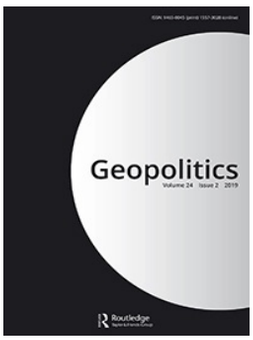

Routledge
Taylor & Francis Group

Geopolitics

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/fgeo20

Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity

Margie Cheesman

To cite this article: Margie Cheesman (2020): Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity, Geopolitics, DOI: 10.1080/14650045.2020.1823836

To link to this article: https://doi.org/10.1080/14650045.2020.1823836

Published online: 04 Oct 2020.

GEOPOLITICS
https://doi.org/10.1080/14650045.2020.1823836

Routledge
Taylor & Francis Group

Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity

Margie Cheesman

Oxford Internet Institute, University of Oxford, Oxford, UK

ABSTRACT

This paper critically examines the implications of 'self-sovereign identity' (SSI) for border politics and migration management. SSI refers to user-controlled, decentralised forms of digital identification. Closely linked with the distributed ledger technology blockchain, SSI is presented by advocates as a tool to empower marginalised groups, including refugees. Among other benefits, some claim that SSI removes the need for powerful, centralised institutional structures by giving individuals control and ownership of their identity information. However, through ethnographic research in an international aid organisation, I find that SSI is an embryonic technology with indeterminate properties and benefits. I identify a series of competing logics in the debates around SSI's emancipatory potential, which relate to four issues: (i) the neutrality of the technology, (ii) the capacities of refugees, (iii) global governance and the nation state, and (iv) new economic models for digital identity. SSI is simultaneously the potential enabler of new modes of empowerment, autonomy and data security for refugees *and* a means of maintaining and extending bureaucratic and commercial power. I situate SSI in a genealogy of systems of identity control and argue that, in practice, it is likely to feed into the powers of corporations and states over refugee populations.

Introduction

> When you're a small farmer and let's say you are disrupted by conflict, you cross a border, and all of your history is lost if you have lost your documentation. Even if you haven't, it may not be valid. But if you've got something that is stored on a digital identity, you can use that history wherever you go. [...] We talk a lot about the power of blockchain in terms of empowering individuals because they control access to their own data – self-sovereign data. But the people we are helping are a long way from understanding what it would mean to have self-sovereign data management. [...] This is an empowering technology at the core, and the faster we can get it to people, the faster we can tackle issues like global hunger.
>
> Robert Opp, United Nations World Food Programme (WFP)[1]

CONTACT Margie Cheesman margaret.cheesman@oii.ox.ac.uk Oxford Internet Institute, University of Oxford, Oxford OX1 3JS, UK

This article has been republished with minor changes. These changes do not impact the academic content of the article.

'Self-sovereign identity' (SSI) refers to user-controlled, decentralised forms of digital identification. In the quote above from an aid industry leader, SSI is presented as being not just a viable solution to the documentation issues associated with displacement. In facilitating a secure and permanent user-held identity record, it beckons forth the ideal future of humanitarian data management and border politics. SSI is widely attributed with emancipatory potential. Closely linked with the distributed ledger technology, blockchain, SSI is proposed as a tool to empower marginalised groups, including refugees. Among other benefits, some advocates claim that SSI removes the need for powerful, centralised state and corporate structures by giving individuals control and ownership of their identity information, which is a vital asset in contexts of forced migration.

SSI is gaining traction in the discourses of policymakers, researchers and practitioners working in aid and migration management. Notable interest includes UNHCR, the Red Cross, the UN Migration Agency and global government agencies (UNHCR 2018; Red Cross 510 2018; IOM & APSCA 2018. As a result, public-private initiatives have recently been set up to develop decentralised identity technologies. These involve established aid actors and national authorities as well as technology start-ups and companies such as Microsoft, Evernym, Consensys and Accenture (Allison 2019; ID2020 2019). An indicative example is the ID2020 Alliance pilot project in which the non-profit technology providers iRespond, associated with the Sovrin Foundation (part of the SSI software company Evernym), and the International Rescue Committee have used biometrics and blockchain to provide medical identities to refugees in Mae La camp, Thailand (Sovrin 2018). Their identification system is intended to enhance refugees' informational privacy: individuals' identities are verified at medical centres by iris scan, which links to a unique 12-digit code (stored along with the anonymised health data on a blockchain), and renders the in-situ sharing of paper IDs and personal information (name, address, date of birth) redundant (Piore 2020). Greater autonomy for refugees is putatively achieved as individuals now share their records with health professionals by allowing their iris to be scanned, with oral consent given each time this happens. However, questions about the necessity of blockchain and the assumption that iris-scanning is privacy-enhancing prevail. It is not clear that this identification system needs a blockchain as opposed to a more traditional database. The extent to which each refugee truly owns and manages their data is also unclear, and whether consent is truly meaningful in this context.

The Mae La Camp example reflects broader issues in how SSI is discussed and implemented. Its potential as a means of empowering refugees with blockchain-enabled privacy, control and autonomy in identification processes is alluring, and emergent scholarship dubs refugee SSI a 'quest' of crucial importance (Wang and De Filippi 2020, 10). Yet, SSI is a deeply contested

concept and its capabilities are not fully understood. The indeterminacy around its potential is further fuelled by the lack of concrete examples: SSI is much discussed but rarely seen in practice. This paper responds to an urgent need to critically assess the potentials and implications of SSI in relation to refugee rights and border politics. Findings are based on ethnographic research with a large multinational humanitarian technology organisation, here known as Tech-for-Aid, and the SSI start-ups they were networked with. The research was undertaken during 2017, just after the emergence of blockchain as a widely touted 'disruptive' technology.

I suggest that a series of competing discursive logics are at play as participants encounter SSI and imagine how this technology may or may not enable the restructuring of border politics. The competing logics relate to four issues: **(i) the neutrality of the technology, (ii) the capacities of refugees, (iii) global governance and the nation state, and (iv) new economic models for digital identity**. I show that the emancipatory potential attributed to SSI comes into tension with key debates around technology politics, capitalist strategies, the state's claimed monopoly to assign and verify claimed identities, and refugees' technical capacities, which are routinely understood as limited – as reflected in the WFP representative's statement above. Overall, I argue that the competing logics identified destabilise SSI's potential as a tool of refugee empowerment rather than state or corporate control.

In the Background section, I provide an overview of blockchain and SSI, situating these novel topics within longer scholarly conversations about the politics and practice of refugee identification. Then, I introduce the field-site, the methodological approach to this organisational ethnography, and the analytical framework of competing logics. The first empirical section examines divergent understandings of SSI. Participants view it as inseparable from the sensitive social classification work and privacy issues which identification systems are fraught with. Yet, identification and SSI are also often depoliticised by participants and treated as neutral tools of representation. In response to this tension in how SSI is viewed, I advocate a conceptualisation of SSI that accounts for the way in which data practices do not just represent refugee populations but *enact* them as governable subjects and enable mobility control apparatuses (Ruppert, Isin, and Bigo 2017; Scheel, Ruppert, and Ustek-Spilda 2019).

In the second empirical section, I examine how aid industry participants imagine refugee end users of SSI and categorise their capacities to act. These categories highlight the participants' mixed and uncertain view of the technical aptitude and agency of refugees. Entrenched understandings of refugees as a generalisable 'type' of (passive, technically inproficient, victim) person ultimately hamper aspirations of their self-sovereign empowerment. The third section examines the incorporation of SSI into traditional institutional logics. I show that, despite the considerable hype about the disruptive effects of SSI,

anticipated SSI projects in the aid industry do not seek to circumvent or challenge the monopolistic role of states in sorting and classifying subjects. Nor, I argue, do they necessarily secure refugees' access to the most important forms of recognition such as citizenship and the rights and protections that come with it. In the final empirical section, I find that Tech-for-Aid business models based on profiling and value extraction come into tension with SSI ideals promoting the re-orientation of data power and capital towards neoliberal subjects. I contribute to literatures critically examining the interventions of corporations in aid and their increasing role in producing and enacting migrants and migration (Isin and Ruppert 2019; Martin and Taylor 2020; Taylor and Broeders 2015).

