7 Inequitable Internet

Reclaiming digital sovereignty through the blockchain

Richard Wilson and Andrew Colarik

Introduction

Science fiction writer William Gibson is widely credited for saying, "The future is already here, it's just not very evenly distributed" (Fresh Air, 1993). The words, although spoken decades ago, seem particularly poignant today. The advent of the Internet was nothing short of revolutionary. The ability to share and access information bypassing the bounds of time and space fundamentally changed society on the whole. Economies were particularly disrupted as entirely new business models emerged leading to productivity gains unseen since the first Industrial Revolution. Even as the hockey-stick trend of growth continued, a parallel and negative trend emerged alongside growing inequity. Today, Technology's Frightful Five, (Manjoo, 2017, p. B1) a moniker applied to Amazon, Apple, Alphabet, Facebook, and Microsoft, is worth a staggering three trillion dollars. The success of these companies, once valued for their innovation and disruption, are increasingly an illustration of the trend of consolidation among an exclusive few.

The rise of monopolies in the increasingly important digital space carries with it the conventional dangers associated with traditional monopolies, such as reduced innovation and artificially inflated prices. But the fact is that so much of the content and services society relies on is accessed through the platforms provided by these powerful corporations that their monopolistic tendencies have increased societal and security risks. Even as the disparity between content creator and platform provider grows, a new and profitable asset class, data, the question of sovereignty and security persist. The process by which data is gathered, stored, and distributed is convoluted and opaque to the majority of users interacting with the collecting institutions. These same organizations continue to demonstrate an inability to properly safeguard users' digital identities which erodes social trust in digital technologies. A new technology, the blockchain, has the potential to assist in mitigating these issues. If the proper stakeholders are involved in the development and governance of this technology, the social and security benefits may be prodigious.

With the above in mind, this chapter first offers a synopsis of the consolidation of market power among a few technology corporations and some of the implications this presents; a discussion of the opaque, one-sided nature of the

data economy; and a supported view of the fractured and increasingly vulnerable ecosystem of digital identity management. The authors contend that these issues are interrelated and mutually reinforcing, which pose both a social and security risk to fundamental digital interactions. A preferred outcome to the issues is then proposed and the blockchain is offered as a potential mitigating technology. The benefits of public interest organizations participating in governance consortiums early are then discussed, and key measures are proposed to address the hurdles to the widespread adoption of the technology.

To establish a case for growing disparity in the digital economic space, it is necessary to delineate the concentration of wealth and power and demonstrate the "tendency towards the creation of natural monopolies on the Internet" (Esteve, 2016). The headlines of the business section hint at monopolistic practices regularly. Facebook's acquisitions, WhatsApp and Instagram – two start-up companies operating in the social media space – illustrate the trend of the disruptive competitors being swallowed by the digital giants (Allen, 2017). But these examples are more anecdotal than complete representations of the magnitude of consolidation in the digital space. It is necessary to first understand what these companies are truly selling to understand how far the concentration has progressed. Consider that Google has an 88% market share of the highly lucrative market of search advertising. Facebook owns 77% of social traffic on mobile devices, while Amazon controls three-quarters of the e-book market (Taplin, 2017). These alarming figures illuminate the power and control these companies have acquired in highly coveted and profitable revenue streams, and they are increasingly representative of the rule rather than the exception. The result is a landscape of a very few companies that "create, apply, and optimize digital technology to control massive consumer and business markets" (Andriole, 2017). The vertical and lateral integration business practices on display lead to a system in which Amazon controls retail but also cloud-computing; where Google controls mobile search and online payments. The monopolistic practices of these technology firms carry with them the traditional fears, such as reduced innovation and price-fixing. But when companies control vast swaths of the digital landscape, they control all social and economic interactions in that space in a distorted power relationship with the user.

Value creation vs. value capture

An example of the risks involved when disproportionate power relationships arise can be seen in the tumultuous move of the media industry into the digital realm. As the Internet matured and media became a digital product, traditional marketplaces began to erode into the digital economic space. Technology companies quickly leveraged their user bases to form and operate transaction model platforms. YouTube connects video bloggers with an audience base and the App Store connects Apple device users with software application programmers. In each case the creators of the content are matched with the potential customers and the platform extracts a percentage of the profit (Allen, 2015). Benefitting from creating a marketplace is a perfectly reasonable business model; the problem the

media industry faces is one of the disproportionality of returns between creators and content providers. Consider the current value appropriated by content creators that these transaction platforms rely on. An app developer often cedes 30% of the sale revenue to the App Store, a musician is paid an average of 0.005 cents per stream, and a YouTube star makes $150.00 per one million views (Conte, 2017). These figures point to a disparity in the power relationship between an industry which must utilize the digital space to remain viable and the powerful companies that control market entry and continued sustainability.

