of potential alternatives to these technologies.

Understanding the Technology

To better understand how the technology in question works, we conducted a literature review of explanatory documents and presentations released by developers, industry associations, academic researchers, government technologists, and relevant NGOs with significant in-house technical expertise. This review focused on the fundamentals of blockchain technology, including public key cryptography, the different consensuses that may be used, the difference in architecture between public versus private and permissionless versus permissioned systems, and the functioning of smart contracts.

In particular, this work was focused on establishing the primary strengths and limitations of blockchain technology compared to alternative technologies to help focus and inform subsequent investigation and analysis of existing deployments and proposals.

Evaluating Use-Cases

1. **Investigate the human rights context for each chosen focus area.**
   - We reviewed human rights literature, including UN Special Rapporteur statements, non-governmental organization reports, and classic international human rights conventions, to identify human rights that stand to be particularly impacted by private and public sector deployments of blockchain systems. Based on this analysis, we
2. **Conduct desk research on how the technology is being used or is proposed to be used in each chosen focus area.**
   - We leveraged media reporting, reports from local or international NGOs, government announcements, and other authoritative sources to compile a list of planned or actual deployments of the technology in each chosen focus area. We recorded the details that have been made public about these deployments, how they were proposed to work, the impact they have had (if already deployed), the governance structures they intersect with, and any gaps where details have not been made public.
   - At the same time, we reviewed reports and publications by think tanks, advocacy organizations, academics, government agencies, developers, and industry groups to understand current thinking about the broader potential opportunities and obstacles to using blockchain in each area.
   - From these reports, we compiled a list of developers, researchers, advocates, and operators involved in the deployment, operation, governance, and investigation of the technology in each of the chosen focus areas.
3. **Reach out to the individuals identified in each area of focus, and request interviews to gather additional information.**
   - In the case of developers, we used the interviews as an opportunity to clarify how the systems would work, how they would intersect with or replace existing systems and technological tools, why these systems were deemed superior to the systems they would replace, what challenges emerged in building and deploying the technology, and what key safeguards they recommended to ensure responsible use.

- In the case of organizations that were involved in the use and operation of blockchain systems, we used the interviews as an opportunity to learn more about the benefits they had seen from its use, the problems the technology may have introduced, the issues that remained even after deployment had occurred, and the safeguards they recommended to ensure responsible use.
- In the case of civil society organizations, researchers, and advocates, we used the interviews as an opportunity to gain insight into the key problems facing each of the chosen focus areas, understand which of these problems could be improved through the use of blockchain and which could not, whether the blockchain uses they were familiar with had delivered on their promised benefits, and what key risks and concerns they saw with the technology.

4. **Based on the results of the literature review and interviews, draft a set of findings for each of the chosen focus areas.**
   - For each chosen focus area, we drafted a crafted a set of draft findings that laid out how blockchain was being used, presented a high-level set of potential benefits and risks that we had found during our research, and laid out the problems in the area that we did not believe could be solved with blockchain.

5. **Refine recommendations through workshops and consultations with experts.**
   - Our draft findings for each chosen focus area were sent to an array of experts in each area, ensuring that at least one developer, one user, and one independent researcher was given the chance to review our material for each subject. In addition, we held a workshop and several follow-up interviews to review our findings and receive feedback on them.
   - Based on the feedback received, we drafted our final report.

Developing Recommendations for Corporate Policies and Procedures

1. **Conduct a review of existing literature on corporate policies and practices with respect to business, human rights, and technology.**
   - We reviewed reports and publications by think tanks, advocacy organizations, academics, government agencies, developers, and industry groups to understand the current sets of issues being debated as part of a conversation around blockchain use and governance.
   - From these reports, we compiled a list of researchers, advocates, academics, and policymakers around the world involved in the crafting of these use and governance recommendations for blockchain.

2. **Reach out to individuals involved in developing and deploying blockchain tools to understand their current practices and processes.**
   - We spoke to developers and users across all four focus areas to understand the companies' approach toward identifying and mitigating risks, making their processes transparent, and providing remedy to any individuals who may have their rights violated through the use

of their tools. We also had conversations with experts in business and human rights to understand the key policies which must be in place to fulfill companies' responsibilities.

3. **Based on the results of the literature review and interviews, draft a set of recommendations for blockchain companies.**
   - Using our findings from desk research and stakeholder interviews, we drafted a set of recommendations for company policies and procedures, focusing on how companies can identify potential human rights risks, what steps they should take to mitigate them, how they should communicate information about their policies, practices, and tools to outside stakeholders, and how they should approach remedy for any affected individuals.

4. **Refine recommendations through workshops and consultations with experts.**
   - Our draft findings were sent to several developers and experts in business and human rights for feedback. In addition, we held a workshop and several follow-up interviews to review our findings and receive feedback on them.
   - Based on the feedback received, we drafted our final report.

Endnotes

1 For an overview of blockchain technologies providing greater technical detail than included in this report, readers are encouraged to review Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone, *Blockchain Technology Overview*, NISTIR 8202 (Gaithersburg, MD: National Institute of Standards and Technology, October 2018), doi:10.6028/NIST.IR.8202.

2 "Art. 17 GDPR: Right to erasure ('right to be forgotten')," General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 of the European Parliament, Article 17, https://gdpr-info.eu/art-17-gdpr/.

3 Heena Vinyak, "Crypto Attack: The Five Worst Hacks That Shook the Crypto World," Cointelegraph, November 4, 2019, https://cointelegraph.com/news/crypto-under-attack-the-five-worst-hacks-that-shook-the-crypto-world.

4 Lucas Marx "Storing Data on the Blockchain: The Developers Guide," Macoded, July 5, 2018, https://malcoded.com/posts/storing-data-blockchain/.

5 Kenny Li, "The Blockchain Scalability Problem and the Race for Visa-Like Transaction Speed," Hackernoon, January 26, 2019, https://hackernoon.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44.

6 "Bitcoin Energy Consumption Index," Digiconomist, n.d., https://digiconomist.net/bitcoin-energy-consumption.