Overall, this work reveals the paradoxes and indeterminacies surrounding SSI: it is simultaneously the potential enabler of new modes of empowerment, autonomy and data security for refugees (as suggested in aid industry discourses) *and* a means of maintaining and extending bureaucratic and commercial power. I situate SSI in a genealogy of systems of identity control and argue that, in practice, it is likely to feed into the powers of corporations and states over refugee populations

Background: Identification, Digital Identity and SSI

The documentation of individuals' identities by states and other official institutions is a globally pervasive and long-established mechanism of bordering and governance – from the efforts to issue papers securing French citoyens free movement during the Revolution, to the use of identity cards in the Rwandan genocide and Nazi Germany (Caplan and Torpey 2001). In contexts of forced migration, identity systems can be led by host governments, aid agencies, or both. Through refugee registration and identity management systems, people's movements are managed, but also their needs, vulnerabilities and eligibilities are determined and their access to protections and services is authorised (UNHCR 2019). Access to formal identification, whether through traditional means (such as passports and national identity cards) or newer digitally-enabled systems, is associated with legal recognition, rights, welfare and the resistance of exploitation, trafficking, and undue deportation or detention (Manby 2016; Szreter and Breckenridge 2012).

Within the framework of UN Sustainable Development Goal 16.9, digital identity is touted as a means of enabling inclusive societies in which everyone has portable, sustained access to legal status and rights, including social and medical services, police protection and economic inclusion. It offers a potential solution to the fact that, in many real-world cases, a range of issues prevent access to formal means of identification, including the loss or damage of documentary evidence, statelessness and the absence of or exclusion from a national ID system. For example, the passports of many Syrian citizens have

been systematically destroyed by Islamic State; in Somalia the costs of obtaining identity documentation are prohibitive for most citizens; discriminatory practices exclude particular groups from the right to nationality such as Rohingya Muslims in Myanmar and ethnic minorities in the Côte d'Ivoire (Bingham 2019; GSMA 2017).

Identity has never been a straightforward sociological or philosophical concept. In the digital age, its meanings are even further entangled. Within the aid sector, it signifies (i) official forms of 'foundational' identification issued by governments, (ii) identities issued by public or private sector service providers including aid agencies and banks, but also (iii) the de facto identities individuals accumulate online. Identity information is most closely associated with personal and demographic information, such as name, birth date, ethnicity, phone and SIM number and biometric profile. However, the humanitarian data ecosystem is now more extensive, also including attributes garnered from the digital traces left by everyday transactions, communications and behaviours, for example, through social media networks, mobile and credit records (Gillespie, Osseiran, and Cheesman 2018; Latonero et al. 2019; Martin 2019).

The generation, processing and exposition of individuals' data and metadata poses considerable additional risks for already at-risk populations (ICRC and Privacy International 2018). This is shown by existing digital refugee identification systems deployed by actors in aid and migration management. There is a pervasive absence of informed consent, data subjects lack knowledge and control over how their personal information is collected and used and face extensive bureaucratic challenges changing or updating it, there is very limited transparency around data flows and sharing with third parties, as well as function creep and a worrying tendency of using humanitarian data for non-humanitarian purposes such as ad targeting (Kaurin 2019; Omidyar Network 2017; Privacy International 2019; Schoemaker, Currion, and Pon 2018). Contemporary securitised bordering depends on increasingly sophisticated and invasive data practices of surveillance, social sorting and criminalisation by states (Amoore 2006; Dencik and Metcalfe 2019; Lyon 2008). Indeed, studies show that to evade control and persecution by hostile and discriminatory governments or undertake informal work, some refugees go to dangerous lengths to avoid identification systems; others need to obscure or redefine their identity to achieve support as a refugee or reach a desired destination (Currion 2018; Schoemaker et al. 2020; Slavin 2019).

For some, including participants in this empirical research, the user-centred, privacy-enhancing properties associated with SSI offer a solution to these problems. The most common purported benefits of SSI centre around notions of user-centricity, decentralisation and privacy. Instead of powerful institutions and organisations monopolising identification, SSI could give individuals greater control over how much personal data they share, when,

and with whom. This is because the private keys to identity credentials are held by the user of the technology, not a centralised issuing authority. It is imagined, for example, that individuals could use an SSI interface on a mobile device to hold their digital ID(s) and manage data exchanges. In the humanitarian sector, this is projected to fundamentally shift the distribution of power by giving individual aid subjects control, choice and oversight over the exchange of sensitive personal information (Davies 2017). This, in turn, could be a potential means of preventing the exploitations, abuses and political consequences associated with humanitarian data harvesting, enabling greater safety and empowerment of refugees.

How and whether these humanitarian ambitions for SSI will be achieved is, however, debated. This is closely related to the lack of consensus around SSI's essential properties and principles, which is reflected in the great variation in systems labelled as SSI. Key grounds for contestation include: whether SSI involves one or many IDs for each user; whether identity data should be held with (tech-savvy) individuals in a digital wallet or federated by service providers (which might mean refugees cannot store and review their data independently); what fair governance models and achievable standards might be; and, in general, what decentralisation actually involves. For example, while one SSI initiative might position itself as a new kind of central registry by issuing and authorising single, unitary IDs, another might follow an 'eggs in different baskets' approach to data security and facilitate users in independently holding multiple IDs (Evernym 2019b). Some bemoan the conflation of 'true SSI' with ill-defined concepts such as 'user-centric' digital identity, which may not require blockchain technology or use it to its full imagined, decentralised potential. Indeed, others promote a radical version of SSI that mainly involves 'self-attested' claims (Evernym 2019a). These include identity claims that are not validated by existing institutions such as governments, but instead are made by individuals and validated using blockchains.

The Significance of Blockchains in Digital Identity Debates

Among technical communities, SSI has long been part of discussions about Internet standards and the decentralisation of power and trust (Allen 2016). These discussions garnered new force with the invention of the cryptocurrency Bitcoin in 2008, which used blockchain as its underlying infrastructure. Blockchain is often associated with inherent characteristics such as immutability and transparency, yet there are different types of blockchains with different properties (Walch 2017a). These incorporate different protocols and algorithms and include not only public, open access, peer-to-peer networks but also private and permissioned systems, which resemble more traditional proprietary databases (and so prompt the question, do you really need a blockchain?). Nonetheless, across different interpretations and

approaches to blockchains, they are consistently viewed as technologies of decentralisation, privacy and truth.

Decentralisation

Blockchains are all *distributed ledger technologies*. This means they are types of shared databases which do not rely on a central point of control but, rather, distribute authority across a network of nodes. The nodes all maintain a continuously updated ledger, i.e. a set of records, detailing every transaction that takes place in the database. The records are not necessarily financial: they can include any unit of value, from exchanges of cryptocurrency to medical or identity information. All of the distributed nodes within a network share the same *consensus algorithm*. These are designed to allow transactions to be completed and information to be synced, even if the actors in the network do not trust each other. Different blockchains deploy algorithmic decision-making to different extents – no blockchain is 100% algorithmic. Evidence suggests that blockchains shift rather than eliminate trust, and the idea that there are no power concentrations in decentralised systems has been disproved in research on notable examples like Bitcoin and Ethereum (Campbell-Verduyn and Goguen 2018; Walch 2019). However, despite this, blockchains are widely presumed to replace the need for human intermediaries, organisations and social processes with 'neutral' technocratic consensus, governance by algorithms and trust-in-the-code (Zook and Blankenship 2018). They are associated with cypherpunk utopias of digital freedom and individual self-determination (Hütten 2018). Just as Bitcoin facilitates pseudonymous international exchanges outside the mechanisms of banks and other centralised financial authorities, libertarian SSI proponents suggest that blockchain will de-centre powerful authorities and intermediaries in digital identification and put the user in a position of greater power.

