BLOCKCHAIN TECHNOLOGY AND INTERNATIONAL RELATIONS: DECENTRALIZED SOLUTIONS TO FOSTER COOPERATION IN AN ANARCHIC WORLD?

Bernhard Reinsberg

WP 508
September 2018
BLOCKCHAIN TECHNOLOGY AND INTERNATIONAL RELATIONS:
DECENTRALIZED SOLUTIONS TO FOSTER COOPERATION IN AN
ANARCHIC WORLD?

Centre for Business Research, University of Cambridge
Working Paper No. 508

Bernhard Reinsberg
Centre for Business Research
University of Cambridge

Email: br385@cam.ac.uk

September 2018
Abstract

Blockchain technology enables ‘trustless’ interactions among individuals by replacing centralized enforcement with distributed consensus. It therefore has been used for commercial applications, including transfer of cryptocurrency, digital file storage, digital identity services, and supply-chain management. This article probes the potential of blockchain technology to foster international cooperation among states—given the lack of a world government to enforce their mutual commitments. The article outlines four facilitators of blockchain-based global governance systems, including the need for credible commitment, the availability of resourceful non-state actors, verification needs that can be addressed through ‘oracles’, and routine interactions. These facilitators are further illustrated for the case of climate governance. Overall, the discussion suggests that blockchains—if appropriately designed to address the underlying cooperation problems—hold significant promise. Their key strength is to enable states to design ‘smart contracts’ that execute automatically when agreed conditions are fulfilled. To some extent, blockchain technology thus challenges the primacy of international organizations. However, even with blockchain technology, international organizations continue to play a role with regard to pre-agreement policy deliberation, validating real-world events, and providing technical assistance for policy implementation.

Keywords: International Relations; trust; anarchy; cooperation; international organizations; Blockchain; Ethereum; smart contracts; decentralized governance;

JEL Classification: F30, O19, O30

Acknowledgements: I am particularly grateful to Giorgio Caselli, Simone Dietrich, Andreas Kern, Axel Michaelowa, Mette Eilstrup-Sangiovanni, Jason Sharman, Ian Shields, Joseph Zammit, Rene Reinsberg, Marek Olszewski, and Sep Kamvar for fruitful discussions and valuable comments. The author declares no conflict of interest.
1. Introduction

On May 31, 2017, about half a year after assuming office, US president Donald Trump announced to withdraw from the Paris climate agreement, in which 195 countries collectively pledge to halt global warming. He motivated his decision with reference to his ‘America first’ doctrine, arguing that the climate deal would kill jobs at home, especially in energy-intensive sectors. Other countries condemned the US withdrawal, while Donald Trump also faced domestic opposition against his decree from several states, cities, and corporations. For example, major US corporations—including Apple, Google and Walmart—and even fossil fuel firms such as ExxonMobil, BP, and Shell reaffirmed their support for the Paris accord which they consider “the best way to transition to a low-carbon economy and stave off the perils of climate change.”

Could blockchain technology have prevented cooperation failure by the US government? In this paper, I introduce blockchains as a new technology with institution-like properties and demonstrate how states can deploy them to promote international cooperation. A blockchain is a cryptographically linked digital ledger of transactions distributed across all participants of a peer-to-peer network. In existing use cases, peers are individuals, but nothing would prevent states from adopting blockchain technology to govern their international interactions. In particular, blockchain technology would allow states to devise so-called ‘smart contracts’—pieces of computer code that run on top of a blockchain and that allow for conditions to be imposed upon transactions. Smart contracts execute (automatically) when pre-specified conditions are met (Swan 2015, 16). Therefore, blockchain technology can enhance the credibility of state commitments by allowing for guaranteed execution of inter-state contracts. In addition, it offers a secure way of making side payments as part of agreements, hence allaying distribution problems. Finally, blockchain technology can also address information problems by leveraging distributed consensus to generate reliable information. From an IR perspective, blockchain technology thus is best understood as a new type of international institution.

International Relations scholars have long been vexed by the issue of how cooperation among egoistic states emerges and can be sustained under conditions of anarchy (Axelrod and Keohane 1985; Krasner 1983; Stein 1982). Indeed, international institutions—the rules of conduct of international politics (Krasner 1983; Martin and Simmons 1998; North 1990)—have been seen as the primary vehicles to promote cooperation. Institutions can promote cooperation by altering the strategic environment in which states interact. For example, they facilitate repeated interaction, which allows states to update their beliefs about their peers while increasing the cost of non-compliance (Keohane 1984; Krasner 1983; Oye 1985). In addition, international organizations (IOs)—featuring
independent secretariats and (in most cases) provisions for monitoring, enforcement, and dispute settlement—increase these costs further while facilitating deeper cooperation by allowing states to make more credible commitments, relying on independent information, and brokering issue linkage. IOs are the most centralized entities in world politics, mimicking several core functions of the state at the international level (Abbott and Snidal 1998).