The disparity has arisen as a contention between the forces of value creation versus value capture. Value creation is the work that is put toward offering a service, resource, capability, or product that is higher than the cost of production. Value capture is the ability to realize profits from the sale of a product or service (Allen, 2017). The digital economy is becoming one in which the ability to realize profits from value creation is unevenly distributed to the few that excel in value capture. The result is a reallocation of billions in revenue from content creators to the powerful monopoly platforms on which they must now reside (Taplin, 2017), as well as leveraging the continued domination of user attention as an advertising revenue stream and control over another revenue source, user data.

Data is the new oil

Every time a person interacts with the digital space through an intermediary, data is created, collected, and stored. Every Google search, every Facebook post and every Amazon purchase generates data. The sheer scope of data that is created each day is staggering, already difficult to comprehend, and is increasing exponentially year by year. According to the International Data Corporation, the global datasphere will expand from 33 zettabytes in 2018 to 175 by 2025 (Reinsel, Gantz, and Rydning, 2018). Additionally, with new users joining every day, the Internet of things is a rapidly (IoT) growing space. Houses, cars, and even jewelry are coming online and every new device is filled with sensors that collect data that is sent to be processed and stored on the Internet. More and more of people's environment and interactions are moving into the digital sphere to be "mediated by digital services" (Kosinski, Sitwell, and Graepei, 2012). But here again, the uneven power relationship of users with digital intermediaries is evident in the way user data is gathered, analyzed, stored, and distributed.

An entire economy has arisen around, "collecting, aggregating, analyzing, and monetizing personal data" (World Economic Forum, 2011). The scope of value in this new economic realm is so vast experts have commonly compared it to the oil industry. In this context it is surprising how little the questions around data ownership and the rights of users arise. When questioning who has sovereignty of user data, it seems natural to believe that users would have at least some control over how their data are managed. The General Data Protection Regulation (GDPR), otherwise known as the Right to be Forgotten, was derived out of the European Union's case against Google and is but one of the first steps needed in challenging the prevailing control and ownership of data. In the current digital landscape,

however, this is rarely the case unless a person resolves to opt-out of the increasingly essential services that digital intermediaries administer. While the GDPR is a first step, the precedent has already been set and is now the norm for users to exchange their rights to control their personal data for the ability to access digital services (Foer, 2017). For example, every time a user searches Google their search is aggregated into metadata owned by Google in exchange for benefitting from Google's search algorithms. Also, the data from social media interactions on platforms, such as Facebook, are exchanged for access to the platform. The economy of data has evolved into an opaque environment in which many users are unaware of how much data they are trading, how that data is being used, and who in fact controls and stores it (World Bank, 2016). The exchange of data for services also creates a byproduct; significant privacy and security risks to the user.

In the digital space it seems that privacy is in exceedingly short supply. Polling data from the United States has shown that a majority of respondents are concerned about digital privacy (Rainie and Duggan, 2016). Proponents of the current framework attest that the privacy concerns accompanying data collection are conflated and benign. But research has shown that the process for identifying a private user from metadata is startlingly feasible and, in many cases, a simple algorithmic process (Kosinski, Sitwell, and Graepei, 2012). In this way data that a user considered to be private, or at least not directly linked to their personal identity, may be stored and sold by an entity outside of their control and later linked to their identity. In many cases, the pretense of anonymity is not even pursued. In China, it is estimated that 70% of users will have personally identifiable information leaked from sources they viewed as protected (Han, 2017). When companies and institutions maintain a wealth of user data, the consumer becomes transparent and opportunities to discriminate, through prices or otherwise, are available (Martin, 2015; Schudy and Utikal, 2015). The risks to privacy are significant, and they will continue to grow as the business of aggregating and selling data matures. These concerns arise within the realm of controlled and deliberate distribution of data. The problems compound when sensitive data is maliciously seized by unknown actors.

