REASSESSING EXPECTATIONS FOR BLOCKCHAIN AND DEVELOPMENT

MICHAEL PISA

Growing interest in whether and how blockchain technology can help address a variety of social and economic challenges has given rise to a community of thinkers, innovators, and policymakers who are exploring the potential social impact of the technology and its implications for development.

On one level, things are happening quickly in this space. Over the last two years, the largest development organizations have begun to examine how using the technology might help them meet their goals. This includes the World Bank, which established a Blockchain Lab in 2017; the United Nations, which reports that 15 UN entities are carrying out blockchain initiatives; the Inter-American Development Bank, which is exploring the use of blockchain as a platform for asset registries; and USAID, which recently published a primer on the topic.[1.] Several nonprofit humanitarian organizations are also evaluating blockchain as a potential platform for aid distribution and for developing their own proofs-of-concept. This is all happening as the number of startups pitching ideas continues to grow and distributed ledger models continue to evolve.

Despite these advances, however, the number of pilot projects underway remains quite small. While this could be just a matter of timing—many of the organizations mentioned above are now reviewing project proposals—it may also reflect hurdles to implementation that have received insufficient attention.

Given that blockchain technology is still in an early stage of development, it makes sense that most discussions about its use have focused on its potential rather than on obstacles. Too often, however, boosters of the technology have overstat-

ed its capabilities and failed to consider obstacles to its adoption. This imbalance has led to unrealistic expectations about what blockchain solutions can do, how easy they will be to implement, and how quickly they can scale, if at all. The result has been a widening gap between expectations and reality that has naturally led to growing skepticism about blockchain.

The best way to address these doubts is to take them head on and to rebalance the conversation away from starry-eyed accounts of the technology's promise and toward the obstacles that are likely to slow its implementation and the steps that must be taken to overcome them.

This brief essay explores a key but often overlooked hurdle to using blockchain solutions, which is the complexity that decentralized solutions necessarily introduce. The benefits of such solutions at times appear to exceed the added cost of complexity, but often they do not. With this tradeoff in mind, the paper considers two use cases, digital ID and healthcare supply-chain management. The paper also suggests how the development community can shift the conversation in a more useful direction.

UNDERSTANDABLE EXCITEMENT LEADS TO UNREALISTIC EXPECTATIONS

Enthusiasm over the potential of blockchain technology to address a wide variety of social and economic challenges is largely based on the notion that it allows for "trustless collaboration." This widely held view is captured in a recent report published by the United Nations Development Program and the company Blockchain, which states that "the decentralized, transparent, verifiable nature of [blockchain] means we can trust people and organizations precisely because trust is no longer an issue."[2.]

The notion that blockchain technology can be a substitute for trustful relationships is, in most cases, misguided. By solving the "double spend," problem, which occurs when the same unit of currency is used in more than one transaction, the original blockchain outlined by Satoshi Nakamoto in 2008 removed the

ABOUT THE AUTHORS

Mike Pisa is a Policy Fellow at the Center for Global Development, where his work focuses on how digitalization is shaping economic development, and how policymakers can maximize the benefits and minimize the risks associated with the adoption of new technologies. Prior to joining CGD, Pisa spent eight years at the U.S. Treasury Department working in a variety of roles, including Senior Advisor to the Under Secretary for International Affairs, Deputy Director of Treasury's Office of International Banking, and acting U.S. Financial Attaché in Afghanistan from 2009 to 2011. Pisa received a PhD in political science from the University of California, San Diego.

need to rely on trusted intermediaries to oversee the transaction of digital assets. However, when the problems we want to solve involve changes in the real "off-chain" world, the need for human agency, and therefore trust, remains.[3] For example, creating a blockchain-based land registry does not remove the need to trust the bureaucrats who upload land titles because, like all databases, blockchain does nothing to improve the reliability of inputs. At best the technology can enhance trust in some relationships by increasing the transparency and immutability of transactions and records.