However, the scope for institutions to promote cooperation remains limited. Far from being direct enforcers of rules, most IOs can only indirectly enforce such rules, as they rely on voluntary cooperation of states (Simmons 2010). For instance, IOs can authorize sanctions and coordinate sanctioners (Drezner 2000; Haftel and Thompson 2006; Voeten 2001), reinforce reputational pressures (Checkel 2001; Kelley and Simmons 2015; Tomz 2007), and empower domestic actors (Dai 2007). However, enforcement problems become more acute with growing numbers of states involved (Snidal 1994). States motivated by the need to enhance compliance face clear limitations to designing IOs with greater autonomy. As long noted by principal-agent literature, IOs—acting through international bureaucrats—can misuse delegated authority to pursue independent agendas that are not in the collective interest of their member states (Barnett and Finnemore 2004; Graham 2014; Hawkins et al. 2006; Nielson and Tierney 2003). In addition, the current system of IOs is prone to being hijacked by powerful states. This is because wherever authority is centralized, the marginal returns to wielding influence on it increase. A voluminous literature shows that IOs cater to the core interests of the most powerful states. For example, powerful states use IOs to reward their allies with bigger loans, faster disbursement, and less conditionality (Dreher and Jensen 2007; Dreher, Sturm, and Vreeland 2015; Kilby 2013). Lack of effectiveness of IOs thus is often the result of big power interference (Bermeo 2016; Lall 2017; Stone and Steinwand 2008). Finally, IOs are costly to establish, maintain, and dismantle (Jupille, Mattli, and Snidal 2013). The sheer number of IOs and the significant overheads in their budgets suggest non-negligible costs. Over the past 200 years, over 500 IOs have come into existence (Pevehouse, Nordstrom, and Warnke 2004); many of them provide patronage funding to government elites (Gray 2018), and even the most efficient ones—such as the World Bank—regularly spend about 35% of their budgets on overheads (World Bank 2016, 26).

The core question I address in this article is whether—and if so how—blockchain technology can be deployed, potentially in conjunction with existing organizations, to make global governance more effective. In the introductory example, blockchain technology could have helped raising the costs for the current US president to renego on the Paris deal, for instance by allowing for secure transfer of funds from pro-Paris firms to anti-Paris workers to compensate for job losses due to the low-carbon market transition. Under the
current system, it was relatively easy for Donald Trump to scrap the deal because the costs of doing so were low— involving some reputational damage— while the incentives to stay were small. If the powerful US corporations that verbally supported the deal had found a way of credibly underpinning their pledges with real money, the US government might have decided to stay in, given that it could have compensated the losers of the green transition.

While my article highlights how blockchain technology can be used to enhance the effectiveness of international relations, specifically for the issue area of climate governance, its key goal is to develop a theoretical argument outlining conditions under which states are likely to adopt blockchain technology to govern their interactions. Taking a rational-institutionalist view, I assume that states will do so where the associated benefits are highest. My analysis suggests that states will adopt blockchain technology in policy areas where states seek to make credible commitments; where resourceful non-state actors exist; where there is a need for verification that can be remedied through oracles; and for routine interactions.

As the first to explore the potential uses of blockchains in global governance, this article makes three contributions to pertinent strands of literature. First, by focusing on how blockchain technology can advance climate governance, I make a timely contribution to influential work by political scientists studying renewable energy transitions (Aklin and Urpelainen 2018). My article also relates to current work in energy studies exploring how blockchain technology can enhance the functioning of carbon markets (Fu, Shu, and Liu 2018; Khaqqi et al. 2018). None of these studies addresses use cases at the level of climate governance though. By introducing global governance as a potential use case, my article contributes to the emerging literature on blockchain technology, which focuses primarily on the description of use cases (e.g., Hileman and Rauchs 2017; Krishna, Fleming, and Assefa 2017; Swan 2015; Wigley and Cary 2017). I complement these studies with an analytical perspective, while also highlighting avenues for future research on the issue.

Second, the article helps understand a new empirical phenomenon through the lens of International Relations theory. Recently, scholars have grappled with the notion of anarchy, exploring the various ways in which the international system is hierarchically stratified (Mattern and Zarakol 2016; McConaughey, Musgrave, and Nexon 2018; Musgrave and Nexon 2018). The blockchains discussed in this article can be understood as a new type of international institution to facilitate decentralized cooperation and that is most beneficial in non-hierarchical interactions where commitment problems are larger. While scholars have long examined under which conditions international cooperation becomes possible (Dietz, Ostrom, and Stern 2003; Keohane 1984; Oye 1985),
this article discusses how a blockchain-based governance system among states would be implemented. By explicating how a ‘blockchain federation’ would mediate cross-national interactions involving IOs, governments, sub-state actors, and non-governmental actors, it also relates to works in complex governance and the new interdependence approach (Bulkeley et al. 2014; Farrell and Newman 2014; Kahler 2016).

Third, I discuss whether (and if so how) novel (digital) technologies can address cooperation dilemmas—an issue thus far absent in the International Relations domain. To be sure, there is comparative politics research examining why states adopt new technologies such as the internet (Milner 2006) and ‘scripts of modernity’ such as the New Public Management program, which challenged the understandings of the role of the state in public service delivery (Gingrich and Ansell 2009; Hall and Soskice 2001; Osborne and Gaebler 1992). The latter research emphasizes how the growing availability of low-cost information technology facilitated efficiency-driven outsourcing of government services, while raising concerns about democratic legitimacy and data protection (Heeks and Bailur 2007; Zysman and Newman 2006). However, nothing comparable exists at the international level. Touching upon issues of contract enforcement, there is substantive literature on international courts (Abbott and Snidal 2000; Simmons and Danner 2010; Voeten 2014). By examining smart contracts, my article provides a complementary perspective to enforcement and discusses conditions under which they can solve enforcement problems.

2. Blockchain technology

‘Blockchain technology’ refers to a cryptographically linked digital ledger of transactions distributed across all participants of a peer-to-peer network. It thus is a bundle of previously existing technologies combined in an ingenious way to implement trusted governance systems in which participants do not need to trust each other or a central authority.

