Analyzing the Role of Blockchain Technology in Strengthening Democracies

By Noam Unger, Austin Hardman, and Ilya Timtchenko

Introduction

Rapid technological change has led to a global deluge of data. Certain aspects of shared information—authenticity, verification, speed, and integrity—are key to good governance and to helping democracies deliver for their citizens. Blockchain and other types of distributed ledger technology (DLT) offer potential benefits that institutions and governments can leverage in various ways to support democratic governance. Blockchain’s increasing use for identity management, land rights, citizen representation, the tracking of goods and services, and other uses necessitates deeper and broader understanding by U.S. foreign policy stakeholders. Given that U.S. foreign policy prioritizes strengthening democratic governance around the world, including through more inclusive access to services and greater transparency, accountability, and integrity in the public sphere, U.S. policymakers must seriously grapple with the opportunities and challenges associated with the increased integration of blockchain technology. Ukraine’s embrace of digitization and use cases for blockchain offer helpful insights into how and in which contexts this technology may be applied.

Whenever there is a lack of transparency in elections, government transactions, bureaucratic systems, and media, there is an opportunity for corruption to ensue, diluting citizens’ trust in democratic institutions. Certain technological advancements can potentially be a valuable tool for increasing the transparency and accountability of democracies. One such innovative tool is blockchain, a form of DLT that allows a group of users to cooperatively maintain a record of transactions.

Blockchain is often associated with the use case of cryptocurrency, but it can be applied to other domains to track both tangible and intangible goods and transactions. Blockchain is a form of tamper-resistant DLT that ensures that all transactions are recorded and validated. This technology
achieves extraordinary levels of data integrity for information once it is loaded into the shared ledger. Essentially, the movement or transfer of anything of value can be logged and verified, instilling trust and confidence by raising the costs of malicious activity during that process. This opens the technology to a wide range of applications. Within governance and democratic strengthening efforts, blockchain has recently been introduced in various places to increase government accountability, combat misinformation, reduce costs and the mishandling of data, and quickly trace financial transactions.

Box 1: What Is Blockchain?

**Distributed ledger technology** (DLT) describes a category of technologies that enables the storage of data within and transfer between multiple data stores. Network participants share this ledger of transactions, allowing for synchronized data recording with no central storage hub. Instead, peer-to-peer transmission takes place, recording the same information across many devices. The “ledger” is stored across multiple locations and is visible to all parties.

Blockchain is **not singular in design**. It can be classified into different types based on which access and governance models are used. The two main categories are private and public blockchains. Private blockchains restrict access to a specific group of participants, while public blockchains allow anyone to join, build, and use applications on the network. Within each of these categories, there are also permissioned and permissionless blockchains. Permissioned blockchains require participants to have explicit permission to host infrastructure and validate network transactions, whereas permissionless blockchains allow anyone to be a validator.

Blockchains that are public and permissioned offer several advantages. They can provide high performance and scalability, processing thousands of transactions per second, and can ensure fast and secure transaction finality. Permissioned governance that provides security, efficiency, and visibility into who is involved in decisionmaking processes and network operation can be combined with public accessibility to all citizens, making the technology a compelling choice for many applications.

While blockchain and DLT have the capability to help address global challenges and strengthen democratic institutions, the innovative applications of blockchain are still in early stages and not fully understood by key stakeholders in Washington. The United States and its strategic partners must assess and play a role in shaping the next innovative applications of blockchain technology before the opportunity passes. In some respects, China is already possibly years ahead of the United States and many other countries in applying this rapidly evolving technology. Users of the **digitized Chinese yuan** number over 120 million in China (although **conflicting reporting** creates some doubt about how widely this currency is actually being used). To create a regulatory and policy environment in which the implementation of DLT strengthens democracy without compromising privacy or muzzling technological innovation, policymakers need a comprehensive understanding of the opportunities as well as the **limitations** on where and how this technology can be most readily and helpfully adopted. The strategic application of blockchain technology in certain scenarios can enhance trust and better protect information, but implementers must also be mindful of the technology’s shortcomings and challenges.
The United States and its strategic partners must assess and play a role in shaping the next innovative applications of blockchain technology before the opportunity passes.