It is also important to recognize that, while early excitement about blockchain focused on the transformative potential of public, permissionless networks like Bitcoin and Ethereum, interest and investment have shifted strongly toward permissioned ledgers in which only verified parties can participate. These closed networks are much more likely to help centralized actors achieve efficiency gains than they are to lead to their displacement.

THE COST OF COMPLEXITY

As noted above, much of blockchain's appeal rests on the often mistaken notion that it can eliminate the need to rely on trusted third parties. Yet even when the assumption holds, moving from a centralized to a decentralized solution always comes at the cost of added complexity.

This increased complexity can take different forms. At the most basic level, moving from a system in which a single actor verifies who owns what to one in which many actors share this responsibility requires using a consensus protocol, even the most efficient of which adds delay.

Likewise, moving from a system in which a trusted third party stores data in a centralized "silo" to one in which data is stored on a distributed network often requires adding layers of encryption to control who can see what. While some of these encryption approaches are no more complex than those used by centralized databases, others, like those that rely on zero-knowledge proofs, are more computationally intensive.[4] In addition, the cost of permanently storing documents on an ever-growing blockchain will inevitably force organizations to develop off-chain storage solutions, which will further complicate how data are managed and secured.

Additional layers of complexity may be required, depending on the use case. For example, using blockchain as a platform for digital identification raises the question of how individuals manage their private keys.

Perhaps the biggest challenges raised by shifting from centralized to decentralized models relate to legal and regulatory considerations. In the first instance, companies interested in using the technology must determine how they can comply (if at all) with existing data security and privacy laws. In the second, policymakers must consider whether to change existing laws to facilitate the use of decentralized models. As Graglia and Mellon note, "blockchain is unusual in that it is a social technology, designed to govern the behavior of groups of people through social and financial incentives. It is therefore inherently political."[5] For that reason, developing reforms aimed at supporting decentralized approaches could take a significant amount of time and be contentious.

Whether the benefits of using a decentralized model exceed the added cost of complexity ultimately depends on the use case in question. In recent years, a variety of decision models have been created to help guide the process of weighing these tradeoffs (a recent iteration is pre-