Vulnerable digital identities

To transact and interact with institutions in the digital space, users must possess and share a digital identity. Internet storefronts, social media platforms, government institutions, etc. must have a means of authenticating users to process transactions or interactions within a network. That identity is then stored with the interaction data which can range from cell phone call records to financial information to employment background checks. This information can range from innocuous to vitally important, and institutions have an obligation to maintain the security of private records. However, this is increasingly proving a challenging task. In 2017, the consumer credit reporting agency, Equifax, reported a breach in their security systems that resulted in the theft of 143 million files (Rosenzweig, 2017). These files contained extremely sensitive financial information for millions

of users. In 2015, the Office of Personnel Management of the US government experienced a breach of 21.5 million records. Among the lost records were fingerprint scans, background checks, and Social Security Numbers (Naylor, 2016). When these two instances are combined with the mounting corporate breaches of customers' personal and financial information, the unforeseen consequences are staggering. In all of these cases the people injured were not in control of their digital identity and records.

Consumers now have a fragmented and decentralized digital identity that is maintained with every institution they interact with (Chester, 2017). This is in stark contrast to a centralized system such as a consumer maintaining their personal driver's license and using it for identification on a case by case basis. The digital space is more akin to a system in which each institution generates its own driver's license and maintains a functioning copy indefinitely. In this environment a person does not necessarily own their identity. A measure of sovereignty is held by every organization the user interacts with in a range of security settings. For an individual to cede such precious control creates a poorly considered trust environment between the user and the institution, and it is becoming increasingly apparent that the consumer is shouldering more risk than the institutions charged with protecting their identities. As power and wealth in the digital space continue to condense, these security risks will continue to intensify.

The goal

As presented above, the current path would appear untenable for the whole of society. Monopolistic practices; opaque, one-sided data economies; and a fragmented, vulnerable identity ecosystem are all interrelated problems. Together they pose a security risk that is so vast in scope and potential that a course correction is absolutely necessary if security is to be a societal focus and a true balance of power between producer and consumer is to be restored. So what should be the goal in considering a change of course?

The consolidation of wealth and power in the digital economy may be summarized as an issue of the inability for consumers to opt-out of the essential services and the disproportionate ability of powerful companies to capture value from products and services. An attainable goal in this space would be simply the creation of platforms to challenge the incumbent corporations monopolizing their fields (Catalini and Ganz, 2016). The mere availability of choice for consumers and a reduced barrier to entry for content creators addresses the issue in a manner that can disrupt market power and force corporations to better serve their user base.

The problems of the metadata economy and the current authentication regime are similar. In the case of data, users are unable to practically control and track what information is collected and trafficked from their digital interactions. To interact with any service, users must authenticate their identity by providing sensitive information to be stored with a myriad of institutions indefinitely. In these arenas, the way data and identity ownership are conceived must be completely

reversed in which data belong to the user and the services are treated "as guests with delegated and finite permissions" (Zyskind, Nathan, and Pentland, 2015). In this way, users regain the ability to control their data and provide consent to services using it. This approach allows the benefits derived from sharing data to be retained while lowering the individual's risk and increasing data usage transparency.

The barriers

The goals seem achievable: Greater ability to participate in markets and consumers retaining greater control of their data and identities. Why then, do the problems persist? Perhaps powerful lobby interests and a dearth of viable alternative systems are possible challenges? They do not, however, fully explain why regulation has been so ineffectual or why innovative new models of data protection have not disrupted the status quo. In many countries any proposed regulation will face an arduous march toward enactment. Governments are faced with the burden of creating a bureaucracy to enforce regulation while corporations face challenges in compliance. Regulating Internet marketplaces and data flows is especially limited as they inherently are not bound to any single jurisdiction (Cuomo et al, 2017). Effective regulation must then achieve consensus among many stakeholders. For example, the European Union has been very assertive in their push to regulate monopolies and data protection while the US has been far more willing to let industry self-regulate (Goldfarb and Tucker, 2010). The $2.7 billion dollar fine levied against Google and the Right to be Forgotten exemplifies the differing regulatory climates leading to a patchwork system that can be difficult to navigate.

Alternatively to regulation, when problems arise in a socioeconomic system, the market is sometimes able to self-correct with innovation in business models and technology. Unfortunately, the market is proving unable to match the task. The incumbent corporations are integrating both vertically and laterally, leveraging their market power to absorb new entrants. The data economy precedent is set and current market players are content with the status quo. The multitude of identity management systems that have been proposed have not achieved the critical mass required to be a centralized, secure system (Lazarovich, 2015). Businesses have simply not been able to produce viable solutions in these spaces. Fortunately, a technology is emerging that, although not a panacea, has the potential to significantly alter the current system and is presented in the next section.

