METAPHILOSOPHY

METAPHILOSOPHY
Vol. 48, No. 5, October 2017
0026-1068

BLOCKCHAIN, THE GREATER GOOD, AND HUMAN AND CIVIL RIGHTS

KOBINA HUGHES

Abstract: The central theme of this paper is that the development of a technology that is predicted to have a major impact on the way we transact with each other should be a matter where the needs of society at large are taken into account. Where the technology is one that emerges from the domain of the Internet, inclusivity becomes even more acute in order to avoid widening the already existing gap in reaping the "digital dividend." With blockchain, the obligation could even be seen as a moral one, as blockchain is said to have the potential to negate the scope for the abuse of trust by states and institutions. This could be a game changer in areas such as public procurement and the conduct of elections where abuse can lead to the denial of essential resources and a concomitant loss of life, or to conflict and mass killings. Blockchain presents an opportunity for the Internet development community to claim a degree of recognition in the human rights realm by aiding civil intervention in areas where military intervention has been deemed inappropriate.

Keywords: blockchain, human rights, inclusion, cyber access, digital divide, anti-corruption, electoral processes, moral responsibility.

Introduction

Blockchain has been described as "one of the most fundamental inventions in the history of computer science" and as being "at the heart of the fourth industrial revolution" (Schwab 2016). It is seen as having the potential to radically transform the way in which we live and transact with each other because it solves the problem of trust in transacting with third parties: "The formidable innovation introduced by this technology is that the network is open and participants do not need to know or trust each other to interact: the electronic transactions can be automatically verified and recorded by the nodes of the network through cryptographic algorithms, without human intervention, central authority, point of control or third party (e.g. governments, banks, financial institutions or other organizations)" (Atzori 2015, 2).

The issue raised in this paper is that blockchain may have a contribution to make towards the improvement of services for the wider community and in the protection of human rights and that while there are a number of blockchain developments aimed at the welfare of the vulnerable, progress in this area would benefit from a more structured approach.[1]

In less than a generation the Internet has demonstrated its potential to improve the lives of billions of individuals and accelerate the economic development of countries. Billions remain offline, however, and the "digital divide" could result in significant numbers of the global population being omitted from the benefits that the Internet brings. McKinsey and Co. highlighted this concern in its August 2014 report on Internet access: "This is an issue for all of us. The voices, ideas, and contributions of the offline population can't be heard and often can't be made until they're connected. It is therefore crucial to identify and aggressively pursue opportunities to make the Internet accessible to all." McKinsey reported that nearly 4.5 billion people were offline (meaning that only 43 percent of the world's population had regular access to the Internet). McKinsey further reported that in the world's poorest countries, only one in ten people was online, that 3.5 billion of the offline lived in just twenty countries, that nearly one billion of those 3.5 billion were illiterate, and that between 1.1 billion and 2.8 billion individuals could not get online via a mobile network because they did not live within an area with network coverage. The concern is whether, if left to its own devices, blockchain will spontaneously do things that might be for the greater good (including the good of the offline billions) or whether it will simply develop in the more commercial and lucrative direction that its investors and developers are (understandably) likely to pursue. As one of blockchain's key features is its ability to negate the potential for the abuse of power through the exploitation of dependency and trust relationships, we could usefully explore its potential to disrupt abuse by governments engaged in corrupt practices and human rights abuses.

The related question of whether or not Internet access is itself a basic human right has been the subject of U.N. review in recent years. Following developments in Estonia, France, Costa Rica, and Finland that leant towards recognition of a right of access, the U.N.'s Special Rapporteur reported in June 2011 that the Internet had become "an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress."[2] On 1 July 2016, the U.N. passed a Resolution that (amongst other things) affirmed "the

[1] Blockchain initiatives in the human rights and improved services for all arenas include (i) the Refunite project, reconnecting refugee families (https://refunite.org/), and (ii) reducing the cost and effectiveness of money transfers. See, for example, "11 Money Transfer Companies Using Blockchain Technology," LTP, 23 October 2015. At https://letstalkpayments.com/11-money-transfer-companies-using-blockchain-technology-2/ (last accessed on 11 September 2017).