Privacy/security

The most utopian advocates and vendors of blockchain-enabled SSI imagine it will facilitate a privacy-enhanced, decentralised future in which digital identity is no longer un-consentingly monetised by third parties, with information more secure thanks to cryptography (Davies 2017). Indeed, contemporary SSI discourses are enmeshed with concerns around profiling and surveillance by centralised authorities and the mass harvesting of personal information by powerful tech monopolies such as Facebook (Stevens 2018). Blockchains deploy cryptographic techniques in order to authenticate and secure information in a way that maximises its confidentiality, anonymity and integrity (DuPont 2019, 30). These techniques include *public and private keys*, pairs of long numbers associated with each identity which are used to authorise transactions, and *hashes*, mathematical ways of creating and uniquely identifying blocks of transactions, which are then chained together to create the

records (ibid). However, blockchains are not all privacy-enhanced technology in and of themselves: anonymity is not failsafe, and surveillant entities can still assert control, especially in permissioned/private networks (Bohr and Bashir 2014; Orcutt 2018; The Royal Society 2019). Cryptographic approaches to hiding information such as *zero-knowledge proofs* are unproven, and cryptocurrency users have encountered major challenges with safely managing their public and private keys: if a private key is stolen from its owner, there is no recourse and the thief can use it to authorise transactions (Zook and Blankenship 2018, 252). Yet, blockchains are largely seen as means of facilitating identification and tracking information in a way that supports privacy and mitigates surveillance.

Truth/immutability

The cryptographic techniques and distributed architecture also mean that blockchains are difficult to alter (each block contains the previous block's unique hash) and so have come to be understood as a tamper-proof way of making immutable, permanent records. Even though blockchains may share the same garbage-in-garbage-out issues as any database, they are widely seen as achieving greater accuracy, authenticity and veracity in digital identity practices. It is therefore supposed that SSI will improve the processes of humanitarian organisations by reducing putative issues with fraud and the misallocation of aid (Pisa 2018). For refugees, SSI is proposed as a more secure, persistent, empowering means of recognition and socio-economic inclusion across borders.

Despite the litany of benefits that vendors, advocates and other optimistic commentators associate with blockchains, different blockchains have very different implications and so generalisations and overstatements need to be unpicked. As we have seen in the controversy around Facebook's proposed cryptocurrency, Libra, which has itself been labelled an SSI initiative (Orcutt 2019), blockchain-based systems promoting open, decentralised standards can in fact position a set of major global companies as powerful identity gatekeepers in the name of financial inclusion. In refugee contexts, little is known concretely about what impact blockchains and 'self-sovereign' systems will have for end-users and established aid and migration sector actors alike. This is an opportune moment to investigate how far SSI is challenging the dominant models of migration data politics. Could blockchain-enabled SSI really circumvent practices of tracking, surveillance and mobility control by established migration management institutions? Could SSI empower refugees with more digital autonomy and privacy, whilst equipping them with genuinely meaningful socio-political rights and protections? I provide insight on what blockchains are imagined to be and do and for whom, unpicking what is at stake when SSI first collides and colludes with the aid industry.

Materials and Methods

This paper takes an ethnographic participant-driven approach to understanding SSI discourses in the aid industry. Understanding the imagined future of SSI demands close-up, engaged and situated methodological approaches which can apprehend its different aspects, nuances and modalities. Ethnography is not simply a method of end-user research but an important means of understanding the specific motives, logics and practices of those who have the power to design, implement or decide about technology (Seaver 2014). It is particularly well-suited to researching SSI given its contested, contingent and uncertain nature. I engage with the speculative quality of SSI head-on and seek to examine not its technical features but rather the imaginary horizons on which it operates (Dourish and Bell 2011; Nagy and Neff 2015).

I draw on a framework of *social logics* to ground this research. Methodologically, logics are a 'basic unit of explanation' and can be 'usefully contrasted with laws, self-interpretation and mechanisms' (Glynos and Howarth 2007, 8). They are useful for empirical research as a way of characterising social processes, and the styles of reasoning around them, by situating them within their specific context (Cremin 2012; Glynos and Howarth 2007; Lutz 2017; Madianou 2019a). Logics are suitable for this research because they provide analytical clarity and can be used to 'characterise, explain and criticise social phenomena' (Glynos and Howarth 2007, 8) but at the same time recognise inherent complexity, messiness and uncertainty. For instance, Madianou (2019a, 2019b) shows that a logics approach is fruitful in pinpointing the core assumptions and concepts about technology in a rapidly changing and multifaceted sector such as the aid industry.

In particular, I utilise the notion of *competing logics* to capture how, at any point in time, countervailing social processes can operate simultaneously (Howarth, Glynos, and Griggs 2016). This has been usefully applied in Critical Border Studies to understanding the 'before and after' of emergent security technologies: how contestations around their funding, design and imagined adaptation 'in the field' should already be understood as bordering practices which foreground how devices are deployed (Bourne, Johnson, and Lisle 2015). Like Bourne et al, I trace the ambivalent, anticipatory work involved in developing a potential border technology, recording the contested contours of SSI's coming into being. The *competing logics* approach does not suggest simply that there is incoherence or binary contradiction in how refugee SSI is imagined. Rather, it indicates that complexity and multiplicity in current imaginings of SSI are inherent; any attempt to remove or reduce them to a unitary position is fundamentally flawed. Examining the competing logics around SSI helps to reckon with the contingent, heterogeneous and entangled intra- and extra- organisational dynamics in contemporary

humanitarianism, including the influences of the state and the private sector. It serves as an analytical tool to expose the geopolitical realities and rationalities this novel technology encounters as it is incorporated into the aid industry.

Situated research was conducted over a period of one month in 2017 at a Europe-based Tech-for-Aid office. Participants principally included (i) 25 Tech-for-Aid employees, but also (ii) a constellation of wider aid industry professionals and start-ups networked with Tech-for-Aid. Tech-for-Aid professionals specialise in research and practice about topics such as humanitarian response, gender and connectivity, health technologies, financial inclusion and identification. Their work supports the organisation's non-profit social good agenda whilst also contributing to the agendas of corporate and government stakeholders, such as humanitarian donors and technical partners. The ethnographic study was informed by engagements with wider technical and aid industry actors discussing SSI in conferences, workshops and pitches, as well as in online materials and forums. At the time of the research, Tech-for-Aid was engaged in knowledge-gathering around novel technologies for refugee identification, such as biometrics, blockchain and SSI. My role involved collaborating to develop knowledge artefacts (reports, visual resources, presentations) and planning and facilitating workshops, focus groups and interviews. This participatory work contributed to critical discussions around the future of aid and identification and offered a unique opportunity to understand the imaginaries of blockchain in a period when the technology was novel, surrounded by uncertainty but also promising.

Results

Competing Logics (I): the Neutrality of the Technology

This paper proposes that SSI should be considered part of a longer genealogy of classification systems that have not merely represented people, but have made or *enacted* them as governable subjects (Scheel, Ruppert, and Ustek-Spilda 2019; Scott 1998). Identification regimes sustain power geometries, biases and discriminations, and the technologies they rely on should be seen as part of the political struggle to control people's movement (Isin and Ruppert 2019; Madianou 2019a; Scheel 2019). The work of imagining, debating and developing potential border technologies like SSI is itself a practice of bordering and enactment (Bourne, Johnson, and Lisle 2015). At Tech-for-Aid, however, research participants apprehended digital identity in multiple ways, and the political struggles in which SSI would necessarily be imbricated were not always acknowledged.

Identity was widely understood by participants as 'just practical' and as a 'basic concept – we avoid airy fairy philosophical debates'. They described it as 'very simply about what needs to be proven for a person to be recognised or

accepted in a particular context'. SSI was imagined as merely a way of extending this rational, neutral function by further 'stabilising' individuals' identity claims. It was supposed that blockchain's reputed properties of immutability and cryptographic security could help deliver greater certainty in the authentication of identity data in precarious contexts where populations struggle to prove their rights. In this regard, participants adopted a technocratic and avowedly apolitical approach to the role of SSI. With claims like 'blockchain puts the power back in truth', the technology was assumed to facilitate factually incorruptible, un-mediated, autonomous digital records-making. Such assumptions are common, and neglect the significant role of human decision-making and social trust in blockchain systems (Dupont and Maurer 2015; Swartz 2017; Walch 2017b). The depoliticised approach to data complements the aid industry's longstanding 'anti-politics machine' wherein complex issues are made into merely technical problems to be solved (Ferguson 1990). It also accords with ideals in migration and border management about how 'total security' and certainty in states' sovereign decision-making can be realised by impartial, reliable and accurate technology (Amoore 2013; Bourne, Johnson, and Lisle 2015, 313). In discussing the potential of SSI, participants most often focused on the structure and quantity of identity data that would be made available rather than its quality, social construction and political sensitivities. SSI was welcomed as a way of getting more and better data which, in turn, was seen as an easy way to facilitate better aid.

