Defending Internet Freedom through Decentralization: Back to the Future?

Chelsea Barabas

Neha Narula

Ethan Zuckerman

The Center for Civic Media &

The Digital Currency Initiative

MIT Media Lab, August 2017

Executive Summary

The Web is a key space for civic debate and the current battleground for protecting freedom of expression. However, since its development, the Web has steadily evolved into an ecosystem of large, corporate-controlled mega-platforms which intermediate speech online. In many ways this has been a positive development; these platforms improved usability and enabled billions of people to publish and discover content without having to become experts on the Web's intricate protocols.

But in other ways this development is alarming. Just a few large platforms drive most traffic to online news sources in the U.S., and thus have enormous influence over what sources of information the public consumes on a daily basis. The existence of these consolidated points of control is troubling for many reasons. A small number of stakeholders end up having outsized influence over the content the public can create and consume. This leads to problems ranging from censorship at the behest of national governments to more subtle, perhaps even unintentional, bias in the curation of content users see based on opaque, unaudited curation algorithms. The platforms that host our networked public sphere and inform us about the world are unelected, unaccountable, and often impossible to audit or oversee.

At the same time, there is growing excitement around the area of decentralized systems, which have grown in prominence over the past decade thanks to the popularity of the cryptocurrency Bitcoin. Bitcoin is a payment system that has no central points of control, and uses a novel peer-to-peer network protocol to agree on a distributed ledger of transactions, the blockchain. Bitcoin paints a picture of a world where untrusted networks of computers can coordinate to provide important infrastructure, like verifiable identity and distributed storage. Advocates of these decentralized systems propose related technology as the way forward to "re-decentralize" the Web, by shifting publishing and discovery out of the hands of a few corporations, and back into the hands of users. These types of code-based, structural interventions are appealing because in theory, they are less corruptible and resistant to corporate or political regulation. Surprisingly, low-level, decentralized systems don't necessarily translate into decreased market consolidation around user-facing mega-platforms.

In this report, we explore two important ways structurally decentralized systems could help address the risks of mega-platform consolidation: First, these systems can help users directly publish and discover content directly, without intermediaries, and thus without censorship. All of the systems we evaluate advertise censorship-resistance as a major benefit. Second, these systems could indirectly enable greater competition and user choice, by lowering the barrier to entry for new platforms. As it stands, it is difficult for users to switch between platforms (they must recreate all their data when moving to a new service) and most mega-platforms do not interoperate, so switching means leaving behind your social network. Some systems we evaluate directly address the issues of data portability and interoperability in an effort to support greater competition.

We offer case studies of the following decentralized publishing projects:

Freedom Box, a system for personal publishing
Diaspora, a federated social network
Mastodon, a federated Twitter-like service
Blockstack, a distributed system for online identity services
IPFS (Interplanetary File System), a distributed storage service with a proposed mechanism to incentivize resource sharing
Solid (Social Linked Data), a linked-data protocol that could act as a back-end for data sharing between social media networks
Appcoins, a digital currency framework that enables users to financially participate in ownership of platforms and protocols
Steemit, an online community that uses an appcoin to incentivize development and community participation in a social network

Considering these projects as a whole, we found a robust and fertile community of experimenters developing promising software. Many of the projects in this report are working on deeply exciting new ideas. Easy to use, peer-to-peer distributed storage systems change the landscape for content censorship and archiving. Appcoins may transform how new projects are launched online, making it possible to fund open-source development teams focused on

developing shared protocols instead of independent companies. There is also a renewed interest in creating interoperable standards and protocols that can cross platforms.

However, we have reason to doubt that these decentralized systems alone will address the problems of exclusion and bias caused by today's mega-platforms. For example, distributed, censorship-resistant storage does not help address problems related to bias in curation algorithms – content that doesn't appear at the top of your feed might as well be invisible, even if it's technically accessible. And though censorship-resistance and decentralization are noble goals that will undoubtedly appeal to tech-savvy and politically inclined users, most users are not ideologically motivated and have no interest in shouldering the additional cost and responsibility of running these complex systems directly. They will want to engage with the Web through friendlier, third-party publishing platforms, and these platforms will suffer from the same forces that drive consolidation today.

It's important to remember that today's mega-platforms are built on top of the Web's already distributed and open protocols. The real issue to address is this natural tendency towards market consolidation. Underlying these concerns is the predominant business model for platforms on the Web – user-targeted advertising. Advertising based business models encourage the consolidation and the hoarding of user views and data, driving platforms to become ever larger.

The challenges decentralized systems as a whole face are as follows:

User and developer adoption. Technical feasibility alone does not guarantee the sort of widespread adoption necessary to build a useful social network. Some of the more mature tools developed in this space have faced serious difficulties in attracting a permanent user base, and the problems those platforms suffer from may hinder the growth of new systems as well. Social networks, in particular, are difficult to bootstrap due to network effects. We generally join social networks because our friends are already there. Systems like Steemit and Diaspora are currently incompatible with existing social networks, planning to supersede existing communities like Reddit and Facebook, rather than integrate with them. Taking a competitive, rather than complementary, position in the market creates a difficult barrier to entry for new projects. Similarly, interoperable protocols require adoption at the developer level. Solid, which hopes to

bridge between existing and novel social networks, faces a serious adoption challenge: Why should developers choose to switch to Solid's new data model, and what's the incentive for Facebook to make their data interoperable without legal requirements forcing them to do so?

Security. Another major issue is security. "Decentralized" networks generally means anyone can join, which implies these systems have to take strong precautions to enforce security, usually by pushing the responsibility of security to users in the form of managing public key cryptography. It is extremely difficult to develop software that is both cryptographically secure and easy to use. Most of these systems, like IPFS and Blockstack, do not yet have a good story for how users will manage their private cryptographic keys and gain a good mental model of complex security protocols. As companies like Signal, an encrypted messaging service, have recently demonstrated, this is not impossible to achieve, but it requires an intense focus on usability that we did not see in many of the tools we review in this report.

Monetization and incentives. Given that user data is so important for monetizing these platforms, there is little incentive for the mega-platforms to adopt interoperable protocols – they would rather own all the data. Similarly, content that is viewed and clicked on the most generates the most advertising revenue, so mega-platforms have an incentive to prioritize viral, attention-grabbing or feel-good content. Steemit offers a fascinating alternative model to prioritizing and monetizing content. However, it replaces opacity with a semi-transparent free market model that concentrates power in a few hands and, if not carefully crafted, might even incentivize *more* clickbait. Designing robust reward mechanisms for community-governed content is still an open problem, but if solved, this could be integral to placing curation control in the hands of a community.

Resisting market consolidation? Platforms benefit from economies of scale in multiple ways – it's cheaper to acquire resources like storage and servers in bulk and as platforms become larger they become more useful as a social network and usually, more profitable. Even in decentralized systems like Bitcoin, there has been a natural market consolidation in the form of large mining pools. This type of consolidation into a few super-participants might be inevitable due to economies of scale. We are increasingly persuaded that this isn't necessarily a bad thing, and that a more realistic goal might be the development of a robust, competitive marketplace

that offers a range of ground rules for online speech, rather than a return to a purely peer-to-peer architecture for communication online.

Recommendations: We advise investors–whether motivated by civic or fiscal concerns–both to watch this space closely and to advocate for the pre-conditions that we believe will enable a healthier marketplace for online publishing. A precondition for the success of these distributed platforms is a shift towards user-controlled data, the ownership of a user's social graph and her intellectual property created online. It will be difficult for new platforms to develop without widespread support for efforts towards data portability and rights over data ownership. Data portability also enables new models for aggregation.

Small, thoughtfully curated news sources will be made more powerful by having access to the user data currently locked inside mega-platforms, but right now, federated clients that interoperate between different platforms are borderline illegal – fixing this may require adjusting overly broad regulations, like the Digital Millennium Copyright Act. We believe that these user-controlled data rights are essential to develop a more robust market and allow new efforts to emerge from existing communities. Though individual users might not directly care about or understand these rights, their adoption will free developers to create applications that leverage users' existing data, so that they can provide compelling, interesting new experiences, even with a small user base.

In envisioning a marketplace for open speech platforms that support more generative and censorship-resistant discussions, we recommend focusing on supporting existing efforts that provide alternatives to Facebook's opaque curation and ranking. These alternatives might look more like Reddit's sub-communities, with different rule sets to enable different types of conversation, overseen and administered by members of the community with a system for due process when contentious issues arise.

Funding developers directly to create a diverse ecosystem of publishing platforms and curation websites is another place to make a difference. In particular, foundations are in an excellent place to fund the development of user-friendly software to implement common security practices that are common across many applications. An example of this is Let's Encrypt, which makes

using secure HTTP (HTTPS) easier for small website administrators. Most small platforms do not have the resources to directly hire experts in usability and security.

Another fascinating space to watch and explore is that of Appcoins. Recently there has been a dramatic upsurge in the adoption of appcoins as a mechanism for funding new projects and platforms. Appcoins potentially provide a way to circumvent the existing open-source or VC-funded software development models to create systems where users collectively own their data. Creating an alternative business model to advertising could end up pushing the markets to create entirely new, different types of applications than the ones we've seen so far, which mainly rely on user data and views. New funding models means smaller projects could more easily bootstrap small, personalized communities. However, this space also has a lot of potential for scams, and it might be unreasonable to expect users to manage a financial stake in many different networks.

Table of Contents

Executive Summary……...1

Introduction

The Rise of the Centralized Web……....8
Risks Posed by the Centralized Web……15
Structural Interventions as a Possible Solution……...27

Section II: Federation

Freedom Box……33
Diaspora……34
Mastodon……...39

Section III: Open Protocols……43

Authentication……...46
Blockstack…… 51
Interoperability…….. 59
IPFS……61
Solid……69

Section IV: Appcoins……...76

Steemit……...87

Conclusion……..104

The Rise of the Centralized Web

Between 1989 and now, the World Wide Web transformed from an obscure system for publishing technical notes to a basic infrastructure of commerce, learning and social interaction. In celebrating the rise of the web and the ways it now provides interpersonal connection for billions of people, we often forget that the web has undergone dramatic organizational and infrastructural shifts. These shifts force us to reexamine one of our most cherished hopes for the web: that it could be a space for civic debate and social inclusion, opening previously closed conversations to a broader set of citizens.

When Tim Berners-Lee designed and implemented the hypertext transport protocol, he was designing a system for use by physics researchers, mostly academics who had access to university computing resources. In pre-web days, academic computing users had accounts on shared computers, and the social norms of the time meant that users had a great deal of control over the computing resources they used. By the early 90's, the emergence of the open web helped normalize this idea of distributed control of content. While thousands of people had published online using FTP, Gopher, Archie and WAIS (Wide Area Information Server), the web's increased usability meant that millions of people could then publish their own webpages.

As the web gained more widespread adoption, legal scholars and online advocates began to conceive of it as an important new battleground for preserving core social values, such as freedom of expression. For them, that battleground was situated squarely in the technical underpinnings of the web itself. Particular emphasis was placed on ***the structural factors that helped to preserve individual freedoms*** online, particularly against the encroachment of powerful actors such as the State. This perspective is well illustrated in the writings of early web advocates, such as John Perry Barlow's *A Declaration of the Independence of Cyberspace*, in which the author proclaimed, "We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here."[1]

Two decades after its publication, the tone of Barlow's Declaration rings a bit naive. The web is a far more complicated place than the egalitarian, immaterial utopia Barlow depicts. But in the 1990's, writing like this deeply resonated with early advocates of cyberspace, who saw the technical architecture of the web as a powerful vehicle for achieving transformational social change through the free exchange of ideas. According to media historian Fred Turner, many of these ideas were an extension of left leaning counterculture movements from the 60's and 70's, which sought to replace hierarchical social structures with new models of governance based on self-sufficiency and shared consciousness, rather than the laws of the ruling class.[2]

Legal scholar Lawrence Lessig has perhaps most clearly articulated the idea that code itself is a mechanism for negotiating power and control over speech online. He, along with many other web enthusiasts, celebrated and defended the development of open protocols such as TCP/IP, which he argued deeply impacted the "regulability" of the Internet. TCP/IP is the protocol used to exchange data across a network, without knowing the content of the data or who the sender and recipients are in real life. According to Lessig, TCP/IP is a great example of how we are able to use code to build in strong protections for important values such as freedom of speech–the easier it is to set up point-point communication between parties, the harder it is to regulate and limit the exchange of certain kinds of data.[3]

Similarly, HTTP was lauded as a critical component of the web's open and distributed structure, because it enabled anyone with a web server to publish their own content, which (hypothetically) anyone with a web browser could then find. There was no need to ask permission and few possible consequences for actions taken for sharing

---

[1] "A Declaration of the Independence of Cyberspace" http://seteici.eu/wp-content/uploads/2013/06/John-Perry-Barlow_Independance-of-Cyberspace.pdf. Accessed 19 Feb. 2017.
[2] Turner, Fred. *From counterculture to cyberculture: Stewart Brand, the Whole Earth Network, and the rise of digital utopianism*. University of Chicago Press, 2010.
[3] "Code Is Law - Harvard Magazine." 1 Jan. 2000, http://harvardmagazine.com/2000/01/code-is-law-html. Accessed 19 Feb. 2017.

ideas online. In theory, one could reach the whole world through the World Wide Web. In reality, that narrative was again oversimplified. The early web was quite chaotic and hard for users to navigate. The organization of content was highly distributed. It was assumed that users would be both publishers and readers, that each person would have a homepage composed of links that she authored and used to document useful resources and shortcuts across the web.

This distributed wayfinding architecture made it difficult to find resources online, especially as more and more people started making their own websites. Moreover, users needed a baseline of technical know-how in order to set up and run their own server for publishing. This created a significant barrier to entry for new users to participate fully in the dream of the open web.

Even though the Internet was built on distributed protocols, the web needed to consolidate around a few curated service platforms in order to become practical for everyday people to use. This trend towards consolidation has serious implications for two key functions of the web–publishing and discovery of content.

Due to improvements in usability today's web is much easier to use and open to vastly more people, but centers on a small number of points of control. The owners of those points of control–primarily large, for-profit, publicly traded companies–comprise a new class of elite power players, ones that have enormous influence on our online interactions. And because so many of our interactions–commercial, interpersonal and civic–are mediated online, we have inadvertently given these companies a great deal of control over our political lives and civic discourse. This trend is reflected in the growing number of user petitions for sites like Facebook to stop censoring content and banning the accounts of historically marginalized voices.[4]

In light of these developments, concerned open web advocates have begun to call for the "re-decentralization" of the web. This framing points directly to the structural

[4] "Petition demands Facebook 'stop censoring and banning the accounts ...." 10 Oct. 2016, http://alldigitocracy.org/petition-demands-facebook-stop-censoring-and-banning-the-accounts-of-blacks-and-trans-activists/. Accessed 19 Feb. 2017.

and organizational consolidations of power and influence that we see around mega-platforms like Google and Facebook, as well as the organizational challenges that emerge from the way certain key technical processes, such as naming (via the Domain Name System), are carried out online. Decentralization has become the new moniker under which technologists and free speech advocates have organized to re-establish the web as an open infrastructure for everyday people.

But what does "decentralization" mean? Echoing back to the rhetoric of the early web, re-decentralization advocates tend to focus on structural interventions that might realign power relationships between institutions (governments, corporations, etc.) and end users. Advocates like Brewster Kahle have urged open web advocates to investigate ways we might "lock open the web" with code, enabling more peer-to-peer interactions in the place of mediated private platforms.[5] The urge here is to return to the good old days of unmediated publishing without the need for third-party intermediaries who can exercise undue influence over our interactions online. In contrast to other strategies that might focus on legal frameworks or market competition, the appeal of structural interventions is that, in theory, they are less corruptible and more resistant to corporate and political capture. Structurally decentralized systems strive to avoid any chokepoints where a single actor can constrain use of the system, while hoping to preserve the usability of centralized systems.

In some ways, this line of thinking is a reincarnation of the cypherpunk worldview, which first emerged in the 1970's alongside significant developments in the study of cryptography. Technological advances in encryption, such as the widely used RSA encryption algorithm and the Diffie-Hellman key exchange, made it possible for an individual with modest computing resources to enjoy strong privacy protections, even in the face of governments and corporations with significantly greater resources. Many celebrated these technological breakthroughs as a critical safeguard for user privacy in

[5] "Locking the Web Open: A Call for a Distributed Web | Brewster Kahle's ...." 11 Aug. 2015, http://brewster.kahle.org/2015/08/11/locking-the-web-open-a-call-for-a-distributed-web-2/. Accessed 19 Feb. 2017.

an increasingly digital world. Still others–the cypherpunks–strove to harness cryptographic innovations in order to drive much broader social and political changes.