These four technologies are blockchains, cryptography, peer-to-peer networks, and consensus mechanisms. First, blockchain is a data structure in which information is stored in blocks and linked to previous blocks. Second, blocks are linked via cryptography, which allows everyone to verify that a transaction occurred while preserving data privacy. Third, blocks are transmitted to the entire network, thereby building resilience against attacks. Fourth, every blockchain is governed by a consensus mechanism, thus rendering central authorities for validating transactions unnecessary. If a network participant wants to initiate a new transaction—creating a new block in the blockchain—all network participants must first accept its validity. As the integrity of a
participant cannot be readily assumed, the consensus mechanism holds key to the sanctity of the data.

Blockchain technology is particularly useful where participants need to access, verify, send, or store information securely (Wigley and Cary 2017). This follows from its technological features, notably *immutability* (no one can alter past transactions), *security* (encryption is hard to undo), *verifiability* (everyone can verify that a given transaction occurred and that the rules of the system are being followed), *transparency* (everyone can see all transactions though encryption ensures privacy is maintained), and *resilience* (information remains accessible even when some participants go offline). The first blockchain application was Bitcoin, which was introduced at the height of the Global Financial Crisis and conceived by its founder as a decentralized alternative to fiat money backed by central banks (Nakamoto 2008). But the technology has emancipated itself from its roots. Existing blockchain-based applications extend well beyond cryptocurrencies, covering diverse areas such as digital identity services, land registries, supply-chain management, and crowdfunding climate finance.

Two fundamental blockchain designs must be distinguished. In *permissionless* blockchains, everyone can write consensus data. To prevent fraud, participants need to put real assets on the line that they would lose if they were to write data that contradicts the consensus among all participants. For instance, in the Bitcoin economy, the authoritative blockchain is the one with the highest ‘proof of work’, which involves solving a computationally costly cryptographic problem (Buerger 2016; Nakamoto 2008; Ravikant 2013). *Ethereum*—a general-purpose blockchain underlying many real-existing blockchain projects—operates an enhanced proof-of-work mechanism that prevents participants with concentrated computational power from hijacking the system but has begun experimenting with a proof-of-stake algorithm. This algorithm randomly selects validators for block creation, with the probability of selection depending on its own deposit. If a proposed block does not get included in the blockchain, a validator loses its staked deposit (Baliga 2017). Hence, all the above systems need an underlying natural currency to ensure the sanctity of the blockchain. The natural token provides incentives against fraud, for example to alter the record of transactions.

Permissionless blockchains are advantageous whenever central authorities cannot be trusted and establishing trust among individuals would be prohibitively costly. The former condition holds in ‘rogue states’, which may use centralized data to suppress opposition, while the latter condition holds for most anonymous market exchanges. Therefore, permissionless blockchains have proliferated in these areas, with a key application being cryptocurrencies (Gupta et al. 2017; He et al. 2016; Pani 2016). Other applications that in most cases use
the Ethereum blockchain include decentralized file storage, proof of identity, land registries, and notary services (Swan 2015, 22). Some of these applications require encoding real-world assets on the blockchain with a unique identifier such that these assets can be traced, controlled, and exchanged on the blockchain (Swan 2015, 14), and the ‘Internet of Things’ (Valkenburgh 2016).

In so-called permissioned blockchains, the ability to manipulate the blockchain is restricted. Permissions can be issued by a central authority; alternatively, consortium systems rely on the collective decision of participants without involving a central authority to govern participation rights. In contrast to permissionless network, the identity of every participant in a permissioned network is known. Permissioned blockchain networks do not abrogate the requirement that every node on the network perform all of the computation for the entire network, but they break this computation into particular segments and thereby increase overall performance and reduce transaction costs relative to permissionless blockchains. This federated consensus is possible because sets of validators are chosen based on the expectation they will not collude in a coordinated effort to falsify data relayed to the network (Baliga 2017). A key example of a blockchain using federated consensus is Ripple, a system to settle cross-border financial transactions within minutes.

Permissioned blockchains (with pre-identified authenticated users) may be a better choice for limited-purpose decentralized computing tasks, where consensus need not be open to all potential participants and participants can be trusted not to collude against the interests of the group (Valkenburgh 2016). An example is a consortium of banks that use a private blockchain to settle derivatives. Recent developments in blockchain theory suggest hybrid models that overcome these tradeoffs by combining different types of blockchains in a ‘heterogeneous multi-chain framework’ (Wood 2017). The heterogeneous nature of this architecture enables different kinds of consensus systems interacting in a fully decentralized ‘federation’ which allows permissionless chains and closed networks to have trust-free access to each other.

As a generalized blockchain, Ethereum allows for sophisticated blockchain applications through the Ethereum Virtual Machine (EVM)—basically a computer running on top of the Ethereum blockchain that can both encode programs and execute them (Swan 2015, 21). Such applications include smart contracts, decentralized applications, and decentralized autonomous organizations.

First, ‘smart contracts’ encode arbitrary state transitions and therefore allow participants to devise more complex transactions, for example requiring a specified quorum of participants to endorse transactions—so-called ‘multi-
signature escrows’ (Buerger 2016; Diedrich 2016; Szabo 1994). By bringing contracts on the blockchain, they inherit all its key properties—immutability, censor-proofness, transparency, and auditability. Smart contracts are unstoppable because they are defined by the code and executed (or enforced) by the code, and no central authority can censor them because they are executed simultaneously across the network (Diedrich 2016). Consequently, smart contracts hold promise to drastically reduce transaction costs for routine activities, for example to settle market transactions, where a buyer could use a smart contract to automatically release payment to a supplier of a good once the good has arrived at a specified location (Krishna, Fleming, and Assefa 2017). In the design of such contracts, Ethereum allows for high flexibility as regards decision-making quorums, spending limits, and asynchronous decisions (Buerger 2016).