The blockchain

In 2008 a pseudonymous group named Satoshi Nakamoto released a white paper introducing the blockchain, the technological underpinnings of the Bitcoin cryptocurrency. A blockchain is essentially a distributed ledger that records interactions on a network. A full copy of the ledger is maintained on a multitude of network nodes, and, periodically, all nodes participate to achieve a consensus that the ledger is correct; the ledger version is then time-stamped and appended

to the chain of all previous versions (Hoser, 2016). Essentially, the ledger records a chain of sequential transactions in a non-reputable manner and then distributes the updated ledger across a network. The distributed element of blockchain provides some unique characteristics not offered by legacy client-server databases. Because the ledger is distributed rather than centralized, all network participants can view transactions in their entirety giving the ledger a transparency unavailable in centralized systems. User authentication and authorization to transact are handled with public key infrastructure (PKI) cryptography. Because the ledger is validated by all users through consensus algorithm processing and each ledger chained to the previous with a hashed timestamp, the ledger is effectively tamper-proof, immutable, and easily auditable (Arun and Carmichael, 2017). The transparency and immutability make the blockchain a particularly compelling technology in a myriad of use cases. Because of this, although initially conceived as an alternative to third-party institutions, research has shown that institutions stand to gain from employing blockchains in closed, "permissioned" networks as well (Underwood, 2016).

At first it can be difficult to understand how a ledger recording the transactions of digital coins could be a technology able to disrupt the digital economy and return data sovereignty to Internet users. It must be remembered that Bitcoin is merely structured data in the same way a Google search, a smartphone application, and a password are all simply blocks of data. Therefore, any data that can be grouped for processing can be envisioned as a coin or some other moniker. On this foundation, it becomes apparent that the benefits of the blockchain – transparency, integrity, and immutability – can be applied to almost any form of data (Arun and Carmichael, 2017; Catalini and Ganz, 2016). What can be done with coins can be done to any rational grouping of data or information.

Further work in this space has also been done to introduce smart contracts into blockchain technology. These are simple codified rules that can self-execute within the network (i.e. when x conditions are met, execute action y). This again spawns the possibility that the ledger technology can automate and self-execute transactions within a codified rule set (Snow et al, 2014). The concept that all forms of data may reside on a distributed ledger and that ledger can automate actions within codified conditions open the technology to uses far beyond transacting cryptocurrencies. There are many models and frameworks of the initial research of blockchain technology that can be deployed as a digital marketplace, a data transaction platform and, more relevant to this paper, as an identity management tool. The most relevant to this discussion are presented in the following sections and begin to outline a possible solution to restoring digital sovereignty.

Peer to peer business models

Blockchain, from its inception, was developed as a transaction platform. Bitcoin, despite its history, has proven that trust in value transactions can be maintained on a peer to peer network outside of the control of a central authority. It is a short leap then, as previously discussed, to imagine other forms of value being transacted

on a blockchain network. Peer to peer marketplaces such as journalism, music, applications, etc. can arise with very low barriers to entry. In fact, the ability to cheaply transact could spawn entirely new business models in which micropayments dominate the manner in which media and services are consumed (Tang, 2018). Freelance journalists could receive a payment directly from their readers while musicians could distribute their content directly to fans at any pricing model they see fit. Content creators can also benefit from the transparency of the blockchain (e.g. a team of academic researchers could track the use and distribution of a white paper) (McConahey and Holtzman, 2015). An auditable trail of intellectual property (IP) use stands to benefit any content creator and could reduce IP theft.

These possible developments point toward a future in which the modes of value capture are not completely dominated by a few powerful tech companies. The ability of marketplaces to arise on a peer to peer network with low transaction costs has the real possibility to challenge the current makeup of the digital economy (Mainelli, 2017). This is not to say that technology companies will be completely eroded, but a compelling alternative has the potential to disrupt the current market domination. Blockchain, employed as a marketplace, has the power to forestall antitrust regulation and spur innovation in the digital economy.

User-controlled data

The blockchain has the potential to reallocate control of user-generated data from the collecting corporations back to users themselves. The foundations of this concept are similar to those governing the transactions of media discussed above. Because blockchains are governed by code, the rules, both technical and legal, can be programmed into the ledger itself. Once the code is written and understood by transacting parties, all members of the network may be reasonably assured that their data will be used in accordance with the governing principles of the network (Zyskind, Nathan, and Pentland, 2015). This, in theory, leads to early adoption and increased usage and deployment.