Whilst identity technologies were often depoliticised in this way, participants sometimes reckoned with the socio-political factors at play in constructing refugee identification systems and the data they comprise: 'Refugees flee persecution on the basis of identity, political, religious, ethnic or otherwise, so we need tight control on how that information is shared'. For example, bearing in mind the risks of making records distributed, immutable and open source in contexts where certain people groups such as Rohingya refugees are persecuted, one participant posed the question, 'how would we avoid incorporating people's ethnic identities in the data, even if it is encrypted?' Aid industry participants discussed how systems designed to provide legal identity are used to track, denationalise and repatriate stateless people, as in the case of the Rohingya in Myanmar and Bangladesh (Taylor and Mukiri-Smith 2019). Throughout these discussions, they were acutely aware that with recording, curating and sharing sensitive information comes great risks. Noticeably, everyone was attuned to the contextual nature of identity issues, with several participants bringing up the point that 'one-size-fits-all doesn't work' since identity 'ecosystems' vary considerably in different global contexts. For example, there was uncertainty about the robustness of SSI in contexts where there are government Internet shutdowns and patchy technical infrastructure, as well as the exclusionary knock-on effects of digitalisation. This reflects how understandings of

identity and classification were complex and heterogenous. SSI was a neutral, factual representation tool that could improve humanitarian identification systems *and* a context-dependent technology that could adversely affect certain refugee groups by fixing their identity. Debates around SSI complicate the well-trodden depoliticisation argument in critiques of aid (pace Ferguson): refugee identification was both approached as strongly political, embedded in complex social problems and settings *and* neutralised more than ever by association with blockchain.

Competing Logics (II): the Capacities of Refugees

By changing the technical affordances of refugee actors, SSI will (re)configure identities in particular ways and in doing so shape refugees' capacities to act. Designing and deploying an identity system involves imagining its subjects, their needs and agentive capacities. During the study, participants focused on identifying viable SSI use cases for forcibly displaced persons, and in collaborative workshops mapped out visual depictions of 'user journeys.' The imagined users of SSI were categorised as refugees, but participants also conflated the documentation issues they face with those of asylum seekers, economic migrants, and stateless people. What SSI could offer and to whom was debated and emerged as indeterminate. The types of rights claims SSI was supposed to facilitate – asylum, refugee status, citizenship – was not always clear. An inherent tension throughout the research was that participants offered different speculations about how migrant users would utilise the technology. Projections of sovereign agency and empowerment rubbed up against generalisations about refugees' deficiencies in digital literacy and access.

The label 'refugee' comes with significant conceptual baggage and stereotypes (Betts et al. 2014; Fiddian-Qasmiyeh 2016; Zetter 1991). Dominant humanitarian and refugee protection discourses emphasise the vulnerability of displaced persons and engage in racialised forms of othering (Etem 2020). SSI's emancipatory promise of user-held identities potentially challenges the discourses that posit refugees as passive victims and 'beneficiaries', which have been critiqued as justifying paternalistic, top-down aid industry apparatuses (Malkki 1995; Turner 2019b). The diagrams of SSI 'user journeys' produced in these workshops were pervaded by utopian visions of participatory aid. The ownership and control of personal information in the digital age was framed as a sovereign right and necessary goal by SSI proponents and sceptics alike. Just as Turner and others have observed in humanitarian discourses fetishizing new technology and the 'refugee entrepreneur', SSI was about shifting away from characterisations of refugees as generically unskilled dependents reliant on the largesse of states and international aid (Lenner and Turner 2019; Scott-Smith 2016; Turner 2019a). Instead, they could be capable of curating,

managing and 'leveraging' their own digital identities and engaging in free-market capitalism by using SSI to 'become bankable' or sell their personal data.

However, at the same time, the longstanding refugee vulnerability trope was expressed anew. Visions of SSI-enabled digital and economic agency explicitly came into tension and were hampered as participants cast refugees as generally lacking in digital and literacy skills. Participants were doubtful that user-administrated identity could be achieved: 'If I don't even understand what my data trail is, how will refugees?' 'We can't trust that refugees will be able to manage their private keys, or even own their own mobile'. Tautologous generalisations were made about refugee women: in cases of male domination in the 'developing world', 'they don't have enough agency to assert more agency'. Competing logics emerged in how the digital capacities and capabilities of refugees were imagined. On the one hand, refugees' fortunes were about to be transformed through the emergence of a radical and disruptive new technology. On the other, those very refugees ultimately lacked the capacity and autonomy to allow that transformation to take place.

These discussions opened a range of pressing and hard-to-answer questions around the necessary capacities for SSI. For example, one brainstorming activity generated the question 'What's the SSI equivalent of password recovery?!' Any implementation would involve a comprehensive key management system which would likely require a demanding set of digital security skills and safety nets. A participant from the Gender and Technology team pointed out that such as demanding system would disproportionately exclude already marginalised and disadvantaged groups such as the elderly and disabled. What's more, participants agreed that the sovereign ownership of personal data and management of all data exchanges would introduce huge responsibilities on individuals. This was considered a potential abdication of humanitarian organisations' and states' obligation and liability in providing refugee protection. Indeed, the role of these established institutions in SSI was a topic of great uncertainty and one with important bearings on global governance and border politics.

Competing Logics (II): Governance and the Nation State

Blockchain is often seen as a sophisticated non-human governance system and thus a new and improved kind of institution (Davidson, De Filippi, and Potts 2018). Radical blockchain projects align with Bitcoin's libertarian ideals of non-hierarchical decentralisation, privacy and autonomy, and seek to free people from the 'tyranny of middle-men' (Maurer, Nelms, and Swartz 2013; Swartz 2017). It is argued that identity and belonging should be entirely self-attested, as with the Bitnation, the 'decentralised, borderless, voluntary nation' which advocates for digital self-governance (Tempelhof et al. 2017). The Decentralised Identity Foundation aims to develop the engineering tools

necessary for an ecosystem of decentralised digital technologies. Microsoft and other members propose that centralised corporate and state authorities should no longer have the power to issue, maintain and revoke identifiers (Sabadello 2019). Some proponents of self-sovereignty suggest that this is inevitable and that traditional forms of identification such as the international passport system will be uprooted. They argue that SSI may, in the future, entirely remove the function of nation states by obviating the need for intermediaries in border control and migration management: 'The result of these technologies gaining traction might be that states need to "compete" on a more open market for the allegiance of citizens much like companies compete for customers or engagement' (Hudson 2019).

State sovereignty has long been a territorialised concept: in most discourses, to be a refugee is to be displaced and uprooted from a geographically defined nation state (Malkki 1992). The idea that, through SSI, the classification function of states should be redistributed among individuals poses a revolutionary shift in border politics. If individuals were able to design and curate their own digital identities, then they could also exert control over their subject positions. This would mark the de-territorialising of sovereign power – but only if, at least initially, existing geographically defined sovereign states recognised the new digital identities, which is unlikely. Nonetheless, this radical disruption to the cornerstone of the international order is often presented as one of the utopian capabilities of SSI.

However, this study finds there is indeterminacy around whether SSI should be interpreted in this way. A high degree of scepticism about such a radical vision was expressed by participants. The emancipatory potential of decentralised, user-owned modes of identification came into tension with the geopolitical reality of the nation-state system in which states' prerogative is to control the legitimate means of movement – or, indeed, identification (Torpey 2000). In this reality, technologies of identification have since 9/11 intensified regimes of surveillance, securitisation and control (Bennett and Lyon 2008).

At different stages in the ethnographic research, there were tensions between logics of radical decentralisation in visions of blockchain-enabled SSI as a privacy-enhancing commons resource, and incorporative logics seeking to maintain the powerful functions of state authorities in managing migration. Tech-for-Aid professionals debated whether the future of SSI lies in individuals self-asserting their identity, owning and managing identities issued to them by third parties, or both. Most felt the very term 'self-sovereignty' seemed to suggest the former, especially during the initial stages of their engagement with the concept. Some SSI technologists networked with the aid industry promoted a radical long-term future in which individuals could have 'blockchain marriages' and birth certificates. In brainstorms with one SSI start-up, participants mapped out a model that would allow refugees to

build an amalgam of different identity claims. The composite identity would be constituted by socially attested elements such as photos and testimonies given by family and friends and this 'could help paperless people access services since it's proof of their existence'. One Tech-for-Aid professional suggested this kind of social reputation system could work in somewhere like Tanzania, where communities consider 'award letters' based on interpersonal trust relationships the most important identity documents. These ideas were akin to the SSI future imagined by Evernym: 'I can imagine a baby born in a remote village and receiving her first "credentials" from her family and friends, who each give her attestations about her birth and their recollections of it. Pictures, videos, songs, and other precious memories could be added to her brand new digital wallet' (Evernym 2019a).