7 Nick Szabo, "Smart Contracts," 1994, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

8 "Ratifications of fundamental Conventions by country," International Labour Organization (ILO), n.d., https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:10011:0::NO::P10011_DISPLAY_BY,P10011_CONVENTION_TYPE_CODE:1,F.

9 ILO, *Global estimates of modern slavery: Forced labour and forced marriage* (Geneva: 2017), https://www.alliance87.org/global_estimates_of_modern_slavery-forced_labour_and_forced_marriage.pdf.

10 “Corporate due diligence and corporate accountability: European Parliament resolution of 10 March 2021 with recommendations to the Commission on corporate due diligence and corporate accountability,” European Parliament, 2020/2129(INL), March 10, 2021, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0073_EN.pdf; Know the Chain, *2021 Apparel and Footwear Benchmark Report* (London: 2021), https://knowthechain.org/wp-content/uploads/2021-KTC-AF-Benchmark-Report.pdf.

11 Hannah Boles, *Tracking Progress: Assessing Business Responses to Forced Labour and Human Trafficking in the Thai Seafood Industry* (New York: Praxis Labs, 2019), http://www.praxis-labs.com/uploads/2/9/7/0/29709145/09_hu_report_final.pdf.

12 Jerwin Tholen et al., *Is there a role for blockchain in responsible supply chains?* (Paris: OECD, 2019), http://mneguidelines.oecd.org/Is-there-a-role-for-blockchain-in-responsible-supply-chains.pdf.

13 “Strengthen your certification with the latest tech,” OpenSC, n.d., https://opensc.org/certifications.html.

14 Gertrude Chavez-Dreyfuss, “Harvard, Levi Strauss, U.S. think tank in blockchain tie-up on worker welfare,” Reuters, January 24, 2019, https://www.reuters.com/article/us-usa-blockchain-harvard/harvard-levi-strauss-u-s-think-tank-in-blockchain-tie-up-on-worker-welfare-idUSKCN1PI2FA; and “A New Way to Measure Worker Well-being,” Levi Strauss & Co., January 24, 2019, https://www.levistrauss.com/2019/01/24/new-way-measure-worker-well/.

15 “Building Sustainable Supply Chains,” New America, March 31, 2021, https://www.newamerica.org/digital-impact-governance-initiative/events/building-sustainable-supply-chains/.

16 “How tech is transforming the fight against modern slavery,” slavefreetrade, June 18, 2021, https://slavefreetrade.org/how-tech-is-transforming-the-fight-against-modern-slavery/; and “Brian Iselin: Can Blockchain Technology Make Trade Slave-Free?,” The Inc. Tank, Ed Snider Center for Enterprise & Markets, January 2019, https://edsnidercenter.org/inctank-podcast-brian-iselin/.

17 Christine Chow et al., “Supply Chain Human Rights Risk Management: Blockchain and Emerging Technology,” DLA Piper, Hermes, RCS Global, and Everledger, November 2018, https://respect.international/wp-content/uploads/2019/08/Supply-Chain-Human-Rights-Risk-Management-2018.pdf.

18 “Illegal Fishing and Human Rights Abuses at Sea: Using Technology to Highlight Suspicious Behaviors,” Oceana, June 2019, https://usa.oceana.org/publications/reports/illegal-fishing-and-human-rights-abuses-sea#.

19 Jason Judd, “Beneath the Surface: A review of literature and initiatives for identification of forced labour in fishing [Draft],” Cornell, February 2020, https://cornell.app.box.com/s/pdawct980a8m64aeiz4qma5uzyjgo94u; and Chow et al., “Supply Chain Human Rights Risk Management.”

20 Ibid.

21 For an example of a fish logged this way, see “FJ00001,” Traseable Solutions, n.d., https://www.traseable.com/story/FJ00001/.

22 Interview with Uttam Kumar and Brett Haywood, Sea Quest Fiji.

23 Interview with Bubba Cook, WWF.

24 Interview with Uttam Kumar and Brett Haywood, Sea Quest Fiji; and Cook, *Blockchain: Transforming the Seafood Supply Chain*.

25 Cook, *Blockchain: Transforming the Seafood Supply Chain*.

26 “Blockchain for Traceability in Minerals and Metals Supply Chains: Opportunities and Challenges,” RCS Global, December 20, 2017, https://www.rcsglobal.com/wp-content/uploads/2018/09/ICMM-Blockchain-for-Traceability-in-Minerals-and-Metal-Supply-Chains.pdf; and Chow et al., “Supply Chain Human Rights Risk Management.”

27 Luz Fernandes Espinosa, "BBVA and Wave carry out the first blockchain-based international trade transaction between Europe and Latin America," BBVA, November 27, 2017, https://www.bbva.com/en/bbva-and-wave-carry-first-blockchain-based-international-trade-transactioneurope-and-latin-america/.

28 "Building Sustainable Supply Chains," New America.

29 Ibid.

30 Bradley Soule, "Blockchain technology – Could this be the supply chain's weakest link?," Open Channels, August 20, 2018, https://www.openchannels.org/blog/oceanmind/blockchain-technology-could-be-supply-chains-weakest-link.

31 For an indicative overview of the limitations of current tools and processes for assessing labor conditions it the seafood industry, see Judd, "Beneath the Surface." Also see: "MSC's Revised Chain of Custody Certification Fails to Adequately Address Forced Labor and Child Labor in Seafood Supply Chains," Public Statement from Human Rights and Environmental Organizations, June 10, 2019, https://www.hrw.org/news/2019/06/10/mscs-revised-chain-custody-certification-fails-adequately-address-forced-labor-and#; "Beyond Social Auditing," Business & Human Rights Resource Centre, https://www.business-humanrights.org/en/big-issues/labour-rights/beyond-social-auditing/.