Second, so-called decentralized applications (dApps) essentially combine several smart contracts and can be encoded as smart programs in the EVM. A dApp has its backend code running on the Ethereum blockchain and thus imports all its desirable properties—pseudonymity, censor-proofness, auditability, and transparency. A dApp also has a frontend code and user interfaces that can refer to the backend.

Third, an even more sophisticated application—decentralized autonomous organizations (DAOs)—link several smart contracts together to form a self-governing system (Buerger 2016; Diedrich 2016; Swan 2015). A DAO is a virtual entity that has a certain set of members which have the right to modify its code and spend its funds. The members would collectively decide on how the organization should allocate its funds, for example by requiring a two-thirds majority on important issues (while participants do not necessarily have an equal number of votes). This mimics actually existing collective organizations such as IOs, but uses smart contracts for enforcement.

3. Blockchain technology and international relations

A rational-institutionalist view would contend that states will adopt blockchain technology where the net benefits of doing so are highest (or where the additional benefit compared to existing institutional solutions is highest). ‘Adoption’ hereby refers to encoding all international agreements on the blockchain so that they inherit its properties. I consider variation in the severity of commitment, distribution, and information problems, and in the types of inter-state contracts, to develop four conjectures on when and where states are more likely to adopt blockchain technology to govern international affairs.
Severity of commitment problems

In an anarchic world, states must fear for their survival when being cheated upon (Grieco 1988; Mearsheimer 1994; Waltz 1979). Since no authority—not even centralized IOs—can enforce state commitments *ex post*, IOs often serve as commitment devices *ex ante*, for instance through costly accession procedures (Martin 2017). Like traditional IOs, blockchain technology can serve as a commitment device, but with the added benefit of credibly enforcing commitments under certain circumstances. Because smart contracts cannot be stopped (as they run on top of the blockchain), they imply guaranteed punishment; hence, states bound by them are disciplined by the credible threat of punishment. As shown further below, states cannot fully escape the constraining effect of smart contracts, for instance by opting out of them in the first place. State behavior can be effectively constrained only if states have staked resources upon their commitments—‘proof of stake’ in the language of blockchains. States need to put something on the line so that if they do not follow through on their promises, they lose staked money. While no authority can force states to underlay their commitments with hard assets, the blockchain allows them to signal commitment by putting funds in custody (rather than making upfront payments). Smart contracts automate the commitment cycle by making explicit the conditions under which states lose a staked asset—leaving no discretion. As a result, problems of moral hazard would be eliminated, and costs of verification and enforcement of promises would be reduced.

Why would states want to be bound by smart contracts? Realists would contend that by hardening the bite of international law through smart contracts, blockchain technology might discourage states from making substantial commitments in the first place, with the result that compliance is higher on paper, but not actual levels of cooperation. This is tantamount to arguing that states self-select into those agreements that they expect to comply with, assigning no independent effect to international law (Downs, Rocke, and Barsoom 1996; Simmons 2010; von Stein 2005). However, there are two reasons to believe that states have interests to eliminate uncertainty at the enforcement stage. First, all governments—especially those with limited tenure such as democratically elected ones—have incentives to lock in policy. By adopting institutions from which exit is costly, they can effectively tie the hands of their successors and limit policy reversals (Boylan 2001; Goodman 1991; Tallberg, Sommerer, and Squatrito 2016). Second, guaranteed enforcement allows states to make more credible commitments to each other, without exposing themselves to undue risk because smart contracts can be programmed to not enter into force as long as a quorum of states complies with them.
Hence, the prospect of guaranteed enforcement can provide sufficient incentives for states to cooperate voluntarily through a blockchain-based governance system. If enforcement problems and the related lack of credible commitment are key inhibitors to intergovernmental cooperation, blockchain technology, and particularly smart contracts, hold promise to promote cooperation. Against this background, I propose the following conjecture.

*Conjecture 1:* States are more likely to deploy blockchain technology when enforcement problems and lack of credible commitment are more salient.

Issue areas in which these commitment problems are pervasive include foremost security, but also trade and climate change. In addition, the commitment obviously becomes more credible only for those states that participate in the blockchain governance system.

*Severity of distribution problems*

If—as some scholars argue—distributional problems are the main impediment to cooperation, the primary role of institutions is not to prevent cheating (because a once-chosen equilibrium is self-enforcing) but to help states choose among multiple equilibria with different distributional implications (Koremenos, Lipson, and Snidal 2001; Morrow 1994; Stein 1982). As argued by neoliberal institutionalists, institutions help states to do so by facilitating issue linkage and side payments (Keohane 1984).

Blockchain technology, particularly smart contracts, can be used to streamline these processes. Each state would encode in a smart contract what it would be willing to surrender in order for its favorite equilibrium to be chosen. The blockchain as a decentralized ledger of such commitments would then serve as ‘market maker’—like a trading computer on the stock market—and identify the Pareto-optimal allocation of benefits. Presumably, the efficiency gains from using blockchains for this purpose are not large but increasing in the extent to which state bargaining follows a standardized protocol, occurs rather frequently, and involves easily traceable assets. Multilateral trade negotiations provide an example that matches these conditions closely. These negotiations have long followed an informal procedure by which the most powerful states define the agenda and reach agreement in informal minilateral settings that they seek to extend to the membership at large. As the ambassador of Costa Rica stated, trade policy “is still being negotiated in a [...] widely inefficient manner” (Troyjo, Quintella, and Da Silva 2017, 60)—as it fails to search the bargaining space for globally optimal deals that make all countries better off.
Blockchain technology is particularly promising where non-state actors—both domestic and transnational—have incentives to affect state behavior to affect the distribution of benefits. By allowing these actors to devise smart contracts that promise to pay states for compliance, the resulting blockchain ecosystem would address the staking problem by contributing money from sources other than states. In other words, blockchains promise to be more effective if they allow states to realize (additional) gains from cooperation rather than suffering punishments from non-cooperation. Returning to the example in the introduction, the US multinationals favoring the Paris deal likely were the most resourceful actors with an interest to prevent the US government from withdrawing from the deal.