However, the possibility of self-attested identity was largely eschewed by aid industry professionals: 'It's just not possible for refugees to have absolute supremacy over their identity claims. How do we know if they are verified, or if their social credentials are biased or corrupt?' 'The categories and elements of identity can't just be made up by refugees, they have to comply with normal systems.' Those working on the legal side of Tech-for-Aid were especially concerned that SSI may not be compliant with the established protocols of states, regulators and banks. One participant questioned, 'What is the point of identification if it ignores the requirements of states and aid organisations?' Another was concerned that there would be no centralised body to go to if the system crashed and asked, 'where would all the data be physically stored, if not with an institution we know is trustworthy?'. These perspectives reflect the wider de-radicalization and incorporation of blockchain and its adoption within established institutions and power relationships (Swartz 2017).

Most proponents of SSI now suggest that it need not undermine the powers of states, or indeed any third party, in identifying individuals. Rather, SSI could 'strengthen' the state-citizen relationship as individuals gain greater levels of consent and agency in their dealings with government and other organisations and institutions (Evernym 2019a). Throughout this research, SSI start-ups keen to partner with Tech-for-Aid promoted a version of self-sovereignty that involved important certifications being verified by trusted centralised authorities such as banks, government agencies, universities and hospitals. Moving away from notions of radical disintermediation and the circumvention of states via blockchain, these logics reinforced the ultimate power of established intermediaries, such as states, as 'anchors of trust' in endorsing decisions.

During use-case brainstorming exercises, participants anticipated a range of refugee-centred improvements to existing identity management processes. With SSI's putative benefits of data minimisation, cryptographic protections and disclosure control, 'It could help when someone doesn't want to reveal to

their government that they are HIV positive or part of a persecuted ethnic group unless they absolutely have to'. However, participants expressed uncertainty as to whether refugees would be allowed to control their disclosure of data in different situations. They were generally sceptical about whether governments or other institutions would accept selectively disclosed identity claims. They did not seek to challenge the ultimate power of states in classifying and managing subjects (e.g. through deportation) via official national identification regimes. Rather, they examined the possibilities of using SSI to support refugees' access to alternative, 'functional' forms of identity. This would help them build a non-official (but not necessarily self-asserted) profile with which to access some services and potentially ascertain official identification. Rather than circumventing the role of states, participants described functional identity as helping refugees 'reduce dependency and reliance' on them.

Functional identity is a useful option for ensuring that individuals have continuing access to aid and services, such as a health cards provided in a refugee camp. In cases where state-issued legal identity is inaccessible to refugees, participants deemed functional alternatives crucial in refugees' access to resources. At Tech-for-Aid, different types of 'identity resources' refugees could leverage to build this alternative identity were discussed, including mobile phone numbers. Participants expressed uncertainty about whether a 'functional' proof of existence would help refugees acquire official national ID, which in many contexts is necessary to access financial services or work. At Tech-for-Aid, it was unclear if this could also be legally recognised and help people access the most important services and rights, particularly refugee status and citizenship. In several discussions, participants agreed SSI would work more easily in countries that already have a national ID system and support digitalisation: 'It could take off in Zambia – the government is open to innovation there'. They also pointed out that supporting access to identity in contexts where people already may have means of recognition does not address the most pressing cases of inequality and exclusion, and individuals and governments in those contexts 'won't imagine the value of an alternative ID'. Ultimately, participants agreed that 'states are the bottom line', and that ' will surely be difficult to get governments to accept SSI' whether as a functional identity wallet or as a radical alternative to state-issued documentation. While the legal protections functional SSI would offer were uncertain, proponents suggested it could beckon forth new economic models in migration data management.

Competing Logics (III): New Economic Models

Many SSI proponents contend that it can subvert the monopolistic ownership of, and value extraction from, identity information by American tech

platforms such as Facebook and Google (Gropper, Shea, and Riedel 2019). An important component of self-sovereign empowerment was the idea of circumventing the established models of platform capitalism by profit-oriented tech companies, data brokers and other ruthless actors (Srnicek 2017). For some, SSI held the potential to radically shift the extractive, surveillant structures in contemporary data economies. Radical approaches to blockchain see it as 'the ultimate market mechanism' which facilitates trade and exchange in any unit of value outside established financial systems (Swartz 2017). Some participants, specifically those from SSI start-ups rather than the Tech-for-Aid organisation itself, advocated not only the permanent control of data by refugees, independently from third party vendors, but also envisioned that individuals could monetise that personal information. Identity information is widely viewed as a valuable commodity (Birch 2014), and this logic is taking hold in the aid industry.

Participants envisioned how refugees could personally profit in various ways from data exchanges with companies and institutions. For example, one start-up outlined a social credit scenario in which people were rewarded with cryptographic tokens for good behaviour, for example, by providing attestations about the identity of family and friends. In another example, workshop participants suggested 'refugees should be the custodians of their own healthcare' and envisioned another user journey in which 'self-sovereign identity becomes even more useful and powerful over time' as data from interactions with medical services are recorded securely and in real time, and can be used by the SSI start-up to build insurance profiles. In this case, SSI profits refugees, who can access insurance and control their health records, and medical practitioners, who have real-time medical information. It also benefits the start-up, who are positioned as the new intermediary and would take a cut from users' charges to data consumers such as insurance companies.

Discussions around possible economic models of SSI confirmed the increasing significance of corporations as aid actors. As Taylor and Broeders (2015) point out, 'commercially generated big data is becoming the foundation for country-level "data doubles", i.e. digital representations of social phenomena and/or territories that are created in parallel with, and sometimes in lieu of, national data and statistics.' They suggest that the subjects of aid are now increasingly visible and commodifiable to third parties, caught in the waves of information capitalism. In this study, the goals and logics of some proponents about SSI as a public good or commons resource (Allen 2016) came into tension with the profit-oriented models of SSI start-ups as well as Tech-for-Aid participants' concerns about maintaining existing revenue streams for stakeholders like technology partners and mobile network operators.

Aid industry discourses often approach digital connectivity as a taken-for-granted social good, despite robust evidence that its impacts are asymmetrical across geographies and socio-economic stratifications (Friederici, Ojanperä,

and Graham 2017). For example, aid industry participants imagined a range of 'functional' SSI use cases that were specifically about extending refugees' access to SIM registration (which usually requires ID) and therefore mobile phones. Participants saw mobile connectivity as a crucial resource for refugees, rather than confronting its dialectical tendencies which also expose people to particular forms of precarity, risk and surveillance (Gillespie, Osseiran, and Cheesman 2018). The Tech-for-Aid organisation also had vested interests in promoting the use of mobiles, as key stakeholders in their work included mobile infrastructure providers. They considered 'financially sustainable' public-private partnerships key to good aid innovation. For them, the provision of digital identities was key to implementing other humanitarian interventions in projects that involve mobile technology such as SMS health reminders. The horribly named 'mobile penetration' agenda complemented the outlook of start-ups, who anticipated that access to mobiles would be fundamental in users' adoption of SSI since 'mobiles are already also portable and self-managed'. Overall, SSI discourses at Tech-for-Aid sit within the wider global picture of information capitalism (Cohen 2019).

Discussion and Conclusion

The great irony of blockchain is that the industries most interested in utilising it, such as banking, want to do so in order to enhance existing institutional practices and efficiencies – the very practices the technology was invented to circumvent (Swartz 2017; Zook and Blankenship 2018). Proponents of SSI argue that this engagement from powerful intermediaries is due to the existential threat posed by SSI: 'The disintermediation and destruction of current data broker business models provide very strong economic incentive to hijack and subvert the goals of the SSI community' (Gropper, Shea, and Riedel 2019). However, in this study, participants approached SSI with competing logics. Some saw SSI as a panacea to the problems of centralised identification. Radical proponents in SSI start-ups envisioned in the long-term a libertarian utopia of stateless, market-based individualism. At the same time, most Tech-for-Aid participants saw SSI as a superstructure which could complement existing identification systems, whilst giving refugees greater privacy and agency in engagements with new and established identity providers such as companies and governments. Accordingly, I suggest SSI must be located in genealogy of systems of identity control: in practice, it is likely to feed into the powers of corporations and states over refugee populations.