32 Tholen et al., *Is there a role for blockchain in responsible supply chains?*

33 For an example of work to develop data reporting standards, see: *Responsible Minerals Initiative, Responsible Minerals Initiative Blockchain Guidelines*, Second Edition (Alexandria, VA: Responsible Minerals Initiative, March 2020), http://www.responsiblemineralsinitiative.org/media/docs/RMI%20Blockchain%20Guidelines%20-%20Second%20Edition%20-%20March%202020%20FINAL.pdf.

34 David Noonan, "What Does a Crooked Election Look Like?," *Scientific American*, October 30, 2018, https://www.scientificamerican.com/article/what-does-a-crooked-election-look-like/.

35 Freedom House's *Freedom in the World 2021* report employed three indicators to assess electoral processes of all countries and territories. Indicator A3 asked "are the electoral laws and framework fair, and are they implemented impartially by thee relevant election management bodies?" This indicator was scored on a scale of zero to four, four being the highest rating. Seventy percent of countries and territories scored between zero and three, indicating some degree of unfair electoral laws or partisan election management. "Countries and Territories," Freedom House, 2021, https://freedomhouse.org/countries/freedom-world/scores.

36 Drew Desilver, "In past elections, U.S. trailed most developed countries in voter turnout," Pew Research, November 3, 2020, https://www.pewresearch.org/fact-tank/2020/11/03/in-past-elections-u-s-trailed-most-developed-countries-in-voter-turnout/.

37 Richard Wike and Alexandra Castillo, "Many Around the World Are Disengaged From Politics," Pew Research Center, October 17, 2018, https://www.pewresearch.org/global/2018/10/17/international-political-engagement/.

38 Email correspondence between the authors and Arne Koitmäe, head of the Estonia State Electoral Office; "General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia," State Electoral Office of Estonia, June 20, 2017, https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf; and "e-governance," e-Estonia, n.d., https://e-estonia.com/solutions/e-governance/.

39 Drew Springall et al., "Security Analysis of the Estonian Internet Voting System," *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (November 2014), doi:10.1145/2660267.2660315.

40 Josh Benaloh et al., "End-to-end verifiability," End-to-End Verifiable Internet Voting Project, February 2, 2014, https://arxiv.org/ftp/arxiv/papers/1504/1504.03778.pdf; and Alex Berke, "Crypto Voting + US Elections: Reality," MIT Media Lab, January 23, 2020, https://www.media.mit.edu/posts/crypto-voting-us-elections-reality/.

41 Burke, "Crypto Voting + US Elections: Reality."

42 "Frequently Asked Questions," Voatz, n.d., https://voatz.com/faq/; Brian Fung, "West Virginians abroad in 29 countries have voted by mobile device, in the biggest blockchain-based voting test ever," *Washington Post*, November 6, 2018, https://www.washingtonpost.com/technology/2018/11/06/west-virginians-countries-have-voted-by-mobile-device-biggest-blockchain-based-voting-test-ever/; Forrest Senti, "The Denver Mobile Voting Pilot: A Report," National Cybersecurity Center, August 1, 2019, https://cyber-center.org/wp-content/uploads/2019/08/Mobile-Voting-Audit-Report-on-the-Denver-County-Pilots-FINAL.pdf; and Ymarú Rojas, "La oposición logra que seis millones y medio de venezolanos participen en la consulta contra Maduro [The opposition gets six and a half million Venezuelans to participate in the referrendum against Maduro]," ABC Internacional, December 13, 2020, https://www.abc.es/internacional/abci-oposicion-logra-seis-millones-y-medio-venezolanos-participen-consulta-contra-maduro-202012131204_noticia.html.

43 "Frequently Asked Questions," Voatz.

44 Interview with Voatz executives.

45 "Frequently Asked Questions," Voatz; Forrest Senti, *The Denver Mobile Voting Pilot: A Report* (Colorado Springs, Colorado: National Cybersecurity Center, August 2019), https://cyber-center.org/wp-content/uploads/2019/08/Mobile-Voting-Audit-Report-on-the-Denver-County-Pilots-FINAL.pdf; Larry Moore and Nimit Sawhney, "Under the Hood: The West Virginia Mobile Voting Pilot," Voatz, 2019, https://sos.wv.gov/FormSearch/Elections/Informational/West-Virginia-Mobile-Voting-White-Paper-NASS-Submission.pdf; and "Voatz Mobile Voting Platform – An Overview: Security, Identity, Auditability," Voatz, July 2020, https://voatz.com/wp-content/uploads/2020/07/voatz-security-whitepaper.pdf.

46 Moore and Sawhney, "Under the Hood"

47 Interview with Voatz executives.

48 "Frequently Asked Questions," Voatz; Moore and Sawhney, "Under the Hood"; Senti, *The Denver Mobile Voting Pilot*; and "Voatz Mobile Voting Platform," Voatz.

49 Lucas Mearian, "Utah county moves to expand mobile voting through blockchain," Computerworld, October 21, 2019, https://www.computerworld.com/article/3446836/utah-county-moves-to-expand-mobile-voting-through-blockchain.html.

50 Anthony Fowler, "Promises and Perils of Mobile Voting," *Election Law Journal* 19, no. 3 (September 2020), doi:10.1089/elj.2019.0589.

51 David Jefferson et al., "What We Don't Know About the Voatz 'Blockchain' Internet Voting System," University of South Carolina, May 1, 2019, https://cse.sc.edu/~buell/blockchain-papers/documents/WhatWeDontKnowAbouttheVoatz_Blockchain_.pdf; and Michael A. Specter, James Koppel, Daniel Weitzner, "The Ballot is Busted Before the Blockchain," 29th USENIX Security Symposium, August 2020, https://www.usenix.org/conference/usenixsecurity20/presentation/specter.

52 Specter, Koppel, and Weitzner, "The Ballot is Busted Before the Blockchain."

53 Ibid.

54 Ibid.

55 "Voatz Response to Researchers' Flawed Report," Voatz, February 13, 2020, https://voatz.com/2020/02/13/voatz-response-to-researchers-flawed-report/.

