Blockchain Applications to International Affairs: Reasons for Skepticism

Angela Walch

Georgetown Journal of International Affairs, Volume 19, Fall 2018, pp. 27-35 (Article)

Published by Johns Hopkins University Press
DOI: https://doi.org/10.1353/gia.2018.0004

Dialogues

Blockchain Applications to International Affairs

Reasons for Skepticism

Interview with Angela Walch

Georgetown Journal of International Affairs: Can you start by giving us an overview of what blockchain is and why it is so revolutionary?

Angela Walch: The easiest way for me to describe blockchain is that it's a form of group record keeping. A group of parties, small or big, gets together and decides to keep a joint record together rather than delegating that responsibility to one of the parties in the group.

That is said to be significant because by doing it together, you eliminate the need to rely on the particular third party you're delegating to. It spreads the trust around, in some ways.

Another reason that people say that blockchain is potentially revolutionary is because this record that's created is distributed. It sits on the computer systems of all of the computers in the network. There's some variation on how particular ones are structured—some choose to let only certain more powerful computers in the network have a copy of the record—but the general premise is that it's distributed among everyone.

Right now, we delegate to governments the responsibility for keeping track of birth records. You don't keep track of every single person's birth certificate in your community. The government does that. So, blockchain is different from that in that all of the nodes are keeping a record. That's one of the reasons why there are potential scalability concerns—if everyone's keeping a record of the data instead of one party doing it, that's a whole lot of data we're keeping track of.

Another reason people say that blockchain is potentially transformative is because the record that's created is supposed to be very hard to change. You'll often see the word *immutable* or *permanent* to describe this record. I've critiqued that concept in the past; I think there's quite a bit of overstatement about just how hard this record is to change. If that's true, that's an incredibly powerful concept. If no one can mess with it once the record's been created, you've eliminated one way that people might commit fraud. Having a record that is very robust and difficult to change is a really attractive thing.

Angela Walch specializes in blockchain technologies, money and the law, governance of emerging technologies, and financial stability. Walch is an associate professor at St. Mary's University School of Law, a research fellow at the Centre for Blockchain Technologies at University College London, and a graduate of Harvard Law School. Prior to teaching, she practiced corporate law at Ropes & Gray in Boston, served as an attorney in the office of the General Counsel at Harvard University, practiced transactional law at Sainsbury's in London, and served as general counsel for an events company. She has published several pieces on blockchain technology and cryptocurrencies, including "The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk" in the *New York University Journal of Legislation and Public Policy*, "The Path of the Blockchain Lexicon (and the Law)" in the *Review of Banking & Financial Law*, and "Call Blockchain Developers What They Are: Fiduciaries," an influential op-ed in *American Banker*. Walch has presented her research at leading universities and conferences around the world and has been quoted in the *New York Times*, the *Wall Street Journal*, *TIME*, and other media outlets.

There are some other characteristics that it's said to have. You might notice the way I'm phrasing it—it's said to have this, it's said to have that—I'm saying that because the technology is still extremely immature and very poorly understood, and there's a lot of experimentation. People are still working out what its actual characteristics are.

Another powerful characteristic it's said to have is that you can rely on this record because it's going to reflect truth. With blockchain technologies like Bitcoin or other cryptocurrencies that actually have a token built into the system, I think you can count on it being true that one bitcoin or one ether was actually transferred to someone else, and you can trust the record of those transfers. The moment that you start building things on top of those blockchains, like property records or voting records, then you're still very much reliant on processes outside of the technology to ensure the truth and legitimacy of the record. If you don't control who gets to make changes to it, someone could easily put something untrue into the record.

Also, it's said to be very secure. There's a debate among technologists about where the security comes from. One of the places it may come from is the cryptography that's used in the systems that link these records together in a way that's really hard to break. Essentially, as each record is added, it's linked to the one that came before, that's linked to the one that came before, and so on. This chain of records means that if you tamper with it, the change would show up because you're tampering with this entire chain of data.