Blockchain and Democracy

Democratic backsliding around the world should be a concern for democracies everywhere. Democracy is in a worldwide recession in terms of both quality and prevalence, the causes of which are contested. The cornerstones of flourishing democracies, however, are widely agreed upon and include free and fair elections; a free press; individual rights; economic, political, and religious freedom; and a rule of law equally applied. Governments and societies grappling with how best to support and strengthen democracies should assess how technologies such as blockchain can be applied as practical tools to uphold these foundational principles. The applications may vary considerably, as demonstrated by the following non-exhaustive examples.

PROTECTING DIGITIZED GOVERNMENT DOCUMENTS

Identity is inextricably intertwined with democracy. There are clear incentives for all governments, democratic or otherwise, to provide their citizens with means of unique identification, such as for the delivery of key services and benefits. Democracies have a special interest in ensuring individuals’ identities are protected so that the rights and privileges guaranteed to those individuals can be preserved. For example, government-issued identification is a key ingredient for voting, a core democratic responsibility. Likewise, passports assign unique “international standard serial numbers” which allow customs officials to quickly verify identity and citizenship as well as which travel privileges may apply to an individual. Government agencies such as the U.S. Social Security Administration assign identifiers to help administer medical benefits, financial aid, and other social services and benefits.

Worldwide, nearly 1 billion people have no proof of legal identity and are excluded from services and the formal economy. Digital identity can serve to close this “identity gap” by helping deliver immutable and easily accessible identification to those lacking verifiable identity documents, as well as by strengthening the resiliency of existing paper identification. During natural disasters, conflicts, and other crises, citizens may not have the time or ability to grab their paper government documentation, which is necessary to freely move and receive services. DLT’s ability to safely guard such digitized information could alleviate the difficulty of attempting to verify a person’s identity during hectic scenarios in which physical documents are destroyed or inaccessible. Governments could be better equipped to manage refugee crises and natural disasters and administer standard social services, while individuals could have more control of their data. An important factor in realizing this vision entails working toward applications of digital identity systems that empower people rather than surveil and exclude them.

SECURING LAND REGISTRATION

Land title registries track the ownership of land and property for a given region. The efficient registration of land is an essential component of ensuring property rights, a backbone of any free society. Land registration poses another set of government records for which an agency could
maintain a blockchain to improve efficiency and ensure the quality of data storage and transfers. Some countries are already experiencing positive results from deploying DLT in the land registration process. For Georgia, the collapse of the Soviet Union and persistent corruption during early independence caused many property disputes. In response, Georgia was an early adopter of blockchain-based land registration, registering more than 1.5 million land titles in 2018. The Georgian government was able to provide citizens with digital certificates, legitimizing ownership with a timestamp and other cryptographic proof in under three minutes. Importantly, blockchain may help streamline the land registration process, but oversight is still critical to ensure the initial integrity of the data.

Similar technology can be applied to other asset registrations and government services. For example, the private sector uses blockchain technology to track the shipment of goods and monitor supply chains. Likewise, government agencies have the potential to reduce labor costs and waste by incorporating blockchain in some types of foreign aid delivery and monitoring, the tracking of welfare funds, and the registration of voters, vehicles, and intellectual property.

**FACILITATING FAST AND DIRECT FINANCIAL TRANSFERS AND OTHER ECONOMIC APPLICATIONS**

The financial services industry is already advancing applications of blockchain technology. Blockchain’s peer-to-peer system has enabled the excision of some intermediaries, instantaneous processing, and the elimination of fees when sending money anywhere in the world. Blockchain technology is not a digital currency, but it is highly associated with digital currencies because decentralized cryptocurrencies such as Bitcoin function using blockchain.

Yet cryptocurrency is only a small subset of how blockchain can be and is being used by governments and financial institutions globally. For example, stablecoins, as the name suggests, attempt to provide a stable value by pegging their worth to a real-world “reference” asset such as the U.S. dollar. They can be used to pay for goods and services while benefiting from the low transaction costs of some blockchains. Blockchain technology has also induced the majority of the world’s governments to actively explore managing their national currencies by incorporating central bank digital currencies, with China, Sweden, and others actively exploring their use.