56 "Our Full Report on the Voatz Mobile Voting Platform," Trail of Bits, March 13, 2020, https://blog.trailofbits.com/2020/03/13/our-full-report-on-the-voatz-mobile-voting-platform/.

57 "Voatz Security Assessment Volume I of II: Technical Findings," Trail of Bits, March 12, 2020, https://github.com/trailofbits/publications/blob/master/reviews/voatz-securityreview.pdf.

58 “Charting A New Forward Course in Election Security,” Voatz, March 13, 2020, https://voatz.com/2020/03/13/charting-a-new-forward-course-in-election-security/; “Responses & Comments for (Trail of Bits Report),” Voatz, May 10, 2020, https://voatz.com/wp-content/uploads/2020/07/V-Responses-ToB-I.pdf; and Emanuel Maiberg, Jason Koebler, and Lorenzo Franceschi-Bicchierai, “A Mobile Voting App That’s Already in Use Is Filled With Critical Flaws,” Motherboard, March 13, 2020, https://www.vice.com/en/article/n7jk9x/mobile-voting-app-voatz-severe-security-vulnerabilities.

59 Astghik Grigoryan, “Russian Federation: Experimental E-voting to Be Conducted in Moscow City Duma Elections,” Library of Congress, 2019, https://www.loc.gov/item/global-legal-monitor/2019-06-24/russian-federation-experimental-e-voting-to-be-conducted-in-moscow-city-duma-elections/.

60 “Moscow Voters Debate: Did Blockchain-Based Online Voting Undermine The Opposition?,” Current Time, September 24, 2021, https://en.currenttime.tv/a/moscow-voters-debate-did-blockchain-based-online-voting-undermine-russia-s-opposition-/31476383.html.

61 Interview with Stanislav Andreychuk, Golos.

62 Kirill Polyakov, “How Moscow organized voting on blockchain in 2020,” ICT Moscow, February 8, 2021, https://ict.moscow/en/news/how-moscow-organized-voting-on-blockchain-in-2020/.

63 “Кибервыборы v1.0: как создавалась система блокчейн-голосования в Москве [Cyber-election v1.0: how the blockchain voting system was created in Moscow],” Moscow Department of Information Technology, December 13, 2019, https://habr.com/ru/article/480152/; Elena Rozhkova and Angelina Galanina, “Бесперебойные выборы [Uninterrupted elections],” Kommersant, September 1, 2020, https://www.kommersant.ru/doc/4474649; and Anna Baydakova, “Russia’s New Blockchain Voting System Isn’t Ready, but It’ll Be Used This Month Anyway,” CoinDesk, September 1, 2020, https://www.coindesk.com/policy/2020/09/01/russias-new-blockchain-voting-system-isnt-ready-but-itll-be-used-this-month-anyway/.

64 Pierrick Gaudry and Alexander Golovnev, “Breaking the Encryption Scheme of the Moscow Internet Voting System,” in Joseph Bonneau and Nadia Heninger, eds., *Financial Cryptography and Data Security. FC 2020. Lecture Notes in Computer Science*, vol. 12059 (2020), doi:10.1007/978-3-030-51280-4_3.

65 Gaudry and Golovnev, “Breaking the Encryption Scheme of the Moscow Internet Voting System.”

66 Denis Dmitriev, “«Медуза» нашла уязвимость в системе интернет-голосования. Часть голосов можно расшифровать еще до официального подсчета [Meduza found a vulnerability in the Internet voting system. Some of the votes can be deciphered even before the official counting],” Meduza, July 1, 2020, https://meduza.io/feature/2020/07/01/meduza-nashla-uyazvimost-v-sisteme-internet-golosovaniya-chast-golosov-mozhno-rasshifrovat-esche-do-ofitsialnogo-podscheta.

67 Denis Dmitriev, “Власти фактически выложили в открытый доступ персональные данные всех интернет-избирателей [The authorities actually made the personal data of all Internet voters publicly available Thousands of invalid passports took part in voting on the amendments],” Meduza, July 9, 2020, https://meduza.io/feature/2020/07/09/vlasti-fakticheski-vylozhili-v-otkrytyy-dostup-personalnye-dannye-vseh-internet-izbirateley.

68 Nikita Korolev, “База данных пошла на второй тур [The database went to the second round],” Kommersant, August 4, 2020, https://www.kommersant.ru/doc/4442021.

69 Leonid Bershidsky, “In Russia’s So-Called Election, Tech Was a Big Loser,” Bloomberg, September 23, 2021, https://www.bloomberg.com/opinion/articles/2021-09-23/in-russia-s-so-called-election-tech-was-a-big-loser; “Moscow Voters Debate,” Current Time; and Dmitri Kuznets and Alexander Ershov, “Stop the steal, rock the vote Meduza explains the debate about the legitimacy of Moscow’s online elections,” Meduza, September 28, 2021, https://meduza.io/en/feature/2021/09/29/stop-the-steal-rock-the-vote.

70 “After hackers break Moscow's prototype Internet voting, city officials stop sharing contest results on GitHub,” Meduza, August 19, 2019, https://meduza.io/en/feature/2019/08/20/after-hackers-break-moscow-s-prototype-internet-voting-city-officials-stop-sharing-contest-results-on-github.

71 Stephen O’Neal, “Transparency of Russia’s Blockchain Voting Setup Put Under a Microscope,” Coin Telegraph, July 17, 2020, https://cointelegraph.com/news/transparency-of-russias-blockchain-voting-setup-put-under-a-microscope.

72 Interview with Stanislav Andreychuk, Golos.

73 “В «Голосе» рассказали о непрозрачности новой системы онлайн-голосования: в регистрации отказывают беспричинно [Golos spoke about the opacity of the new online voting system: registration is refused without reason],” Open Media, May 13, 2021, https://openmedia.io/news/n3/v-golose-rasskazali-o-neprozrachnosti-novoj-sistemy-onlajn-golosovaniya-v-registracii-otkazyvayut-besprichinno/; Lilia Yapparova, “‘Electronic voting must die’ Election expert Sergey Shpilkin explains how Russian officials thwart independent analysis,” Meduza, September 20, 2021, https://meduza.io/en/feature/2021/09/20/electronic-voting-must-die; and “Moscow Voters Debate,” Current Time.