The intellectual roots of the cypherpunk movement are grounded in the work of people like David Chaum, who first proposed the use of cryptographic primitives to create anonymous digital cash in the early 80's.[6] Cypherpunks took ideas like this and extended them even further. For them, cryptography was a critical vehicle for individual freedom, one that could significantly weaken the reach of governments and other powerful institutions. The most extreme adherents to the cypherpunk worldview embraced a philosophy sometimes referred to as crypto-anarchism, which envisioned a world in which all laws and regulations were supplanted by mathematically verifiable code. Important values and enforcement mechanisms could be encoded directly into software that would carry out critical social processes through the secure exchange of information.

Forty years later, the cypherpunk dream has not (yet) been realized. Security scholar Arvind Narayanan argues there is simply not a high user demand for upsetting fundamental power structures through crypto-enforced contracts, particularly in democratic societies where governments are chosen by the people.[7] Moreover, the vision of code as a functional stand-alone governance institution breaks down amidst the reality of unpredictable and imperfect humans, messy social systems, and buggy code. In order for cryptographic systems to be practical, Narayanan argues, they need to provide clear paths to recourse for users when things go wrong. To do this, technological solutions must effectively interact with other modes of governance and enforcement, such as existing legal systems.[8]

In spite of these struggles, the cypherpunk movement has experienced a renaissance in recent years thanks to the rise of projects like Bitcoin. Bitcoin is a

---

[6] Chaum, David. "Security without identification: Transaction systems to make big brother obsolete." *Communications of the ACM* 28.10 (1985): 1030-1044.

[7] Narayanan, Arvind. "What happened to the crypto dream?, part 1." *IEEE Security & Privacy* 11.2 (2013): 75-76.

[8] I.e. Anonymous digital markets for physical goods are not useful if users can't pursue legal recourse in the event that goods aren't actually shipped once they have been paid for.

peer-to-peer cash system that enables the secure exchange of digital tokens without the need for a trusted third party like a bank or credit card company. Bitcoin enthusiasts frame the potential of this technology in terms of its “decentralizing” impact. Rather than placing one’s trust in a closed network controlled by elite financial institutions, Bitcoin offers users an open alternative by “decentralizing” critical processes of secure value exchange, like transaction validation and currency issuance. The decentralized architecture of Bitcoin provides guarantees for certain user protections, such as resistance against censorship. Bitcoin achieves censorship-resistance through two mechanisms: First, there is no consistent mapping of digital Bitcoin identity to real-world identity -- anyone can join the system and create as many “accounts” as they wish. However, these accounts are pseudonymous, not anonymous, and identities can be uncovered by carefully examining the flow of transactions. Second, theoretically, anyone has the ability to verify and update the Bitcoin ledger by entering into a process known as “mining.” Mining is the process by which participants in the network process and secure new transactions. Mining is not gated, but practically, it lies in the hands of the few who are willing to make the financial investment in the necessary hardware.

On the one hand, Bitcoin faces many of the hallmark struggles of a cypherpunk project -- it is cumbersome to use and demand for alternative financial services has not been high enough to push Bitcoin into the mainstream. At the same time, Bitcoin has captured public imagination and provided the conceptual framework for a new generation of projects that strive to distribute critical processes and services that currently fall under the purview of large, for-profit companies. Like the early cypherpunks, many of these projects seek to “disrupt” this new class of power elites–the digital platform owners–by developing peer to peer protocols for the exchange of information, and supporting crowdsourced methods for curating content and managing user reputation.

This school of thought has greatly influenced the thinking of open web advocates who are concerned about the increased consolidation of the web around a few large platforms. For advocates of an open web, the clearest path forward lies in a return to a

more distributed web architecture, one that hearkens back to the early days online. Yet this framing of the issue fails to account for the fact that all of the centralized services that have come to dominate the market today were built *on top of* the distributed architecture of the original web.

Distributed, peer-to-peer protocols like HTTP and SMTP are still the functional rails on top of which today's web runs. However, practically speaking, the web is now heavily consolidated around just a few service providers. This consolidation is most clearly illustrated in the distribution of online advertising dollars, which roughly reflects the distribution of viewership on the web. According to a 2016 report, 85 cents of every new dollar spent on online advertising went to just two companies–Facebook and Google.[9] It appears that structurally decentralized architecture doesn't inherently lead to decentralized, competitive markets. This points to the need for developing a more nuanced understanding of the role that structural/technical decentralization plays in addressing the new class of risks to personal and political speech that we observe online today.

A good first step would be to recognize that structural centralization in and of itself may not be a negative development. Indeed, many positive benefits in terms of usability, efficiency and performance can come from consolidating resources and managing economies of scale. But these perks come with a cost. What we might gain in terms of convenience and efficiency, we then lose in terms of control and freedom. In developing a strategy to address contemporary challenges online, we must develop a more fine-grained understanding of what we view as the threats that accompany increased "centralization" of the web. Only then can we weigh the costs and benefits of different interventions intended to re-decentralize the web.

Some of those interventions might come in the form of peer-to-peer alternatives to corporate social media platforms. Others might be structural checks and balances that help us safeguard against abuses of power by today's online hegemons. Still others

[9] "Media Websites Battle Faltering Ad Revenue and Traffic." 17 Apr. 2016, https://www.nytimes.com/2016/04/18/business/media-websites-battle-falteringad-revenue-and-traffic.html. Accessed 19 Feb. 2017.

might be hard coded structural limitations on power–ways to offload liability from large players so that they cannot comply with external pressures to violate important user rights, such as a user's privacy or rights against self-incrimination. In order to understand which strategies are best suited for which risks, we need to get a more detailed understanding of the specific chokepoints we want to address.

In the following section, we outline the new set of risks that have emerged alongside the consolidation of our communication online. In delineating these risks, we also point to potential strategies for solving them. In subsequent sections, we will we dive into specific projects aiming to decentralize different layers of the web.

Risks Posed by the Centralized Web

It's undeniable that the rise of large publishing platforms like Facebook, Twitter and Medium has enabled a significantly more user-friendly web. But at what cost? Today just two websites, Facebook and Google, account for 81% of all incoming traffic to online news sources in the U.S.[10] Over the last two years Facebook has overtaken Google as the number one source of incoming traffic, and current projections indicate that this trend is likely to continue over the coming years. Google now processes 3.5 billion search queries per day, roughly ten times more than its nearest competitors (Baidu, Yahoo, Microsoft, Yandex).[11] In 2016, Facebook supported an average of over 1.2 billion active users per day.[12] Recent surveys conducted by the Pew Research Center reveal that a clear majority of Facebook and Twitter users (63% on both sites) report using these platforms to access news on current events and other issues beyond the sphere of family and friends.[13]

---

[10] "Facebook now drives more traffic to media sites than Google | Fortune ...." 18 Aug. 2015, http://fortune.com/2015/08/18/facebook-google/. Accessed 19 Feb. 2017.
[11] "Google Search Statistics - Internet Live Stats." http://www.internetlivestats.com/google-search-statistics/. Accessed 19 Feb. 2017.
[12] "Facebook: global daily active users 2016 | Statistic - Statista." https://www.statista.com/statistics/346167/facebook-global-dau/. Accessed 19 Feb. 2017.
[13] "The Evolving Role of News on Twitter and ...." 14 Jul. 2015, http://www.journalism.org/2015/07/14/the-evolving-role-of-news-on-twitter-and-facebook/. Accessed 19 Feb. 2017.

The rise of social media as a source of news cuts across nearly all demographic groups in the US. For Millennials, Facebook is by far the most dominant source of news on government and politics, on par with television news consumption for the Baby Boomer generation.[14] In light of these trends, it is clear that a small and shrinking number of online platforms will have very significant influence over what media the public consumes on a daily basis. We can understand this influence in terms of two key aspects of online speech: these platforms control what is possible to publish, and they control whether others are likely to discover it. In the following section, we explore specific risks related to the publication and discovery of online speech.

Risk 1: Top-down, Direct Censorship

Users face an increased risk of censorship as our digital publishing ecosystem becomes increasingly consolidated around a few popular platforms. Generally speaking, service platforms controlled by a single company are more prone to top-down censorship and surveillance pressures from government than decentralized alternatives. In order to stay in business, corporate social media networks which own user data must comply with local laws and regulations related to free speech and censorship. Otherwise, they could face legal repercussions that make it difficult for them to operate in certain jurisdictions. This was the case in the spring of 2016, when Facebook blocked users in Thailand from seeing satirical pages that poked fun at the King and Thai Royal Family.[15] In a notice posted in lieu of the blocked content, Facebook explained that it took down the pages in order to comply with a local Thai law that prohibits defamation of the Royal family. Apparently the junta government has been increasing pressure for sites like Facebook and Line to comply with court orders to block content it deems “a threat to peace and order” in the country.[16] Platform companies face a complex calculus in these cases. If Facebook decides to block pages on the basis of lese majeste, they

[14] Ibid.
[15] "Facebook Blocks Thailand From Page Satirizing ... - Khaosod English." 5 May. 2016, http://www.khaosodenglish.com/politics/2016/05/05/1462426398/. Accessed 19 Feb. 2017.
[16] "Thailand Military Government To Pressure Facebook, Line To Censor ...." 3 Feb. 2016, http://www.techtimes.com/articles/129603/20160203/thailand-military-government-to-pressure-facebook-line-to-censor-content.htm. Accessed 19 Feb. 2017.

will set a dangerous precedent, and may end up being forced to block more content by subsequent governments. On the other hand, companies like Facebook could decide to ignore local rulings and simply ensure they have no assets or personnel in those countries so those laws cannot be enforced.

Additionally, there have been many instances in which social media platforms like Twitter and Facebook have come under attack by national governments. This is particularly common during politically sensitive times, such as during the 2009 presidential election in Iran and amidst the outbreak of Arab Spring protests in Tunisia in 2011, when the government used malware to steal the passwords and take over the accounts of users who were critical of the Tunisian government.[17]

But these issues are not limited to far distant lands where political revolution is bubbling up just under the surface. Just this August, a group of activists submitted a public letter to Facebook CEO Mark Zuckerberg, lobbying for a new “anti-censorship policy” after it was revealed that the platform, at the request of law enforcement, had taken down videos of a Baltimore woman who was shot and killed by the police.[18] This incident was not the first time that Facebook has taken down content related to police killings in the U.S. Earlier this year, a video capturing the police shooting death of Philando Castile was removed from the platform in what was later described as a “glitch.” Activist groups have contested this description, claiming that the police had a role removing the footage from Castile’s girlfriend’s account as it began to go viral across the Internet.[19]

One reason these networks are susceptible to this type of surveillance and control is because they are required to comply with the local laws and regulations of the countries where their users reside. However, another reason is because of the way they

---

[17] "Tunisia plants country-wide keystroke logger on Facebook - The ...." 25 Jan. 2011, https://citizenlab.org/2011/01/tunisia-plants-country-wide-keystroke-logger-on-facebook/. Accessed 19 Feb. 2017.

[18] "Activists call for Facebook 'censorship' change after Korryn Gaines ...." 24 Aug. 2016, https://www.theguardian.com/technology/2016/aug/24/facebook-live-anti-censorship-policy-korryn-gaines-letter. Accessed 19 Feb. 2017.

[19] "Facebook 'glitch' that deleted the Philando Castile ... - The Register." 8 Jul. 2016, https://www.theregister.co.uk/2016/07/08/castile_shooting_police_deletion/. Accessed 19 Feb. 2017.

have chosen to architect their systems. Unlike in distributed systems like BitTorrent, platforms like Facebook, YouTube and Twitter can delete content legal authorities determine to be offensive. This causes two problems: First, because these companies want to maintain good relationships with governments, and governments can make it very difficult to access these sites from within their borders, the companies will comply with censorship requests. Since the networks are controlled by companies with clearly defined leadership who can potentially be prosecuted, it's clear who to ask when seeking to censor content.

Second, because these companies completely control the software stack of how that content is ingested, stored, curated, and served, the companies are *able* to comply with such requests. An example of a structural change that makes it nearly impossible to comply with surveillance requests is when WhatsApp moved to using end-to-end encryption for users' messages–WhatsApp itself, despite being part of Facebook, actually cannot reveal unencrypted data to anyone who might request it, because they only store encrypted messages on their servers, and not the decryption keys.[20][21] A key goal of this paper is to explore these types of structural changes.

Risk 2: Curatorial Bias / Indirect Censorship

In recent years, questions have been raised regarding the potential for unintentional or international biases to be embedded in the curation algorithms of major platforms like Facebook. Building on research from Robert Epstein and Ron Robertson that suggest Google could tip an election by optimizing its search results,[22] Jonathan

[20] This has led to some interesting legal battles in courts that seek to pressure WhatsApp to share user data. For example, in 2016 a Brazilian judge temporarily ordered the shutdown of the service after the company failed to comply with a request for encrypted data.
[21] "WhatsApp Blocked in Brazil as Judge Seeks Data - The New York Times." 2 May. 2016, https://www.nytimes.com/2016/05/03/technology/judge-seeking-data-shuts-down-whatsapp-in-brazil.html. Accessed 19 Feb. 2017.
[22] "How Google Could Rig the 2016 Election - POLITICO Magazine." 19 Aug. 2015, http://www.politico.com/magazine/story/2015/08/how-google-could-rig-the-2016-election-121548. Accessed 19 Feb. 2017.

Zittrain notes that Facebook could influence electoral behavior by controlling what messages different readers see.[23]

More subtle, but no less worrisome, are the unintentional ways in which Facebook and others tend to optimize for viral, feel-good content that will garner a large number of "likes." For example, in 2014 Facebook came under fire from media critics, who pointed out that there were marked differences in the way that Facebook and Twitter covered the outbreak of the protests in Ferguson, Missouri during the summer of 2014.[24] Recent scholarly work has demonstrated the critical role that Twitter played in bringing these protests to the national spotlight.[25] Thanks to organic grassroots conversation about what was going on the ground in Ferguson, Twitter was able to surface breaking news from the frontlines, well before mainstream media had picked up the story.

In contrast, on Facebook, the most prominent story found on most Americans' newsfeeds at the time was the Ice Bucket Challenge, a fundraising campaign for research to cure Lou Gehrig's disease. As media scholar Zeynep Tufekçi pointed out, the Ice Bucket Challenge was perfect for the Facebook algorithm–it was viral, feel-good content–whereas more difficult and nuanced conversations about race and police violence could only be found on a platform with less top-down algorithmic influence.[26] The urgency of this debate has significantly heightened in recent months, as individuals from across the political spectrum have expressed concerns about the proliferation of "fake news," or click-bait headlines that confirm voters' pre-existing political preferences and beliefs at the expense of fact-based coverage of current events.[27]

---

[23] "Information Fiduciary: Solution to Facebook digital gerrymandering ...." 1 Jun. 2014, https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering. Accessed 19 Feb. 2017.

[24] These protests were sparked by the fatal police shooting of an unarmed African-American man named Michael Brown.

[25] Tufekçi, Zeynep. "Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency." *J. on Telecomm. & High Tech. L.* 13 (2015): 203.

[26] "What Happens to #Ferguson Affects Ferguson: – The Message - Medium." 14 Aug. 2014, https://medium.com/message/ferguson-is-also-a-net-neutrality-issue-6d2f3db51eb0. Accessed 19 Feb. 2017.

[27] "Facebook and Twitter have a civic duty to protect us from fake ... - Wired." 24 Feb. 2017, http://www.wired.co.uk/article/social-medium-message. Accessed 27 Feb. 2017.

Given the significant amount of leverage that social media platforms like Facebook and Twitter have over the content we consume (both online and offline, via indirect influence over mainstream media coverage), this incident has raised important questions about how unintentional bias manifests in the curation of content on these sites. Much of this debate centers on the need for greater transparency and accountability for the way today's curation algorithms are constructed. As Tufekçi points out, "I wonder: What if Ferguson had started to bubble, but there was no Twitter to catch on nationally? Would it ever make it through the algorithmic filtering on Facebook? Maybe, but with no transparency to the decisions, I cannot be sure."

Yet, the concept of transparency is not nearly as straightforward in the age of algorithmic curation. Curation algorithms are complex, living pieces of code that evolve over time. We are only beginning to develop the analytical frameworks necessary for understanding how slippery concepts like "bias" and "fake news" are encoded into algorithmic decision-making processes.[28] We are even further from understanding how to translate those frameworks into practical accountability procedures.

Zittrain has advocated for greater transparency and ethical standards in how algorithms are designed and broadly implemented on major social media sites, arguing that "The most important fail-safe is the threat that a significant number of users, outraged by a betrayal of trust, would adopt alternative services, hurting the responsible company's revenue and reputation."[29] Zittrain points to the potential for transparency to fuel competition-driven consumer protections, whereby consumers make decisions about what platform to use based on the reputation and curation decisions made by the site. Of course, Zittrain's proposal requires interoperability across platforms and low switching costs in order for it to be practical to leave on social network to join a different one. Ultimately, Zittrain's solutions face the same problem Rebecca MacKinnon's

[28] Sandvig, Christian, et al. "Auditing algorithms: Research methods for detecting discrimination on Internet platforms." *Data and discrimination: converting critical concerns into productive inquiry* (2014).
[29] "Information Fiduciary: Solution to Facebook digital ... - New Republic." 1 Jun. 2014, https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering. Accessed 27 Feb. 2017.