Given participants' cognisance of the power struggles and contextualities of refugee identification, and their agreement that, in order to be useful and valid, 'self-sovereign' identities would still have to fulfil the requirements of established institutions and corporations, the extent to which identification and SSI were simultaneously depoliticised was surprising. Projections of blockchain's

objective incorruptibility contributed to the neutralisation of digital identity practices. This depoliticised lens is dangerous: it ignores the bureaucratic, intersectional biases in classification systems (Sim and Cheesman 2020). Encoded biases about race, ethnicity, class and gender, instantiate longstanding discriminatory social effects. For example, when metrics of poverty are used to predictively identify child abusers, or when in homeland security settings, all credibility, authority and credibility are attached to a fixed, racialised risk identities which vulnerable or marginalised people are left to dispute themselves (Amoore 2006; Eubanks 2017). Drawing on the example of the Rohingya refugees, Madianou argues that identity technologies produce and 'ossify' discriminations and in doing so, data practices bolster rather than mitigate inequalities and actually can be constitutive of humanitarian crises (Madianou 2019a). If SSI continues to be routinely depoliticised in the aid industry, the particular ways in which identities are configured, the social biases they instil, and the adverse consequences of this social sorting will be neglected.

As Scheel et al (2019, 582) suggest, 'the politics of migration management do not happen after knowledge about migration has been produced. They happen in and through the data practices that are mobilised to know (and enact) migration as an actionable reality.' These data practices which bolster inequalities comprise imaginative work. In Tech-for-Aid discussions, the category of 'refugees' was constructed as a generalisable 'type' of person – rather than as it should be, 'a broad legal or descriptive rubric that includes within it a world of different socioeconomic statuses, personal histories, and psychological or spiritual situations' (Malkki 1995). Participants imagined and categorised refugees' digital capacities and literacies as generically insufficient for achieving 'self-sovereignty'. In doing so, they *enacted* refugees as aid subjects and delimited the conditions of possibility that allow them to become rights-claiming data citizens (Ruppert, Isin, and Bigo 2017). The ideal subject of SSI is technologically expert, more expert than most refugees or any other people. Participants' incorporative visions of SSI did not attribute refugees the agency to enact themselves. In this way, SSI debates extended into a new digital domain the longstanding tendency of humanitarian discourse to cast refugees as a homogenous group of largely passive, disempowered recipients of aid.

Simultaneously, discussions about SSI resonated with emergent humanitarian ideals of the resilient, self-reliant, entrepreneurial refugee. These ideals signal an overarching shift from state-based to market-based aid, where faith in markets and technology elides questions of structural socio-economic change and substantive political rights (Duffield 2013; Scott-Smith 2016; Turner 2019a). In the aid industry, the power to enact populations is now distributed among private and public actors (Isin and Ruppert 2019; Martin and Taylor 2020; Taylor and Broeders 2015). The 'self-sovereign' ownership and control of identity data does not mean that corporations will cease to

demand payment for access to their services. The promise of profit for refugees must compete with the power asymmetries of platform capitalism and the asymmetrical relations of aid. The imagined webs of socio-technical relations bringing 'self-sovereign' identities into being involved social credit and risk profiling systems. These instantiate and reinforce inequalities: subjects with the most credentials considered valuable, such as clean medical records, profit more. Privacy unravels as others, which in refugee contexts may include individuals with especially sensitive or 'risky' personal attributes, avoid the 'negative inferences attached to staying silent' (Peppet 2011). In some scenarios, data sharing could be coercive rather than voluntary if refugee groups are not in a position to turn down the economic value offered for their personal information. Already, it has become common practice in humanitarianism that personal data is also used for practices such as commercial exploitation and surveillance. SSI could extend these functions.

Latonero et al argue that 'there are clear deficiencies in a system that depends on legally recognised ID certificates in the form of paper documents that are easily stolen, lost, or destroyed and also difficult to replace once inside the EU', giving the example of Libyan refugees crossing the Mediterranean who have their documentation seized by smugglers and other exploiters (Latonero et al. 2019). For aid industry participants, the aim of SSI is to address this problem by providing refugees with inalienable, portable, self-owned digital identities. However, data property rights do not automatically bring individuals meaningful oversight, understanding and control with regard to their digital transactions, or undermine exercises of power by data monopolies. Nor do alternative approaches such as SSI resolve root problems refugees face in the core challenge of accessing official or 'foundational' identity. As Taylor and Mukiri-Smith put it, 'Although working and eating are fundamentally important, the rights of citizenship are still the bedrock on which they are based' (Taylor and Mukiri-Smith 2019). The imagined horizons of SSI as discussed by Tech-for-Aid participants did not propose to support refugees' long-term wellbeing by aiding their legal claims for asylum. In this study, the basic 'identity' imagined in the discourse of SSI – i.e. recognised existence as a certain person – is not the same as 'citizenship', in the sense of a person with political and social rights. Rather than empowering refugees with meaningful rights, experimental digital solutions have been shown to amplify existing patterns of control and neglect the issues people themselves find most pressing (Dencik and Metcalfe 2019; Madianou 2019b). Concepts of SSI, whilst surrounded by indeterminacy and scepticism, threaten to follow suit.

The aid industry discourses examined in this study signal the need and desire for more empowering and secure futures for refugee identification. In attending to the competing logics at play in aid industry discussions of SSI, it shows that radical technologies both challenge and are incorporated into

traditional settings. I have demonstrated how SSI was not simply or straightforwardly depoliticised as a neutral identity representation tool and lauded as the potential new apparatus for surveillance and business interests. It was also embroiled in ambivalent political debates about how refugees' interests could be re-centred in international regimes of data privacy, power and profit. SSI is imbued with hype, uncertainty, confusion but also promise. The multitude of competing positions traced in this research show that the future remains unmade: whether, and how, SSI realises any of its revolutionary, mundane, invasive and emancipatory potentials depends on how the discourses mapped here are realised in practice. Overall, there is great risk that, rather than realising any emancipatory potential attributed to SSI, such schemes will be incorporated into existing mechanisms of power and domination. This must be avoided if SSI is to have a pro-social impact and enhance the wellbeing of refugees.

Note

1. Robert Opp, United Nations World Food Programme, Director of Innovation and Change Management, 'Can Blockchain End Hunger?' Keynote, The Netherlands, September 28th 2017, Available at: https://www.youtube.com/watch?v=5iK5h6BOpNo, Last accessed on: 15th January 2020.

ORCID

Margie Cheesman http://orcid.org/0000-0001-9521-4658

References

Allen, C. 2016. The path to self-sovereign identity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

Allison, I. 2019. ConsenSys and microsoft tackle human rights abuses with blockchain-based identity system. *International Business Times*. https://www.ibtimes.co.uk/consensys-microsoft-tackle-human-rights-abuses-blockchain-based-identity-system-1562722.

Amoore, L. 2006. Biometric borders: Governing mobilities in the war on terror. *Political Geography* 25 (3):336–51. doi:10.1016/j.polgeo.2006.02.001.

Amoore, L. 2013. *The politics of possibility: Risk and security beyond probability*. Durham: Duke University Press.

Betts, A., L. Bloom, J. Kaplan, and N. Omata. 2014. Refugee economies: Rethinking popular assumptions. 1–44. https://www.rsc.ox.ac.uk/files/files-1/refugee-economies-2014.pdf.

Bingham, L. 2019. People v. Côte d ' Ivoire: The right to citizenship for minorities. *Open Society Justice Initiative*. https://www.justiceinitiative.org/litigation/people-v-c-te-divoire.

Birch, D. 2014. *Identity is the new money*. London: London Publishing Partnership.

Bohr, J., and M. Bashir. 2014. Who uses bitcoin? An exploration of the bitcoin community. 2014 12th Annual Conference on Privacy, Security and Trust, PST 2014, 94–101. https://doi.org/10.1109/PST.2014.6890928.