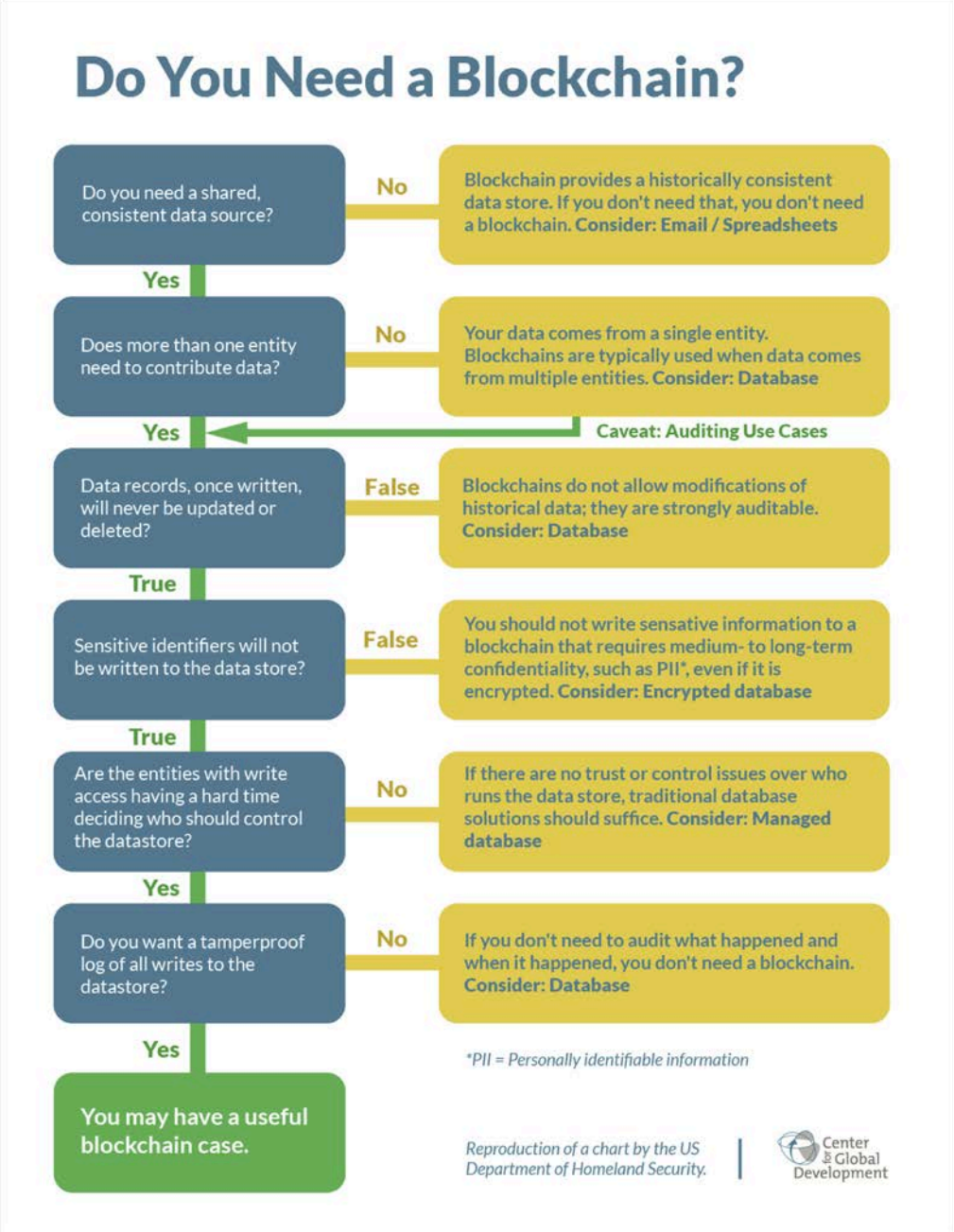

Figure 1. DHS S&T Security and Privacy Lessons Learned: Most Organizations Don't Need a Blockchain

Source: The United States Department of Homeland Security

sented in Figure 1).[6] In general, these models suggest that, in the vast majority of cases, organizations are better off using simpler (i.e., centralized) database models. Below we explore two development use cases through this tradeoffs lens.

Use Case #1: Providing a Platform for Refugee IDs

Roughly 1.1 billion people, or 1 in every 7 in the world, lack proof of their legal identity. This problem disproportionately affects children and women from rural areas in Africa and Asia, and is even more acute for the world's more than 21 million refugees.[7] Without legal identification, it can be difficult to access health and education services, open a bank account, get a loan, and vote.[8] Governments also have become increasingly interested in providing digital legal IDs, as recent advances in technology have made it easier to do so and the share of business conducted online grows.

At the same time, there is growing concern worldwide about the vulnerabilities associated with the storage and use of personal data by governments and companies. Many believe that both problems could be solved by using a self-sovereign identity (SSI) approach to identification. This model aims to shift control to individuals by allowing them to "store their own identity data on their own devices, and provide it efficiently to those who need to validate it, without relying on a central repository of identity data."[9] Until recently, such a solution was technically infeasible; blockchain technology appears to make it possible.

There is great interest in the development community about whether the SSI model could help to improve the lives of the world's poorest, with some even suggesting that it could help relieve the migrant crisis.[10] Some of the organizations now exploring the technology's potential to this end include Microsoft, Accenture, UNHCR, and ID2020.[11,12]

Under the generic SSI model, some individuals use a digital wallet on a blockchain to store certifications from trusted authorities (e.g., banks, credit-rating agencies, hospitals, passport authorities) who assert that the individual possesses certain attributes. For example, each person could store the following certified claims in her wallet: "credit rating over 700," certified by a credit rating agency; "is over 21," certified by a government; "has blood type B," certified by a hospital. When the user must prove that she has certain attributes to service providers (e.g., when she must prove that she is older than 21 to enter a bar or that she has a credit rating above 700 to obtain a loan), she can share them without sharing any additional personal information.