As I said, there's a lot of experimentation happening and there are many different variations that people are making to the core technology, which came to us through cryptocurrencies, the first of which was Bitcoin. It started in the Bitcoin world and has gone on from there. The first non-cryptocurrency group that took a look at this technology was the finance sector. After the finance sector got excited, people started seeing broader implications and broader applications for the technology. Blockchain technology is absolutely relevant to a journal of international affairs because when you think about it, if the fundamental technology is about group record keeping, well, record keeping is involved in every single human practice, whether that's finances, voting, citizenship records, medical records, records of a supply chain, what have you. It has broad application because record keeping has broad applications.

GJIA: We can't help but find it a tad ironic that a technology supported by people who generally want less government is beginning to be used by governments themselves. Is there any potential for government abuse of blockchain, or is it as transparent as it seems to be? Are there any other abuses of power we should watch for as this technology continues to grow?

AW: There's a lot going on in the government space right now. Almost every day, there's a new report from a policy organization or a government itself about potentially using blockchain technology in their systems and how it will absolutely increase the transparency of their systems, the robustness of their data, and therefore the trust that people place in government. That is a really, really desirable thing right now. Look at what is going on in the world. People don't trust anything. There's a failure of trust in many of our institutions, including government, which is a massive, massive problem. It would be very nice to think that a technology like this could come along and help. We're seeing experimentation in areas like voting, disbursement of aid, or giving refugees an identity that they can use after

they've had to flee their country. This is all sounding really good, and it absolutely may be.

However, the problems that I see occurring are several:

One, there's a ton of confusion in the space and a lot of overstatements about the technology's capabilities. This is problematic because investing in a new technology is significant in terms of resources like time and money. We want to be sure that we know what we're getting into before we make a big transition, particularly in critical systems like voting or identity. That's why it's so important for people to be honest and accurate and precise about the technology's capabilities when they're discussing it.

Sadly, particularly in the government setting, I see a lot of sloppiness and overstatements about what the technology can do. Let's just take the word *immutable* or *permanent* as an example. People say that the blockchain record, like in Bitcoin or Ethereum or any other public blockchain system, is immutable. Then they go on to say that blockchain technology itself is immutable, suggesting that the feature exists in any variation of the technology, or what people want to label as blockchain technology. The problem is that the bucket of what people describe to belong in blockchain is highly varied and uncertain and debated among technologists as to which particular combination of features actually would give rise to a permanent, tamper-resistant record. People are changing everything about it, from how you do the verification process of the record, to the cryptography that is used, to how the parties who can participate in the record-keeping process can join (whether anyone can join or only a very limited group of people can join or whether you just have one party running it). For example, take what's happening with the World Food Programme of the UN.[1] They are apparently using a private variation of Ethereum, but the World Food Programme runs the system itself last I heard, which sounds a little weird because to me the defining feature of blockchain is that it's a group record-keeping project. People are calling things blockchain, and it's highly debatable whether a given project would fall into that category.

Estonia is another potential example of that. It is so hard to figure out how blockchain is actually related to what's going on in Estonia. Estonia is very much celebrated for its use of the digital in how it governs. It's got a digital identity system, it offers e-residency to people around the world, and since blockchain became trendy a few years ago, a repeated "urban legend" is that Estonia uses blockchain technology in its digital identity system. As far as I can tell from people I consider legitimate, that's not true. It was simply a rebranding by the company who was already providing the technology to call what they were doing already "blockchain."[2]

I guess this is probably true with any technology, but there are lots of incentives at play here. The government market is extremely lucrative, and lots of companies in the space are, I'm sure, very legitimate and have the best of intentions, but there are always going to be people grabbing on to the latest buzzword if that's going to get them government business. I think there needs to be a lot of skepticism and scrutiny about what's going on on the business side of this.

Just this past week, there was an article saying that Sierra Leone was the first nation on earth to run a "blockchain election."[3] The problem is that it just wasn't true. A company in the space says that they entered the votes into their private blockchain system. A few days later, the official government organization that is responsible for Sierra Leone's voting systems specifically stated that blockchain was not used in the election and contested the statement. This goes back

to the fact that all the incentives are there for people in the industry to sell the tech to governments. I just think governments and policymakers need to be extremely skeptical because they're a very attractive target and it's easy to describe this stuff as being a panacea. Be skeptical that you're actually achieving good.

Another one of the selling features of the technology is that because it is supposedly decentralized and transparent, it affects the exercise of power. Power concentration in tech is a huge concern as we're finding with these social media and other mammoth technology companies like Facebook and Google. The easy answer is to say that centralized is bad and therefore decentralized is good. In other words, "What is decentralized? Blockchain technology is decentralized! So therefore that is the answer."