Bourne, M., H. Johnson, and D. Lisle. 2015. Laboratizing the border: The production, translation and anticipation of security technologies. *Security Dialogue* 46 (4):307–25. doi:10.1177/0967010615578399.

Campbell-Verduyn, M., and M. Goguen. 2018. Blockchains, trust and action nets: Extending the pathologies of financial globalization. *Global Networks* 1–21. doi:10.1111/glob.12214.

Caplan, J., and J. Torpey. 2001. *Documenting individual identity: The development of state practices in the modern world*. Princeton: Princeton University Press.

Cohen, J. E. 2019. *Between truth and power: The legal constructions of informational capitalism*. Oxford, New York: University Press.

Cremin, C. 2012. The social logic of late capitalism: Guilt fetishism and the culture of crisis industry. *Cultural Sociology* 6 (1):45–60. doi:10.1177/1749975511427650.

Currion, P. 2018. The refugee identity – caribou digital. https://medium.com/caribou-digital/the-refugee-identity-bfc60654229a.

Davidson, S., P. De Filippi, and J. Potts. 2018. Blockchains and the economic institutions of capitalism. *Journal of Institutional Economics* 14 (4):639–58. doi:10.1017/S1744137417000200.

Davies, R. 2017. Knowing me, knowing you: Self-sovereign digital identity and the future for charities. Charities Aid Foundation. https://www.cafonline.org/about-us/blog-home/giving-thought/the-future-of-doing-good/self-sovereign-digital-identity-and-the-future-of-charity.

Dencik, L., and P. Metcalfe. 2019. The politics of big borders: Data (in)justice and the governance of refugees. *First Monday* 7 (4). https://firstmonday.org/ojs/index.php/fm/article/view/9934/7749.

Dourish, P., and G. Bell. 2011. *Divining a digital future: Mess and mythology in ubiquitous computing. MIT Press*. Vol. 41. London and Cambridge Massachusetts: Massachusetts Institute of Technology. doi:10.1016/S0033-8389(02)00063-5.

Duffield, M. 2013. How did we become unprepared? Emergency and resilience in an uncertain world. *British Academy Review* 21 (21):55–58.

DuPont, Q. 2019. Cryptocurrencies and blockchains. *Polity*. doi:10.3233/ip-190006.

Dupont, Q., and B. Maurer. 2015. Ledgers and law in the blockchain. http://kingsreview.co.uk/magazine/blog/2015/06/23/ledgers-andlaw- in-the-blockchain/

Etem, A. J. 2020. Representations of Syrian refugees in UNICEF ' s media projects: New vulnerabilities in digital humanitarian communication. *Global Perspectives* 1:1. doi:10.1525/gp.2020.12787.

Eubanks, V. 2017. *Automating inequality: How high-tech tools profile, police, and punish the poor*. New York: St Martin's Press.

Evernym. 2019a. 7 myths of self-sovereign identity. *Medium*. https://medium.com/evernym/7-myths-of-self-sovereign-identity-b16648c3090d.

Evernym. 2019b. "Staying true to SSI principles : Our concerns about GADI." https://www.evernym.com/blog/ssi-principles-our-concerns-about-gadi/.

Ferguson, J. 1990. *The anti-politics machine development, depoliticization, and bureaucratic power in Lesotho*. Cambridge: Cambridge University Press.

Fiddian-Qasmiyeh, E. 2016. Representations of displacement from the Middle East and North Africa. *Public Culture* 28 (3):457–73. doi:10.1215/08992363-3511586.

Friederici, N., S. Ojanperä, and M. Graham. 2017. The impact of connectivity in Africa: Grand visions and the mirage of inclusive digital development. *Electronic Journal of Information Systems in Developing Countries* 79 (1):1–20. doi:10.1002/j.1681-4835.2017.tb00578.x.

Gillespie, M., S. Osseiran, and M. Cheesman. 2018. Syrian refugees and the digital passage to Europe: Smartphone infrastructures and affordances. *Social Media + Society* 4

(1):205630511876444. no. SI: Forced Migrants and Digital Connectivity. doi:10.1177/2056305118764440.

Glynos, J., and D. Howarth. 2007. *Logics of critical explanation in social and political theory*. London: Routledge. https://doi.org/10.1017/CBO9781107415324.004.

Gropper, A., M. Shea, and M. Riedel. 2019. How SSI will survive capitalism. *Github*. https://github.com/WebOfTrustInfo/rwot8-barcelona/blob/master/draft-documents/how-ssi-will-survive-capitalism.md.

GSMA. 2017. Refugees and identity: Registration and aid delivery. *GSM Association*. https://www.gsma.com/mobilefordevelopment/resources/refugees-and-identity/.

Howarth, D., J. Glynos, and S. Griggs. 2016. Discourse, explanation and critique. *Critical Policy Studies* 10 (1):99–104. doi:10.1080/19460171.2015.1131618.

Hudson, A. 2019. Will we still need countries in the future? *Metro*. https://metro.co.uk/2019/08/07/will-we-still-need-countries-in-the-future-10529492/amp/?__twitter_impression=true.

Hütten, M. 2018. The soft spot of hard code: Blockchain technology, network governance, and pitfalls of technological Utopianism. *Global Networks* 19:3. doi:org/10.1111/glob.12217.

ICRC, and Privacy International. 2018. The humanitarian metadata problem: 'Doing no harm' in the digital era. https://privacyinternational.org/report/2509/humanitarian-metadata-problem-doing-no-harm-digital-era.

ID2020. 2019. The ID2020 Alliance.

IOM & APSCA. 2018. *5th border management and identity conference (BMIC) on technical cooperation and capacity building*. Bangkok: BMIC. http://cb4ibm.iom.int/bmic5/assets/documents/5BMIC-Information-Brochure.pdf.

Isin, E., and E. Ruppert. 2019. Chapter 11: Data's empire: Postcolonial data politics. In D. Bigo, E. Isin, & E. Ruppert (Eds.), *Data politics: Worlds, subjects, rights*, (pp. 207–228). London: Routledge.

Kaurin, D. 2019. Data protection and digital agency for refugees. *World Refugee Council Research Paper*, no. 12. https://www.cigionline.org/sites/default/files/documents/WRC Research Paper no.12.pdf.

Latonero, M., K. Hiatt, A. Napolitano, G. Clericetti, and M. Penagos. 2019. Digital identity in the migration & refugee context. *Data & Society*. https://datasociety.net/output/digital-identity-in-the-migration-refugee-context/%0Ahttp://files/22755/Digital Identity in the Migration & Refugee Contex.pdf%0Ahttp://files/22754/digital-identity-in-the-migration-refugee-context.html.

Lenner, K., and L. Turner. 2019. Making refugees work? The politics of integrating Syrian refugees into the labor market in Jordan. *Middle East Critique* 28 (1):65–95. doi:10.1080/19436149.2018.1462601.

Lutz, P. 2017. Two logics of policy intervention in immigrant integration: An institutionalist framework based on capabilities and aspirations. *Comparative Migration Studies* 5:1. doi:10.1186/s40878-017-0064-0.

Lyon, D. 2008. Biometrics, identification and surveillance. *Bioethics* 22 (9):499–508. doi:10.1111/j.1467-8519.2008.00697.x.

Madianou, M. 2019a. Technocolonialism: Theorizing digital innovation and data practices in humanitarian response. *Social Media + Society* 5:205630511986314. doi:10.1177/2056305119863146.

Madianou, M. 2019b. The biometric assemblage: Surveillance, experimentation, profit, and the measuring of refugee bodies. *Television and New Media* 20 (6):581–99. doi:10.1177/1527476419857682.

Malkki, L. 1992. National geographic: The rooting of peoples and the territorialization of national identity among scholars and refugees. *Cultural Anthropology* 7 (1):24–44. doi:10.1525/can.1992.7.1.02a00030.

Malkki, L. 1995. Refugees and exile: from 'refugee studies' to the national order of things. *Annual Review of Anthropology* 24 (1):493–523. doi:10.1146/annurev.anthro.24.1.493.

Manby, B. 2016. Identification in the context of forced displacement. *The World Bank*. doi:10.1596/24941.