Storing verified claims on a blockchain has several potential benefits for users. The first is control: SSI could enable a person to manage both whom she shares her personal information with and how much information she shares. Such a system could also be more convenient, since it could allow people to provide verified information with the touch of a button rather than having to access and submit a wide variety of documents. Finally, the near-impossibility of tampering with records on a blockchain could provide greater confidence about their authenticity.

Proponents of the model cite several ways that SSI models could improve refugees' well-being. First, storing identification documents and important records on a blockchain could make it easier for refugees to verify their identity and obtain appropriate services if they relocate (e.g., a refugee who can provide a trusted immunization record could avoid being given the same vaccines in a differ-

ent camp).[13.] Using an SSI model could also allow refugees who are unable to obtain a government ID to build a composite identity through multiple claims. They also could use their digital wallet to store a history of their economic transactions, which would allow them to develop a credit history that could be used to access financing.

While these features are promising, the model also has serious limitations. Most importantly, because the SSI approach continues to rely on trusted third parties to provide the certifications stored in each person's digital wallet and to store the data on which those claims are based, it can do nothing to solve the core challenge of providing foundational IDs. In addition, the portability of IDs generated and stored on a blockchain depends entirely on how many organizations (either on or off the network) are willing accept them. For that reason, getting multiple governments and development organizations to agree on a single SSI approach is a prerequisite to developing an effective model.

The SSI model also introduces complexities that may make it difficult to scale, including challenges related to key management. Since a user's identity is tied to her private/public key pair, a person who loses a key will need to start the identity proofing process from scratch to reestablish their digital identity.[14.] The irrevocability of data stored on the blockchain also raises concerns about data privacy, which is crucial when dealing with refugees, who often are politically persecuted. It is therefore important for software developers creating ID solutions to take a "privacy by design" approach.[15.]

In sum, while excitement about the SSI approach and the ways it could improve the lives of the world's most vulnerable people is understandable, the model's complexity is a major barrier to its adoption.

Use Case #2: Managing Healthcare Supply Chains

The World Health Organization estimates that one in ten medical products used in low- and middle-income countries is either substandard or falsified, with most reported cases (42 percent) coming from Africa.[16.] This problem stems in part from poor supply-chain management, which prevents local health clinics from knowing the provenance of the medical supplies they use. Improving the ability to track and trace the movement of medical goods across the supply chain would help address this problem.

Interest in improving healthcare supply chains is not limited to developing countries. The U.S. Drug Supply Chain Security Act passed in 2013 calls for the development by 2023 of an interoperable electronic system to identify and trace the movement of prescription drugs distributed in the country. The European Union passed similar legislation in 2016. Both initiatives have spurred investment in possible solutions, including blockchain.

Following the lead of companies with large logistical operations, like Walmart and Maersk, the pharmaceutical industry is now exploring the technology's potential for its own supply chains. Over the last year, several initiatives that aim to use blockchain to meet track-and-trace regulations have been announced, including The MediLedger Project and a collaboration between DHL and Accenture.[17.]

The idea of using blockchain technology as a platform for supply chains holds great promise. By providing a single, tamper-resistant ledger on which transactions can be viewed by all actors with appropriate permissions, the technology could reduce many of the frictions and vulnerabilities in existing supply-chain networks. Having greater visibility of the

movement of goods could reduce the costs and time associated with reconciliation, minimize the potential for counterfeiting, expedite recalls, and aid inventory management.

Supply chains also meet many of the criteria set forth in Figure 1 regarding when a blockchain solution may be useful, including the involvement of multiple actors who need both read and write database access, the desirability of a tamper-proof transactions log, and the potential inability to trust a single actor in the supply chain to store the data. And while the technology cannot fully substitute for trust between supply-chain partners (e.g., those at the end of the supply chain must still trust pharmaceutical manufacturers to provide accurate information about the ingredients they use), it can enhance it by providing "a single source of truth" that has been agreed to by all actors on the network.