[2] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. General Assembly, 16 May 2011, at paragraph 85. At http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (last accessed on 10 September 2017).

importance of applying a comprehensive human rights-based approach in providing and in expanding access to [the] Internet" and requested that "all States make efforts to bridge the many forms of digital divides."[3] This was reported, slightly inaccurately, by the press as the U.N. having resolved that access to the Internet is to be considered a basic human right.[4] In response to these developments at the U.N. an extremely important point was made in an article by Vint Cerf in the *New York Tim*es:

> [P]hilosophical arguments [over whether Internet access is a human right, a civil right, or neither] overlook *a more fundamental issue: the responsibility of technology creators themselves to support human and civil rights.* The Internet has introduced an enormously accessible and egalitarian platform for creating, sharing and obtaining information on a global scale. As a result, we have new ways to allow people to exercise their human and civil rights.... As we seek to advance the state of the art in technology and its use in society, we must be conscious of our civil responsibilities in addition to our engineering expertise.... Improving the Internet is just one means, albeit an important one, by which to improve the human condition. It must be done with an appreciation for the civil and human rights that deserve protection.[5]

The proposition that technology creators have a responsibility to support human and civil rights is the very same point advocated in this article. The idea isn't new. The Human Rights Center at the University of California at Berkeley, for instance, has been developing initiatives in this area for more than twenty years and has pioneered innovation in the use of technology in the exhumation of mass graves, for example.[6]

If blockchain is unlikely, in the absence of a conscious effort, to develop capability in an area of such fundamental importance as the protection of human rights then we need to consider how the necessary stimulus is to be provided. As a counterpoint, it has to be recognised that blockchain technology, like the Internet or any other technology, is to some extent neutral, and can be used by malicious agents, such as corrupt governments, as well good agents to realize their outcomes.

[3] Human Rights Council, Thirty-second session, Agenda item 3, Resolution adopted by the Human Rights Council on 1 July 2016, 32/13. The promotion, protection and enjoyment of human rights on the Internet. At https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/156/90/PDF/G1615690.pdf?OpenElement (last accessed on 11 September 2017).

[4] "Internet Access Is Now a Basic Human Right: Part 1—Chips with Everything." Tech podcast. At https://www.theguardian.com/technology/audio/2016/jul/29/internet-access-human-right-tech-podcast (last accessed on 11 September 2017).

[5] Emphasis added. "Internet Access Is Not a Human Right," *New York Times*, Opinion Pages, 4 January 2012. At http://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html?mcubz=1 (last accessed on 11 September 2017).

[6] See "Soul of the New Machine: Human Rights, Technology & New Media." At https://www.law.berkeley.edu/research/human-rights-center/multimedia/soul-of-the-new-machine-human-rights-technology-new-media/ (last accessed on 17 September 2017).

Furthermore, there is regulatory risk to blockchain technology being outlawed or regulated by governments, particularly corrupt ones. These concerns make the need for action by those with an interest in preventing human rights and other abuses even more important.

Policy, Priorities, Inclusivity and Coordination

If blockchain is really going to change things as radically as is being predicted then we need to consider whether it can be used to develop systems, tools, and techniques that further the principles of freedom, justice, and peace in the world, and that champion human rights and the rule of law.

Advances in drone technology and mobile phone communications have led to improved access to services, humanitarian relief, the preservation of the environment in regions where medicines are delivered to remote areas, telemedicine, and the surveying and mapping of land to prevent illegal mining and the contamination of water bodies. If these technologies that were not heralded with quite as much fanfare can do so much to help alleviate suffering and to protect and preserve rights and resources, could blockchain have similar impacts or even greater ones if channelled effectively?

While the potential of blockchain to impact accountability and transparency in government has already received some attention from developers, the trend would appear to be towards the development of new, more streamlined, less costly end-user-controlled products and services to compete with products traditionally offered by banks and the financial services sector, and the development of commercially more advantageous schemes for coalface workers (e.g. music industry rights claims and improving conditions for workers in cyber-enabled businesses, such as Airbnb and Uber [Tapscott 2016]). These developments, though welcome, are clearly not priorities for the poor and vulnerable in developing countries.