**Conjecture 2**: States are more likely to deploy blockchain technology where non-state actors have (financial) incentives to affect global governance regulations.

The conditions of this conjecture are most likely fulfilled in the area of climate change, with a significant green economy and a majority of consumers supporting the global environment, but also in trade, where export-oriented firms and the workers they employ may be a powerful lobby.

**Severity of information problems**

Lack of information is an impediment to cooperation as it further exacerbates enforcement problems and distributional issues. The key promise of blockchain technology is to alleviate information problems, given the way it represents data and the difficulty to tamper with the data. Hence, blockchain technology holds significant promise wherever verification that an event happened is necessary but unreasonably costly. This is particularly true where existing IOs have limited authority to collect information, for high-stakes issue areas, and issue areas with limited externalities so that other states do not experience changes in behavior by a given state. Verification demands thus should be highest in security and somewhat lower in climate change, trade, and human rights.

While blockchain technology promises to remedy information problems, it varies in its cost-effectiveness of doing so, depending on the type of transactions that ought to be verified. Blockchain technology can address a need for verification most efficiently if the underlying transactions involve digital assets (e.g., financial transfers in blockchain token). Blockchain technology is somewhat less useful where real-world events first need to be digitally represented as input to the blockchain (e.g., verifying existence of a non-digital object in exchange for a payment). It is least useful compared to traditional IOs
where it requires subsequent enforcement of digital output in the real world (e.g., removal of a physical closure of a border).

**Conjecture 3:** States are more likely to deploy blockchain technology where there is an elevated need for verification and verification is feasible.

Blockchain-based verification is cheapest when assets are digital, for example verifying if a government-owned account on the blockchain violates a deficit limit. To verify ‘off-chain events’ (those that occur in the real world but do not involve exchange of digital assets), such as the outcome of a presidential election, states can use so-called oracles. For instance, satellite imagery is a technological oracle that can verify physical installments that countries might have promised to undertake. Another type of oracle is a blockchain-based prediction market, which allows anyone to obtain accurate estimates of the probability that a specified event happened. Predictions are accurate because market participants stake real money on their predictions. Reporters also have incentives to report because they receive guaranteed payments through smart contracts. Furthermore, states which have the most interest in accurate information will act as market makers and provide liquidity to initiate a prediction market. Finally, blockchain technology is ineffective when verification is infeasible. Ascertaining whether a state has eliminated certain biological weapons is impossible because no reliable oracle exists (as non-state actors might not have access to such information).

**Complete contracts**

As long noted by rational design theorists (Abbott and Snidal 2000; Koremenos, Lipson, and Snidal 2001; Rosendorff and Milner 2001), states design more flexible agreements under conditions of uncertainty. So-called ‘soft law’—non-legally binding commitments (Abbott and Snidal 2000)—provide additional flexibility that may be desirable under conditions of uncertainty, including uncertainty about state preferences, state behavior, and the state of the world (Koremenos, Lipson, and Snidal 2001).

Many international agreements which include escape clauses, treaty reservations, and non-legally binding provisions are ‘incomplete contracts’, in which “parties would like to add contingent clauses but are prevented from doing so by the fact that the state of nature cannot be verified (or because states are too expensive to describe ex ante)” (Hart and Moore 1999). For example, the Stability and Growth Pact (SGP) allows Eurozone member states to temporarily violate the deficit criteria under ‘unexpected adverse economic circumstances’—as defined essentially by a majority of states themselves. Smart contracts do not eliminate the possibility for escape clauses, but the
computerized language of these contracts requires states to make ambiguity explicit. The SGP cannot be made smart because it must defer to states (or a designated agent) to evaluate its condition, which lowers the efficiency gain from automated implementation while reducing the credibility of member state commitments. In other words, there is a tradeoff between guaranteed enforcement and contractual flexibility. But hopes are that the capacity of blockchain technology to reduce informational problems can enlarge the scope for completeness by making states of nature more easily verifiable.

Its informational benefits notwithstanding, blockchain technology will be more attractive to states to govern routine-type interactions. A blockchain-based governance system makes routine activities such as (secure) exchange of documents, bilateral lending, or cross-border infrastructure projects cheaper because the blockchain offers a secure way of accessing, verifying, sending, and storing information. Previously, without blockchain technology, states had to rely on trustworthy intermediaries, even for routine interactions. An example would be an IO that collects information from its member states on fishing quotas. Each state could then realize net absolute gains from replacing the IO with a blockchain-based fishing information system, which would perform this task more cheaply.
<table>
<thead>
<tr>
<th>Example</th>
<th>Security cooperation</th>
<th>Trade governance</th>
<th>Climate governance</th>
<th>Human governance</th>
<th>Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Disarmament treaty (successive commitments to reduce stocks of weapons)</td>
<td>Trade liberalization of tariffs and non-tariff barriers</td>
<td>De-carbonizing national economies (schedules of commitments of GHG emission reductions)</td>
<td>Respect for human rights (democratic elections, among others)</td>
<td></td>
</tr>
<tr>
<td>Conditions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Severity of commitment problems</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>Severity of distribution problems</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>Severity of information problems</td>
<td>Demand for verification</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Ease of digitally tracing events and extent to which on-chain enforcement coincides with enforcement in the real world</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>Prevalence of routine interactions</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>Prediction</td>
<td>Blockchain-based global governance</td>
<td>Somewhat likely</td>
<td>Likely</td>
<td>Likely</td>
<td>Unlikely</td>
</tr>
</tbody>
</table>
Conjecture 4: States are more likely to deploy blockchain technology to govern routine interactions, compared to discretionary operations.