**Cryptocurrency is only a small subset of how blockchain can be and is being used by governments and financial institutions globally.**

There are also other applications for blockchain in the realm of financial inclusion. Pilot projects in the Global South are looking into how blockchain can be used to issue insurance policies, administer payouts to farmers, close credit gaps, and provide a way to save for those who do not have a savings account. For example, moving money is often made expensive due to bank fees. Leaf, a Rwandan-based project, uses blockchain to enable money transfers without banking fees. The Leaf wallet uses the public Stellar blockchain to help people send, save, and transfer money directly from their mobile phone without the need for personal banking history or in-depth financial literacy. Likewise, smart contracts are being used to carry out insurance agreements with African farmers to protect their livelihoods during extreme weather. If a predetermined amount of rain is recorded within 24 hours in the insured farmer’s region, which can result in destruction of crops, the farmer will receive an automated payment. Blockchain
technology is increasingly being incorporated into specific finance-related applications while also helping to create **global networks of interoperable financial systems**.

**CONTENDING WITH A PROLIFERATION OF DEEPFAKES**

In a rapidly approaching future with generative artificial intelligence and pervasive deepfake technology, it will be imperative for both governments and private consumers of information to be able to discern what is credible. In many respects, this eventuality has already arrived. The health of democracies is uniquely reliant on an informed citizenry. The intentional dissemination of false information, such as propaganda from authoritarian nations and extremist organizations, often aims to obfuscate reality. The need for verifiable information and data is additionally intensified amid the fog of war, when manipulative information operations are pervasive and the accuracy of situational understanding can be a matter of life and death.

The use of emerging technologies by state actors for strategic disinformation campaigns is a national security issue. For this reason, the United States adopted its **first federal laws** related to deepfakes in 2019. The FY 2020 **National Defense Authorization Act** (NDAA) required a report on the weaponization of deepfake technology by foreign entities and established a competition with a $5 million prize to stimulate research on machine-manipulated media. Such efforts are not preventative but merely raise awareness of the issue at hand. Beyond increasing awareness, InterAction's **Disinformation Toolkit 2.0** notes how some internationally focused organizations are exposing disinformation campaigns, conducting forensic analyses, coordinating with technology companies, providing digital literacy training, and collaborating with global policymakers. This landscape of mounting policy attention and analysis related to disinformation and deepfakes shapes the context in which applications of blockchain technology are finding their footing.

DLT may offer opportunities to counteract the nefarious aims of certain categories of deepfakes. **The Starling Lab for Data Integrity** is experimenting with innovative applications of blockchain technology and decentralized systems of storage to bolster trust in digital media. The persistence and safety of digital ledgers support the creation of more trustworthy digital assets where details are corroborated by independent third parties acting as notaries public. Decentralized storage pools can guarantee the safekeeping of information for the long term.

News agencies are beginning to **explore** applications for DLT to better record their reporting and make data, such as the location and date of photographs, permanently accessible. **Reuters**, for example, has partnered with Canon to develop a professional camera and in-house workflow for photojournalists that freezes and stamps the pixels of a picture the moment a photo is snapped and then registers the photo and corresponding details onto a public blockchain. Especially considering **Russia's propaganda campaigns** against Ukraine, blockchain's potential to verify what information has been altered could be instrumental as authoritarians increasingly deploy **gray zone** tactics that rely on manipulating the information environment. This verification of alterations only applies to information once it has been stored in a blockchain and cannot account for manipulation prior to that point.

**ADVANCING JUSTICE AND THE RULE OF LAW**

A transparent judicial system is key to the rule of law that undergirds functioning democracies. DLT's capturing, storing, and verifying of data could be used to better **manage court judgments, warrants,**
and criminal histories. Researchers are exploring blockchain's ability to corroborate data on several systems as a tool for preserving evidence. The United Kingdom's Ministry of Justice proposed using DLT to preserve and protect mass quantities of body camera footage to be used in court. Similar applications could be useful for international courts and other human rights watchdogs.

The recent hacking of the computer systems of the International Criminal Court (ICC) raises concerns over the safety of centrally located data that could later be used to prosecute the most serious of crimes. The use of blockchain to store and verify data related to war crimes and atrocities aims to assist the courts by providing more trusted and tamper-resistant data for associated proceedings. Governments or other entities seeking to achieve accountability for large-scale human right abuses or wartime atrocities for the purposes of transitional justice may particularly benefit from the use of blockchain to ensure evidence has not been manipulated and to support chain of custody for documentation of abuse.

Additionally, “smart contracts,” which automate transactions once the coded conditions are met, could help judicial systems by minimizing disputes, alleviating stress on courts, and making business and government services more efficient.