On the blockchain, permission to use data would be transacted and a pair of keys, guest and owner, would be generated. A hash pointer would allow the guest to access the specified data in exchange for a service or alternate form of value (Lazarovich, 2015). This model allows the user to control their data through the ability to consent and revoke use. The user is also able to benefit from the transparency inherent in blockchains to track how their data is being used. Research has shown that when users are in control of their data, they become more willing to share it (Arun and Carmichael, 2017). This model allows for user control while retaining the benefits that corporations and governments derive from the use of metadata.

Identity sovereignty

Similar to metadata sharing, the blockchain could potentially return sovereignty of digital identities back to individuals. Where data may or may not be linked to

a specific user, digital identities exist purely to identify users in the digital space. Current uses of identities are used to authenticate users by means of passwords, biometric scans, etc. and to authorize users or control their interaction capability (Baars, 2016). Identity management can be built into a blockchain network, in much the same manner as data, through transacting permissions. In the case of identity management the data store could contain, rather than raw data, certified documents that verify identity and personal attributes. The obvious uses here would be documents such as passports and driver's licenses but the opportunities are much greater than basic authentication documents. Tax and financial records, student report history, medical records, and more could be placed in a user-controlled identity store following their certification by trusted third parties (Mainelli, 2017). Once the identity store is in place, the transaction ledger operates in much the same fashion as a raw data ledger. The user transacts permission to access the data store to authenticate and authorize interactions with the institution. Once an organization has authenticated an individual and determined their authorization level, an identity token can be generated. The identity token, based on PKI cryptography, would be used to control all interactions with the institution eliminating the need for a corporation to store private records linked to individuals (Pratini, 2017). This model would allow users to share only the personal information required while retaining the ability to revoke access to records. For example, a user could share healthcare records with their care provider and completely revoke access when they change doctors. This model of identity management is more centralized and reduces the fragmented redundancy of the current system while maintaining access rights in a distributed manner.

Policy Discussion

This paper has argued thus far that the blockchain is one viable solution to the unequal power relationships that have emerged from the deployment of digital technologies. The authors would be remiss if they did not mitigate the exuberance that blockchain technology offers with a larger policy discussion that clarifies some of the major issues moving forward.

Regulation vs. governance

The preceding examples show that, even in the conceptual stages, the blockchain holds the potential to fundamentally disrupt the trend of power consolidation among technology corporations. It also introduces transparency and control into the currently opaque and vulnerable regimes of data sharing and identity management. Excitement in the business community has reached a fever pitch spawning 130 start-up blockchain companies and over $1.5 billion in investment (Michalik, 2017). Public response to the technology has generally been characterized in two fashions. Markets such as the European Union and the United States have adopted a wait and see approach (Parker, 2017). This approach is far from passive but also not explicit, characterized instead by regulators gathering knowledge to avoid

premature legislation. On the other end of the spectrum, smaller countries such as the UAE, Ukraine, Estonia, and Sweden are moving substantial government records and processes onto the blockchain in a bid to embrace and sponsor the fledgling technology (Finck, 2018). This approach does much to bolster blockchain companies but may be difficult to scale and potentially premature to deploy in large-scale jurisdictions. Estonia's E-Residency program currently serves approximately 30,000 citizens (Prisco, 2015), a far cry from the hundreds of millions in the United States. Recognizing these limitations in the current regulatory approaches, a middle ground appears increasingly necessary to address large markets.

A strong case can be made that public interest in regard to blockchain deployment would be better served with a shift in focus from regulation towards governance. Regulation, a means of top-down control, carries with it the pitfalls of stifling innovation, introducing costs associated with compliance and enforcement, and being too slow to evolve with the technology and market (Byrne, 2016). Governance, however, is a means for stakeholders to collaboratively guide the development of a technology (Tapscott and Tapscott, 2016). Governance consortiums are being convened, but participation is invariably industry-dominated and the focus is on the development of common protocols rather than the fostering of public good (Gabinson, 2016). There is an opportunity here for governments and public interest groups to sponsor consortiums that place issues, such as financial inclusion, data protection, and digital identity, front and center. Conversations between public and private sectors early could have the added benefit of forestalling the need for regulations enacted when the technology matures. Blockchains can be built around agreed governance and regulation, essentially self-automating compliance through code. Regulations rely on extrinsic compliance through consequences, but when rules are breached on a blockchain, the transaction simply fails to process (Yeoh, 2017). For these reasons, it is imperative that the public sector join the governance conversation early to foster the public good they are charged to protect.