Ranking Digital Rights project struggles with: increasing transparency about platform behavior is most impactful when users can actually switch platforms.

This emphasis on competition stands in contrast to the "benevolent monopoly" paradigm proposed by prominent technologists such as Peter Thiel, who argues that large companies without significant competitors can be more creative and effective in developing new, valuable services for their customers.[30] These two paradigms are not mutually exclusive. The concept of an "information fiduciary" could be useful for ensuring that mega-platforms are checked for blatant abuses of their immense curatorial power, whereas competition might be the best way to fuel a healthier ecosystem of consumer choice for those concerned about a broader set of biases in the way that their newsfeeds are curated.

However, if competition is ever going to be a meaningful path towards resolving these issues, we must develop practical methods for lowering the costs of switching between different platform providers. In subsequent case studies, we will discuss the challenges of overcoming network effects and data lock-in, as well as explore strategies that might enable greater competition between incumbent mega-platforms and new platform alternatives.

Risk 3: Abuse of Curatorial Power

In recent months, Facebook has come under fire due to accusations that its employees systematically suppress the discovery of conservative content on their platform. These accusations were sparked by anonymous accounts from former Facebook employees, who claimed that they routinely removed conservative-leaning news stories from the network's influential "Trending" news section, even when such stories were identified as a hot topic by the platform's curation algorithm.[31] Facebook

[30] "Peter Thiel: Competition Is for Losers - WSJ - Wall Street Journal." 12 Sep. 2014, http://www.wsj.com/articles/peter-thiel-competition-is-for-losers-1410535536. Accessed 27 Feb. 2017.
[31] "Former Facebook Workers: We Routinely Suppressed Conservative ...." 9 May. 2016, http://gizmodo.com/former-facebook-workers-we-routinely-suppressed-conser-1775461006. Accessed 27 Feb. 2017.

has since denied the claims, saying that the company "found no evidence that the anonymous allegations are true."[32]

Regardless of whether the accusations hold weight, the most important take-away is that it would be very difficult for an outside observer to detect such changes. The company has no legal or normative obligation to disclose how it prioritizes content on its site. Determining how the company automatically identifies content to remove, or how it prioritizes the display of certain content requires “algorithmic auditing”, which is difficult to conduct and may not be possible under existing laws and regulations.[33]

Moreover, the influence of mega-platforms like Facebook is not limited simply to the curation of external content. It is also perhaps the most powerful broker of social influence and signaling online. In 2010, Facebook ran a pilot to understand the impact of “political mobilization messages” on voter turnout for that year’s U.S. Congressional election. Researchers found that users were .39 percent more likely to vote if they were notified when their close friends had voted on Facebook.[34] During the 2010 midterm elections, that translated to an estimated 340,000 additional votes, a margin that could have changed the outcome of close high-stakes elections, such as the 2000 U.S. presidential election, especially if applied selectively (i.e. if Facebook had urged members of one party to vote and not provided similar nudges to the other side.). Mechanisms like this could play a significant role in influencing human behavior on an unprecedented scale, yet we have no checks and balances in place to ensure that this influence is not abused.

These developments have sparked growing concerns over the potential for Facebook to intentionally influence important civic events, such as the 2016 presidential election. In a statement released earlier this summer, the Republican party expressed

---

[32] "Tom Stocky - My team is responsible for Trending Topics,... | Facebook." https://www.facebook.com/tstocky/posts/10100853082337958. Accessed 27 Feb. 2017.
[33] "Sandvig v. Lynch - Complaint | American Civil Liberties Union." https://www.aclu.org/legal-document/sandvig-v-lynch-complaint. Accessed 27 Feb. 2017.
[34] "A 61-million-person experiment in social influence and ... - James Fowler." 13 Sep. 2012, http://fowler.ucsd.edu/massive_turnout.pdf. Accessed 27 Feb. 2017.

such concerns, saying “With 167 million US Facebook users reading stories highlighted in the trending section, Facebook has the power to greatly influence the presidential election. It is beyond disturbing to learn that this power is being used to silence viewpoints and stories that don't fit someone else's agenda."[35]

Historically, major media outlets have been viewed as both private entities and public service institutions, beholden to government regulations that seek to ensure that broadcast content serves the public interest. For example, under a law passed in 1934, the Federal Communications Commission requires “legally qualified” political candidates to have equal opportunities for airtime on broadcast TV and radio stations. The FCC promised to enforce this law earlier in 2015, after long-shot political candidate Lawrence Lessig filed several requests with NBC affiliates to speak on air after Hillary Clinton was invited to guest star on the popular Saturday Night Live Show.[36]

This example is quite tricky–the fairness doctrine was repealed in the 1980s under Reagan and these prescriptions are much weaker than they used to be. As of now, that precedent has not carried over into the digital sphere. But as more and more of our media migrates over to digital, networked spaces one must ask whether or not such regulations should be extended to these realms as well. Perhaps it is okay to have just a few large platforms serve as content curators, as long as we can understand and hold them accountable for the way they wield that curatorial influence. However, it remains unclear how to translate concepts of public accountability to the digital sphere of networked publishing.

Risk 4: Exclusion

Mega-platforms like Facebook and Twitter aren’t just sites for passive consumption of content. They also provide important civic spaces for social and political discourse. The idea that underlies the civic media movement is that making and

---

[35] "MakeThisTrend: Facebook Must Answer for Conservative Censorship." https://gop.com/makethistrend-facebook-must-answer-for-liberal-bias/. Accessed 27 Feb. 2017.
[36] "FCC Chief Vows to Require “Equal Time” on TV for Candidates - The ...." 22 Oct. 2015, https://www.theatlantic.com/politics/archive/2015/10/fcc-chief-vows-to-require-equal-time-on-tv-for-candidates/457482/. Accessed 27 Feb. 2017.

disseminating media is a form of civic engagement and power. The current opportunities to make media are unprecedented. An estimated one in four people in the world have an active Facebook account,[37] and hundreds of millions more are connected by other large, centralized social networks.

In theory, this massive networked public sphere provides an unprecedented opportunity for everyday people to reach a global audience and engage in conversations with people from around the world. But the reality is not so straightforward. As adoption of Facebook has grown, so has the complexity of implementing effective community governance policies and user safeguards. Terms of service and community regulation efforts have unintended consequences, which are increasingly exacerbated the more monolithic the platform becomes. Media activist Jillian York has highlighted a wide range of groups who have been excluded and censored on the site, ranging from plus-sized women and LGBT groups to journalists and indigenous communities.[38]

In some cases, exclusion is the result of clunky terms of service–such as when Facebook's real name policy made it challenging for members of the transgender community to open and maintain accounts under adopted names or pseudonyms, used widely within the LGBT community.[39] While the policy was intended to help minimize the number of inactive and fake accounts on the platform, it inadvertently excluded individuals with non-traditional names and those who need to use pseudonyms in order to protect their real identity (i.e. activists living under oppressive political regimes). In other instances, Facebook's community governance standards have been misused to erase people whose personal situations are in conflict with mainstream norms and practices. This was the case when photos of topless aboriginal women and

---

[37] "Number of monthly active Facebook users ...." https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/. Accessed 27 Feb. 2017.

[38] "A complete guide to all the things Facebook censors hate most — Quartz." 29 Jun. 2016, https://qz.com/719905/a-complete-guide-to-all-the-things-facebook-censors-hate-most/. Accessed 27 Feb. 2017.

[39] "Facebook real-name policy controversy - Wikipedia." https://en.wikipedia.org/wiki/Facebook_real-name_policy_controversy. Accessed 27 Feb. 2017.

breastfeeding mothers were mislabeled as inappropriate content by other Facebook users because their breasts were uncovered.[40]

But perhaps the most blatant examples of abuse of community standards stems from intergroup conflict–when one set of users actively seeks to suppress content from another group. This was the case in 2010 when some users formed a Facebook group called “Facebook Pesticide,” with the expressed purpose of reporting and removing outspoken Arab atheists and Muslim reformists from the site.[41] To accomplish this goal, members of the group would coordinate reports of abuse against accounts they deemed unacceptable. While Facebook does not make explicit exactly how they choose to take down profiles, it seems that the platform automatically disables accounts after a certain number of reports are submitted. Automated enforcement of terms of service amplifies these problems of online speech. It's not feasible–or legally desirable–for Facebook to monitor the speech of over one billion members. Instead, they rely on reports from other users.

If several users flag content as inappropriate, it will likely be deleted. The technique is particularly effective when used on content in languages that Facebook's administrators don't read, such as Arabic. The platform does not inform users when their profile has been removed, nor the reason for de-activation from the site. This makes it challenging for users to seek recourse and reintegration back into the site. These issues are exacerbated by the lack of alternative publishing networks with comparable reach around the globe. Given that Facebook is the most widely used social network in the world, those who are excluded from the site face serious consequences.[42]

This is not a theoretical problem. Users are blocked every day from Facebook as part of ongoing political disputes. Israeli activists, non-government groups and

---

[40] "A complete guide to all the things Facebook censors hate most — Quartz." 29 Jun. 2016, https://qz.com/719905/a-complete-guide-to-all-the-things-facebook-censors-hate-most/. Accessed 27 Feb. 2017.
[41] "On Facebook Deactivations – Jillian C. York." 8 Apr. 2010, http://jilliancyork.com/2010/04/08/on-facebook-deactivations/. Accessed 27 Feb. 2017.
[42] Crawford, Kate, and Tarleton Gillespie. "What is a flag for? Social media reporting tools and the vocabulary of complaint." *New Media & Society* 18.3 (2016): 410-428.

government departments frequently flag Facebook accounts of Palestinian journalists and activists, seeking their removal from the platform.[43] As the political climate in the US grows more tense after Donald Trump's election, some Facebook users report that they have been flagged and suspended from the service for expressing unpopular political opinions.

Exile from the platform not only makes it hard to engage in important civic discourse, but it also has important implications for how Internet users are able to access a broader range of services outside the site. In 2008, Facebook rolled out a new service called Facebook Connect, which allows third-party sites to piggyback off of the platform's robust identity authentication and management system, rather than implement their own from scratch. In many ways, this service is a win-win for both users and websites, as it significantly lowers the costs of building out a secure identity infrastructure for smaller sites, while also simplifying account management for end users by minimizing the number of usernames and passwords they must remember. As a growing number of sites adopt Facebook Connect, some have likened the service to a kind of "driver's license for the Internet," the new de-facto standard for identity on the web.[44] But for all the benefits we gain in convenience, we must consider the equally serious risks of widespread exclusion this trend poses for those who are unable to access the Facebook platform, due to conflicts with clunky terms of service and abuse of community governance guidelines.

As the above examples illustrate, terms of service on mega-platforms, even when thoughtfully authored and enforced, can have far-reaching unintended consequences. When speech and access are limited in this fashion, those speaking have few alternatives. They can try to influence the platform owners, often by naming and shaming, publicly decrying their ill treatment. But power asymmetries make that prospect difficult. For example, in spite of continuous lobbying from the LGBTQ

---

[43] "Facebook 'blocks accounts' of Palestinian journalists - News from Al ...." 25 Sep. 2016, http://www.aljazeera.com/news/2016/09/facebook-blocks-accounts-palestinian-journalists-160925095126952.html. Accessed 27 Feb. 2017.

[44] "Facebook Wants to Supply Your Internet Driver's License." 5 Jan. 2011, https://www.technologyreview.com/web/27027/. Accessed 27 Feb. 2017.

community, in partnership with organizations like the Electronic Frontier Foundation, Facebook has yet to implement significant changes to their real name policy.[45] Of course, members of the LGBTQ community could publish on their own, but they lose the network effects of a system like Facebook, and they find themselves using less user-friendly tools and reaching smaller audiences.

It remains unclear how mega-platforms like Facebook should go about balancing the needs of marginalized groups with the broader goal of keeping the mainstream safe on a global scale. What is clear is that these tech companies operate and own a new sphere of influence, one which has transformed the Internet from a public commons to a gated corporate community. As more speech moves online, the ability of Facebook and other platforms to determine who can participate in important civic conversations becomes deeply concerning.

Structural Interventions as a Possible Solution to Centralized Control

The above analysis encourages us to think in terms of chokepoints. On the Internet of 1994, two major chokepoints existed that could prevent you from publishing online -- your Internet service provider could refuse to provide the connectivity that allowed your web server to be online, or your domain name registrar could refuse to serve your domain name. In practice, because of the culture of common carriage and of a neutral and open net, these constraints were very seldom seen. Today, new chokepoints exist in terms of both publication and discovery of content. These chokepoints are largely situated around the rise of large social network platforms, which not only own and operate the user interface for interacting with online content, but also the underlying physical architecture that stores and manages the data we generate.

Social media platforms have become a critical communications and information infrastructure–a highly standardized and ubiquitous system that remains largely unseen

[45] "Facebook real-name policy controversy - Wikipedia." https://en.wikipedia.org/wiki/Facebook_real-name_policy_controversy. Accessed 27 Feb. 2017.

and unfelt, until something goes wrong.[46] When incidents occur, and imperfections of the system are revealed, however, the gradual privatization of the web becomes apparent, and the line between public infrastructure and private property is blurred. This blurring of the public and the private has made it challenging to develop clear strategies for addressing emerging risks to free speech online, such as curation bias, exclusion and both direct and indirect censorship (through obscurity as well as through blocking the posting of content).

In the face of this ambiguity, a recurring cycle of what Ananny and Gillespie term "shocks and exceptions" have emerged as the prevailing response to breakdowns in platform governance.[47] "Shocks" are moments when users collectively become aware of the public implications of private platforms, in the wake of an incident in which users' expectations of "how things should work" don't match up with the operational reality of the platform. Shocks can give rise to public outcry, which in turn can lead to specific calls for change, or dissipate after some rapid response from the platform (a public apology, a quick reversal of a new policy, etc.).

Oftentimes, platform responses come in the form of "exceptions," or policies that pause usual business practices in order to uphold a competing value that is not directly related to financial gain.[48] These exceptions tend to bypass fundamental reform (i.e. an overhaul of terms of service, new metrics for content curation and remuneration) in favor of actions that are limited to a very specific set of circumstances. These policies are self-implemented, without the support of a formal accountability system to ensure that they are upheld in the future.

Case-by-case exceptions enable platforms to defuse public outrage, without necessarily engaging in more sustained efforts to ensure the public interest in the face of complicated socio-technical problems. For example, in 2014 Facebook sparked outrage after it published results from a 2012 experiment that sought to understand the

[46] Ananny, Mike, and Tarleton Gillespie. "Public Platforms: Beyond the Cycle of Shocks and Exceptions." Conference presentation, Oxford Internet Institute, 2016.
[47] Ibid.
[48] Ibid.

extent to which the company could manipulate users' emotions via their news feed.[49] The company publicly apologized for the poor timing and communication of the research, and voluntarily instated a set of new policies to manage future research experiments.[50] However, those policies are not accessible to the public and there is no clear way for average users to monitor their effective implementation over time.

In light of these challenges, it is not surprising that technologically sophisticated users of the web would seek architectural solutions to these chokepoints. As Lessig observes, "code is law"–systems that cannot be censored, architecturally, are more desirable than techno-social systems, in which we rely on companies to resist attempts to take down content.[51] In recent years, we have seen a surge in interest in designing technical interventions that might break up the power vested in mega-platforms, and restore greater agency and choice directly into the hands of the user.

Early Internet pioneer and activist Brewster Kahle has been a prominent figure in rallying enthusiasm around the idea of structurally "locking the web open." In the summer of 2016 Kahle convened a group of technologists to build strategies around tools and services that enable peer-to-peer communication, without the need for third party intermediaries or platform-specific log-ins and passwords.[52] This implicit desire for permanence and incorruptibility has been echoed in the work of many blockchain enthusiasts, who envision a world run by "smart contracts" that can autonomously execute rules and procedures on behalf of a collective, without the need for cooperation from individuals or third party institutions.[53] Still others have opted to focus on important chokepoints along "the stack" of the web, particularly with regard to the storage and

---

[49] "Facebook sorry – almost – for secret psychological experiment on users." 2 Oct. 2014, https://www.theguardian.com/technology/2014/oct/02/facebook-sorry-secret-psychological-experiment-users. Accessed 27 Feb. 2017.
[50] "Facebook sorry – almost – for secret psychological experiment on users." 2 Oct. 2014, https://www.theguardian.com/technology/2014/oct/02/facebook-sorry-secret-psychological-experiment-users. Accessed 27 Feb. 2017.
[51] Lessig, Lawrence. "Code is law." *The Industry Standard* 18 (1999).
[52] "Locking the Web Open, a Call for a Distributed Web | Internet Archive ...." 11 Feb. 2015, http://blog.archive.org/2015/02/11/locking-the-web-open-a-call-for-a-distributed-web/. Accessed 27 Feb. 2017.
[53] "Decentralized Blockchain Technology and the Rise of Lex ... - SSRN." 20 Mar. 2015, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664. Accessed 27 Feb. 2017.

retrieval of data,[54] or the opening up of proprietary algorithms that support machine learning on major publishing platforms.[55]

This diverse array of structural interventions reflects the multi-faceted nature of the challenges we face as a result of platform-driven chokepoints. There is unlikely to be a one-size-fits-all solution to the risks we outlined above. As we discussed in our risks section, free speech can be limited through bad faith actions on the part of the platform host, or as the result of manipulation and abuse from a community of other users on the site. But it could also be the by-product of unintended consequences of the rules, regulations, and algorithms developed to maintain an online community, or as the result of external pressures from governments to censor content they deem undesirable.