ELEVATING CITIZEN REPRESENTATION AND VOICE

According to a 2021 CSIS report, blockchain-based voting systems hold some potential benefits for securing elections, though they also present a range of risks. Generally speaking, blockchain could reduce the risk of election tampering, as such a system would require the collusion of multiple major entities to alter recorded ballots. There may also be potential for the use of blockchain to further augment trust in mobile and internet voting, which can, in turn, result in greater turnout and reduce voter error. Blockchain-backed e-voting could additionally enhance the physical safety of voters and remove certain types of voter coercion associated with in-person polling, although coercion in private settings can also pose a significant problem. Election transparency may be another benefit, as civil society groups could monitor the election results if granted access to the blockchain network and armed with the requisite technical knowledge to understand it. The transparency associated with blockchains also needs to be balanced with privacy rights associated with voters’ abilities to keep their individual voting selection secret. Further possible advantages include stronger resiliency against network disruptions compared to other internet voting schemes, more secure voter registries, and timely election night reporting systems.

While there have not been many pilot projects related to blockchain voting, the Voatz mobile blockchain voting system, used during the 2018 U.S. midterm elections in West Virginia, for example, may have contributed to higher voter turnout on the scale of 3 to 5 percentage points. However, other studies have demonstrated the opposite. For example, in Belgium a similar pilot project resulted in a slightly negative effect on voter turnout. As uses of blockchain expand, there is also increased attention to theoretical applications of blockchain to voting. For example, the concept of liquid democracy, a modern and flexible approach to direct democracy with implications for referendums, voting proxies, and mass-scale voting, could be propelled by blockchain to help verify that votes cast are the same as votes counted.

One key challenge is that although blockchain may help with the prevention of some ballot tampering, election systems and platforms are still dependent on other hardware and software that may make
them vulnerable to exploitation that is **difficult or even impossible** to control. Therefore, at a fundamental level, blockchain is not a silver bullet for solving the insecurity of online voting.

**The Ukrainian Context**

Ukraine, sitting at the cutting edge of the digital revolution, offers a unique context that is experimenting in the digital and blockchain space.

**TECHNOLOGICAL READINESS**

Ukraine’s information and communications technology (ICT) industry was immensely successful before Russia’s full-scale invasion in February 2022, with some dubbing it the “**emerging tiger of Europe**.” In fact, despite challenges posed by the war, it is the only sector of the Ukrainian economy that has grown amid the conflict, exhibiting growing **export** volumes from 2021 to 2022. The Ukrainian government has also proactively **not drafted IT workers** as soldiers and has extended tax breaks to small and medium-sized businesses in the industry. These measures have allowed ICT businesses to stay solvent and continue operating and exporting services. The challenges Ukraine is facing are in many ways unique, but this also means that it can serve as a breeding ground for unique innovations. Equipped with over 200,000 skilled IT workers and the demand for creative solutions due to the war, Ukraine is primed to rapidly test technologies.

Ukraine demonstrated its technological adaptability with the embrace of cryptocurrency in early fundraising efforts when banks lacked liquidity following Russia’s full-scale invasion. **MoneyGram** halted payments to Ukraine until it could confirm its banking partners in the country were operational. The Ukrainian government, ranked fourth **globally** for cryptocurrency adoption, began publicly soliciting **cryptocurrency** donations online days after the invasion. Cryptocurrency’s capability to facilitate transactions instantly across borders was attractive for the nation as it entered total war. At least **20 million** dollars in cryptocurrency were deposited directly to the Ukrainian government in the first months of the war.

Ukraine had more **mobile phone subscriptions than people in 2020**, but the war has damaged the digital infrastructure necessary for mobile subscriptions to be operable. Since Russia’s invasion, more than **4,000 Ukrainian telecommunication stations** have been seized or destroyed and over **60,000 kilometers** of fiber-optic lines have been compromised. The restoration of many lost towers can be attributed to the bravery of Ukrainian telecommunication workers. The public-private partnership between the Department of Defense and SpaceX’s Starlink has enabled battlefield communications at the cost of approximately **$20 million per month**. Without investments in digital infrastructure, all digital solutions, including those involving blockchain, are futile.