Issue area predictions

Based on the above conjectures, it is possible to assess the potential usefulness of blockchain technology across different issue areas (Table 1). In security cooperation—plagued by enforcement problems and lack of information—demand for blockchain technology may be high. However, for a range of security problems, verification is infeasible and blockchain technology thus holds no promise.

In trade cooperation, distributional concerns are more important, even though cheating continues to matter. The current system—with the WTO at its epicenter—offers states a legal procedure to challenge purported violations of trade policy obligations but is slow and lacks ultimate enforcement capability. Moreover, trade policy bargaining is arcane and formally excludes firms (and others) which are directly affected by trade policy. While blockchain technology has nothing to offer to ascertain breaches of trade law (WTO expert authority is still needed for this purpose), it can foster compliance, for example by securely channeling resources of affected firms on the complainant side that incentivize defendant countries to remove unlawful protections. Further, states reluctant to fully liberalize trade, for example because they need tariffs as a source of revenue, could pledge to zero out tariffs in return for money collected from firms with an interest in liberalized trade. These examples show that—in addition to the existing business-to-business blockchain solutions to streamline global trade finance (Chatterjee 2017; Troyjo, Quintella, and Da Silva 2017; Wigley and Cary 2017)—trade governance is an area where blockchain technology is potentially useful, specifically with respect to facilitating deeper trade commitments (incentivized by non-state actor payments) and preventing violations of trade commitments. It is least useful to ascertain whether certain measures actually violate trade law.

As further illustrated below, blockchain technology holds promise also for climate governance (Chapron 2017), provided that the challenge of bringing real-world events (for example evidence of re-forestation in a given area) can be solved. In contrast, the area of human rights is a least-likely case for blockchain-based governance. This is because the underlying asset—respect for human rights—is hard to trace digitally on a routine basis and to enforce in the real world. As long noted by International Relations scholarship, states have comparatively fewer incentives to enforce human rights abroad, and the non-state actors that are most interested in better human rights records lack powerful financial means.
4. Climate change and blockchain-based global governance

In the following, I examine the potential of blockchain technology to enhance the effectiveness of climate governance. Climate governance is a most-likely case for the adoption of blockchain-based global governance, given the general willingness of most states to cooperate with other states, the existence of individual initiatives to support climate action, the demand for reliable information, and the presence of routine interactions.

The prevention of climate change—through the reduction of greenhouse gas emissions into the atmosphere—is a global public good and as such suffers from a collective action dilemma: Any reduction by one state is as good as any reduction by another, therefore states hold out for doing costly reductions on their own but wait for others to do the job. In addition, as the costs of decarbonizing economies are unevenly distributed, states face a distribution problem.

The Kyoto Protocol was a binding international agreement in which industrialized states committed to reduce their emissions through national measures and three market-based mechanisms, facing fines in case they failed to reach their emission reduction targets which led to the exit of two major emitters. While the Kyoto regime is a top-down approach, its successor regime—the Paris agreement—takes a bottom-up approach in which states set their own targets but communicate them internationally (Hale 2016). The Paris accord hence replaces hard law by reputational concerns and network effects (Falkner 2016). States can also count emission reductions outside their jurisdiction toward their national target.

Blockchain technology could help states achieve faster the goals of the Paris agreement by making emission reductions trading more efficient, promoting climate-related crowdfunding and transparent allocation of such funding to individual projects, and facilitating peer-to-peer energy trading (UNFCCC 2017). While policy networks—including the Climate Ledger Initiative (CLI) and the Climate Chain Coalition (CCC)—have discussed these applications at the recent UNFCCC summit in Bonn, scholars have developed these ideas further and turned them into actionable proposals. With regard to emissions trading markets, recent proposals show how blockchain technology can be used to overcome the fragmentation of emission reductions trading markets, to mitigate the risk of double-counting, and to incentivize investment into long-term abatement technology (Fu, Shu, and Liu 2018; Jackson et al. 2018; Khaqqi et al. 2018). Another area of blockchain-based applications is climate-related crowdfunding. WeiFund provides an example of an open crowdfunding platform implemented through smart contracts on the Ethereum blockchain (Aganaba-Jeanty, Anissimov, and Fitzgerald 2017). Other projects seek to find innovative...
ways to mitigate the carbon footprint of blockchain technology itself, for instance by using transaction fees in the network to buy real-world carbon credits. Finally, blockchain technology is already being used for peer-to-peer energy trading. For example, SolarCoin is a community-based solar electricity reward program. Any solar installation can register with the network and receive SolarCoins for a verified amount of solar electricity produced. Users can spent coins for solar energy within the network or exchange them for fiat currencies (Wigley and Cary 2017, 28).

The set of potential applications of blockchain technology for climate governance is much larger. To be sure, since nationally determined contributions are not meant to be binding, it makes little sense to translate them into smart contracts. However, if states share the objective of halting climate change but are primarily concerned with cheating—that is, (other) states not following through with de-carbonization—smart contracts would be useful. If states fail to honor their commitments, the money staked upon them could be channeled to the Green Climate Fund or similar entities that support climate change adaptation in the most affected developing countries. A blockchain-powered incentive system might thus have helped the international community to attain its climate-related goals, even when key states were to renege on their commitments.