When it comes to determining what the critical issues for cyber-excluded or low-resource communities are, what the priority areas for action should be, what the strategies for implementation and the role of those there on the ground should be, inclusion becomes vital. Divergent views will emerge. For example, the scope for electoral fraud in wealthy, industrialised nations is in the main much less than in poorer countries and vote-rigging on the basis of an absence of records is generally much more difficult. As a consequence an interest in directing blockchain or digital development in this area may not be seen as having the same degree of urgency. As Andreas Antonopoulos once remarked in an interview, "In terms of voting, the real question is what problem are you trying to solve, which is often the case when geeks come into politics? What problem are you trying to solve with voting: verifying the integrity of the vote? We don't really have a voting fraud problem, at least not to [*sic*] the United States" (Frauenfelder 2016).

Another concern about developing blockchain's humanitarian potential is the lack of direction and coordination. The absence of central control has been a badge of pride for cyber citizens from the early beginnings of the public Internet (Barlow 1996). Indeed, the Internet Society has argued that the historic and future success of the Internet as an open and trusted platform for innovation and empowerment depends on a decentralized, collaborative, and multi-stakeholder approach to governance. It argues that the decentralized and community-driven management approach of the Internet is what has enabled its growth and innovation.

A recent report by the Global Commission on Internet Governance argued, however, that "Internet governance is one of the most pressing global public policy issues of our time" and helpfully proceeded to set out three possible future scenarios for the Internet (GCIG 2016). In the worst-case scenario the Internet collapses for a number of reasons. The second scenario is one of stunted growth where some users capture a disproportionate share of "digital dividends" while others are permanently locked out, and a world of digital haves and have-nots results. In the third scenario, the Internet is "energetic, vigorous and healthy," producing unprecedented opportunities for access to information and knowledge, growth, development, and innovation. As the report says, the third scenario is the scenario to which most of the world aspires, but "[r]ealizing this future requires concrete actions to ensure that the Internet will be open, secure, trustworthy and inclusive of everyone." The fact that the report specifically places an emphasis on social justice and human rights as a feature of the third scenario and that it recognises the need for direction and focus to steer developments in that direction is extremely encouraging.

Corruption and Electoral Fraud

One of the root causes of suffering in developing countries is governments that fail to fulfil their sovereign responsibility to protect their populations from harm.[7]

[7] The Responsibility to Protect, Report of the International Commission on Intervention and State Sovereignty, December 2001, at paragraph 1.35: "It is acknowledged that sovereignty implies a dual responsibility: externally—to respect the sovereignty of other states, and internally, to respect the dignity and basic rights of all the people within the state. In international human rights covenants, in UN practice, and in state practice itself, sovereignty is now [to] be understood as embracing this dual responsibility. Sovereignty as responsibility has become the minimum content of good international citizenship." At http://responsibilitytoprotect.org/ICISS%20Report.pdf. (last accessed on 11 September 2017).

The doctrine of the Responsibility to Protect was developed by the U.N. over the past two decades, following the atrocities in Somalia (1993), Rwanda (1994), Bosnia (1995), and Kosovo (1999). The doctrine provides justification for intervention by U.N. member states in the affairs of a sovereign state where the state fails in its duty to protect its own citizens and engages in "atrocity crimes." While sanctions and other soft measures are not entirely excluded, the doctrine is primarily concerned with military intervention: "The emerging principle in question is that intervention for human protection purposes, including military intervention in extreme cases, is supportable when major harm to civilians is occurring or imminently apprehended, and the state in question is unable or unwilling to end the harm, or is itself the perpetrator."[8]

Heads of State and Government at the 2005 World Summit deliberately limited the scope of the Responsibility to Protect to the four crimes of genocide, war crimes, ethnic cleansing, and crimes against humanity ("atrocity crimes" or "mass atrocity crimes") (U.N. 2005). The Secretary-General's 2009 Report on Implementing the Responsibility to Protect explained: "The responsibility to protect applies, until Member States decide otherwise, only to the four specified crimes and violations: genocide, war crimes, ethnic cleansing and crimes against humanity.... To try to extend it to cover other calamities, such as HIV/AIDS, climate change or the response to natural disasters, would undermine the 2005 consensus and stretch the concept beyond recognition or operational utility" (U.N. 2009, 8). Accordingly, economic crimes (as well as "calamities, such as HIV/AIDS"), invariably the precursors to atrocity crimes, were excluded from the ambit of the doctrine. Given that the failure of leadership and government are at the heart of both atrocity crimes and economic crimes, the only possible justification for intervention in one but not the other is that there is no (immediate) violence or bloodshed in the case of economic crimes.