**COMMITMENT TO DIGITIZATION**

Digitization is synonymous with resiliency, a characteristic often ascribed to Ukraine in its battle against Russia. Prior to the war, Ukraine committed to going paperless in September 2021 with a bill **prohibiting officials from requiring paper documents**. The bill was the latest advancement in digitization following the successful experimentation with electronic identification cards and international passports by the application **Diia**. Ukraine had issued **nearly a million biometric travel passports** to Ukrainian citizens in the Russian-controlled Donbas region before the war. **Diia**, a premier government
application used by half of Ukraine’s population, offers an expanding list of digital documents, including identification cards, driver’s licenses, and Covid-19 vaccination certificates. In a unique blend of entertainment and education, Diia has trained almost 1.5 million citizens in digital skills through over 90 free-to-access educational series based on European standards. Given the wartime reliance on social services, digitization efforts have accelerated since the war’s outbreak. Kostiantyn Kosheленко, deputy minister of social policy for digital transformation, recently expressed his commitment to making government services more resilient and client oriented. Applying to be a candidate for child adoption, for example, is now an online government service in Ukraine. The Ministry of Digital Transformation’s mission to “move 100% of government services online” is a core element of Ukraine’s war strategy and a key ingredient for large-scale utilization of blockchain-enabled applications.

APPLICATIONS OF BLOCKCHAIN
Supported by a government that has trumpeted digitization as critical to the country’s future, Ukraine and its partners have combined blockchain technology and photogrammetry to counter disinformation and to document and preserve evidence of Russian war crimes. E-Enemy, for example, is a government-built app that allows users to photograph and geolocate any attacks, thereby providing a first-person perspective of atrocities for posterity and eliminating the potency of deepfakes. War crimes investigators can then “hash” data on war crimes, thereby enabling future prosecution of these heinous acts. Starling Lab, a joint Stanford University–USC Shoah Foundation research center, in partnership with social enterprise Hala Systems, has been preserving possible evidence of Russia’s war crimes in Ukraine via a cryptographic dossier. The aforementioned hacking of the ICC combined with Russia’s espionage efforts to covertly infiltrate the court hint at the urgent need to ensure greater protection for evidence of war crimes.

Ukraine’s president Volodymyr Zelensky himself has noted the importance of digitizing all accounting of military supplies, an effort that could potentially benefit from blockchain technology. Furthermore, the UN Refugee Agency was awarded the Best Impact Project Award during the 2023 Paris Blockchain Week for a pilot project in Ukraine where it used blockchain to provide financial assistance to displaced people; this assistance could be converted into cash and used for rent, food, utilities, and medical expenses.

PROPERTY REGISTRATION AND BLOCKCHAIN
Digital solutions for Ukraine’s economic modernization and resilience go beyond the more obvious war effort. Some of the first Ukrainian pilot projects using blockchain were electronic land auctions. In May 2017, the Cabinet of Ministers of Ukraine formally agreed to implement blockchain to help manage the State Register of Property Rights on Real Estate as well as the System of Electronic Trading in Arrested Property. A complaint of foreign investors is that land ownership is still not a possibility in Ukraine given current laws. Legal reform is needed to change this reality, and there is an argument that Kyiv should amend its laws to inspire foreign investors to participate in the country’s economic recovery. This demand may incentivize the Ukrainian government to further explore incorporating blockchain technology in land registration.

Additional Considerations and Challenges
Despite the benefits of blockchain for advancing democratic institutions, the technology is clearly a neutral tool and can be used by good actors as well as malign ones. There are some underlying concerns regarding the risks that DLT systems pose for democracy.
MALIGN FOREIGN ACTIVITY

Foreign actors are known to use blockchain technology for adversarial activity against the United States and its partners. For example, Russia has attempted to use the anonymity associated with some cryptocurrencies to bypass sanctions. The terrorist organization Hamas and two other militant groups–Palestinian Islamic Jihad and Hezbollah–have also used cryptocurrency to evade sanctions in order to raise funds for their notorious terrorist attacks. Hamas and Palestinian Islamic Jihad raised more than $100 million via cryptocurrency between August 2021 and June 2023.

It is not clear, however, how much longer cryptocurrency will be thought of as a safe haven for illicit behavior since Bitcoin and other cryptocurrencies are more traceable than other forms of payment. Investigators have been able to quickly identify and prosecute criminal activity through logged cryptocurrency transactions. For example, within days of the Hamas attack on Israel on October 7, 2023, the U.S. Treasury sanctioned two senior Hamas officials along with cryptocurrency exchange Buy Cash Money and Money Transfer Company, as well as six other individuals involved in the financial operation to fund terrorism. Additionally, the arrest of the perpetrators behind the 2016 Bitfinex hack, in which 119,754 bitcoins were stolen, was only possible, in large part, thanks to the immutable ledger that undergirds Bitcoin. (It is important to note, however, that blockchain's traceability is irrelevant without oversight.)