In this report we will evaluate the potential impact of structural interventions based on their ability to address at least one of the following questions:

1) Does this intervention enable users to independently publish, discover or curate content, reducing the need for a platform intermediary like Facebook?
2) Does this intervention help create a market where there are more platforms on which to publish, by reducing switching costs or enabling greater consumer agency to make informed choices?

The first strategy is consistent with the cypherpunk approach to solving problems: embed safeguards and limits on power directly into the underlying infrastructure and, whenever possible, give users autonomy over where and how their content is published. Yet, solutions that enable content to persist in the face of censorship pressures are not necessarily going to make that content discoverable. The reason censorship via Facebook is so powerful is because Facebook is a major curator

[54] "IPFS - Content Addressed, Versioned, P2P File System (DRAFT 3)." https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf. Accessed 27 Feb. 2017.
[55] "The decentralization of knowledge: How Carnap and ... - First Monday." http://firstmonday.org/ojs/index.php/fm/article/view/7109/5655. Accessed 27 Feb. 2017.

of content–if your post is suppressed in Facebook's newsfeed it might as well not exist at all. To address this challenge comprehensively, we must also develop better strategies for discovering and filtering content within peer-to-peer architectures.

This could come in the form of tools that support peer-to-peer interaction, ones that do not require an intermediary such as Facebook to locate, serve and curate content on behalf of users. But it could also come in the form of greater consumer choice in the face of unsatisfactory experiences on dominant platforms. Increased choice could be the by-product of structural adjustments that make it easier for consumers to switch from one service to another, as well as increase the diversity of high quality alternatives available in the market.

Early efforts to promote informed consumer choice include Rebecca MacKinnon's Ranking Digital Rights project, which seeks to rank large web companies on their efforts to preserve user interests.[56] MacKinnon's hope is that mega-platforms like Facebook would be transformed from authoritarian "Internet sovereigns" into a sort of accountable ruling class, who are beholden to the needs of their loyal subjects.[57] Work like this is a critical first step, but its success necessitates the presence of real, comparable alternatives in the market of online publishing. To date, this has proven quite difficult to achieve. Very few users choose networks for ideological reasons–they choose based on usability, features and where their friends are publishing. That means these competitive platforms need to be as good–or probably much better–than existing leaders to invite migration.

Greater competition could be fostered if structural adjustments were made to reduce the friction in opting out of and switching between online services. For example, increased interoperability between platforms would mean that leaving Facebook for a competitor doesn't mean severing and rebuilding hundreds of relationships. In the following case studies, we will examine structural interventions that make it easier for new platforms to bootstrap a minimal viable user base, effectively leveling the playing

[56] "Ranking Digital Rights - Ranking ICT sector companies on respect for ...." https://rankingdigitalrights.org/. Accessed 27 Feb. 2017.
[57] "Consent of the Networked." https://consentofthenetworked.com/. Accessed 27 Feb. 2017.

field for new platforms entering the market alongside competitors that can leverage significant economies of scale and powerful network effects.

But even if a solution is technically feasible, there are many reasons why it might not ultimately become integrated into our current online systems. If the service is not easy to use, or requires additional costs and effort on the part of the user to operate, it is less likely to gain widespread adoption. Of course, widespread adoption might not be necessary if interoperability between applications is increased, or the service is one that doesn't require others to join in order to be useful (i.e. decentralized personal data storage). However, historically open source alternatives to Facebook etc. have struggled to develop products that are user-friendly enough for mass consumption. We will take a close look at the factors which shape the usability of each of the interventions we present below.

In addition to user adoption, it's important to consider the technical trade-offs that might drive a developer's decision to adopt a given technical framework or tool. Decentralized infrastructure can be cumbersome to build and expand upon, and sometimes sacrifices key performance outcomes for the sake of disintermediation. We will evaluate each of our tools from the perspective of developers, to determine whether or not a given intervention is likely to be embraced by the technical community that would need to implement it.

Finally, we will examine whether or not each intervention is viable from a business perspective. Decentralized infrastructures can directly impact the way online services are able to capture value through their platforms. If an intervention undermines the prevailing business model of the web–which is based largely on the monetization of user generated data for targeting and advertisements–then we must understand how the companies that might adopt this intervention would be able to survive. It is through these three criteria–user adoption, developer opt-in and business viability–that we will ultimately evaluate the strength of each of the case studies we examine below.

SECTION II: FEDERATION

Freedom Box, Diaspora and the Challenges of Federated, Open Source Social Media

In the mid-2000's open Internet activist Eben Moglen identified control over our networked data infrastructure as the next battleground for consumer protections online. As a legal scholar, Moglen argued that the rise of cloud storage services posed a direct threat to our Fourth Amendment rights to freedom and privacy, because it removed sensitive personal information from the sacredness of the home, where we have strong privacy protections in place, to private infrastructure that is ultimately owned and operated by for-profit companies.

According to Moglen, "Everybody understands that that which you keep close is more yours to regulate and control than that which you voluntarily give away to a stranger to keep for you… So the server that protects your freedom should be in your house."[58] The rise of "the cloud" marked an important shift in the relationship between users and the data they generate online, whereby service providers became the primary owners of both the physical infrastructure and the software that is needed to support online applications. This has serious implications for how content is published and disseminated online. In spite of these growing concerns, Moglen and other like-minded individuals struggled to gain traction with large online service providers to provide stronger privacy guarantees, such as encryption by default, to their customers.

In light of these struggles, Moglen launched a project called Freedom Box in 2010, with the aim of shifting away from large, corporate owned server farms to a more community-oriented model for managing communications online. In contrast to projects with similar goals, such as Own Cloud[59] and Media Goblin,[60] the Freedom Box[61] team

[58] "Eben Moglen: How We Can Be the Silver Lining of the Cloud - YouTube." 1 Sep. 2010, https://www.youtube.com/watch?v=NsKTtWgn0uM. Accessed 27 Feb. 2017.
[59] "ownCloud." https://owncloud.org/. Accessed 7 Mar. 2017.
[60] "MediaGoblin." http://mediagoblin.org/. Accessed 7 Mar. 2017.

resisted the urge to return back to the personal server model that was prominent in the early days of the web, opting instead for a more grassroots community model of service provision. According to James Vasile, former Director of the Freedom Box Foundation, a small group of users would ideally be able to access a more secure means of engaging in online activities for which they wanted better privacy guarantees, via a friendly local tech enthusiast who set up and maintained a Freedom Box for the neighborhood.

The Freedom Box itself would provide “out of the box” privacy guarantees, such as encrypted communication services. Rather than require users to download and run additional software on their own, the Freedom Box team sought to build in better default settings into hardware that consumers were already in the habit of buying. As such, they focused on building Freedom Box firmware into an affordable router. Routers were an ideal piece of technology for the Freedom Box team to focus on building around, because they are an extremely common piece of hardware that most households need to purchase in order to connect to the Internet. In addition to performing the normal functions of a router, the Freedom Box includes additional features, such as the ability to communicate between peers and filtering for advertising and malware. The hope was that by selling routers with custom firmware, the Freedom Box team would adjust the default settings for going online automatically, without requiring effort or specialized knowledge on the part of users.

Moreover, the Freedom Box project has been part of a broader push by privacy and consumer rights advocates towards supporting open, federated social networks like Diaspora. Federation is the idea of a group of organizations or individuals working together to support a common standard of operation. The goal of Diaspora, founded in 2010, was to provide a federated social network: a distributed social networking service that addressed consumer privacy concerns by enabling users to host their own content on a friendly community device, like Freedom Box. Diaspora would also serve as a

[61] "FreedomBox - Debian Wiki." 28 Aug. 2016, https://wiki.debian.org/FreedomBox. Accessed 7 Mar. 2017

social aggregator of content from more mainstream sites like Facebook, until eventually the decentralized alternative had enough traffic to stand on its own. Ultimately, one of the goals of the Freedom Box project was to mitigate the power of large social media sites like Facebook by building in support for open source projects like Diaspora by default. This would include making the Freedom Box router a node in the Diaspora network, as well as enabling easy account sign up when users are setting up their Freedom Box for the first time.

In 2013, the first Freedom Box was released on the market, combining a standard Dreamplug router with a secure digital card (SD card) with custom firmware that enabled additional ad blocking, malware detection and support for things like OpenPGP. This enabled users to leverage the web of trust for authentication of TSL/SSL communications through the use of familiar tools, such as one's web browser or a secure shell. We were unable to find specific data on the number of users who have purchased a Freedom Box set, or downloaded the free software, but we heard anecdotally from core contributors to the project that their software had experienced fairly limited uptake.[62] The relatively low level of adoption Freedom Box has experienced is probably best attributed to nascent consumer demand for these types of products. The Freedom Box team was quite deliberate in designing their intervention around a familiar product (the router), in a way that minimized the amount of effort and technical know-how the average consumer needed to have.

Nevertheless, the Freedom Box has struggled to compete with the default freemium model of large platforms like Facebook and Amazon, whose platform services are already coupled with free data storage and identity management functionalities. This challenge is not unique to the Freedom Box project. Projects like OwnCloud and remoteStorage, as well as companies like Cozy Cloud, offer privacy-preserving cloud products and services that could support federated social media platforms, but these models for self-hosting require additional cost and effort to run, either in the form of

[62] James Vasile, interview by Chelsea Barabas, October 10, 2016, interview 1, transcript.

subscription fees or set-up costs. The limited adoption of these personal cloud solutions likely points to the lack of market demand for these kinds of services.

Even if Freedom Box were able to achieve mass adoption, the most important question for us to ask is whether or not such an intervention directly addresses any of the risks regarding control over the publication and dissemination (through discovery and filtering) of speech online. The Freedom Box project aimed to give greater autonomy and control over user publishing, by shifting from corporate owned hardware to a community ownership model for storing content. They also explicitly sought to enable users to discover and filter one another's content by supporting projects like Diaspora, which enabled a set of users to exchange information and interact within a federated framework.

In theory, Freedom Box could have lowered the barrier for users in switching over from incumbent services like Facebook to more distributed alternatives, for example by enabling the easy setup of a Diaspora account. It could have also increased user agency and the potential for interoperability, by providing the basis for a personal data store that users could use to port their data across different platforms. If, in addition, applications had adopted this data storage model, then when users wanted to switch social media platforms due to concerns over censorship or exclusion, it would be much easier to do so.

The Diaspora project was launched by a group of Moglen's students who were inspired by the potential for Freedom Box to support such a federated alternative to Facebook. Unfortunately, the project never matured to a point where it was ready to integrate into the Freedom Box package. While Diaspora's idea of an open source alternative to Facebook initially receive a lot of interest, the young leaders of the project were not prepared to manage the huge influx of volunteers and interest they received.[63] The alpha release of the Diaspora software was deeply problematic, riddled with basic

[63] "Fear of Repression Spurs Scholars and Activists to Build Alternate ...." 18 Sep. 2011, http://www.chronicle.com/article/fear-of-repression-spurs/129049. Accessed 27 Feb. 2017.

security errors in the code.[64] At the same time, the founders of the project received a lot of pressure from Silicon Valley venture capitalists to "pivot" the project to a more profitable business model. Eventually the core team fell apart and the Diaspora platform was handed over to the open source community, who has done a nice job of building out a support website to facilitate new users in signing up for the service. Today it supports just under 60,000 active participants, but the platform remains very niche and turnover of new users is high.[65]

Diaspora illustrates the challenges that open source projects face in developing tools and services that offer competitive alternatives to private social media platforms like Facebook and Twitter. These challenges are threefold: First, these projects often lack sufficient resources for development or it is difficult to coordinate those resources. In the case of Diaspora, the challenge was that it was difficult to manage the sudden influx of developer interest they received when the project was covered in the media. Most open source projects, however, face the opposite problem–they lack the resources necessary to develop a product that can compete with private platforms with enough money to hire top-notch full-time developers. The median number of developers on open source projects is one, and it remains an open question how one might bootstrap resources to fund open source projects and protocols that would enable robust peer-to-peer alternatives to private services.[66]

Second, maintaining these platforms as open, federated services slows feature development because of the effort required to coordinate multiple services and implementations. Most services like Diaspora focus primarily on federating nodes, and they manage that pretty well… on networks a tiny fraction of the size of Facebook or Twitter, In Diaspora, there are over three hundred nodes contributing to the network. The Diaspora community publishes statistics on the uptime, software version and

---

[64] "Security Lessons Learned From The Diaspora Launch | Kalzumeus ...." 23 Sep. 2010, http://www.kalzumeus.com/2010/09/22/security-lessons-learned-from-the-diaspora-launch/. Accessed 27 Feb. 2017.

[65] "Looking at the stats (http://pods.jasonrobinson.me/) for JoinDiaspo…." https://spyurk.am/posts/574601. Accessed 27 Feb. 2017.

[66] Michlmayr, Martin, and Benjamin Mako Hill. "Quality and the reliance on individuals in free software projects." *Proceedings of the 3rd Workshop on Open Source Software Engineering*. 2003.

location of each node on the network, so that new users can make an informed decision about where node to host their content. While most users tend to opt-in to one of the top three nodes on the network, there are hundreds of others around the world for them to choose from, in the event that a user wanted to switch to a different geographic location or service provider.

But the greater challenge for platforms like Diaspora is to achieve federation *across* networks. Cross-platform federation is important, because it enables individuals to speak to each other without subscribing to the same service or relying on the same codebase (and thus, the same developers). This is a critical aspect of enabling greater agency and choice for users, because it reduces the friction of switching from one platform to another. Instant messaging is an excellent example of this -- right now, if a user wants to switch to a new messaging application, then it's unlikely that they'll be able to communicate with their contacts who are using a different service. This wasn't always the case. For example, XMPP is a protocol that lets different messaging services exchange messages. Google chat used to support XMPP, but recently opted out, possibly due to the fact that most users were not using the federated features to speak with their friends across different messaging services.

Today, most open source federated projects only focus on federating with other nodes in their network, not across services, or only with the most popular social media platforms like Facebook or Twitter. This is due in large part to the fact that federated platforms bear the additional burden of coordinating across different clients, which makes it tough for them to remain agile and adaptable over time. For example, Signal, a popular encrypted messaging application, opted for a non-federated protocol, because it proved too challenging for them to respond to user demand for new features when using federated models. According to Signal's lead developer, Moxie Marlinspike, "It's undeniable that once you federate your protocol, it becomes very difficult to make changes. And right now, at the application level, things that stand still don't fare very well in a world where the ecosystem is moving.[67]

[67] "Open Whisper Systems >> Blog >> Reflections: The ecosystem is ...." 10 May. 2016, https://whispersystems.org/blog/the-ecosystem-is-moving/. Accessed 27 Feb. 2017.

As a result of these challenges, open source platforms often cannot match the usability and quality of performance of privatized platforms like Facebook and Twitter. Diaspora is certainly not alone in this struggle -- projects like Media Goblin, Identi.ca, and Buddy Cloud are all attempts by free and open source software advocates to create federated social web platforms. Groups of developers have also gotten together to develop specifications, software, libraries and apps to support a federated web experience.[68] However, these technologies have not been packaged in a way that makes them easy to use for the average end-user. This has led to a world in which there are a smattering of technically functional open source platforms that, in practice, look like a bunch of digital ghost towns. These challenges are further exacerbated by laws like the Digital Millennium Copyright Act, which have been used to stop users from aggregating data about themselves across multiple sites.[69]

The exception to this rule is Mastodon, a project begun by German software developer Eugen Rochko in October 2016 as a decentralized alternative to Twitter. Mastodon uses OStatus, an open protocol for federation of microblogging and status update services, which is also used by identi.ca, GNU Social and other distributed publishing platforms. Rochko's key innovation was around user-experience. Mastodon looks almost identical to Tweetdeck, a popular interface to Twitter initially developed by Iain Dodsworth using Twitter's API, acquired by Twitter in 2011. (Rochko told a reporter that he kept a window with Tweetdeck open in it while developing the software[70].)