The cost of economic crimes in money and lives, however, is arguably higher than that associated with atrocity crimes. Africa alone is

[8] The Responsibility to Protect, Report of the International Commission on Intervention and State Sovereignty, December 2001, at paragraph 2.25. Paragraph 4.19 reads:

> In the Commission's view, military intervention for human protection purposes is justified in two broad sets of circumstances, namely in order to halt or avert:
>
> - large scale loss of life, actual or apprehended, with genocidal intent or not, which is the product either of deliberate state action, or state neglect or inability to act, or a failed state situation; or
> - large scale "ethnic cleansing," actual or apprehended, whether carried out by killing, forced expulsion, acts of terror or rape.
>
> If either or both of these conditions are satisfied, it is our view that the "just cause" component of the decision to intervene is amply satisfied.

estimated to be losing more than $50 billion annually in illicit outward financial flows, per the United Nations Economic Commission for Africa (UNECA 2016, 78). The ONE Campaign estimates that at least $1 trillion is being taken out of the budgets of developing countries each year through a web of corrupt activity and suggests that the vast sums being diverted are preventing some countries from financing their fight against extreme poverty, disease, and hunger. In the ONE Campaign's assessment, a combined total of 7.9 million deaths per annum in low-income and lower-middle-income countries in the decade to 2025 could be prevented if these diverted revenues were instead properly invested in the health systems of those countries (Hector 2014). By way of comparison, in 2015 somewhere in the region of fifty-five thousand people were killed in the on-going Syrian war, including twenty-one thousand civilians. The total number of deaths in the five years of that conflict stood at around two hundred and fifty thousand by the end of that year (Deutsche Welle 2016).

As economic crimes will not lead to intervention by the U.N. under the doctrine of the Responsibility to Protect, other actors who have the potential to restrain abuse in this area could usefully step in. Given that a breach of trust lies at the heart of economic crimes and given that the key feature of blockchain is its decentralized approach to achieving consensus and trust through a proof-of-work consensus algorithm, blockchain technology could be an important factor in plugging the intervention gap left behind by the U.N. in its implementation of the doctrine of the Responsibility to Protect by adding a new cyber weapon to the fight against corruption and other economic crimes and holding offending states to account. In so doing, the axiological nature of blockchain is put in play.

Electoral processes can lead to conflict and killings when they are perceived as not having been conducted in a free and fair manner (UNDP 2009, 7). The scope for election rigging is high in poorer countries, which, typically, have a one-party state or two parties splitting voters in a 50:50 "winner takes all" electoral environment.

Registers of births and deaths are often not robust or reliable for a variety of reasons. Records may only go back a few decades, meaning that many adults do not have birth certificates. Death certificates are seldom obtained, and the necessary (manual) entries in registers are not made, leading to a preponderance of ghost voters. Likewise, and for the same reasons, there is a preponderance of underage voters. Problems with the accuracy of I.D. systems means that bussing rogue voters in from neighbouring countries for registration and voting can and does occur, especially where colonial borders cut through ethnic groups and border crossers can swell the votes for a particular candidate. In a nutshell, the outcome of an election can be heavily influenced (if not pretty much predetermined) by the absence of a credible voters' register at the outset.

As with economic crimes, the question is whether, given that a breach of trust lies at the heart of electoral fraud, blockchain could help address the problem of electoral fraud and the conflict and violence that can sometimes follow, and whether tightening up electoral processes is another candidate for concerted blockchain developer action. If so, once again, blockchain's axiology is put in play.