Recording supply-chain data on a shared ledger could also unlock new capabilities not possible under the current model, in which data remains siloed in individual companies. For example, pharmaceutical companies could analyze aggregated data to predict stockouts before they happen and monitor disease outbreaks in real time. Using a blockchain platform in combination with electronic sensors at different stages of the supply chain could also help to monitor and verify that vaccines have been stored at appropriate temperatures.

Perhaps the most critical obstacle to achieving this vision is meeting the pharmaceutical industry's demand for data privacy. To date, manufacturers and distributors have been unwilling to share commercially sensitive data with one another. Solving this problem requires the use of permissions secured by encryption, which adds a layer of complexity. For example, the company Chronicled, which runs The MediLedger Project, is using zero-proof theorems that allow "transactions to be publicly verifiable without having to contain sensitive information."[18.]

Several prerequisites must be met before a blockchain can serve as a supply-chain platform. The most basic is the need to assign a unique identity (i.e., serial number) to each product in the supply chain through a process called serialization. While this process sounds simple, it requires a high degree of coordination around a set of (ideally global) standards. The next step is making sure that all actors on the supply chain have the ability to scan products and make use of the data provided. Most experts believe that establishing industry-wide serialization will take years.[19.]

Another necessary prerequisite is a supportive legal environment. Experts in the highly regulated health sector are just beginning to consider how decentralized models fit with the existing legal framework and what reforms might be needed to enable new approaches. To state the obvious, companies are unlikely to use a blockchain-based platform until they have confidence that it meets these regulations. At the same time, policymakers will only pursue reform once they have developed expertise around decentralized models. This again points to the need for patience, as well as education.

Despite these challenges and the likely long transition period, supply-chain management appears to be an area where the benefits provided by blockchain technology could exceed the cost of complexity. Determining this will ultimately depend on information gleaned from pilot projects.

CONCLUSION

Whether using a decentralized governance model is worth the added cost of complexity depends entirely on the attrib-

utes of the case in question. While the costs of doing so appear to outweigh the benefits in most instances, there are a few areas in which blockchain technology could help address longstanding challenges in new and more effective ways.

Given the development community's interest in exploring blockchain technology, it is important to set a course that allows for effective experimentation and learning. Here are a few suggestions for how to move the discussion forward in a useful direction:

Get specific. There is a glut of "blockchain for development" surveys, including this essay, and none is terribly useful.[20] Since blockchain models and the value they provide differ greatly across use cases, analysis should focus on specific applications. This will require pairing sector specialists with technical experts, ideally with a policy person in the mix.[21]

Get real. Blockchain boosters often exaggerate the technology's capabilities and overlook hurdles to adoption, which lead to unrealistic expectations. There also is a tendency for blockchain enthusiasts to assume that centralized solutions are always second best (or worse) and that trust is always lacking. These assumptions should be questioned in every use case.

Get data (and share it). Blockchain startups are often quick to publicize their pilot project "successes" while failing to provide metrics to support their claims. Without these data, the development community will struggle to determine what approaches are most likely to work and at what cost. Organizations that fund pilot projects should require the startups they partner with to collect and report these data.

Cultivate patience. In many ways, getting the technology right is the easy part. The more difficult challenges involve getting multiple actors to agree to a common set of standards and establishing legal and regulatory compliance. Doing both will require answering complicated questions with little precedent, such as who owns data stored on a blockchain, who is liable, and what is needed for the data to be accepted by all parties. For this reason, going from pilot to scale will take much longer than is commonly acknowledged. The development community can accelerate this process by conducting more pilots, collecting and sharing more data, and having more conversations about what an enabling regulatory framework could look like.

Acknowledgements

I am grateful to the following people for taking the time to review this paper and provide their insights: Susan David Carevic, Alan Gelb, Rachel Alexandra Halsema, Paul Nelson, Stela Mocan, John Polcari, and Aaron Sparks.

---

1. Nelson, Paul. "A Primer on Blockchain," 2018. Available at https://www.usaid.gov/digital-development/digital-finance/blockchain-primer.