With an interface familiar to advanced Twitter users, Mastodon experienced a wave of popularity in April 2017. In a single week, Quartz[71], Vice[72], Engaget[73] and Wired

---

[68] "24. Decentralizing the web by making it federated - Unhosted." https://unhosted.org/decentralize/24/Decentralizing-the-web-by-making-it-federated.html. Accessed 27 Feb. 2017.

[69] "Facebook v. Vachani - Ninth Circuit." https://cdn.ca9.uscourts.gov/datastore/opinions/2016/07/12/13-17102.pdf. Accessed 27 Feb. 2017.

[70] Sasha Lekach, "The Coder Who Built Mastodon is 24, Fiercely Independent and Doesn't Care About Money", Mashable. http://mashable.com/2017/04/06/eugen-rochko-mastodon-interview/. Accessed 17 August, 2017.

[71] Joon Ian Wong, "How to use Mastodon, the Twitter alternative that's becoming super popular", Quartz. https://qz.com/951078/the-complete-guide-to-using-mastodon-the-twitter-twtr-alternative/. Accessed 17 August, 2017.

[72] Sarah Jeong, "Mastodon Is Like Twitter Without Nazis, So Why Are We Not Using It?", Motherboard (Vice Media).

[74] wrote about the service, identifying it as an alternative and threat to Twitter. Driven by this publicity, the userbase expanded quickly, and now features between 800,000 and 1.5 million users on between 1,200 and 2,400 servers[75]. While the precise number of users changes as servers go up and down, Mastodon has been significantly more successful than any other distributed social network to date, but is still orders of magnitude smaller than successful commercial social networks.

What's particularly interesting about Mastodon is the geographic concentration of users. Three of the five largest Mastodon instances are based in Japan[76], and those three sites host roughly 60% of all Mastodon users. The users are not only concentrated geographically and linguistically - they are concentrated in terms of interest.

The largest Mastodon instance globally - pawoo.net - was set up by a Japanese company called Pixiv, and configured so that Pixiv users can easily create accounts on pawoo.net. Similar to US site DeviantArt, Pixiv invites users to share art, often art with strong sexual themes. One of the most popular categories of art on Pixiv is ロリコン - "lolicon". Short for "Lolita complex", lolicon is a form of anime imagery that portrays children in sexual situations, sometimes including explicit graphical depictions of sex. Child pornography is illegal in Japan, but lolicon, which generally features manga-style illustrations instead of photographs, is legal and common in Japan.

---

https://motherboard.vice.com/en_us/article/783akg/mastodon-is-like-twitter-without-nazis-so-why-are-we-not-using-it. Accessed 17 August, 2017.

[73] Nicole Lee, "Mastodon's Sudden Popularity Should Serve as Twitter's Wakeup Call", Engadget. https://www.engadget.com/2017/04/07/mastodons-sudden-popularity-should-serve-as-twitters-wakeup-ca/. Accessed 17 August, 2017.

[74] Margaret Rhodes, "Like Twitter But Hate The Trolls? Try Mastodon", Wired. https://www.wired.com/2017/04/like-twitter-hate-trolls-try-mastodon/. Accessed 17 August, 2017.

[75] Because Mastodon is a decentralized network, it is difficult to maintain an accurate count of users and instances. The Mastodon Network Monitoring Project offers a dashboard that tracks active instances of Mastodon at https://dashboards.mnm.social/dashboard/db/mastodon-network-overview?refresh=1h&orgId=1. Those figures can vary wildly. In the morning of August 17, 2017, the dashboard was reporting 1.48m registered users, while by that evening, it reported only 781,552. In addition, because Mastodon is open source software configurable by users, some administrators have tinkered with code to make their sites misreport user numbers. While MNM filters out the obvious fakes, it is possible that some sites are modestly misreporting their userbases to increase their prominence.

[76] https://mnm.social/, accessed August 17, 2017.

Matthew Scala, who writes about Japanese online culture, argues that growth of Mastodon in Japan is closely related to lolicon[77]. Twitter is extremely popular in Japan, but routinely censors lolicon accounts. When Pixiv made Mastodon accessible to its 20 million users, many quickly adopted the platform as a space to socialize and share imagery. A cursory glance at timelines of the other major Japanese Mastodon instances suggest that lolicon is popular in those communities as well.

This use case for Mastodon confirms our hypothesis that usability matters. Not only did Mastodon make OStatus-based distributed publishing platforms more accessible by wedding them to the familiar Tweetdeck interface, but Pixiv helped build the user base by making it easy for existing users to register for the service. The popularity of Mastodon in a subcommunity suggests another rule for adoption: existing communities may turn to decentralized solutions when they can no longer communicate due to getting barred from centralized social networks. This path to adoption may turn out to be a stumbling block for Mastodon in the long term, as stigma associated with sub-communities that adopt the tool may prove a barrier to wider adoption of the platform.

In conclusion, the projects like Mastodon, Diaspora and Freedom Box represent various generations of federated publishing. As the first prominent project in this space, Freedom Box sought to introduce better default settings for user privacy and control on the web by baking key user protections directly into hardware that all households need to purchase in order to go online–the router. In theory, this strategy offered great promise for widespread adoption by tapping into an existing consumer market for hardware. In practice however, the lackluster adoption of Freedom Box demonstrates how low levels of demand are for privacy preserving technologies that require any additional cost or effort to adopt. This makes it challenging to compete against services that offer free, seamless hosting of data generated on their platform.

In addition, projects like Diaspora illustrate the challenge of open source projects and federation as vehicles for developing better alternatives to large, private social

[77] Matthew Scala, “Mastodon WTF Timeline”, Ansuz (personal blog). http://ansuz.sooke.bc.ca/entry/335. Accessed August 17, 2017.

media sites. The coordination costs of federated protocols make it challenging for services to remain competitive in a rapidly changing market of communication applications. As this market becomes increasingly consolidated, the tendency to move away from federation becomes stronger for large companies because consumers don't seem to value interoperability with other service providers over other features. Thus, the Freedom Box model struggles to adequately address all three of our barriers to impact: user adoption, developer opt-in and business viability. These examples highlight the importance of developing foundational technologies that reduce friction and lower switch over costs, while minimizing the need for users to adopt new behaviors or take on additional costs.

The comparative success of Mastodon shows that even highly publicized decentralized social networks, which take usability seriously, will likely have challenges in scaling to the size of commercial social networks. Mastodon's growth has been in no small part due to controversial subcommunities being evicted from centralized platforms and relocating to decentralized alternatives. It is possible that Mastodon could grow significantly in the short term, but face long term barriers to growth if its key users are associated with highly controversial content.

SECTION III: OPEN PROTOCOLS

Blockstack, IPFS and Solid

As the Diaspora and Freedom Box projects illustrate, there are many challenges involved in bootstrapping a new social network. Existing mega-platforms benefit from network effects and economies of scale. Not only does a new network have to attract a user base from scratch, but it is often more expensive for the new network to provide the same services as the mega-platform: large companies like Facebook, Google, and Amazon pay less per unit of compute power and storage space because they purchase and manage it in bulk. A smaller company purchasing less of each resource would not be able to negotiate the same low prices. Moreover, the most successful model for monetization of social publishing platforms is advertising. Existing mega-platforms have huge troves of data on user behavior. New platforms start out at a competitive disadvantage to existing networks that already control the advertising space.

These challenges are exacerbated by the fact that most data is locked into silos owned by large incumbent social platforms, making it difficult for users to switch between different social networks. These silos are increasingly based on their own data models, and have their own authentication and access control mechanisms in place. This makes it challenging for developers to build services that can operate across platforms, or for users to publish and curate their own content in a way that can easily connect with audiences using other applications. The content a user publishes on Medium, for example, can be viewed and commented on only through Medium. Users can syndicate their content to other platforms, but only if both platforms allow it, or the user copies the data manually. For example, a third-party WordPress plugin allows WordPress posts to be cross-posted to Medium because both sites support the RSS syndication protocol. In today's ecosystem, self-publishing requires users to be fairly tech savvy–they might need to administrate their own servers and re-implement features that the mega-platforms provide by default, like liking and commenting. But

even if users can manage to independently publish, it does not guarantee that others will be able to easily find and consume their content.

One way of addressing these challenges is to make it easier for platforms to *authenticate* and *interoperate* on the same user data. In this section, we examine projects that attempt to make it easier for applications and users to achieve this by breaking data out of siloed management processes. Freeing user information from application silos not only puts users more in control of their data, it makes it much easier for a user to switch between applications and publish on their own in the face of censorship attempts. Ideally, users would not have to recreate all of their data and then keep multiple copies up-to-date. Rather, users could give new applications immediate access to their existing information, which could be used to reach new audiences, while supporting revenue streams for the new application.

Historically, open standards have been critical for supporting interoperability and data portability. The World Wide Web represents one of the largest, most successful implementations of shared open standards to date. The web rests on three important open standards, which serve as the backbone for its decentralized nature:

1. URIs and URLs: A system of globally unique resource identifiers and locators, such as *http://example.org* that delineate where content is found on the web. URLs enable a web page to link to any other web page in a decentralized manner. URIs provide a universal name space so that anyone can rent a domain name and create a new page.

2. HTTP: A file transport protocol which defines how messages are formatted and transmitted, and what actions web servers and browsers should take in response to various commands.

3. HTML: A common language for text markup, which enables users to format websites in a way that can be viewed in any browser, and in combination with the above, link to any site across the web.[78]

[78] Newer standards like CSS and Javascript have enabled rich, dynamic web applications, more akin to full-featured programs.

These open standards make it easier to link to and switch between web sites, because a user's browser can properly display any site in which the technical implementation follows known formats and guidelines. Because of open standards, anyone can make a website and be confident that it will work on most computers and mobile phones around the world. The concept of open protocols is what many attribute to the web becoming a "permission-less" platform for knowledge sharing. As adoption of the web took off in the 1990s, early pioneers organized to ensure that these core technologies evolved over time, through a consensus-driven global standards process run by the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C).[79]

But it seems that these fundamental building blocks for decentralized sharing on the web are necessary but insufficient for ensuring the free flow of communication online. After all, mega-platforms have developed on top of these protocols. And as these platforms have emerged, there has been a gradual erosion in the adoption of shared protocols, in favor of "native applications" built on proprietary operating systems, like Android and iOS, that provide a more responsive and adaptable experience for the end user. In recent years, there has been a surge of projects that seek to build out a new generation of open protocols to support interoperability and data sharing across platforms. Unfortunately, many of these protocols fail due to low uptake and other sociotechnical challenges of technology adoption.

In the following section, we will discuss three projects that aim to implement open protocols to reinvigorate decentralized publishing on the web. Some of these projects seek to address known deficiencies in our current paradigms for handling identity and naming online. Blockstack is implementing an alternative to the current DNS/URL naming framework. Others seek to support more decentralized paradigms for handling content storage and versioning. The Interplanetary File System is creating a new

[79] Since the early 1990's there have been many attempts to create open standards for the web beyond URLs, HTML, HTTP, CSS, and Javascript. The W3C operates on an industry membership model - companies pay a fee to contribute and participate in defining standards; as of November 28, 2016 the W3C has 422 members. Browser vendors, like Google with Chrome and Apple with Safari, then implement the standards the W3C has adopted.

transport protocol to address challenges around preserving links to content online. Solid aims to introduce a more interoperable, human-meaningful linking structure directly into the web. While none of these projects is a decentralized publishing and discovery system in its own right, the three projects are critical pieces of infrastructure that developers could use to build a robust, decentralized publishing platform.

Authentication: Naming and Identity on the Internet

Identity and naming are key aspects of publishing online, because they are what enable people who want to read a user's content to find it and verify that the content was really created by the user they intended to find, as opposed to someone pretending to be them. Verifiable identity is an important aspect of engaging with one another and consuming content online. The most prevalent way to handle identity management on the web today is by creating a new set of login credentials for each new service one wants to use. Users share, publish, and link their usernames across these services together to form a connected "identity". Most websites have their own username/password based login systems. They verify that you are really "you"–the person who originally signed up with that username–by ensuring that you know a secret only that person should know, the associated password.

It has become increasingly popular for applications to outsource this functionality to large, reputable sites like Google and Facebook, so users can use their existing Google or Facebook credentials to login to many different applications. Using Facebook or Google for authentication makes it easier for a new user to experiment with a service, as they don't have to go through the time consuming process of creating a new user identity.

However, as we discussed in the risks section, the overreliance on a single identity provider can have worrisome ripple effects. If a dominant identity provider disappeared or, perhaps more likely, if a user's account were suspended or compromised, then the user would be locked out of all other sites that depend on those

credentials for identity authentication.[80] This could make it very challenging for users to publish and consume content across the web.

Another technique for establishing identity online is public key cryptography, though this is rarely used. In this paradigm, a user has two important pieces of information -- a public key, which everyone knows, and a private key, which only the user knows, and never shares with anyone. The user can use her private key to decrypt messages encrypted with her public key, and to sign messages, by showing that she is the owner of the private key (without revealing what it is). For example, if Jane registers her public key at a well-known public key directory, like pgp.mit.edu, then anyone can verify that content she has signed was in fact created by her. It is nearly impossible for someone else to pretend to be Jane without compromising her private key, or the public key directory.

Though cryptographic keys can be generated independently and thus are entirely under the user's control, putting identity firmly in their own hands, they are not a common way for users to authenticate on the web–perhaps because it's a confusing model to users who are used to usernames and passwords, and there aren't a lot of easy-to-use public key directories that enable users to find one another based on their cryptographic identity. However, many applications use public key cryptography under the hood, without direct user involvement, like encrypted messaging systems Signal and WhatsApp. Also, more applications are being developed to make public key cryptography easier to use, like keybase.io.

There are other forms of identity, naming, and user authentication that leverage domain names, or URLs, as the basis for a user controlled identity. DNS is an important protocol on the Internet used for registering and resolving domain names: it solves the problem of resolving a human-readable name (i.e. google.com) to a specific IP address, or server location (i.e. 69.89.31.226). Users register domain names via domain name registrar through an independent multi-stakeholder organization called the Internet

[80] One of the examples we described in the first section involved someone losing access to multiple applications when she was banned from Facebook. Facebook Connect has become one of the most popular ways of logging into websites, and as such, if a user violates Facebook's terms of service, he or she could lose access to many different sites.

Corporation of Assigned Names and Numbers (ICANN), formerly under the US Department of Commerce. So if Jane wants to establish her own online identity using DNS she can pay a domain registrar like GoDaddy to register JaneDoe.com, and then use that domain as her "home" on the web. For example, Jane might keep a blog, a list of updates, a picture gallery, and her biography at janedoe.com. Similarly, a publication or aggregator could register a domain name like toptechstories.net and publish articles; by having and sharing a human-readable domain name, it is much easier for users to find them.

There are some projects that aim to help users utilize their websites as a way of creating a user-owned identity and using that to authenticate with third party websites. Once a user obtains a domain name, she can use an open protocol, such as OpenID, IndieAuth, webID, or Mozilla Personas, to authenticate her identity to another application that accepts this form of credentialing. Although this model gives users a lot of autonomy and control over their own identity (a user can put anything they want on their own website, up to what is allowed by their hosting provider; and it isn't too difficult to find alternative hosting providers), it has some weaknesses we must consider. Security is not an integral part of DNS's design; it's possible for people to spoof a domain name and redirect traffic to a different IP address. To overcome this challenge, most websites employ certificates, which are dispensed via a hierarchy of certificate authorities. [81]

A certificate authority binds cryptographic public keys to a specific domain or identity (like a person or an organization) through a process of issuing certificates (this functionality is actually similar to what a public key directory might provide, through certificate authorities often go one step further and actually verify a relationship to a real-world identity). This process enables a user's browser to verify that the website they are visiting belongs to the owner who has registered that domain, by validating the server's certificate–when you see a green lock in the browser URL bar, this means the website has a valid certificate. There are different levels of certificate validation, ranging

[81] "Evaluating web PKIs - Jiangshan Yu." http://www.jiangshanyu.com/doc/paper/PKI.pdf. Accessed 27 Feb. 2017.

from domain validation, a relatively simple validation which is granted when the requestor can prove access to the domain, usually by email, to extended validation, in which the certificate authority does more real-world validation, like showing the domain really corresponds to the company or organization it implies. There are a few large certificate authorities, like Verisign, which serve as the roots of a hierarchical structure of certificate authorities.

Previously, websites had to purchase a signed certificate from a reputable certificate authority in order to provide secure connections and work well with modern browsers. In 2016 a new, free certificate authority was released: Let's Encrypt. Let's Encrypt is a free, automated, and open certificate authority, provided by the non-profit Internet Security Research Group.[82] The project's aim is to provide an easy-to-use, automated way for any website to obtain valid certificates, supporting a more secure web. Both Chromium and Mozilla have named it as important to their plans to phase out non-secure HTTP.[8384] Let's Encrypt only offers the lowest level of certificate validation, domain validation, but it can be set up in a completely automated way and provides a viable path for all websites to upgrade to the more secure HTTPS. A major goal of the project is to be as transparent as possible; Let's Encrypt regularly publishes transparency reports and publicly logs all certificate change transactions.