Admittedly, work is already under way in the field of identity, identification, and digital democracy. Advances, however, need to be more carefully planned and coordinated. In *Code: And Other Laws of Cyberspace, Version 2.0*, Lawrence Lessig discusses the Microsoft-led project to develop an Identity Metasystem (an Identity Layer) on the Internet. While he welcomes the development and takes the view that it will give users the ability to control precisely what data is revealed to those who demand data about them, he raises a sinister point:

> Individuals right now can be effectively anonymous on the Net. A platform for authenticated identity would make anonymity much harder. We might imagine, for example, a norm developing to block access to a website by anyone not carrying a token that at least made it possible to trace back to the user – a kind of driver's license for the Internet. That norm, plus this technology, would make anonymous speech extremely difficult. . . .
>
> In the Internet's first life, encryption technology was on the side of privacy. Its most common use was to keep information secret. But in the Internet's next life, encryption technology's most important role will be in making the Net more regulable. As an Identity Layer gets built into the Net, the easy ability to demand some form of identity as a condition to accessing the resources of the Net increases. (Lessig 2006, 52, 54)

And Ehud Shapiro argues:

> . . . . Internet technology today does not support the right of assembly, and therefore it cannot and does not support democracy. The reason is that even though we can easily form groups on Google, Facebook, you name it, we don't know who the people on [*sic*] the group are. A person [may not] be the person he says he is, or may be multiple personae [or] really fakes operated by the same person.
>
> Fortunately, help is on its way. The United Nations and the World Bank have a goal to deploy electronic identities for all of humanity by 2030. With electronic identities, one can easily verify the person who is on the Internet and have confirmed identity, and therefore eventually support the freedom of assembly on the Internet. And then following it, we will also hopefully be able to form Internet democracy. (2016)

The prospect of cyber identification being a prerequisite to exercising your right to vote may not be that attractive a prospect to those living in tyrannical situations. Development needs to be made in greater collaboration with those affected and their advocacy groups going forward.

Conclusion

This paper queries whether blockchain developers should be encouraged to consider the role that blockchain could play in holding failing governments to account and in protecting the persecuted and the oppressed in addition to developing applications for the better conduct of commerce and the more efficient delivery of government and municipal services.

Atzori argues that while blockchain technology has the potential to allow individuals and communities to redesign their interactions in politics, business, and society at large, with an unprecedented degree of disintermediation through the use of automated, trustless transactions, the traditional functions of the state cannot be substituted with blockchain-based services. Her view is that the state is a necessary central point of coordination in society:

> Admittedly, the blockchain technology can greatly improve structure, management and decision making process of specific realities, making them less dependable on top-down coordination. Yet, decentralization is not always the best choice for all organizations and there are limits to what blockchains are suited for. In particular, algorithms and binary codes are not meant for policy-making, since politics is an art that stems from the ethic sphere of human beings and it belongs to them exclusively, as creatures "endowed with reason and conscience." (Atzori 2015, 22)

It may indeed be the case (for the time being at least) that in matters of policy, reason, and conscience (such as human rights abuses) computational technologies are no substitute for human endeavour. That should not, however, stop us exploring whether blockchain technology could help with holding the state accountable and with interventions where the state is failing in its responsibilities, after the application of reason and conscience. The challenge posed is whether we choose to direct some of the blockchain initiative to flow uphill to the pool of humanitarian protection or whether we simply choose to allow it to develop in the absence of a policy drive directed at preventing abuse.

Technology and human rights is a vibrant and complicated area spanning a number of fundamental aspects of global culture, including governance of the Internet itself, disrupting the position of powerful corporations and vested interests, impacting the role of powerful institutions such as the U.N. in the human rights sphere, interfering with the sovereignty of nation states, raising concerns about personal and global security, cyberwars and terrorism on the Internet, the use and protection of personal data, and matters of life and death in conflict situations.

But the U.N. has determined that intervention in the affairs of member states where states are failing to abide by their obligations will only take place in the event of the perpetration of atrocity crimes and will be military in nature. This leaves a huge intervention gap where civil action might be more effective and where violence or even death may result indirectly from the actions of a state, and blockchain might just be in a position to help plug this gap. Ironically, blockchain didn't even get a mention in the top-ten world changers in the McKinsey report of May 2013.