The strength of non-state actors is another reason why climate governance is likely to witness the use of blockchain technology. Around the globe, sub-state actors (such as cities) and individuals already invest into green energy and lobby their national governments to embrace de-carbonization. States could harness this potential by intertwining the intergovernmental blockchain with (national-level) permissionless blockchains. Imagine that anyone can earn ‘greencoins’ by planting trees (equivalent to ‘mining’ in the Bitcoin system); but to ensure that greencoins have actual value, states could stake real money on them—through a smart contract that takes a monetary deposit from each state (total contributions might be around USD 100 billion). If states fail to comply with their emission reduction targets, their deposit will be taken and redistributed as greencoins to individuals that have planted trees. Verification of trees planted could be achieved automatically by specialized drones or satellite geo-imaging. Instead of planting trees, individuals could also buy up greencoins to support climate change policies. By increasing the exchange value of greencoins, these individuals would provide incentives for more rapid tree-planting.

Obviously, tree-planting is just one example of climate-related activities; states could agree on a list of potential measures along with ways of verification and the incentive system underlying effective decentralized verification. Bringing climate governance on the blockchain would make climate policy more effective (real incentives to promote de-carbonization due to the exchange value of
greencoins) and more legitimate (commitments are more transparent, climate action is auditable, and non-state stakeholders such as the wood pellet industry—instead of lobbying their governments on climate policy—would just buy greencoins or plant trees).

5. Blockchain technology and international relations: a research agenda

Lack of trust in the international system is an obstacle to increased cooperation among states. The notion that anarchy—the absence of a central authority that enforces state commitments—prevents secure relations and mutually beneficial exchange between states is widely accepted in rationalist theories of international relations. As a world government is unlikely to come into existence, the current approach is a system of international institutions (often upheld by IOs) that promote decentralized enforcement of state commitments. Despite their undisputed merits, IOs have several shortcomings, such as lack of capacity to enforce commitments, high administrative costs, and the risk of falling prey to particularistic interests.

Against this background, I examined the potential of blockchain technology as a new type of international institution to make international cooperation more effective. The usefulness of blockchains for global governance is related to greater transparency, ease of verification, and guaranteed enforcement of smart contracts. In light of the reality that the international system has no central authority, blockchain technology can offer a decentralized solution to cooperation problems. It can do so most effectively in conjunction with existing IOs, which continue to perform vital tasks and which can play an active role in stewarding blockchain-based governance.

While blockchain technology is no panacea, it can help promote international cooperation under specific circumstances and appropriate blockchain design choices. First, it is useful when states need a credible threat of guaranteed enforcement, which is when being cheated upon involves existential risks. Smart contracts—combined with staking—cater to this need. Second, blockchain technology is useful when assets are digitally traceable, although prediction markets provide an efficient means to represent off-chain events on the blockchain. Efficiency gains from blockchains are greatest for routine state interactions, such as financial transactions under specified conditions. Third, blockchain technology holds promise when non-state actors that are financially capable and motivated to affect global regulations are present. In this case, a blockchain federation interlinking state-only blockchains and public blockchains through a common currency is the appropriate design. Under these circumstances, states would participate voluntarily in a blockchain-based governance system, thus dispensing with a need of a hegemonic enforcer.
These conditions imply climate governance is a most-likely case for blockchain technology. Use cases involving non-state actors already exist but blockchain-based governance systems among states are close to being established. Similar breakthroughs can be expected for the area of trade policy, monetary cooperation, and development finance. In the last area, IOs are using blockchains to securely provide humanitarian assistance and where donors could use smart contracts to administer conditional aid programs. In security cooperation, use of blockchain technology is hampered by the non-traceability of certain assets and challenges to staking, although state demand for guaranteed enforcement would be highest in this area. Finally, the area of human rights is least likely to adopt blockchain technology in the near future, due to low demand for enforcement, absence of a financially powerful domestic lobby, and verification problems.

The most likely path of how blockchain technology will breakthrough in international relations is one involving two stages. In a first step, states will codify all their existing (and new) agreements as smart contracts and register them on a permissioned blockchain in which all states participate. States will admit entrusted third parties such as IOs for certain functions, for example validation. Governments may decide to give non-members read-only access, thereby making politics more transparent and themselves more accountable. In a second step, the above permissioned blockchain may be interwoven with other blockchains in a federation. The emerging ecosystem would be governed by a set of smart contracts. As described in the climate change case study, a blockchain federation with an incentivized decentralized verification system holds promise to leverage the capacities of non-state actors in solving global problems in a fully transparent way.

Three issues merit particular attention in future research. A first issue pertains to the implications of blockchain-based governance for currently-existing IOs. Some argue that the use of blockchain technology will make IOs more efficient. Some IOs have already explored ways to harness the technology for their ends (Lagarde 2017; Pani 2016). If IOs persist, they will undertake different roles, because some functions that IOs perform today such as the maintenance of a ledger can be more easily delivered by the blockchain. A key strength of blockchains is to streamline execution of any type of contract. Further, with a more credible threat of enforcement, violations of commitments will decrease, along with actual sanctions. Sanctions themselves become more effective using blockchains because states can no longer free-ride on sanctioning efforts of others. But IOs might still be needed as venues to deliberate policies, foster consensus, and build capacities among member states. For yet other functions, IOs may continue to be important but may not be the only actors anymore, as evidenced by the rise of prediction markets which can verify the occurrence of certain events in the same way as IOs. While blockchain technology arguably is
most effective if deployed in conjunction with existing IOs, more research would be necessary to better understand the relationship between blockchains and currently-existing IOs.