The existing certificate authority system is far from perfect, and there are many calls to re-architect or replace it. Certificate authorities can get compromised and start issuing reputable certificates for disreputable servers. For example, in 2011, a Dutch certificate authority, Diginotar, was compromised and issued many fraudulent certificates for common domain names like google.com and facebook.com. This was used to snoop on the web traffic of over 300,000 users in Iran. In 2015 the certificate authority China Internet Network Information Center (CNNIC) was removed from the

---

[82] "About Let's Encrypt - Let's Encrypt - Free SSL/TLS Certificates." https://letsencrypt.org/about/. Accessed 27 Feb. 2017.
[83] "Deprecating Non-Secure HTTP | Mozilla Security Blog - The Mozilla Blog." 30 Apr. 2015, https://blog.mozilla.org/security/2015/04/30/deprecating-non-secure-http/. Accessed 27 Feb. 2017.
[84] "Marking HTTP As Non-Secure - The Chromium Projects." 11 Dec. 2014, https://www.chromium.org/Home/chromium-security/marking-http-as-non-secure. Accessed 27 Feb. 2017.

trusted certificate authority list in Google's Chrome browser due to insecure practices. Also in 2015, Symantec got in trouble with Google for issuing unauthorized certificates for Google domains.[85]

As a result of these compromises, Google has started to take more control of its own certificates: Google has become a root certificate authority itself.[86] Google Chrome is already the most popular web browser, and Android is the most popular mobile OS.[87] [88] This has serious implications for consumer privacy–technically, Google could snoop on everyone's private browsing data, or censor or spoof websites.

In order to provide more transparency, Google has developed a projected called Certificate Transparency (CT). CT is an open framework to audit and monitor digital certificates in real time.[89] CT was created to help address the problem of certificate revocation–the process of taking back certificates that are no longer valid. The problem it solves is that if any certificate authority along a chain has been compromised, all certificates issued along the chain from then on must be deemed suspicious. In order for a user's browser to find out about a compromise, ideally they would receive a notification that the certificate authority, and all certificates derived from it, should be nullified. But in practice, it is difficult to update browsers quickly, before they are attacked. CT is the first step in addressing this–anyone can run a CT server which logs and audits certificate issuance in real time. An owner of a domain can monitor the logs to verify that bad certificates aren't being issued for their domain. CT is an attempt to make a more transparent audit for changes to the certificate authority system, and probably has interesting applications in other domains where monitoring would be helpful.

---

[85] "Google Online Security Blog: Sustaining Digital Certificate Security." 28 Oct. 2015, https://security.googleblog.com/2015/10/sustaining-digital-certificate-security.html. Accessed 27 Feb. 2017.
[86] Ibid.
[87] "Browser market share - NetMarketShare." https://www.netmarketshare.com/browser-market-share.aspx. Accessed 27 Feb. 2017.
[88] "Operating system market share - NetMarketShare." https://www.netmarketshare.com/operating-system-market-share.aspx. Accessed 27 Feb. 2017.
[89] "Certificate Transparency." https://certificate-transparency.org/. Accessed 27 Feb. 2017.

Without a system like certificate authorities putting appropriate security in place, users would not be able to trust the websites they visit, and might have their credentials stolen. As we discussed before, concentrating user credentials and authentication power in a few hands is troublesome for freedom in publishing–it is a way for mega-platforms to restrict users' ability to participate in a trusted online publishing environment. But at the same time, expecting every user to manage their own security (and recover in the case of compromise) is also dangerous. In order for users to aggregate and disseminate their own content, we need an authenticated naming scheme that enables others to easily find trustworthy content. Creating an independent system for identity and naming, one that is easy to use and doesn't suffer from the same limitations as public key directories or DNS and certificate authorities, might make it feasible for users to self-publish and push their content across different applications.

Blockstack

Blockstack is an open source project whose goal is to make online naming and identity management more secure and user-centered by reimagining user credentials, DNS, certificate authorities, and public key infrastructure for the Internet. Similar to public key infrastructure systems, their goal is to provide a way for users to "own their own identity" outside of a mega-platform like Google or Facebook, giving an alternative way of verifying identity and authenticity. Using Blockstack, an author associates a public key with their username of choice, which can then be used to verify that documents associated with that name were produced by that person. The author can include any relevant identifying information as the value (like his website or profile) and then (assuming his private key isn't compromised) can make changes associated with that name in a way that cannot be forged without undermining the Bitcoin blockchain. This is done by cryptographically *signing* the hash (which serves as a unique, digital "fingerprint") of each new version of the website–the hash can be cross checked to verify its consistency with the website's latest version, and the cryptographic signature

cannot be forged unless the keys are compromised. The author gives the actual URL or website to the verifier out of band.

Blockstack is implemented as a layer for storing name/value pairs built on top of the Bitcoin blockchain, by registering Blockstack IDs. Blockstack uses Bitcoin's blockchain to act as a tamper-resistant record of ordered operations, stored in Bitcoin transactions.[90] Users issue two transactions to reserve a name–first a pre-order transaction, which obfuscates the name being reserved but proves that the user was first, and then a register transaction, which completes reserving the name and makes the registration publicly visible. This is done to avoid front running–if everyone could see the name being registered before it was confirmed, a sneaky party might try to claim it first, or might use that information to undermine the user. Both of these transactions must appear on the Bitcoin blockchain, and so might take up to an hour or longer to confirm.

Once a name is registered, the owner of the private key used to sign the transaction registering that name then has control over that name's value; the user can use their private key to make verifiable, signed changes to content, also in the form of Bitcoin transactions. For example, if Jane Doe decides to create a Blockstack username, 'jane.id', she could register that name in Blockstack, and others could see that was only done by someone with Jane's private key (presumably Jane herself). She could then change the content that username points to, for example by updating her profile. Blockstack is designed to separate the storage and agreement of operations on the name/value pairs (like create, update, or delete) from the storage of the actual data being modified and stored. Users can point to content stored in a variety of places–Dropbox, Amazon web Services, IPFS, or their own website–by signing the location of the content (the URL).

Other users can read the Bitcoin blockchain to find the Blockstack-specific transactions, and check the operations on a username to determine its final value. For

[90] Note that Blockstack is designed to be "blockchain agnostic," meaning that their protocols can be used on a variety of different blockchains. The Blockstack has chosen to build on top of Bitcoin right now, because it is the largest, most secure existing blockchain.

example, Bob might be trying to read the latest updates from Jane. He sees some information online that says that Jane stores her content on her website, JaneDoe.com, but he is not sure if this is really the Jane he is looking for. Bob knows that the Jane he is interested in has a username of ‘jane.id’ in Blockstack. He can read the Bitcoin blockchain to find the Blockstack transaction where Jane registered ‘jane.id’.

Then Bob could continue reading the Bitcoin blockchain to find the latest transaction signed with that registered public key to see where Jane stores her content, and validate that it really is JaneDoe.com by checking the signed URL. Theoretically, this could enable users to manage their own personal space on the internet for publishing–Jane can change the location of her content at any time simply by issuing a new Bitcoin transaction, and Bob can find and validate the change by reading the Bitcoin blockchain. In addition, Blockstack would also like to make their usernames usable as a single sign-on identity to login and federate user content across other platforms. The system could enable publishing competitors to more easily bootstrap new services since they could plug into existing, authenticated identities.

But for all its promise, Blockstack may face challenges in assimilating into mainstream use on the web based on our three integration criteria: user adoption, developer opt-in and business viability. User adoption is probably the most challenging area for the Blockstack community to contend with. Prior efforts to support federated identity, such as OpenID, have gained traction only with very niche user bases. At its core, the limited adoption of independent identity systems like OpenID is tied to issues of demand. The average user doesn’t see the need for secure identity and thus isn’t interested in learning more about independently controlled identity solutions in order to adopt them.

As security researchers Whitten and Tygar argue, “People do not generally sit down at their computers wanting to manage their security; rather, they want to send email, browse web pages, or download software, and they want security in place to protect them while they do those things... Designers of user interfaces for security should not assume that users will be motivated to read manuals or to go looking for

security controls that are designed to be unobtrusive."[91] Offering integration with a decentralized identity system is probably not enough of a differentiator to motivate users to put forth the effort to learn how its security tools work. When evaluating Blockstack's potential as a mass identity solution, we must ask whether or not it offers additional benefits over these prior efforts, and if it effectively addresses the usability challenges that other systems have struggled to overcome in the past. It is possible, however, that Blockstack could find itself adopted as an essential component of another, very compelling system.

The Blockstack developers have been very intentional about the design of their system in order to address these challenges. Perhaps the biggest sticking point for Blockstack's usability is related to its dependency on public key cryptography. Historically, strong cryptography has been very challenging for average users to deploy. [92] For example, work evaluating the usability of PGP, perhaps the most well-known public key directory to date, has shown that there is a lot of misunderstanding among users about how public key cryptography works and how to use it effectively.[93] This leads to serious use errors (i.e. accidently exposing secret keys) that nullify the overall security of the system. In order for the decentralized vision of the Blockstack system to work, the average user must either develop a coherent working model of how public key cryptography works, or designers must create intuitive user interfaces that enable average users to effectively manage their private keys.

In light of these challenges, the Blockstack team has made user experience design for private key management one of their top priorities. These design choices illustrate some of the important trade-offs that developers face when building decentralized systems that are also user-friendly. Technically, the most "decentralized" version of Blockstack would require users to download and validate the entire Bitcoin blockchain (currently around 120 GB) in order to validate the location of a friend's

---

[91] Whitten, Alma, and J. Doug Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." *Usenix Security*. Vol. 1999. 1999.
[92] Ibid.
[93] Ibid.

content. This is impractical, given the amount of disk space the Bitcoin blockchain takes, and the technical know-how required to independently manage one's own Blockstack and Bitcoin nodes.

Instead, Blockstack has mapped their cryptographic processes directly onto the familiar username and password procedures that users are already familiar with, and are utilizing third party providers. Today, new Blockstack users can register an identity via a registrar service like onename.com, which manages private keys for users and provides the familiar username/password login interface. Using onename.com, a user creates a password that encrypts a generated private key. The user is provided with a backup file that can be used to restore and reset their password in the event that he forgets his password.

Although the encrypted private keys are stored on Onename's servers, this configuration is arguably more secure than the traditional username/password approach, because the Onename servers do not have direct access to the private keys. The user needs to decrypt the private key before issuing any update or transfer to the account. Therefore, Onename cannot act maliciously on behalf of the user. At the same time, the Onename model suffers from some of the same security problems as the traditional username/password model -- if Jane's Onename password is compromised, for example via a phishing email, the attacker can still take over the account and make changes -- for example by creating a new website and attaching it to Jane's Blockstack ID in order to post embarrassing content.

In the future, the Blockstack developers aim to eliminate passwords from their process altogether. This could happen in a couple of different ways. First, name registrars that build on top of Blockstack could develop alternative methods for managing private keys. Second, Blockstack is working to develop a client that supports a two-factor authentication process that would require authorization from multiple devices (i.e. the user's laptop and mobile phone). Ideally, users would be able to authorize login requests with a simple click of a button, indicating their consent, without the need to remember additional information, such as a password or private key. Even if

passwords were eliminated, however, the initial setup and recovery processes of putting private keys on their devices could prove quite challenging for everyday users. Blockstack is in the process of building a browser with a built-in wallet and built-in private key management that would enable a more seamless experience upon downloading. Of course, getting people to adopt a specialized browser to use your software is far from simple–developers have long bemoaned the challenges of getting users to download the latest version of the browser they already use, much less adopt an entirely new one. The Blockstack team will need to think carefully about how they roll out an effective adoption strategy for their specialized browser. Right now, they are focusing on a "Blockstack installer," which upgrades existing browsers like Chrome and Safari, enabling users to access Blockstack from their default browsers.

The Blockstack project must also consider how to help users recover when their private keys are compromised, for example when they lose a device on which the private keys are stored. Traditional identity management providers accomplish this by providing a way for users to prove their identity, and then the identity management provider will reset their password. **In a decentralized system, there is no authority who can perform a reset.** A related decentralized identity solution in development for the Ethereum blockchain, UPort, has a scheme to do this by letting a user designate "friends" who can perform the reset for them. It remains to be seen whether this works in practice. There are many outstanding challenges–for example, if many users are compromised at once, as has happened with the Sony and Target hacks, a user may not have any friends left with available accounts to help.

The Blockstack developers are currently considering a multiple signature (aka "multi-sig") scheme for achieving this goal, whereby a selected subset of a user's family and friends would cooperate to reset one's password on their behalf. In the coming years, issues related to key recovery and compromised accounts will remain important questions, ones that Blockstack will have to thoroughly contend with if their system is ever to achieve mass adoption.

Another major challenge that Blockstack faces is that it currently does not provide a clear trust structure for users to effectively look up the person that they want to find. For example, earlier this year, developers of Bitcoin were concerned that the Bitcoin compiled code binaries were being intercepted and modified by state actors. In response to this concern, a Blockstack enthusiast encouraged Bitcoin developers to register a human-readable name and public key for the Bitcoin Core open source software project, which could then be used to verify its provenance from the appropriate source. To demonstrate this, the Blockstack enthusiast generated a key for the project, without the permission of any of the Bitcoin Core developers. Ironically, this illustrated how challenging it could be to know which Blockstack id is, in fact, representative of the person or organization one is looking for.

How does a person trying to find the Bitcoin Core project make a decision between bitcoin.id, btc.id, bitcoincore.id, bitcoin-core.id, bitcoin_core.id, and so on? Which is the "right" one, and which is a possibly malicious attacker trying to impersonate the Bitcoin developers? Currently, Blockstack does nothing to help with this problem, and in fact is arguably worse than existing systems because it relies on a much larger trusted code base. The Bitcoin example illustrates how difficult it is to determine what name corresponds to what real-world entity you are trying to find.[94]

In contrast, the existing domain name system at least has legal recourse for cybersquatters, people who obtain domain names in the hopes of selling them to the companies most closely associated with them:

> *"The Anticybersquatting Consumer Protection Act of 1999 authorizes a cybersquatting victim to file a federal lawsuit to regain a domain name or sue for financial compensation. Under the act, registering, selling or using a domain name with the intent to profit from someone else's good name is considered cybersquatting. Victims can also use the provisions of the Uniform Domain Name Dispute Resolution Policy adopted by ICANN,*

[94] "Securing Bitcoin Core releases with Blockstack, a ... - Reddit." 19 Aug. 2016, https://www.reddit.com/r/Bitcoin/comments/4yhhe1/securing_bitcoin_core_releases_with_blockstack_a/. Accessed 27 Feb. 2017.

an international tribunal administering domain names. This international policy results in arbitration of the dispute, not litigation."[95]

A completely disintermediated naming system would offer no recourse for trademark infringement, because there would be no legal entity (or entities) which could apply the law.

To mitigate this challenge, the Blockstack team says, users can link third party attestations to their Blockstack profile. This could include a statement from one's bank or social media account to add additional information that might make it easier for third parties to discern between similar sounding id names. Another company, Keybase.io, is already providing this type of service. Using Keybase, a user can attest to owning usernames on different platforms and social networks, such as Reddit, Twitter, and Github, and other users can verify them. Blockstack has been in the process of implementing a similar strategy since 2014.

Blockstack will have to effectively address these challenges in order to become a viable identity solution for more than just a small group of tech-savvy crypto-enthusiasts. If they are able to make a comprehensive user-friendly experience, then Blockstack could serve as a compelling alternative to the existing DNS and certificate authority systems we describe above. If adopted into the mainstream, systems like Blockstack or Keybase.io could support a more tamper-proof identity system, one that is difficult to censor because it is rooted in the Bitcoin blockchain.

Today Blockstack supports over 4,000 contributing members in its open source community and has registered over 70,000 domain names.[96] The open source code is maintained by Blockstack Inc., a company which recently announced that it raised $4 million in funding from venture capital firms like Union Square Ventures and the Digital Currency Group. It will be interesting to see how this organizational structure will shape Blockstack's prospects of adoption as an open standard.

---

[95] "Is it infringement if someone buys a URL with my company's trademark ...." http://www.nolo.com/legal-encyclopedia/question-url-trademark-infringement-28100.html. Accessed 27 Feb. 2017.

[96] "Funding the New Decentralized Internet - Blockstack." https://blockstack.org/blog/funding-the-new-decentralized-internet. Accessed 27 Feb. 2017.