There are very likely a lot of good ways that the tech can be used, but it shouldn't just be a knee-jerk response because centralized equals bad and decentralized equals good. When you press on the decentralized reputation of blockchain technologies, you end up with much more of a spectrum of centralization to decentralization than anything that you could say is absolutely decentralized. There's concentrated power in many of the cryptocurrency systems like Bitcoin or Ethereum. Recent research has come out pointing out that three or four different mining pools generally control over 50 percent of the network.[4] This means they control what goes into the record. This idea that distributing power widely eliminates potential power abuses is false. We're not actually distributing power all that widely. The problem is that the power is generally unacknowledged; unacknowledged power is undefined and unchecked. You need to be really careful about assuming that just because the buzzword *decentralized* is there that it's okay.

Another way that the use of blockchain technologies by governments could end up being problematic is the potential use of it for refugee data. Refugees are fleeing their countries for very important reasons. They have been persecuted by their government or there's a war going on there or it's dangerous for some reason for them to go back. In many cases, they abandon everything and it's a big problem when they don't have any way to prove who they are when they get to the refugee camp. So, there's a lot of discussion about using blockchain technology to give someone a digital identity. The risk that you run into there is creating a very robust, hard-to-change record that collects everyone's data. If you were a refugee, would you really want to become part of this system? Why would you trust this party and trust that they're not going to go give it to your government? There remain many hard questions here. This is not a simple tech solution. That's probably my overarching message about this technology in the context of government systems: the technology may be able to help some, but the hard problems are those about people. They're not neatly solved by technology; the hard questions remain.

GJIA: What are some of the legal challenges to regulating blockchain? How do governments go about regulating it, and can they? Does the law need to be entirely reimagined in order to govern it, or are legal systems already in place?

AW: This is a question that lawyers and policymakers are wrestling with at the moment. When we're talking about how to regulate blockchain technology, I think the background question there is "Do we really need to regulate the technology, or should we instead be thinking about the ways that the technology is actually being used?" If we regulate those activities, then the technology we're using won't really matter. That's called

activities-based regulation, and I think those principles remain useful. There may be some instances in which more tailored regulation is needed, but I think the core principles are there. You're still dealing with who exercises what power, whether they did it in an acceptable way, and whether people are taking advantage of other people, committing fraud, raising money without giving adequate disclosures, taking people's data and not using it in accordance with the permission that people gave them, or other problems. All of those questions I think the law already has something to say about. It does, however, cause us to have to rethink some of our existing laws.

We're seeing that right now in the area of securities laws. There's a variety of approaches that governments are taking. There's been this craze in the past year for companies to raise money by selling "tokens" instead of shares of stock. The idea is that they're building systems, whether a file-storage system or a music-sharing system in which you'll be able to use a token in order to participate in that system, kind of like frequent flyer-miles or something of that nature. These tokens are using blockchain technology. In the past year, billions were raised in what were called Initial Coin Offerings (ICOs). A lot has changed from 2017 to 2018 because regulators like the SEC have decided that these look like securities. We have a whole body of law that deals with securities in order to protect investors. These ICOs were raising $100 million in a minute or two and they were taking money from investors from all over the world without any scrutiny as to the investors' net worth or sophistication and providing little to no disclosure about what the product was that they were selling. In some cases, the money would be raised and the company would just disappear. So, there's a lot of fraud and scamming in the space.

However, the reasons I'm saying that this may indicate that we want to rethink some of our security laws is because people say that the ICO phenomenon reveals a great unmet demand to be able to invest. The speed and amount at which people were investing demonstrates that there is a demand for these types of investment opportunities that's not being satisfied under the existing security laws. Maybe they are too restrictive. In general, if you're not doing a public offering, an initial public offering, in which the shares are registered and can trade freely among the public, you are very limited in the types of investors who can participate in it. They generally have to have a very high net worth in order to participate. So, there's a lot of talk about how these initial coin offerings were intended to democratize investment opportunities, to make them available to those who hadn't historically been able to participate in this market. That raises questions about whether or not we need to rethink the security laws and whether we should be opening investment opportunities to broader groups of people or if these principles that we've espoused for a long time about peoples' sophistication or net worth are helping to define whether they should be able to invest still stand.