Next steps

Blockchain holds promise to fundamentally alter societies' interactions with the digital space. The technology, however, is far from mature. User interfaces must be developed, Interledger protocols are in their infancy, and privacy remains a concern. The most glaring issue is bringing the technology to scale. Every day new users and devices come online with associated data flows and digital identities. Blockchains, if deployed as a central platform of markets, data sharing, and single sign-on identity management must process massive quantities of transactions, safely and securely. To date, publicly funded research has not been concordant with need. Most public funding is awarded to private industry as innovation grants in specific use cases (Cheng et al, 2017; Higgins, 2017). This stands in stark contrast to the development of the TCP/IP framework for the Internet. In that case, much of the funding and innovation into the plumbing of the Internet

was conducted through general research government funding. The technology was then deployed and the private sector innovated atop the infrastructure. An increase of general research funding may bring about innovations in blockchain foundations to address problems facing scalability (Walport, 2016). This may even lead to a widespread public blockchain upon which private entities could establish community protocols associated with specific use cases.

The second hurdle to widespread adoption will inevitably be the considerable cost of implementing blockchain technology. The financial services industry has conducted exhaustive cost-benefit analyses concerning blockchain deployment and consensus has generally returned that the cost savings are considerable (Cocco, Pinna, and Marchesi, 2017). The spheres of identity management, data sharing, and market inclusion stand to benefit from similar analyses. To be sure, costs do arise when technology companies dominate their markets, or when large-scale personal information breaches occur. These costs must be quantitatively weighed against the cost of replacing legacy IT systems to provide a clearer picture to decision-makers. Both the public and private sectors would benefit from increased clarity on the costs and benefits of widespread deployment in the aforementioned spheres.

Conclusion

Inequality in both power dynamics and economic opportunity are growing in the digital space. The most formidable technology companies are consolidating their power and controlling more and more of fundamental societal interactions. The consolidation trend has contributed to a disparate ability among the powerful to realize profit from products and services, an opaque data economy, and a fractured and increasingly vulnerable identity management system. The problems are interrelated and growing in scale. The trend cannot continue with significant harm done; societies must enact measures that foster market inclusion and restore sovereignty of data and identities back to Internet users. Thus far, regulation and market course corrections have proven unmatched to the task, but a new technology, the blockchain, shows promise. The transparency and immutability offered by the blockchain can mitigate current trends, reduce consumer risk, and restore a measure of public trust. Although blockchain technology is in its infancy, the public sector must be involved in governance discussions early. Government-sponsored consortiums can focus the conversation on public good, and blockchains can be developed with consumer protections built into the code. To spur widespread adoption of the technology, governments should divert funding from specific use case innovation grants to general research into the foundations of the technology itself, focusing on scalability and security. Cost-benefit analysis research must also branch from solely financial services to the realms of data sharing, market inclusion, and identity management. Such research would provide policy makers with vital information to determine where and when deployment is appropriate. Public sector research and funding can bring about a future of growth and security so desperately needed to restore public trust and return equity to the Internet.

References

Allen, JP (2017) *Technology and inequality: concentrated wealth in a digital world*. Cham: Palgrave Macmillan.

Allen, K (2015) 'Big tech's big problem – its role in rising inequality', *The Guardian*. August 2. https://www.theguardian.com/business/economics-blog/2015/aug/02/big-techs-big-problem-rising-inequality, accessed September 1, 2019.

Andriole, S (2017) 'There will be 30 technology companies in 2030, 10 in 2050, and then there will be none', *Forbes*. May 25. https://www.forbes.com/sites/steveandriole/2017/05/25/there-will-be-20-technology-companies-in-2030-10-in-2050-and-then-there-will-be-none/#4af13f77132b, accessed September 1, 2019.

Arun, J and Carmichael, A (2017) 'Trust me: digital identity on blockchain', *IBM Institute for Business Value*. January. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03823USEN&, accessed September 1, 2019.

Baars, DS (2016) *Towards self-sovereign identity using blockchain technology*. Master's thesis, University of Twente.