Blockchain has a potentially important role to play in the future protection of human rights, and developers with an interest in this area should identify two or three areas where blockchain's potential is most promising and work on developing tools in those areas in conjunction with affected communities and their advocacy organisations. Pilot initiatives may include the two areas identified in this paper (economic crimes and election fraud).

Progress will require the acceptance of a responsibility towards those who are at the mercy of bad government and are at the same time likely to be excluded from the "fourth industrial revolution." It will also require a commitment to inclusiveness in devising strategies to hold the powerful to account and direction to enable the development of blockchain tools and organisations aimed at countering the worst forms of exploitation and abuse, thereby giving blockchain an axiology that it would otherwise lack.

Collingwoode Law
P.O. Box YK 1528
Kanda
Accra
Ghana
kobina123@btinternet.com

References

Atzori, Marcella. 2015. "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?" (December 1). Available at SSRN: https://ssrn.com/abstract=2709713 or https://doi.org/10.2139/ssrn.2709713. (last accessed on 10 September 2017)

Barlow, John Perry. 1996. "A Declaration of the Independence of Cyberspace." Electronic Frontier Foundation. Available at https://

www.eff.org/cyberspace-independence (last accessed on 10 September 2017).

Deutsche Welle. 2016. “Death Toll in Syria Tops 55,000 in 2015.” Available at http://www.dw.com/en/death-toll-in-syria-tops-55000-in-2015/a-18953548 (last accessed on 10 September 2017).

Frauenfelder, Mark. 2016. Andreas Antonopoulos in an interview with Mark Frauenfelder: “Bitcoin Is the Sewer Rat of Currencies.” Medium. Available at https://medium.com/institute-for-the-future/bitcoin-is-the-sewer-rat-of-currencies-b89819cdf036 (last accessed on 10 September 2017).

Global Commission on Internet Governance (GCIG). 2016. One Internet. Available at https://www.ourinternet.org/report (last accessed on 10 September 2017).

Hector, Helen. 2014. “Trillion Dollar Scandal: The Biggest Heist You’ve Never Heard Of.” ONE. Available at https://www.one.org/us/2014/12/05/trillion-dollar-scandal-the-biggest-heist-youve-never-heard-of/ (last accessed on 10 September 2017).

Lessig, Lawrence. 2006. *Code: And Other Laws of Cyberspace, Version 2.0*. Second revised edition. New York: Basic.

McKinsey and Co. 2013. “Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy.” Available at http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies (last accessed on 10 September 2017).

———. 2014. “Offline and Falling Behind: Barriers to Internet Adoption.” Available at http://www.mckinsey.com/industries/high-tech/our-insights/offline-and-falling-behind-barriers-to-internet-adoption/ (last accessed on 10 September 2017).

Schwab, Klaus. 2016. *The Fourth Industrial Revolution*. Geneva: World Economic Forum.

Shapiro, Ehud. 2016. *From Biomolecular Computing to Internet Democracy.* Geneva: World Economic Forum.

Tapscott, Don. 2016. “How the Blockchain Is Changing Money and Business.” TED Summit. Available at https://www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business/transcript?language=en (last accessed on 11 September 2017).

U.N. 2005. Resolution adopted by the U.N. General Assembly on 16 September 2005 60/1, at paragraph 138. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/487/60/PDF/N0548760.pdf?OpenElement (last accessed on 11 September 2017).

———. 2009. “Implementing the Responsibility to Protect.” Report of the Secretary-General. A/63/677. General Assembly. Distr.: General. 12 January 2009. Original: English. 09–20610 (E) 280109. *0920610*. Sixty-third session. Agenda items 44 and 107, at paragraph 10(b). http://responsibilitytoprotect.org/implementing%20the%20rtop.pdf (last accessed on 10 September 2017).

U.N. Development Program (UNDP). 2009. "Elections and Conflict Prevention: A Guide to Analysis, Planning and Programming." UNDP Democratic Governance Group, Bureau for Development Policy.

U.N. Economic Commission for Africa (UNECA). 2016. "Measuring Corruption in Africa: The International Dimension Matters." African Governance Report IV, 2016.