When we're talking about how to regulate blockchain technology, I think the background question there is "Do we really need to regulate the technology, or should we instead be thinking about the ways that the technology is actually being used?"

The law can absolutely cover what is going on and how this fundraising is happening, but it does raise questions about whether or not we still like the law that we have.

GJIA: You have written that blockchain coders and miners should be treated as

fiduciaries—that they should have heightened obligations and liability for problems in the chain itself. It makes sense that the ones who create the system should have extra responsibilities, but it is at odds with the decentralized, ungoverned nature of blockchain and cryptocurrencies in particular. How do you see these tensions being addressed?

AW: Right, so this is a very controversial idea. My argument is that there are several forms of governance actually happening on public blockchains, and the messaging around is that these systems are decentralized so that power is distributed and no one is exercising it because you're spreading it around. I think that's absolutely not true. I mentioned earlier how the mining pools are concentrated. All that mining is devoting your computing power to maintaining this group record, basically to validating new transactions that are going to be added to this list. That's what the mining network does. Mining is a terrible name for it. You could also call them "transaction validators" or "transaction processors." It used to be possible for people to participate in mining by just downloading and running the software on their computer, but as the value of Bitcoin increased, it became very lucrative to be a miner because the way you're incentivized to participate in the transaction validation is that you're paid with the issuance of new bitcoins (or whatever applicable cryptocurrency on other public blockchain networks).

People started investing in more and more powerful hardware that would enable them to defeat all the other transaction processors and process their transactions faster so that they would win more Bitcoins. This need to invest in the hardware meant that the mining sector was very much professionalized, and there are now massive server farms all over the world. They tend to concentrate in places where power is cheaper, where they can get some sort of a special discount on the electricity that they're using to run these huge servers. Now, these mining pools have grown up and I see miners exercising power on the network, particularly the ones that have significant portions of the computing power on the network. They make decisions about what software is going to be run, actually, because the network doesn't function unless they run the particular software. So, changes are made to the system through the release of new software, and that means that the people who make choices about the software are those who are governing it. The parties that make decisions about the software are the software developers, then the miners who decide which version of the code they like.

My argument is that there are several forms of governance actually happening on public blockchains, and the messaging around is that these systems are decentralized. . . . I think that's absolutely not true.

What does all that mean? What do you do when you're making recommendations about a new release of software? Well, you're deciding what policy decisions are going to be reflected in that software. Should it be expensive for people to participate in this system? Should it be cheap for them to participate in this system? Should people be able to buy a cup of coffee with Bitcoin? Should people use it only for high-value transactions? All of those end up being reflected in the software. You're also making decisions about how best to achieve your policy goals and checking all the security issues about the software and whether there are bugs in it. So these people are making very important decisions, particularly when there are

multiple billions of dollars now resting on them. So, in public blockchain systems, the governance is very much a work in progress. We started out with Bitcoin, which purported to be sort of anarchic, but it has these unacknowledged governance structures in it, and in most of these systems, there is a group of developers called "core developers" who make the decisions about what changes go into the code. And these systems are generally open source, which means the code is publicly available and that anyone can propose changes to it, but the ones who actually get to make the changes are the core developers.

I think the core developers and miners who provide a certain percentage of the computing power of the network do function as fiduciaries. I think they're fiduciaries of the users of the system, and the fiduciary relationship of the system is one of trust. There's trust here because the code is opaque to everyone except coders. I certainly can't read the code, and I don't know much about you, but I'm guessing you might not be able to read the code either, or to determine whether it's good, bad, going to achieve its goals or not? No. And yet, people are relying on this system for their money, for their value. Any government that chooses to rely on a public blockchain system is essentially outsourcing a lot of decisions to parties like core developers, like miners, who don't necessarily have any obligations to them. They don't necessarily know who they are. They don't necessarily know their qualifications.

Any government that chooses to rely on a public blockchain system is essentially outsourcing a lot of decisions to parties like core developers, like miners, who don't necessarily have any obligations to them.

I'm very skeptical of the use of public blockchain systems by governments because of these governance risks.

GJIA: Going forward, do you see a future for public blockchain systems given the outrageous energy demands required for the systems, the shady nature of the payers, and the lag in validation times for transactions?