74 Fowler, “Promises and Perils of Mobile Voting.”

75 Nicole Goodman and Leah C. Stokes, “Reducing the Cost of Voting: An Evaluation of Internet Voting’s Effect on Turnout,” *British Journal of Political Science* 50, no. 3 (May 2018), doi:10.1017/S0007123417000849.

76 Micha Germann and Uwe Serdült, “Internet voting and turnout: Evidence from Switzerland,” *Electoral Studies* 47 (June 2017), doi:10.1016/j.electstud.2017.03.001; “Questions about the reliability of i-voting,” Valimised, n.d., https://www.valimised.ee/en/internet-voting/frequently-asked-questions/questions-about-reliability-i-voting; “Summary of the ISF report,” Norway Ministry of Local Government and Regional Development, June 14, 2012, https://www.regjeringen.no/en/historical-archive/Stoltenbergs-2nd-Government/Ministry-of-Local-Government-and-Regiona/tema-og-redaksjonelt-innhold/kampanjesider/e-vote-trial/evaluations-of-the-e-voting-trials/evaluation-of-the-e-voting-trials-in-201/summary-of-the-isf-report/id685824/; and Régis Dandoy, “The impact of e-voting on turnout: Insights from the Belgian case,” IEEE, presented at the 2014 First International Conference on eDemocracy & eGovernment, Quito, Ecuador, April 24–25, 2014, 29–37, doi:10.1109/ICEDEG.2014.6819940.

77 Thomas Fujiwara, “Voting Technology, Political Responsiveness, and Infant Health: Evidence from Brazil,” *Econometrica* 83, no. 2 (2015), doi.org/10.3982/ECTA11520.

78 Ibid.

79 “Burundi: Intimidation, Arrests During Elections,” Human Rights Watch, June 1, 2020, https://www.hrw.org/news/2020/06/01/burundi-intimidation-arrests-during-elections#.

80 Denis Dmitriev and Sultan Suleimanov, “Мэрия (случайно?) позволила расшифровать голоса на выборах в Мосгордуму. Мы это сделали и нашли кое-что странное [The mayor's office (by chance?) Allowed to decipher the votes in the elections to the Moscow City Duma. We did it and found something strange],” Meduza, September 13, 2019, https://meduza.io/slides/meriya-sluchayno-pozvolila-rasshifrovat-golosa-na-vyborah-v-mosgordumu-my-eto-sdelali-i-nashli-koe-chto-strannoe.

81 William A. Carter, *CSIS Election Cybersecurity Scorecard: The Outlook for 2018, 2020 and Beyond* (Washington, DC: CSIS, October 2018), https://www.csis.org/analysis/csis-election-cybersecurity-scorecard-outlook-2018-2020-and-beyond.

82 “Election Results Reporting: Risk and Mitigations,” CISA, n.d., https://www.cisa.gov/sites/default/files/publications/election_results_reporting_risk_mitigations_508.pdf.

83 Sunoo Park et al., “Going from Bad to Worse: From Internet Voting to Blockchain Voting,” *Journal of Cybersecurity* 7, no. 1 (2021), doi:10.1093/cybsec/tyaa025; David Jefferson, “The Myth of ‘Secure’ Blockchain Voting,” Verified Voting, October 3, 2018, https://verifiedvoting.org/the-myth-of-secure-blockchain-voting/;

and National Academies of Sciences, Engineering, and Medicine, *Securing the Vote: Protecting American Democracy* (Washington, DC: National Academies Press, 2018), doi:10.17226/25120/.

84 Drew Springall et al., “Security Analysis of the Estonian Internet Voting System,” Presented at CCS’14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, Arizona, November 3–7, 2014, 703–715, doi:10.1145/2660267.2660315; Thomas Haines, Sarah Jamie Lewis, Olivier Pereira, and Vanessa Teague, “How not to prove your election outcome,” 2020 IEEE Symposium on Security and Privacy (SP), 2020, 644–660, doi:10.1109/SP40000.2020.00048; and Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman, “Attacking the Washington, D.C. Internet Voting System,” in Keromytis A.D., eds., *Financial Cryptography and Data Security. FC 2012. Lecture Notes in Computer Science* 7397. (2012), doi:10.1007/978-3-642-32946-3_10.

85 Park et al., “Going from Bad to Worse”; Jefferson, “The Myth of ‘Secure’ Blockchain Voting”; National Academies of Sciences, Engineering, and Medicine, *Securing the Vote*; and Specter, Koppel, and Weitzner, “The Ballot is Busted Before the Blockchain.”

86 Specter, Koppel, and Weitzner, “The Ballot is Busted Before the Blockchain”; and “Voatz Security Assessment Volume I of II: Technical Findings,” Trail of Bits.

87 Park et al., “Going from Bad to Worse.”

88 Fowler, “Promises and Perils of Mobile Voting.”

89 Interview with Stanislav Andreychuk, Golos.

90 Burke, “Crypto Voting + US Elections.”

91 “Maduro-controlled ISP sabotages participation in Venezuelan opposition’s Consulta Popular,” Vesinfiltro, December 12, 2020, https://vesinfiltro.com/noticias/2020-12-07-consulta_popular_en/; and Ludmila Vinogradoff, “La aplicación para votar en la consulta popular de Guaidó, colapsada,” ABC Internacional, December 10, 2020, https://www.abc.es/internacional/abci-aplicacion-para-votar-consulta-popular-guaido-colapsada-202012100158_noticia.html.

92 “Significant Cyber Incidents,” CSIS, last updated September 2021, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

93 Vyjayanti T Desai, Anna Diofasi, and Jing Lu, “The global identification challenge: Who are the 1 billion people without proof of identity?,” World Bank, April 25, 2018, https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity.