On the one hand, standards put forth by for-profit entities can struggle to succeed due to distrust among other industry players, and conflicts of interest between the for-profit entity and the needs of other players in the ecosystem. On the other hand, some of most successful open standards to date have resulted from broad industry coalitions between tech companies. In 2016 Microsoft announced a formal partnership with Blockstack Inc., as part of their effort to develop open source infrastructure that supports "self-sovereign" identity, which "provides a platform to developers for building decentralized, server-less apps."[97] In the coming years it will be interesting to see how other big industry players embrace this vision of the future, and the open source software necessary to make it possible.

Finally, we must ask ourselves whether or not decentralizing this aspect of the web is necessary for dealing with issues of free speech online. While tampering and censorship are important issues for a small subset of online writers, most users are not explicitly censored by government actors via the DNS or certificate authority systems. Wikileaks, for example, found itself dropped by its DNS provider, EasyDNS, as part of the "blockade" against the site in 2010.[98] But a wide range of users have experienced censorship via exclusion from major platforms like Facebook and Twitter. Blockstack could provide a critical piece of infrastructure for those who wish to securely publish their own content independently of major publishing sites like Facebook, but only in combination with other pieces.

Interoperability: Developing shared data models

Today most applications manage their own data, and have their own processes for handling authentication and access controls to their databases. As a result, it is challenging for users to switch between services that operate on similar content, or to migrate their data from one service to another. Moreover, application developers cannot

[97] "Blockstack Core v14 - Microsoft Azure." https://azure.microsoft.com/en-us/marketplace/partners/blockstack/blockstack-core-v14/. Accessed 27 Feb. 2017.
[98] "PayPal Freezes WikiLeaks Account | WIRED." 4 Dec. 2010, https://www.wired.com/2010/12/paypal-wikileaks/. Accessed 27 Feb. 2017.

easily build services that draw from a variety of data sources, because they are restricted to the information made accessible through specific platform Application Programming Interfaces (APIs). These proprietary APIs tend to operate on diverse data formats and closed protocols, which makes it challenging to repurpose data that is generated on a specific platform, creating a siloed effect. For example, Facebook stores the social profile data and interactions of its 1.7 billion users on its servers, and it isn't available in a format users can export to another application, like Google Plus, Diaspora or Ello. Furthermore, platforms constrain access to their APIs, limiting the number of times per day they can be used, making it very difficult to maintain a social network using another company's API.

This trend towards private data silos contributes to many of the risks to online speech we outline in this report. First, it makes it easy for governments to censor content, because they can pressure the corporations that house that content on their servers to comply with takedown requests. Even if users proactively replicate content that they fear might be taken down from a major platform like Facebook, there is no clear method for redirecting others to where that information is newly housed. For example, when the Thai government pressured Facebook to take down a satirical page from its site, the political commentators who ran the page had no clear methods for pointing their audience to an alternative location where that content could be found.

More decentralized methods of data storage could make it difficult, if not practically impossible, for a single entity to censor content. For example, peer-to-peer file sharing services like Gnutella, Limewire, and Bittorrent made it almost impossible for the Recording Industry Association of America to stop the spread of illegal music downloads. In the following sections we will take a look at the InterPlanetary File System (IPFS), a project which aims to enable users to find content even if a specific website owner decides to take it down, or they opt to migrate it over to a new location (i.e. a different URL), and Solid, a framework for building applications which puts users in control of their data.

Data silos create lock-in effects, which make it challenging for users to switch between platforms or self-publish if they are excluded or unhappy with mainstream platforms, like Facebook or Twitter. Both IPFS and Solid have the potential to enable a more vibrant landscape of publishing options by supporting shared protocols and formats for handling data across applications. While these projects are not decentralized publishing platforms in and of themselves, they could serve as critical building blocks for more decentralized and interoperable publishing applications to be built.

Inter-Planetary File System

The Inter-Planetary File System (IPFS) is an open source project that aims to enable peer-to-peer methods for storing and disseminating information on the web. The goal of this project is to give users the ability to publish online without having to trust a single third party server to host their content. Instead, IPFS provides a verifiable means of retrieving content from a distributed network of storage providers. IPFS's main insight is to use hashing functions to point to content, instead of using the IP address of a server where the content is housed. A hashing function is a function that can be used to map a data file of any size to an output of a fixed size, usually in the form of a series of random letters and numbers. The hash produced by a file can serve as a unique fingerprint of that information–for any given file, the hash generated will always produce the same unique value. Conversely, if any aspect of the file is modified, the hash value will change.

The IPFS system uses the hash of a file as its pointer, effectively decoupling the physical server that hosts the content from the address that points to where that content can be found. It does this by storing files in a distributed hash table (DHT). A distributed hash table is a distributed system in which the responsibility of maintaining the mapping from key to value is distributed over all nodes in the system. A DHT replicates data, and can tolerate nodes entering and leaving the system. Clients are assured of the integrity of the data they are receiving by checking the hash of the file they are looking for.

Therefore anyone can easily copy and serve content, making it harder to take that content down, and potentially improving latency by making files accessible in multiple places. IPFS stands in contrast to the way content is currently discovered online today, using URLs and HTTP links to identify a specific server host, where that content lives.

If IPFS were to gain mainstream adoption, it would make content more resilient in contexts where Internet connectivity is weak, or censorship threats are high. IPFS is essentially a distributed file system with a simple protocol that enables easy finding, caching, and serving of files. If those files are appropriately replicated across the network, they could tolerate outages more easily than today's web. The developers on the IPFS project imagine their system could serve as the backbone for a peer-to-peer file sharing network, whereby information is exchanged locally via a mesh-like network. In this way, important digital content could be disseminated, even if access to the Internet is cut off or platforms are pressured to take down specific content.[99]

Not only might IPFS make content more resilient, but it could also enable a more competitive landscape for publishing platforms in the future. Agreeing upon a peer-to-peer protocol and a way for storing and retrieving content is one way we could enable more sharing between applications, as we saw with the web, and thus lower the barrier for a more diverse social media landscape. If combined with a shared common data format, IPFS might reduce switching costs between applications. Many different services could use the same data, thus eliminating the need for the user to replicate the same information, such as their social graph, photos, prior posts, and interaction history each time they sign up for a new service. If it's easier for users to switch between related platforms, then it makes it easier for new services to bootstrap a network, ultimately providing more choices in the market.

As of now, the project has two implementations, in Go and Javascript. The Javascript implementation enables IPFS to run in today's browsers, which significantly lowers barriers to use. Moreover, the IPFS community has worked hard over the last

[99] "Africa|African Nations Increasingly Silence Internet to Stem Protests." 10 Feb. 2017, https://www.nytimes.com/2017/02/10/world/africa/african-nations-increasingly-silence-internet-to-stem-protests.html. Accessed 27 Feb. 2017.

year to support dynamic content that can run via a local area network, without having to connect to the backbone of the Internet. To demonstrate this new capability, they have built a p2p chat client called Orbit, which users can experiment with today.

IPFS has become a favorite amongst decentralized web advocates, and many decentralized social media projects have indicated a desire to integrate their platforms with the project in recent months. Decentralized social network projects like Steemit, Backfeed and Akasha have expressed intentions to eventually integrate with IPFS, because they believe it will help make the content generated on their platforms more resilient to censorship and open to others to use.[100] IPFS is a core aspect of these projects' strategies for providing a "decentralized" social networking service. In contrast to other publishing platforms like Facebook or Twitter, these social media platforms would prefer to build their applications on top of a distributed data layer supported by IPFS, rather than a private cloud infrastructure that they are responsible for maintaining.

In many ways, the IPFS team is trying to make it as easy as possible for developers to opt-in to using their system. Flexibility is a first order goal with IPFS; the developers have written the system in such a way that different protocols can be substituted in and out whenever desired. They have developed a set of multi-formats, which are a set of "self-describing" protocols that the IPFS community is hoping to enter into the process for standardization at the IETF in the near future. For example, the hashes of files are stored as multi-hashes, which delineate the specific function used to derive the hash itself. In this way, IPFS strives to achieve a data format that is not over specified and is "self-describing": the address of the content contains all the information necessary to process it.

It's like writing an address on an envelope, along with instructions for how to read and understand the format of the address. Rather than trying to get everyone to conform to the same addressing conventions in IPFS, one simply needs to explain how each addressing format is structured. This makes it easier for applications to switch

[100] This enthusiasm is not limited to social media platforms. Juan Benet reports that wide range of decentralized applications related to identity, asset exchange, music sharing, supply chain are also actively building on top of IPFS.

between hash functions in the future, or for different applications to use different hash functions and still work together. In this way, IPFS seeks to provide a dynamic and flexible system that can accommodate the preferences and needs of a variety of stakeholders.

With regard to user adoption, the project's founder and chief architect, Juan Benet, says that their aim is to integrate IPFS seamlessly into the stack of the web, without individual users having to consciously opt-in to it.[101] However, users play an integral role in the functioning of the IPFS system. In early writings about the system, it is assumed that participants will contribute excess storage and computational capacity on their personal machines, to replicate and serve content for the network, much as existing users provide capacity to the BitTorrent network. However, it's unclear how many people will actually participate in the network in this way.

Historically, peer-to-peer networks have struggled with the freeloader problem, whereby users consume resources without contributing anything in return. The design of early peer-to-peer systems assumed altruism would serve as a substantial driver for participation in the network. Yet, prior efforts have demonstrated that it becomes increasingly challenging to prevent freeloader behavior as networks scale.[102] Researchers have developed a variety of strategies to address this problem, based on monitoring node behavior and creating incentives for contributions to peer-to-peer systems.

In the original IPFS white paper, Benet discussed plans to implement a protocol to address these issues as well, via a BitTorrent inspired protocol called BitSwap.[103] With BitSwap, peers in the IPFS network would look to acquire a set of blocks, while also broadcasting a set of blocks to offer in exchange. In its initial implementation,

---

[101] "IPFS and Ethereum: Projects, Important News, Demos, and ... - YouTube." 27 Oct. 2016, https://www.youtube.com/watch?v=ltb_2EMgBUI. Accessed 27 Feb. 2017.
[102] Blanc, Alberto, Yi-Kai Liu, and Amin Vahdat. "Designing incentives for peer-to-peer routing." *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*. Vol. 1. IEEE, 2005.
[103] "IPFS - Content Addressed, Versioned, P2P File System (DRAFT 3)." https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf. Accessed 27 Feb. 2017.

nodes could swap blocks on a one-to-one basis. However, this system depends on peers being able to find a counterpart that has a block they are willing to exchange for one of theirs, in a barter-like fashion.

Benet envisioned a more sophisticated version of BitSwap emerging in the form of a marketplace, where block transfer is tracked and remunerated in the form of a currency that can be exchanged for bandwidth to download blocks from the network. A variety of different strategies could be implemented via the BitSwap protocol to optimize for different performance outcomes, such as preventing freeloaders from entering the system or maximizing the frequency of trades in the market place.[104]

The most current instantiation of this strategy is a blockchain-based currency layer called Filecoin[105]. As Benet explains, ""Filecoin is a blockchain protocol designed to do for storage what Bitcoin did for hashing."[106] By this he means that the goal of Filecoin is to incentivize contributions of valuable resources (in the case of Filecoin, storage space and bandwidth) to the network. In Bitcoin, individuals are incentivized to contribute storage space for blocks of transactions and the computational hashing power necessary to secure the network.

According to Benet, today the Bitcoin network consumes more computational power than the world's top five hundred supercomputers combined, at around 2,500,000 terahashes per second.[107] The Bitcoin network has garnered this remarkable amount of resources thanks to the effective implementation of a token-based incentive system, whereby contributors to the network are remunerated with Bitcoin tokens, which can be exchanged for other forms of money. Similarly, the goal of Filecoin is to enable a marketplace that supports incentivized contributions of storage space and the distribution of files, at a comparable scale.

---

[104] Discussed in section 3.4.2 of the IPFS paper: https://arxiv.org/pdf/1407.3561v1.pdf
[105] "Filecoin: A Decentralized Storage Network." Protocol Labs. https://filecoin.io/filecoin.pdf. Accessed 14 Aug. 2017.
[106] "IPFS and Ethereum: Projects, Important News, Demos, and ... - YouTube." 27 Oct. 2016, https://www.youtube.com/watch?v=Itb_2EMgBUI. Accessed 27 Feb. 2017.
[107] "Hash Rate - Blockchain.info." https://blockchain.info/charts/hash-rate. Accessed 27 Feb. 2017.

With Filecoin, individuals can rent space on their hard drive to store other users' data and receive Filecoin tokens in return. Users can then buy Filecoin and spend it to hire nodes to store their data across the network. The Filecoin paper describes two *proof-of-storage* schemes: One called *proof-of-retrievability*, which is used to prove that a copy of a piece of data is stored on physically independent storage, and another called *proof-of-spacetime*, which a storage provider uses to prove that they have stored a copy of a piece of data throughout a specified period of time. Filecoin uses these proofs to construct a blockchain-based verifiable market where users can issue and fulfill storage and retrieval requests; this serves to create a decentralized exchange for storage orders. Miners participate in Filecoin by storing this data, producing proofs, and earn Filecoin tokens in return.

Filecoin supports file contracts and smart contracts. The promise of smart contracts for Filecoin is that they could support sophisticated data storage needs, such as defining parameters for who holds certain types of data (i.e. according to reputation thresholds or geopolitical boundaries), and creating different types of payment strategies. These needs would be delineated in smart contracts, which would be used to connect data providers with storage providers on the network. Work on Filecoin is in early stages, and the details of how this will be effectively implemented have not yet been hashed out. Protocol Labs, the creators of IPFS and Filecoin, did a pre-sale of Filecoin tokens on August 10, 2017, and raised over $200M in less than an hour.[108] This money is intended to be used to hire developers and researchers to fully implement the Filecoin protocol.

Work on Filecoin marks a significant shift in thinking for the IPFS project. Rather than relying on average consumer grade hardware to support the network, Benet has expressed hopes that the Filecoin will help mature the network to a point where those who sell storage do so at a professional level, with industrial grade operations.[109] This evolution runs in parallel to the way that mining in Bitcoin has developed over the last

[108] https://www.coindesk.com/200-million-60-minutes-filecoin-ico-rockets-record-amid-tech-issues/
[109] "IPFS and Ethereum: Projects, Important News, Demos, and ... - YouTube." 27 Oct. 2016, https://www.youtube.com/watch?v=Itb_2EMgBUI. Accessed 28 Feb. 2017.

eight years. In the early days of Bitcoin, mining was carried out on personal computers run by hobbyists. But over the years, mining has become an increasingly specialized activity, one that requires significant investment in specialized hardware and secure facilities with cheap access to energy.[110]

This consolidation of the network has raised questions about how decentralized Bitcoin actually is–if only a small group of professionals run the mining operations that are responsible for keeping the network safe, then can we really call it decentralized, or have we just shifted the power from one set of players (i.e. banks) to another (i.e. Bitcoin miners). Similarly, if IPFS is to achieve storage capacity on par with Amazon S3, it is likely to look more like a network of oligarchs, rather than a purely decentralized network of peers. One might argue that Filecoin and IPFS at least lay a foundation for a more dynamic market of storage providers–we can more intentionally set parameters that are continuously being monitored on the network in order to shift from one storage provider to another. But until Filecoin becomes more concrete, thoughts on the disintermediating potential of IPFS remain largely speculative.

Another open question for IPFS is how, as an open network, it will be resilient to spam. The concept of a Sybil attack–one where attackers overwhelm the system by consuming too many resources–is a key challenge in open systems. For example, in IPFS, an attacker might be able to target a specific piece of content and keep it from being served by overwhelming the server on which it is stored. Attackers could also join the network and flood it with incorrect routing suggestions, essentially rendering it unusable.

Bitcoin addresses this issue through its proof-of-work function, which gates entry into the system and incentivizes participants to validate transactions when mining. Filecoin intends to use a similar approach, called proof-of-retrievability. However, deploying proof-of-retrievability as an incentive mechanism is as yet a completely unstudied area. The authors of Filecoin will have to design a sophisticated incentive mechanism which encourages users to act in a benevolent manner and store files for

[110] DuPont, Quinn. "The politics of cryptography: Bitcoin and the ordering machines." *Journal of Peer Production* 1.4 (2014).

others. Even if they achieve this, the system could still be used for unsavory activity, like serving child porn or supporting ransomware,[111] especially as the challenges of deleting files in a distributed network are especially appealing to those distributing illegal content.

Moreover, with regard to adoption, IPFS faces some serious performance challenges which might impact developers' decisions to build on top of the it. Content on the web is often very dynamic. Managing content updates is a fairly trivial task when the data storage and dissemination is coordinated from a central point of control. However, this becomes much more challenging in a distributed setting, when updates must propagate across the network.