Byrne, M (2016) 'Blockchain: from "what" and "why" to regulating "how"', *Lawyer (Online Edition)*. May 20, p. 5. https://www.thelawyer.com/issues/online-may-2016/blockchain-from-what-and-why-to-regulating-how/, accessed September 1, 2019.

Catalini, C and Ganz, J (2016) *Some simple economics of the blockchain*. NBER Working Paper No. 22952. The National Bureau of Economic Research. December. doi:10.3386/w22952

Cheng, S, Daub, M, Domeyer, A and Lundqvist, M (2017) 'Using blockchain to improve data management in the public sector', *McKinsey Digital*. February. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector, accessed September 1, 2019.

Chester, J (2017) 'How the blockchain will secure your online identity', *Forbes*. May 3. https://www.forbes.com/sites/jonathanchester/2017/03/03/how-the-blockchain-will-secure-your-online-identity/#53b11ca65523, accessed September 1, 2019.

Cocco, L, Pinna, A and Marchesi, M (2017) 'Banking on blockchain: costs savings thanks to the blockchain technology', *Future Internet*, 9(25), 1–20. doi:10.3390/fi9030025

Conte, J (2017) How *artists* can (finally) *get paid in the digital age*. August 23. https://www.ted.com/talks/jack_conte_how:artists_can_finally_get_paid_in_the_digital_age, accessed September 1, 2019.

Cuomo, J, Nash, R, Pureswaran, V, Thurlow, A and Zaharchuck, D (2017) *Building trust in government*. IBM. March 17. https://www.ibm.com/downloads/cas/WJNPLNGZ, accessed September 1, 2019.

Esteve, F (2016) 'The concentration of wealth in the digital economy', *Technology and Inequality*. May 3. http://lab.cccb.org/en/technology-and-inequality-the-concentration-of-wealth-in-the-digital-economy/, accessed September 1, 2019.

Finck, M (2018) 'Blockchains: regulating the unknown', *German Law Journal*, 19(4), pp. 665–692.

Foer, F (2017) 'How silicon valley is erasing your individuality', *Washington Post*. September 8. https://www.washingtonpost.com/outlook/how-silicon-valley-is-erasing-your-individuality/2017/09/08/a100010a-937c-11e7-aace-04b862b2b3f3_story.html?utm_term=.aa99307cff12, accessed September 1, 2019.

Fresh Air (1993) 'Science fiction writer WILLIAM GIBSON', *Terry Gross National Public Radio*. August 31.

Gabinson, G (2016) 'Policy considerations for the blockchain public and private applications', 19 SMU. *Science Technology & Law Review*, 327.

Goldfarb, A and Tucker, CE (2010) *Privacy regulation and online advertising*. http://dx.doi.org/10.2139/ssrn.1600259, accessed September 1, 2019.

Han, D (2017) 'The market value of who we are: the flow of personal data and its regulation in China', *Media and Communication*, 5(2), pp. 21–30. doi:10.17645

Higgins, S (2017) 'US government awards $2.25 million to blockchain research projects', *Coindesk*. May 12. https://www.coindesk.com/us-government-awards-2-25-million-blockchain-research-projects/, accessed September 1, 2019.

Hoser, T (2016) 'Blockchain basics, commercial impacts and governance challenges', *Governance Directions*, 68(10), 608–612.

Kosinski, M, Sitwell, D and Graepei, T (2012) 'Private traits and attributes are predictable from digital records of human behavior', *Proceedings of the National Academy of Sciences of the United States of America*, 110(15), pp. 5802–5805. doi:10.1073

Lazarovich, A (2015) *Invisible Ink: blockchain for data privacy*. Massachusetts Institute of Technology. June. https://dspace.mit.edu/bitstream/handle/1721.1/98626/920475053-MIT.pdf?sequence=1, accessed September 1, 2019.

Mainelli, M (2017) 'Blockchain will help us prove our identities in a digital world', *Harvard Business Review*. March 16. https://hbr.org/2017/03/blockchain-will-help-us-prove-our-identities-in-a-digital-world, accessed September 1, 2019.

Manjoo, F (2017) 'Tech's frightful five: they've got us', *The New York Times*. May 10, p. B1.

Martin, K (2015) 'Ethical issues in the big data industry', *MIS Quarterly Executive*, 14(2), pp. 67–85. http://www.misqe.org/ojs2/index.php/misqe/article/viewFile/588/394, accessed September 1, 2019.