94 “The principle of non-refoulement under international human rights law,” UN Office of High Commissioner on Human Rights, n.d., https://www.ohchr.org/Documents/Issues/Migration/GlobalCompactMigration/ThePrincipleNon-RefoulementUnderInternationalHumanRightsLaw.pdf.

95 Elisa Perrigueur, Vera Deleja- Hotko, Franziska Grillmeier, and Katy Fallon, “Prisons in paradise: Refugees detentions in Greece raise alarm,” Al Jazeera, October 22, 2021, https://www.aljazeera.com/news/2021/10/22/prisons-in-paradise.

96 Clara Long and Ariana Sawyer, “‘We Can’t Help You Here’ US Returns of Asylum Seekers to Mexico,” Human Rights Watch, July 2, 2019, https://www.hrw.org/report/2019/07/02/we-cant-help-you-here/us-returns-asylum-seekers-mexico#.

97 “Types of ID Systems,” World Bank, Identification for Development Practitioner’s Guide, n.d., https://id4d.worldbank.org/guide/types-id-systems.

98 Fennie Wang and Primavera De Filippi, “Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion,” *Frontiers in Blockchain 2* (January 2020), doi:10.3389/fbloc.2019.00028; and “Blockchain Identity Management: The Definitive Guide (2021 Update),” Tykn, May 19, 2021, https://tykn.tech/identity-management-blockchain/.

99 “Decentralized Identifiers (DIDs) v1.0,” W3C, August 3, 2021, https://www.w3.org/TR/did-core/.

100 Adam Piore, “Can Blockchain Finally Give Us The Digital Privacy We Deserve?,” Newsweek, February 22, 2019, https://www.newsweek.com/2019/03/08/can-blockchain-finally-give-us-digital-privacy-we-deserve-1340689.html; Greg McMullen, Primavera De Filippi, and Constance Choi, “Blockchain Identity Services: Technical Benchmark of Existing Identity Systems,” Blockchain Research Institute and Coalition of Automated Legal Applications, July 2019, https://app.hubspot.com/documents/5052729/view/68912918?accessId=6d30db.

101 “About iRespond,” iRespond, n.d., https://www.irespond.org/.

102 Adam Piore, “Can Blockchain Finally Give Us Digital Privacy We Deserve?,” Newsweek, February 22, 2019, https://www.newsweek.com/2019/03/08/can-blockchain-finally-give-us-digital-privacy-we-deserve-1340689.html.

103 Alex Andrade-Walz, “From stateless to self-sovereign: A project that gives life-long identity to the world’s invisibles beginning at birth,” Biometric Update, July 23, 2020, https://www.biometricupdate.com/202007/from-stateless-to-self-sovereign-a-project-that-gives-life-long-identity-to-the-worlds-invisibles-beginning-at-birth.

104 An example of one of these birth attestation credentials may be found at https://www.irespond.org/birthlink.

105 Interview with iRespond; “About iRespond,” iRespond; and Piore, “Can Blockchain Finally Give Us Digital Privacy We Deserve?”

106 Interview with iRespond.

107 Matthew Davie, “Kiva’s next frontier: Kiva Protocol,” Kiva, n.d., https://www.kiva.org/blog/kivas-next-frontier-kiva-protocol; and Wang and De Filippi, “Self-Sovereign Identity in a Globalized World.”

108 “Kiva Protocol FAQ,” Kiva, n.d., https://pages.kiva.org/kiva-protocol-faq.

109 Russ Juskalian, “Inside the Jordan refugee camp that runs on blockchain,” MIT Technology Review, April 12, 2018, https://www.technologyreview.com/2018/04/12/143410/inside-the-jordan-refugee-camp-that-runs-on-blockchain/; and Piore, “Can Blockchain Finally Give Us Digital Privacy We Deserve?”

110 For a prominent example of these risks, see “Equifax Data Breach,” Electronic Privacy Information Center, n.d., https://epic.org/privacy/data-breach/equifax/.

111 Aiden Slavin, Franziska Putz, and Emre Eren Korkmaz, *Digital Identity: An Analysis for the Humanitarian Sector* (Washington, DC: IFRC, May 2021), https://octd.co.uk/DIGID.pdf; and Emrys Schoemaker, Dina Baslan, Bryan Pon, and Nicola Dell, “Identity at the margins: data justice and refugee experiences with digital identity systems in Lebanon, Jordan, and Uganda,” *Information Technology for Development* 1 (July 2020), doi:10.1080/02681102.2020.1785826.

112 Adam Cooper et al., “ID2020 Technical Requirements: V1.0,” ID2020, n.d., https://id2020.org/uploads/files/Technical-Requirements.pdf; McMullen, De Felippi, and Choi, “Blockchain Identity Services”; Wang and De Filippi, “Self-Sovereign Identity in a Globalized World”; and Rhodri Davies, “Knowing Me, Knowing You: Self-Sovereign Digital Identity and the Future for Charities,” Chariteis Aid Foundation, July 21, 2017, https://www.cafonline.org/about-us/blog-home/giving-thought/the-future-of-doing-good/self-sovereign-digital-identity-and-the-future-of-charity.

113 Schoemaker et al., “Identity at the margins.”

114 Slavin, Putz, and Korkmaz, *Digital Identity*; Partnership for Maternal, Newborn & Child Health, “Digital Opportunities for Displaced Women, Children and Adolescents,” WHO, 2019, https://www.who.int/pmnch/media/news/2019/PMNCH-knowledge-brief-2.pdf?ua=1; Schoemaker et al. “Identity at the margins”; and Karthik Muralidharan, Paul Niehaus, and Sandip Sukhtankar, “Building State Capacity: Evidence

from Biometric Smartcards in India," *American Economic Review* 106, no. 10 (October 2016), doi:10.1257/aer.20141346.

115 "Building Blocks: Blockchain for Zero Hunger- Graduated Project," World Food Program, n.d., https://innovation.wfp.org/project/building-blocks.