A second issue pertains to the relation between blockchain-based governance and the nation-state. Blockchain advocates argue that the technology advances democracy by reducing the ability of states to control societal interactions, as exemplified by Bitcoin (Brito and Castillo 2016). Critics contend the technology threatens the nation-state by reducing societal interactions to a trustless exchange for mutual benefit (Atzori 2015). Citing previous experience from the introduction of new technologies, they also contend that blockchains serve to alter the distribution of power, similar to the digitalization of government which favored ‘political-administrative coalitions in public administrations’ (Kraemer and King 2003, 10). While such concerns should be discussed seriously, they are misleading in the specific context of international cooperation, where no legitimate central authority exists. To be sure, the blockchains discussed in this article do not diminish the role of states but involve them as key actors in blockchain-based global governance while helping to make global governance more accountable. While public accountability is ensured through unrestricted read-only access to the blockchain, states could further increase democratic legitimacy by inviting relevant stakeholders (such as NGOs) to participate in the consensus mechanism. A blockchain federation, which would allow states to harness resources from non-state actors, would facilitate transition from the current system in which power is distributed according to (largely non-transparent) lobbying contributions toward blockchain-based governance where parties stake publicly for their interests. In this light, blockchains might offer ways to address democratic deficits of IOs (Dingwerth, Schmidtke, and Weise 2011; Moravcsik 2004; Tallberg et al. 2014). However, the ramifications of new technology with respect to global governance remain underexplored and should be addressed in future research.

A final area of inquiry would address some of the following questions: How much more effective compared to the business-as-usual case would blockchain-based governance in the international arena be? Why has blockchain-based global governance not been implemented yet? What explains variation in regulation of blockchain technology in different countries? Pending the actual use of blockchain and the generation of related data, answers to these questions would further enhance our understanding of the underlying political economy of blockchains and allow for policy recommendations regarding appropriate blockchain designs. If blockchain-based global governance were to be implemented, the focus of inquiry would be to explain why some states participate in it while other states do not. In this regard, existing research in political economy—notably on the adoption of new technologies such as the internet (Milner 2006)—provides testable arguments. To the degree that states
cannot prevent individuals from using permissionless blockchains (unless they completely shut down the internet), their participation in permissioned blockchains is voluntary. A straightforward prediction would be that demand for permissionless blockchains by non-state actors is higher autocracies, while autocratic governments are less likely to join permissioned blockchains as their disutility of being exposed to transparency is greater. This exemplary discussion shows that the unique features of blockchain technology provide for new avenues of testing pertinent theories of international relations and domestic politics.
Notes


2 Both types of blockchains are not much different with respect to their requirements on trust. All blockchains are designed to withstand untrustworthy nodes in the network through their consensus mechanisms, and trust in the blockchain as a whole is based on “the non-predictive distribution of power over block creation among nodes unlikely to collude” (Monax 2017).

3 Every transaction to be recorded in a blockchain requires payment of a fee in a natural currency. Hence, limiting the number of computations reduces transaction costs.

4 The simplest DAO design involves a piece of self-modifying code that changes if a qualified majority of members agree on a change. Although code is theoretically immutable, it can be de-facto muted by having chunks of the code in separate contracts, and having the address of which contracts to call stored in the modifiable storage.

5 DAOs would be governed by three transaction types, distinguished by the data provided in the transaction: proposal transactions, transactions to vote for a proposal, and transactions to finalize a transaction provided enough votes were made (Buerger 2016).

6 I am limited to conjectures because the non-existence of a blockchain-based global governance system prevents me from formulating hypotheses that are actually testable.

7 An example of a promise is a donor commits to pay a recipient a specified amount of aid once the latter has reformed its public financial management system. An international audit firm might be tasked to verify such reform and encode it on the blockchain, which will release automatically the payment from the donor account to the recipient account.

8 An early non-digital analogue to staking is royal intermarriage. Blockchains extend this notion further by allowing arbitrary resources to be staked on commitments.
9 Similarly, international law stipulates that a treaty commitment is not binding until a sufficient number of states have ratified it. This provision allays concerns about other states obtaining relative gains from delaying ratification. It can be easily implemented in ‘blockchain law’ using multi-party escrows (Diedrich 2016).

10 Augur is such a prediction market. It does not run on a single central server and cannot be manipulated. All participants report on the outcome using a consensus-based mechanism. Safe payment is ensured via smart contracts—see https://augur.net/ (accessed October 22, 2017).

11 Fines would be ‘in-kind’ and only relevant if the agreement were to enter a universal second commitment period, which it did not. The United States under the Bush administration declared it would not comply with the protocol, and Canada eventually quit three years after ratifying it with reference to the high cost of complying.

12 Double-counting of emission reductions is a key problem identified in the literature. Under the Kyoto regime, a centralized authority—the UN Climate Secretariat in Bonn—keeps an authoritative ledger of reduction projects. The Paris agreement calls for ‘robust accounting’ (Article 6.2), for example through transaction logs, but does not mention use of blockchain for this purpose.


15 To be sure, the United States never ratified the Kyoto Protocol, but smart contracts could have enabled it to participate in the first place while also raising the cost of non-compliance.

16 This is the collective climate finance commitment under the Copenhagen accord.

17 Similar requirements are in place in the current system, in which all treaties must be notified to the UN secretariat. However, whether states follow through cannot be verified, in part because the UN Treaty Database is cumbersome and not machine-readable.
Before these two steps, IOs themselves might use blockchains to govern their inter-organizational relations. The latter is an increasingly important phenomenon (Biermann and Koops 2017).

Aganaba-Jeanty, Timiebi, Sam Anissimov, and Oonagh E Fitzgerald. 2017. *Blockchain ClimateCup Round Table*. Toronto.


Gray, Julia. 2018. Presented at ISA Conference, April 4-7 *Patronage Explanations for the Survival of International Organizations*.


He, Dong et al. 2016. *Virtual Currencies and Beyond: Initial Considerations*. Washington D.C.