AW: That's a very interesting question because public blockchains are the ones that actually are truly innovative. Every technologist that I respect in the field has said that private blockchains are just really databases, and the only reason we're excited about them is because someone was smart enough to market them with the term *blockchain*.

There's a lot of discussion in the field about energy usage, and people who participate in the systems say, "Well, that's just a tradeoff. It's worth spending all of this power in order to get this record that is permanent or immutable, that it's secure, and so on." So, they say that's simply the cost of it if you want to be able to do things outside the scope of the government world.

I think that's actually a very interesting point from an international affairs perspective—that these public blockchains are kind of deliberately seeking to exist outside the existing sovereign system. We need more political scientists in this space, but there is some discussion and lots of analogizing public blockchain systems to sovereigns. It's said that each system is essentially functioning as a sovereign because the people are choosing to participate in it under a given set of rules. The rules happen to be implemented by code, but it's similar to people coming to live together in a particular way in a state. There is discussion about whether people are going to want to participate in public blockchains as an alternative to their states. There are some interesting companies in this space—there's one called Bitnation

It's said that each system is essentially functioning as a sovereign because the people are choosing to participate in it under a given set of rules. The rules happen to be implemented by code, but it's similar to people coming to live together in a particular way in a state.

that deliberately tries to be its own country. I'm skeptical of this because I think there will always be two worlds. There's a digital, blockchain-focused world that sits on top of the Internet, but then no matter what, you still have the physical world. We haven't figured out how to transcend that.

So, while you can be a citizen of a public blockchain sovereign nation, you're still physically living next to somebody, you still have trash that you're generating and have to get rid of, you still have to get clean water somewhere. I don't see them in any way eliminating the need for states and figuring out how we can live side by side and deal with our very complicated problems of limited resources and those types of things. But there is a techno-utopian argument that this world is too annoying, so let's build a cyber world that we can go to instead. I think that's kind of a cop out or perhaps wishful thinking.

It's interesting to see the blockchain world now starting to fight with the real world in terms of the energy that the blockchain world needs to survive. It draws attention to the fact that the public blockchain world relies on physical infrastructure in the real world. You need power that's generated in a particular way in the real world and you need the Internet. I think some thinking needs to be done about what happened in Puerto Rico with the electrical infrastructure being decimated for such a long time after these recent hurricanes. The techno-utopians say

I don't see them in any way eliminating the need for states and figuring out how we can live side by side and deal with our very complicated problems of limited resources and those types of things

that they don't need anything physical anymore: no cash, no physical money, we can do everything digitally. That's fine, until the real world intervenes and you don't have the infrastructure to support the system. I don't think you can neglect the physical world, and I think it's an oversimplification of reality to expect that we can be purely digital. It's hubristic to me. It suggests that we can conquer our physical world more than I think that we really can. Our existing physical vulnerabilities remain.

There's been some mining, or transaction processing, businesses coming into particular places in the US where electricity was particularly cheap. There's a city in New York that just passed a rule going after miners specifically because the rest of the city's population was paying much higher electricity costs because of the presence of the miners who were sucking up a lot of the cheap electricity.[5] It's the continued fight for resources. Are people going to be willing to subsidize the techno-utopians to have a world that they're building on top of us but using our infrastructure ultimately? These resource battles are just beginning.

The techno-utopians say that they don't need anything physical anymore: no cash, no physical money, we can do everything digitally. That's fine, until the real world intervenes and you don't have the infrastructure to support the system.

Notes

1. Joon Ian Wong, "The UN Is Using Ethereum's Technology to Fund Food for Thousands of Refugees," *Quartz*, November 3, 2017.
2. Dave Birch, "Estonia, Fake News and Digital Identity," *Tomorrow's Transactions*, last modified March 20, 2017.
3. John Biggs, "Sierra Leone Government Denies the Role of Blockchain in Its Recent Election," Tech Crunch, last modified March 19, 2018.
4. Adem Efe Gencer et al., "Decentralization in Bitcoin and Ethereum Networks," Financial Cryptography and Data Security, arXiv.org, last modified March 29, 2018.
5. Lily Katz, "Bitcoin Mining Banned for First Time in Upstate New York Town," *Bloomberg*, March 16, 2018.