ACCESSIBILITY

The accessibility of blockchain technology to the public is also a concern. Whether due to lack of technological familiarity, high expenses, or lack of the necessary equipment to facilitate participation, many communities across the globe are not in a position to use blockchain, which in turn limits democratic participation via DLT systems. Citizens need smartphones and reliable internet access to participate. Digital literacy is another aspect of the divide preventing massive rollout of blockchain-backed government solutions, as technology often faces obstacles to adoption and may be cumbersome, particularly for those who lack digital skills. Tech companies and government entities should collaborate to ensure that such tools are accessible and user friendly. The barrier of entry for users must be lowered before scaling is possible.

LACK OF ACCOUNTABILITY AND SELECTIVE DATA

Without proper reform, blockchain runs the risk of merely reinforcing the status quo. What prevents corrupt regimes from allowing only state-approved, potentially faulty information to be entered onto a blockchain? Is blockchain the next tool to be used by oppressive regimes to fabricate transparent democracy? For example, since 2018, China has permitted the use of blockchain-stored evidence in the country's courts, which may actually be a worrying development given the fact that China, an authoritarian regime, can be very selective with which data to store.

ENERGY CONSUMPTION

Blockchain technology traditionally has had a reputation of being highly energy intensive. Though there has been some progress on this front—and the high energy use is mainly attributed to cryptocurrency—there remain environmental concerns regarding the technology due to its carbon footprint as well as the affordability of energy in specific communities. However, there is hope that the technology will become more efficient, based on analysis showing that with different technological design options, digital currencies can be configured in a manner that is more energy efficient than popular current payment systems like credit and debit cards.
Conclusion

As the world increasingly overflows with data, U.S. policymakers should consider how to best utilize blockchain and other types of DLT to support democratic governance, including identity management, land rights, and the tracking of goods and services. If U.S. lawmakers do not take greater steps to shape the policy and regulatory environment for blockchain-related activity, there is also a risk of damage to U.S. competitiveness. Policymakers should explore new ways democracies can preserve and advance their principles while more efficiently delivering basic government services. At the same time, blockchain must be viewed neither as a panacea nor as solely an instrument of cryptocurrencies. It is a tool that offers intriguing applications for social and governmental progress.

Before proceeding with policy decisions related to blockchain technology, Congress should be equipped with knowledge of how exactly the technology can be applied (or misapplied), and make sure that the populations who are meant to benefit from these technologies are also fluent in their use and have access to the necessary digital public infrastructure. This will allow lawmakers to create a broader system and approach in dealing with DLT so that its benefits can be instrumentalized in service of democratic governance.

Noam Unger is a senior fellow with the Project on Prosperity and Development and serves as the director of the Sustainable Development and Resilience Initiative at the Center for Strategic and International Studies (CSIS) in Washington, D.C. Austin Hardman is a research assistant with the Project on Prosperity and Development at CSIS. Ilya Timtchenko is an intern with the Project on Prosperity and Development at CSIS.

The authors would like to thank Jed Devillers for his research support.

While the authors assume sole responsibility for the content of this white paper, they would like to thank the following individuals who participated in the roundtable discussion on this matter and/or assisted by providing their comments on earlier drafts: Aubra Anthony, Romina Bandura, Jason Brett, Paul Brigner, Jen Brody, Steve Feldstein, Marti Flacks, Adam Fivenson, Andrew Gastwirth, Dave Grimaldi, Zenobia Godschalk, Carole House, David Houston, Katie LaRoque, Shin’ichiro Matsuo, Jim Mazzarella, Brett McDowell, Monique Morrow, Shyam Nagarajan, Caroline Pham, Nilmini Rubin, Max Semenchuk, Basile Simon, Alex Tiersky, and Tomicah Tillemann.

This report was made possible by project support provided by Hedera Hashgraph via Swirlds Labs and was informed by an associated roundtable of experts held on October 3, 2023.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

© 2023 by the Center for Strategic and International Studies. All rights reserved.