McConahey, T and Holtzman, D (2015) 'Towards an ownership layer for the internet', *ascribe GmbH*. June 24. https://assets.ctfassets.net/sdlntm3tthp6/resource-asset-r391/d110e1250fe31959150659144c424feb/5d5f7fde-646f-4b1c-8fe8-e939080348a0.pdf, accessed September 1, 2019.

Michalik, V (2017) *Frost & Sullivan and outlier ventures identify the 2017 global blockchain startup map*. March 27. https://ww2.frost.com/news/press-releases/frost-sullivan-identifies-2017-global-blockchain-startup-map/, accessed September 1, 2019.

Naylor, B (2016) *One year after OPM data breach, what has the government learned?*National Public Radio, Inc. June 6.http://www.npr.org/sections/alltechconsidered/2016/06/06/480968999/one-year-after-opm-data-breach-what-has-the-government-learned, accessed September 1, 2019.

Parker, L (2017) 'European commission "actively monitoring" blockchain developments', *Brave New Coin*. February 17. https://bravenewcoin.com/insights/european-commission-actively-monitoring-blockchain-developments, accessed September 1, 2019.

Pratini, N (2017) 'Identity, privacy, and the blockchain: what do identity and privacy mean in the digital world, and how might blockchain technology play a role?', *Insights on the Future of Finance from Plaid*. May 4. https://fin.plaid.com/articles/identity-privacy-and-the-blockchain, accessed September 1, 2019.

Prisco, G (2015) 'Estonian government partners with bitnation to offer blockchain notarization services to e-residents', *Bitcoin Magazine*. November 30. https://bitcoinmagazine.com/articles/estonian-government-partners-with-bitnation-to-offer-blockchain-notarization-services-to-e-residents-1448915243/, accessed September 1, 2019.

Rainie, L and Duggan, M (2016) Privacy and information sharing. Pew Research Center. January 14. http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/, accessed September 1, 2019.

Reinsel, D, Gantz, J and Rydning, J (2018) 'The digitization of the world: from edge to core', *IDC White Paper – #US44413318*. https://www.seagate.com/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf, accessed September 1, 2019.

Rosenzweig, P (2017) *The equifax hack--bad for them, worse for us*. Scientific American. September 12. https://blogs.scientificamerican.com/observations/the-equifax-hack-bad-for-them-worse-for-us/, accessed September 1, 2019.

Schudy, S and Utikal, V (2015) '"You must not know about me" - on the willingness to share personal data', *Journal of Economic Behavior & Organization*, 141(1), 1–11. doi:10.1016

Snow, P, Deery, B, Lu, J, Johnston, D, Kirby, P, Sprague, AY and Byington, D (2014) 'Business processes secured by immutable audit trails on the blockchain', *Brave New Coin*. November 16. https://bravenewcoin.com/insights/business-processes-secured-by-immutable-audit-trails-on-the-blockchain, accessed September 1, 2019.

Tang, G (2018) *Peer-to-peer decentralized marketplace based on blockchain technology. Version 5.0*. https://lookrev.com/doc/lookrev-whitepaper.pdf , accessed September 1, 2019.

Taplin, J (2017) 'Is it time to break up google?', *The New York Times*. April 22. https://www.nytimes.com/2017/04/22/opinion/sunday/is-it-time-to-break-up-google.html, accessed September 1, 2019.

Tapscott, D and Tapscott, A (2016) *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. New York: Penguin.

Underwood, S (2016) 'Blockchain beyond bitcoin', *Communications of the ACM*, 59(11), pp. 15–17. doi:10.1145/2994581

Walport, M (2016) *Distributed ledger technology: beyond block chain*. London: Government Office for Science.

World Bank (2016) *World development report 2016: digital dividends*. Washington, DC. doi:10.1596/978-1-4648-0671-1

World Economic Forum (2011) *Personal data: the emergence of a new asset class*. January. http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf?utm_source=datafloq&utm_medium=ref&utm_campaign=datafloq , accessed September 1, 2019.

Yeoh, P (2017) 'Regulatory issues in blockchain technology', *Journal of Financial Regulation and Compliance*, 25(2), pp. 196–208. doi:10.1108/JFRC-08-2016-0068

Zyskind, G, Nathan, O and Pentland, A (2015) *Enigma: decentralized computation platform with guaranteed privacy*. https://www.enigma.co/enigma_full.pdf, accessed September 1, 2019.