2. Blockchain Company and the United Nations Development Program. "The Future Is Decentralized: Blockchains, Distributed Ledgers, & the Future of Sustainable Development," 2018. Available at https://www.blockchain.com/whitepaper/index.html.

3. Steve Wilson makes this point in a 2017 speech, available at https://www.youtube.com/watch?v=UH5-wvfVph4&feature=youtu.be&t=348.

4. Samman, George. "The Trend Towards Blockchain Privacy: Zero Knowledge Proofs." Coindesk, September 12, 2016.

5. Graglia, J. Michael, and Christopher Mellon. "Blockchain and Property in 2018: At the End of the Beginning." Working paper for the World Bank Conference on Land and Poverty, March 19-23, 2018.

6. Meunier, Sebastien. "When Do You Need

Blockchain? Decision Models." Medium, August 4, 2016. Available at https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1.

[7.] World Bank. "Identification for Development: Making Everyone Count." ID4D, May 4, 2017. Available at http://pubdocs.worldbank.org/en/332831455818663406/WorldBank-Brochure-ID4D-021616.pdf and http://www.unhcr.org/en-us/figures-at-a-glance.html.

[8.] World Bank. Principles on Identification for Sustainable Development: Toward the Digital Age (English). Washington, DC: World Bank Group, 2018. Available at http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-identification-for-sustainable-development-toward-the-digital-age.

[9.] Lewis, Antony. "A Gentle Introduction to Self-Sovereign Identity." Bits On Blocks, May 17, 2017. Available at https://bitsonblocks.net/2017/05/17/a-gentle-introduction-to-self-sovereign-identity/.

[10.] Warden, Staci. "Can Bitcoin Technology Solve the Migrant Crisis?" Wall Street Journal, June 8, 2016. Available at https://www.wsj.com/articles/can-bitcoin-technology-solve-the-migrant-crisis-1465395474.

[11.] Accenture. "Accenture, Microsoft Create Blockchain Solution to Support ID2020," June 19, 2017. Available at https://newsroom.accenture.com/news/accenture-microsoft-create-blockchain-solution-to-support-id2020.htm.

[12.] See http://www.unhcr.org/blogs/id2020-and-unhcr-host-joint-workshop-on-digital-identity/.

[13.] Thanks to Susan David Carevic, IT officer, World Bank Group, for providing this example.

[14.] Hall, Blake. "5 Identity Problems Blockchain Doesn't Solve." Medium, July 6, 2017. Available at https://medium.com/@blake_hall/5-identity-problems-blockchain-doesnt-solve-ed4badb94398

[15.] See https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/.

[16.] World Health Organization. "1 in 10 Medical Products in Developing Countries Is Substandard or Falsified." Geneva, Switzerland: World Health Organization, November 28, 2017. Available at http://www.who.int/en/news-room/detail/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified.

[17.] Accenture. "DHL and Accenture Unlock the Power of Blockchain in Logistics," March 12, 2018. Available at https://newsroom.accenture.com/news/dhl-and-accenture-unlock-the-power-of-blockchain-in-logistics.htm; MediLedger. Available at https://www.mediledger.com/.

[18.] MediLedger. "The MediLedger Project: 2017 Progress Report." MediLedger, February 2018. Available at https://uploads-ssl.webflow.com/59f37d05831e85000160b9b4/5aaadbf85eb6cd21e9f0a73b_MediLedger%202017%20Progress%20Report.pdf.

[19.] Whyte, Joe. "Pharmaceutical Serialization: An Implementation Guide." Rockwell Automation, October 2017. Available at http://literature.rockwellautomation.com/idc/groups/literature/documents/wp/lifesc-wp001_-en-p.pdf.

[20.] There are, of course, exceptions. Two of the better surveys are Zambrano, Raul. "Blockchain: Unpacking the Disruptive Potential of Blockchain Technology for Human Development." International Development Research Centre, August 2017. Available at https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/56662/IDL-56662.pdf; Nelson, "Primer on Blockchain."

[21.] Thanks to Rachel Alexandra Halsema, IT officer, World Bank Group, for emphasizing this point.