Martin, A. 2019. Mobile money platform surveillance. *Surveillance and Society* 17:213–22. doi:10.24908/ss.v17i1/2.12924.

Martin, A., and L. Taylor. 2020. Exclusion and inclusion in identification: Regulation, displacement and data justice. *Information Technology for Development* 1–17. doi:10.1080/02681102.2020.1811943.

Maurer, B., T. C. Nelms, and L. Swartz. 2013. 'When perhaps the real problem is money itself!': The practical materiality of bitcoin. *Social Semiotics* 23 (2):261–77. doi:10.1080/10350330.2013.777594.

Nagy, P., and G. Neff. 2015. Imagined affordance: Reconstructing a keyword for communication theory. *Social Media and Society* 1:2. doi:10.1177/2056305115603385.

Omidyar Network. 2017. Digital identity and privacy. https://www.omidyar.com/sites/default/files/file_archive/Digital_Identity_POV_Oct17.pdf.

Orcutt, M. 2018. How secure is blockchain technology? *MIT Technology Review*. https://www.forbes.com/sites/forbestechcouncil/2018/10/12/how-secure-is-blockchain-technology/#53672db472f0.

Orcutt, M. 2019. The radical idea hiding inside Facebook's digital currency proposal. *MIT Technology Review*. https://www.technologyreview.com/s/613877/how-facebooks-new-blockchain-might-revolutionize-our-digital-identities/?utm_campaign=the_download.unpaid.engagement&utm_source=hs_email&utm_medium=email&utm_content=74065391&_hsenc=p2ANqtz–vWVr5C94VI3lAIMhzQbRy1.

Peppet, S. R. 2011. Unraveling privacy: The personal prospectus and the threat of a full-disclosure future. *Northwestern University Law Review* 105 (3):1153–204. http://www.cnn.com/2009/LIVING/wayoflife/05/22/aa.pay.as.drive.insurance.

Piore, A. 2020. Can blockchain finally give us the digital privacy we deserve? *Newsweek*. https://www.newsweek.com/2019/03/08/can-blockchain-finally-give-us-digital-privacy-we-deserve-1340689.html.

Pisa, M. 2018. Blockchain for global development. *Innovations: Technology, Governance, Globalisation* 12 (1–2):80–88. https://www.mitpressjournals.org/doi/pdf/10.1162/inov_a_00269.

Privacy International. 2019. Privacy international's contribution to global virtual summit on digital identity. https://privacyinternational.org/blog/2781/communities-risk-how-governments-are-using-tech-target-migrants;

Red Cross 510. 2018"An Initiative of the Netherlands Red Cross Is Exploring the Use of Self Managed Identity in Humanitarian Aid with Tykn.Tech."https://www.510.global/510-x-tykn-press-release/.

Ruppert, E., E. Isin, and D. Bigo. 2017. Data politics. *Big Data & Society* 4 (2):205395171771774. doi:10.1177/2053951717717749.

Sabadello, M. 2019. A universal resolver for self-sovereign identifiers. *Medium*. https://medium.com/decentralized-identity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c.

Scheel, S. 2019. *Autonomy of migration? Appropriating mobility within biometric border regimes*. London: Routledge.

Scheel, S., E. Ruppert, and F. Ustek-Spilda. 2019. Enacting migration through data practices. *Environment and Planning D: Society and Space* 37 (4):579–88. doi:10.1177/0263775819865791.

Schoemaker, E., D. Baslan, B. Pon, and N. Dell. 2020. Identity at the margins : Data justice and refugee experiences with digital identity systems in. *Information Technology for Development* 1–24. doi:10.1080/02681102.2020.1785826.

Schoemaker, E., P. Currion, and B. Pon. 2018. Identity at the margins : Identification systems for refugees. *Caribou Digital Publishing*. www.cariboudigital.net.

Scott, J. C. 1998. *Seeing like a state: How certain schemes to improve the human condition have failed*. New Haven and London: Yale University Press.

Scott-Smith, T. 2016. Humanitarian neophilia: The 'innovation turn' and its implications. *Third World Quarterly* 37 (12):2229–51. doi:10.1080/01436597.2016.1176856.

Seaver, N. 2014. Studying up: The ethnography of technologists. *Ethnography Matters* 1–12. http://ethnographymatters.net/blog/2014/03/10/studying-up/

Sim, K., and M. Cheesman. 2020. What's the harm in categorisation? Reflections on the categorisation work of tech 4 good. *Big Data and Society Blog*. https://bigdatasoc.blogspot.com/2020/03/whats-harm-in-categorisation.html?spref=tw.

Slavin, A. 2019. Distributed ledger identification systems in the humanitarian sector. *Sovrin*. https://sovrin.org/dlt-based-identification-in-the-humanitarian-sector/.

Society, T. R. 2019. *Privacy-enhancing technologies: Protecting privacy in practice*. https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf?la=en-GB&hash=862C5DE7C8421CD36C105CAE8F812BD0.

Sovrin. 2018. Use Case Spotlight : IRespond, Using Sovrin to Provide NGOs with Trusted Digital Identity Systems.

Srnicek, N. (2017). Platform Capitalism. Cambridge and Malden: Polity Press

Stevens, L. 2018. Self-sovereign identity systems for humanitarian interventions a case study on protective cash transfer programs. https://pdfs.semanticscholar.org/f821/4975160857f1f020ff8dbc2db65f88fcac03.pdf.

Swartz, L. 2017. Blockchain dreams: Imagining techno-economic alternatives after bitcoin. In *Another economy is possible: Culture and economy in a time of crisis*, ed. M. Castells, 82–105. Cambridge and Malden: Polity Press.

Szreter, S., and K. Breckenridge. 2012. Recognition and registration: The infrastructure of personhood in world history. *Proceedings of the British Academy* 182:1–36. doi:10.5871/bacad/9780197265314.003.0001.

Taylor, L., and D. Broeders. 2015. In the name of development: Power, profit and the datafication of the global South. *Geoforum* 64 (October):229–37. doi:10.1016/j.geoforum.2015.07.002.

Taylor, L., and H. Mukiri-Smith. 2019. Global data justice : Framing the (Mis)fit between statelessness and technology. *European Network on Statelessness*. https://www.statelessness.eu/blog/global-data-justice-framing-misfit-between-statelessness-and-technology.

Tempelhof, S. T., E. Teissonniere, J. F. Tempelhof, and D. Edwards. 2017. Bitnation governance 2.0: pangea jurisdiction and the internet of sovereignty. *Bitnation*. https://tse.bitnation.co/documents/.

Torpey, J. 2000. *The invention of the passport: Surveillance, citizenship, and the state*. Cambridge: Cambridge University Press.

Turner, L. 2019a. '#Refugees can be entrepreneurs too!' Humanitarianism, race, and the marketing of Syrian refugees. *Review of International Studies* 1:1–19. doi:10.1017/S0260210519000342.

Turner, L. 2019b. The politics of labeling refugee men as ‘ vulnerable . *Social Politics* 0 (0):1–23. doi:10.1093/sp/jxz033.

UNHCR. 2018. Bridging the identity divide – is portable user-centric identity management the answer ? https://www.unhcr.org/blogs/bridging-identity-divide-portable-user-centric-identity-management-answer/.

UNHCR. 2019. Refugee registration. https://www.unhcr.org/uk/registration.html.

Walch, A. 2017a. Blockchain's treacherous vocabulary: One more challenge for the regulators. *Journal of Internet Law* 21:2.

Walch, A. 2017b. The path of the blockchain lexicon (and the law). *Review of Banking & Financial Law* 36:713. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2940335.

Walch, A. 2019. Deconstructing 'decentralization': Exploring the core claim of crypto systems. *Crypto Assets: Legal and Monetary Perspectives* 1–36. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3326244

Wang, F., and P. De Filippi. 2020. Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion. *Frontiers in Blockchain* 2 (January):1–22. doi:10.3389/fbloc.2019.00028.

Zetter, R. 1991. Labelling refugees: Forming and transforming a bureaucratic identity. *Journal of Refugee Studies* 4 (1):39–62. doi:10.1093/jrs/4.1.39.

Zook, M., and J. Blankenship. 2018. New spaces of disruption? The failures of bitcoin and the rhetorical power of algorithmic governance. *Geoforum* 96 (August):248–55. doi:10.1016/j.geoforum.2018.08.023.