116 "Exclusion by design: how national ID systems make social protection inaccessible to vulnerable populations," Privacy International, March 29, 2021, https://privacyinternational.org/long-read/4472/exclusion-design-how-national-id-systems-make-social-protection-inaccessiblle.

117 Rina Chandran, "Ten years on, India's biometric ID excludes homeless, transgender people," Reuters, November 26, 2019, https://www.reuters.com/article/us-india-tech-digitalid/ten-years-on-indias-biometric-id-excludes-homeless-transgender-people-idUSKBN1Y012X.

118 Vindu Goel, "Indian 'Big Brother' using fingerprint identification system for food, benefits and bank accounts," *The Independent*, April 10, 2018, https://www.independent.co.uk/news/world/asia/india-tech-fingerprint-eye-scan-id-food-benefits-bank-accounts-a8297391.html.

119 Lehr and Crumpler, *Facing the Risk: Part 2*.

120 Cooper et al., "ID2020 Technical Requirements: V1.0."

121 Elise Thomas, "Tagged, tracked and in danger: how the Rohingya got caught in the UN's risky biometric database," *Wired*, March 12, 2018, https://www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh; and Piore, "Can Blockchain Finally Give Us Digital Privacy We Deserve?"

122 Michael Kuperberg, Sebastian Kemper, and Cemil Durak, "Blockchain Usage for Government-issued electronic IDs: a Survey," in Henderick A. Proper and Janis Stirna, eds., *Advanced Information Systems Engineering Workshops. CAiSE 2019. Lecture Notes in Business Information Processing* 349 (May 2019), doi:10.1007/978-3-030-20948-3_14.

123 Michael Graglia, Christopher Mellon, and Tim Robustelli, "The Nail Finds a Hammer Self-Sovereign Identity, Design Principles, and Property Rights in the Developing World," New America, October 2018, https://d1y8sb8igg2f8e.cloudfront.net/documents/The_Nail_Finds_a_Hammer_2018-10-17_FINAL.pdf; and Slavin, Putz, and Korkmaz, *Digital Identity*.

124 Eileen Guo and Hikmat Noori, "This is the real story of the Afghan biometric databases abandoned to the Taliban," MIT Technology Review, August 30, 2021, https://www.technologyreview.com/2021/08/30/1033941/afghanistan-biometric-databases-us-military-40-data-points/.

125 Michael Pisa and Matt Juden, "Blockchain and Economic Development: Hype vs. Reality," Center for Global Development, July 2017, https://www.cgdev.org/sites/default/files/blockchain-and-economic-development-hype-vs-reality_0.pdf.

126 Slavin, Putz, and Korkmaz, *Digital Identity*.

127 Lucy Claridge et al., *Moving towards a Right to Land: The Committee on Economic, Social and Cultural Rights' Treatment of Land Rights as Human Rights* (London: Minority Rights Group International & University of East London Centre on Human Rights in Conflict, 2015), https://landportal.org/library/resources/movingtowardsarighttoland/moving-towards-right-land-committee-economic-social-and.

128 Roy L. Prosterman and Tim Hanstad, "Land Reform in the Twenty-First Century: New Challenges, New Responses," *Seattle Journal for Social Justice* 4, no. 2 (May 2006), https://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=1588&context=sjsj; and "For Up to 800 Million Rural Poor, a Strong World Bank Commitment to Agriculture," World Bank, November 12, 2014, https://www.worldbank.org/en/news/feature/2014/11/12/for-up-to-800-million-rural-poor-a-strong-world-bank-commitment-to-agriculture.

129 “Women in Half the World Still Denied Land, Property Rights Despite Laws,” World Bank, press release, March 25, 2019, https://www.worldbank.org/en/news/press-release/2019/03/25/women-in-half-the-world-still-denied-land-property-rights-despite-laws.

130 “Rural Women at Work,” ILO.

131 Michael Georg Link and Nils Muižnieks, “Roma evictions: Europe’s silent scandal,” openDemocracy, June 29, 2016, https://www.opendemocracy.net/en/can-europe-make-it/roma-evictions-europes-silent-scandal/; and Jeetendra P. Aryal and Stein T. Holden, “Cast Discrimination, Land Reforms and Land Market performance in Nepal,” Norwegian University of Life Sciences Centre for Land Tenure Studies, June 2011, http://www.umb.no/statisk/clts/papers/CLTS_WP1_2011.pdf; “After Long Struggle, Kenya’s Nubian Minority Secures Land Rights,” Open Society Justice Initiative, June 5, 2017, https://www.justiceinitiative.org/newsroom/after-long-struggle-kenyas-nubian-minority-secures-land-rights; and Laura Reiley, “Relief bill is most significant legislation for Black farmers since Civil Rights Act, experts say,” *Washington Post*, March 8, 2021, https://www.washingtonpost.com/business/2021/03/08/reparations-black-farmers-stimulus/.

132 Rights and Resources Initiative, *Who Owns the World’s Land? A global baseline of formally recognized indigenous and community land rights* (Washington, DC: RRI), https://rightsandresources.org/wp-content/uploads/GlobalBaseline_web.pdf.

133 Liz Alden Wily, “Customary Tenure: Remaking Property for the 21st Century,” in *Comparative Property Law: Global Perspectives*, edited by M. Graziadei and L. Smith (Cheltenham, UK: Edward Elgar, 2017), 458–78.

134 Laura Notess et al., *The Scramble for Land Rights: Reducing Inequity between Communities and Companies* (Washington, DC: World Resources Institute, 2018), https://files.wri.org/d8/s3fs-public/scramble-land-rights.pdf.

135 “Land Corruption,” Transparency International, n.d., https://www.transparency.org/en/our-priorities/land-corruption.

136 “Registering Property,” World Bank, Doing Business, 2020, https://www.doingbusiness.org/en/data/exploretopics/registering-property.

137 “საჯარო რეესტრის ეროვნული სააგენტო პირველი სახელმწიფო უწყებაა მსოფლიოში, რომელმაც საჯარო სერვისებში ბლოკჩეინის ტექნოლოგიის გამოყენება დაიწყო [The National Agency of Public Registry is the first government agency in the world to introduce the use of blockchain technology in public services],” Georgia National Agency of Public Registry, Facebook, November 16, 2021, https://www.facebook.com/watch/?v=566785837721738&ref=sharing.

138 Interview with Mariam Turashvili, Georgian National Agency of the Public Registry (NAPR).

139 Aanchal Anand, Matthew McKibbin, and Frank Pichel, “Colored Coins: Bitcoin, Blockchain, and Land Administration,” CADASTA, 2017, http://cadasta.org/resources/white-papers/bitcoin-blockchain-land/; J. Michael Graglia and Christopher Mellon, *Blockchain and Property in 2018: At the End of the Beginning* (Washington, DC: New America, March 2018), https://d1y8sb8igg2f8e.cloudfront.net/documents/Graglia_Mellon_blockchain.pdf.

140 Based on interviews with three blockchain providers in the land rights management sector.

141 Rohan Bennett, Todd Miller, Mark Pickering, and Al-Karim Kara, “Hybrid Approaches for Smart Contracts in Land Administration: Lessons from Three Blockchain Proofs-of-Concept,” *Land* 10, no. 2 (February 2021), 220, doi:10.3390/land10020220; and Kairos Future, *The Land Registry in the blockchain – testbed* (Stockholm: Kairos Future, March 2017), https://static1.squarespace.com/static/5e26f18cd5824c7138a9118b/t/5e3c35451c2cbb6170caa19e/1581004119677/Blockchain_Landregistry_Report_2017.pdf.

142 Anastasia Moloney, “Unclear land rights hinder Haiti's reconstruction,” Reuters, July 5, 2010, https://news.trust.org/item/20100705105000-axvt3/.

143 W. Curtis Preston, “Backup lessons from a cloud-storage disaster,” Network World, April 23, 2021, https://www.networkworld.com/article/3615678/backup-lessons-from-a-cloud-storage-disaster.html.

144 Claudia R. Williamson, “The Two Sides of de Soto: Property Rights, Land Titling, and Development,” in *Annual Proceedings of the Wealth and Well-Being of Nations*, Vol. 2, edited by Chamlee Wright (Beloit, Wisconsin: Beloit College Press, 2009-2010), http://www.claudiawilliamson.com/Claudia_Williamson/Research_files/Uptom_Williamson.pdf.

145 Anand, McKibbin, and Pichel, “Colored Coins.”

146 Olivier Acuna, “Colombia launches time-saving blockchain land registry pilot project,” Coin Rivet, August 2, 2018, https://coinrivet.com/colombia-launches-a-time-saving-blockchain-land-registry-pilot-project/; and Qiuyun Shang and Allison Price, “A blockchain-based land titling project in the republic of Georgia,” *Innovations: Technology, Governance, Globalization* 12, no. 1-2 (2018): 10–17, https://direct.mit.edu/itgg/article/12/1-2/10/9837/Blockchain-for-Global-Development.

147 Jacob Vos, Christiaan Lemmen, and Bert Beentjes, “Blockchain-Based Land Administration: Feasible, Illusory or a Panacae?,” paper at the 2017 World Bank Conference on Land and Poverty, World Bank, Washington, D.C., March 20–24, 2017, https://www.researchgate.net/profile/Christiaan-Lemmen/publication/316595854_Blockchain-based_Land_Administration_Feasible_Illusory_or_Panacae/links/590607d14585152d2e966dfc/Blockchain-based-Land-Administration-Feasible-Illusory-or-Panacae.pdf.

148 Olivier De Schutter, *Report of the Special Rapporteur on the right to food* (New York: UN General Assembly, August 2010), A/65/281, https://undocs.org/A/65/281.

149 For further discussion of this point, see: Benito Arruñada, “Blockchain’s Struggle to Deliver Interpersonal Exchange,” *Minnesota Journal of Law, Science & Technology* 19, no. 55 (2018): 56–103, https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1438&context=mjlst.

150 This would be accomplished through the use of multiple signature wallets, described here: Graglia and Mellon, “Blockchain and Property in 2018”; and Anand, McKibben, and Pichel, “Colored Coins.”

151 United Nations Human Rights Office of the High Commissioner, *Guiding Principles on Business and Human Rights* (New York: United Nations, 2011), https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf. The UN Human Rights B-Tech project provides further authoritative guidance on how the UNGPs can be implemented in the technology sector. See: “B-Tech Project,” UN OHCHR, n.d., https://www.ohchr.org/EN/Issues/Business/Pages/B-TechProject.aspx.

152 One representative set of questions that can be used to guide this assessment can be found at “Blockchain – Questions,” CivicSpace.tech, n.d., https://www.civicspace.tech/technologies/blockchain/#questions.

153 Cooper et al., “ID2020 Technical Requirements: V1.0”; World Bank, *Principles on Identification For Sustainable Development: Toward the Digital Age* (Washington, DC: August 2021), https://documents.worldbank.org/en/publication/documents-reports/documentdetail/213581486378184357/principles-on-identification-for-sustainable-development-toward-the-digital-age; Alexandrine Pirlot de Corbion et al., *The Humanitarian Metadata Problem - Doing No Harm in the Digital Era* (London, Privacy International & ICRC, December 2018), https://privacyinternational.org/report/2509/humanitarian-metadata-problem-doing-no-harm-digital-era; and Christopher Kuner and Massimo Marelli, eds., *Handbook on Data Protection in Humanitarian Action. International Committee of the Red Cross* (Washington, DC: ICRC, June 2020), https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

154 For more information on this topic, the UN OHCHR B-Tech Project has provided a series of foundational papers on access to remedy and the technology sector which can be accessed at https://www.ohchr.org/EN/Issues/Business/Pages/B-TechProject.aspx.

COVER PHOTO YOUR123/ADOBE STOCK

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**