IPFS handles changing content by using versioning and a process they call the Inter-Planetary Naming System (IPNS). With IPNS, users can establish an unchanging pointer to content that is frequently updated, such as one's news feed on Facebook or Twitter. If the network is spread out and diverse, there could be delays in propagating the IPNS changes, meaning users will frequently see stale content. Particularly for social media platforms, this poses a significant challenge because content is frequently updated, requiring rapid propagation through the network. For developers who want to optimize for latency, it's unclear why they would opt to build on top of IPFS, other than for ideological reasons.

Theoretically, IPFS would make it easier for users to port their data between applications, without having to recreate it all over again. If implemented in such a way, an alternative to Facebook, for example, could operate on the same IPFS files that Facebook itself would use. This is true in so far as the raw data is now freed from specific proprietary silos, and under the control of the user. In the IPFS system, content is addressed by hash, which can be used to ensure that the data can be found even as it moves across different servers. But just because applications can find the data via its hash doesn't mean that that data will be organized in a format an application can understand.

---

[111] "New Darknet Wants To Match-Up Cypherpunks In Crypto Utopia ...." 31 Jul. 2012, https://techcrunch.com/2012/07/31/new-darknet-wants-to-match-up-cypherpunks-in-crypto-utopia/. Accessed 28 Feb. 2017.

Without a common data format, users data will still be siloed in IPFS by application, because different applications won't be able to read each other's data format. The designers of IPFS have anticipated this problem and proposed a standard called IPLD (Inter-Planetary Linked Data), which is simply a graph of data linking to each other via cryptographic links. But establishing a common data format is very challenging and many efforts in past that have tried to do this have failed. In the following section we will take a look at a project that attempts to provide a comprehensive framework for achieving interoperability on shared data on the web.

Solid

Solid (short for Social Linked Data) is a new project that attempts to extend ideas around open standards to create a platform for building decentralized social applications with linked data.[112] At the heart of this work is an effort to develop a foundation for using shared data schemas, in order to support multiple applications built on the same data. This project is led by Tim Berners Lee, as a collaboration with members of the World Wide Web Consortium and his research group based at the MIT Computer Science and Artificial Intelligence Lab. The goal of Solid is to support a high degree of interoperability between applications, as well as to enable greater portability of data between servers. The Solid team aims to do this by developing a standard API that makes it easy for developers to write applications that allow users to use the same data in different applications instead of leaving it locked inside different application data repositories.

This project combines aspects of both Blockstack (decentralized identity management and authentication)[113] and IPFS (decentralized data storage)[114], while also

[112] Solid is part of the larger parent project CrossCloud.

[113] In order for a variety of applications to identify the same user across platforms, and to share user data, Solid requires a decentralized mechanism for handling authentication and user logins. Currently, the project plans to achieve this with webID, an open protocol for registering a unique ID in a global namespace, web URLs. The webID protocol is being developed in a community group within the W3C to support a standard where people, companies, and organizations are uniquely identified by a URI. WebID is very closely related to OpenID; the important difference between webID and Blockstack is that in Blockstack, all user identifiers are kept in one place, the Bitcoin blockchain; Blockstack could potentially be used as as an identity provider in Solid. In Solid, a user registers with an identity provider (most likely their pod provider), who would then store a webID profile associated with a public key pair. Users can then use their webID credentials to sign into different services and be discoverable to others.

working hard to develop the “glue” that ties these pieces together through shared standards for access control and a standardized data schema. Ultimately, the goal of this project is to render platforms like Facebook and Twitter as merely “front-end” services that present a user’s data, rather than silos for millions of people’s personal data. To this end, Solid aims to support users in controlling their own personal online datastore, or “pod,” where their personal information resides. Applications would generally run on the client-side (browser or mobile phone) and access data in pods via APIs based on HTTP.[115]

The data stored within pods are structured according to the Resource Description Framework (RDF), an open and extensible data format which is a simple knowledge representation language that links different data schemas together. Today, URLs don’t include much information about the types of resources to which they are linking. RDF extends URL linking on the web to include a third element, the relationship between the two resources being linked, and supports the evolution of data schemas over time.[116] For example, a developer might create a simple calendar application which records events at certain times. Later, she might want to add a feature to include a location for events, effectively extending the data schema, and linking events to a new resource location. Other applications (i.e. a social app that delivers notifications when your friends are in the same neighborhood as you) could then operate on this same time/location data. RDF was designed to produce a machine-readable web of knowledge for data portability. Social standards like FOAF (Friend of a Friend) grew out of RDF.

Ideally, RDF would serve as a neutral, flexible, extensible schema that lets disparate applications work together on the same data. This would make it possible for Solid pods to be application agnostic, enabling the development of a variety of applications without the need to modify the underlying server. Pods can offer optional

---

[114] Solid aims to decentralized storage by supporting a pod model, whereby users store their data in “pods” that they control, rather than proprietary platform serve

[115] Data is manipulated through HTTP requests to the specific URI of each data item stored in a user’s pod.

[116] "RDF - Semantic Web Standards - W3C." https://www.w3.org/RDF/. Accessed 28 Feb. 2017.

support for SPARQL, a language used to provide more complex data retrieval queries, including queries that require following links between different applications or servers.[117] For example, applications that require more sophisticated querying, like finding status updates amongst a user's friends-of-friends, would create a SPARQL request to query all the different users' pods. SPARQL is critical for supporting rich, dynamic applications. Most of the data in the example applications the Solid developers have created is stored using various existing standards, like vCards for user contacts.[118]

Solid's success hinges on whether or not developers pick up these tools and write their applications to leverage the Solid specification. The Solid team has worked hard to provide libraries, different pod server implementations, and example applications to support easy development on their platform.[119] Their hope is that they can accelerate adoption by continuously growing the set of libraries and components that work in the Solid ecosystem. If this happens, it could create a virtuous cycle, in which developers opt for Solid's open frameworks, which in turn promotes more pod implementations and increased user awareness. Like the World Wide web, Solid might succeed where other systems have failed because it is non-proprietary, meaning that anyone could implement its protocols without paying fees.

However, it is uncertain whether or not developers will adopt these new standards. On the one hand, the web and its underlying protocols have been extraordinarily successful. The W3C, the standards body responsible for developing and supporting these protocols, has been instrumental in coordinating companies and browser vendors to implement new standards. On the other hand, this process is laborious and sometimes riddled with conflict. The W3C has not seen widespread adoption of its more sophisticated standards and protocols, particularly around the

---

[117] "A Demonstration of the Solid Platform for Social Web ... - Crosscloud." http://crosscloud.org/2016/www-mansour-pdf.pdf. Accessed 28 Feb. 2017.
[118] "vCard Ontology - for describing People and Organizations - W3C." 22 May 2014, https://www.w3.org/TR/vcard-rdf/. Accessed 28 Feb. 2017.
[119] For example, all the applications that they have developed use the rdflib.js library (the core library from Tabulator) to handle RDF resources. Another library is solid.js10, which simplifies the development of Solid applications by abstracting some of the more complex operations. They have also provided modules for authentication and signup that are designed for reuse as web Components.

Semantic web, Tim Berners Lee's vision for a web where data is structured and tagged in a machine-readable way. The reasons for this are complex -- sometimes, there isn't broad consensus about standards, and things die in committee. Other times, standards turn out not to be as useful as their creators thought and they don't get adopted broadly.[120]

If a standard requires many different parties to agree on semantics and the meaning of metadata, it is likely to get mired in endless debate. As is with federation, when a group of people and organizations must come together to debate and make changes, it slows development as compared to a single organization developing its own standard. A single organization with a unified purpose can move with greater speed.

One aspect of successful open protocols and standards is how well-specified they are. Protocols that try to specify every possible use case can be difficult to adopt because application developers need to read and understand complex specifications to use them at all. For example, XMPP core was a successful messaging protocol, but its extensible components were not widely adopted (and as a result XMPP is not widely used today). These extensible components required developers to read hundreds of pages of specification documents in order to implement them properly. In contrast, consider OAuth, a protocol for using one application's login credentials to securely access another application, without revealing any passwords. OAuth has been implemented widely across the web and is widely considered one of the most successful open protocols to date.

Part of the reason for the success of OAuth is its simplicity. In some ways OAuth is *underspecified*, and thus the application developers using it can tailor it to their needs without having to read a myriad of complex specifications. Another reason for the success of OAuth is that it is useful even if only implemented by a subset of applications: being able to use my Twitter credentials to access a new application is helpful, even if it doesn't work with *all* new applications. This benefits Twitter because it improves the spread of its service, it benefits the new application because the

[120] "Why Standards Fail - Zeldman on Web & Interaction Design." 24 Jul. 2009, http://www.zeldman.com/2009/07/24/why-standards-fail/. Accessed 28 Feb. 2017.

application developers do not have to implement a whole new user account system or ask users for their Twitter passwords, and it benefits the user because she does not have to create and remember yet another username and password for this new application.

Developing successful open standards and protocols is not just about their technical implementation, it is also about the social community surrounding them. It's important to define a good process for who controls the standard and how changes achieve adoption. Sometimes standards don't get adopted if they are viewed as "belonging" to one person or organization. Solid is being developed within academia, where there is presumably no commercial interest. But at the same time, the most successful protocols, like OAuth, are the by-product of a broad coalition of industry players. Critics of Solid might argue that the project is too far removed from industry practice, outside of an environment that must contend with the practical needs of real users and real applications.

In particular, Solid's decision to embrace RDF as its data format might pose a serious barrier to adoption. The initial draft of RDF was written in 1997 and, in spite of much work and effort to evolve the protocol over time, it has not experienced much uptake in the developer community. Developers who have worked in the open standards community for a number of years attribute this in large part to the fact that RDF is a fairly complex protocol.[121] Most web developers today do not write applications using RDF -- instead, they store their data using SQL or a simple key/value data format. In order to use Solid at all, application developers will have to port these SQL and key/value application databases into RDF, and will have to learn how to manage RDF and graph databases. Solid's success likely depends on developers embracing RDF and ontologies, something that hasn't happened to date. As we have discussed before, it is difficult to get both users and developers to adopt protocols simply due to ideology, and RDF is a deeply ideological protocol, the centerpiece of a vision from the web's creator that is far from universally shared.

---

[121] "Blaine Cook Live Stream - YouTube." 4 Aug. 2016, https://www.youtube.com/watch?v=TwYOTygZnQ4. Accessed 28 Feb. 2017.

Adoption seems even more unlikely given the growing trend towards native mobile applications, rather than browser-based interfaces. With the advent of mobile, developers are moving beyond the web and HTML in favor of building "native" applications, which can run faster and be more responsive on mobile hardware. Mobile application developers build to operate on two major mobile platform operating systems and APIs -- Google's Android and Apple's iOS. It's unclear how Solid might integrate with these platforms, though if it could, that would be very powerful for gaining developer adoption. In an effort to gain wider use, the Solid team might consider dropping the requirement for RDF and letting developers use their own data models.

The approach of Solid towards promoting interoperability and platform-switching is admirable, but it begs the question: why would the incumbent "winners" of our current system, the Facebooks and Twitters of the world, ever opt to switch to this model of interacting with their users? Doing so threatens the business model of these companies, which rely on uniquely collecting and monetizing user data. As such, this open, interoperable model is unlikely to gain traction with already successful large platforms. While a site like Facebook might share content a user has created–especially if required to do so by legislation that mandates interoperability–it is harder to imagine them sharing data they have collected on a user, her tastes and online behaviors. Without this data, likely useful for ad targeting, the large platforms may be at an insurmountable advantage in the contemporary advertising ecosystem.

Solid might be more appealing to new companies who want to break into a market with large players, but in order to facilitate this, it must both solve the issue that there isn't already an established user base and help developers find a new business model for sustainability. In order for Solid to succeed, we'd have to see a fundamental shift in the economics of the web, from business models that are based on the capture and lock-in of consumer data to something else. This is a common critique of other efforts that try to enable consumer control over data for the sake of increased choice and user agency.[122] This goes to show that in addition to open standards and protocols,

[122] For example, Doc Searle's VRM project tries to fundamentally change the paradigm for vendor-consumer relations to one that is more empowering for the end-user. However, it requires data

we should be thinking about new forms of monetization to pair with this user-controlled data model.

rich companies to cede control of customer transaction data. This data is worth billions of dollars, and it has proven very challenging to find corporate partners who are willing to give up the immense power and revenue potential that comes from that data. More info here: https://blog.p2pfoundation.net/is-vendor-relationship-management-doomed-to-fail/2009/02/16

SECTION IV

Collective Ownership with Appcoins

Over the last few years there has been a wave of projects that have focused on new strategies for fostering collective ownership models for open networks. Central to these new projects are strategies for minting and distributing scarce digital tokens that incentivize individuals and groups to contribute resources (both material and behavioral) in order to bootstrap networks where each looks more like a public commons and less like a business. Many of these projects are inspired by cypherpunk notions of decentralization, whereby a distributed group of people operating a shared protocol is able to handle complex cooperative processes without the need of a traditional business model to coordinate the pieces. These types of cooperative organizations/programs are sometimes referred to as decentralized autonomous organizations, or “DAO”s.

Bitcoin is perhaps the most concrete example of what this looks like in practice. Bitcoin enables the coordination of computational resources in order to carry out a complex process of secure value transmission and storage. This happens in the context of an open network that anyone can join and contribute to, rather than under the purview of a traditional business (i.e. a bank). Bitcoin has renewed interest in thinking more broadly about ways of designing shared digital goods that are collectively owned and managed, rather than privately owned and operated. Central to this new model of networked organization is the concept of Appcoins.[123]

Appcoins are scarce digital tokens that, like Bitcoin, can be distributed to participants in a network in order to incentivize them to contribute to the collective maintenance and use of the network. For example, in Bitcoin, coins are created as an incentive for users to validate and contribute hash power to the network, and thus make

[123] Many token projects choose to run a forked version of Bitcoin with alternative consensus rules, and—therefore—an alternative blockchain, these projects will effectively be running a new cryptocurrency. The new blockchain will account for holdings of a new scarce token often called an “alt-coin.” Some notable examples of alt-coins include Litecoin, Dogecoin, and Filecoin.

the blockchain harder to manipulate. As demand to use the network grows, so does the value of the Appcoin, which can further fuel the growth and evolution of the network over time. Appcoin enthusiasts argue that this approach, enabled by blockchain technology, could offer a new way of thinking about funding open source software projects that support novel forms of cooperative organization online.[124] As Van Valkenburgh of Coin Center explains, Appcoin developers "seek to create a digital platform that generates some kind of cooperative result but does so without utilizing any form of hierarchical or top-down control. The design goal is broad: complex cooperative organization with a network protocol supplanting all traditional legal or business structures."

Appcoins are specifically useful for funding the development of protocols that enable new forms of cooperation at scale–ones that could significantly change the way we think about sustainable business models for the web. According to founder of Coinbase Fred Ehrsam, "Instead of a central company making money by owning and extracting rent from the network they created, a software protocol replaces the central operator, and all of the creators and contributors to the network mutually own it. Contributors to networks look less like worker bees and more like mutual owners in the network they are creating value in." Trebor Scholz, a major proponent of the platform cooperativism movement,[125] urges users to think of themselves as unpaid laborers building wealth for platform owners–Appcoins offer a mechanism through which the profits from that currently unpaid labor could be shared with those who create online work.

---

[124] The term "blockchain" is used to refer to a wide range of technologies, with varying degrees of centralized decision-making control. In the context of Appcoins, a blockchain is often described as having the following characteristics, explained by de Filippi and Wright (2015): "The blockchain is a distributed, shared, encrypted database that serves as an irreversible and incorruptible public repository of information. It enables, for the first time, unrelated people to reach consensus on the occurrence of a particular transaction or event without the need for a controlling authority."

[125] Platform cooperativism is a social movement which emphasizes the importance of democratic governance and collective ownership in the emerging "platform economy." It positions itself in contrast to mainstream notion of the on-demand, sharing economy by placing principles like mutuality, solidarity and compassion at the center of new types of organizational and business models that are mediated by new technology.

There are four main ways that Appcoins might support collectively owned and managed digital networks: by creating a new funding model for open source software, by helping bootstrap new fledgling networks, by enabling greater competition, and as a tool for collective governance. We outline these fours functionalities below, and then examine how they play out in one specific case study of a publishing platform called Steemit.

New Model for Funding Open Source Software

Appcoins enable developers to crowdsource resources to support open source development of network protocols. In the Appcoin crowdfunding model, founding developers of a new protocol can instigate an "initial coin offering" (or ICO) whereby scarce digital tokens are issued on a secure ledger (e.g. a blockchain).[126] In 2017, the number of software projects pursuing ICO funding models has drastically increased, resulting in what some have called a "craze" in the tech industry.[127] Right now, Ethereum is the most popular platform for issuing ICOs.

Ethereum is an open source distributed computing project that aims to support a decentralized virtual machine[128] that can run state-based programs called "smart contracts." Smart contracts are computer programs between distrusting parties that can be used to delineate and execute a wide range of activities. Ultimately, the vision of the Ethereum project is to support a shared, global infrastructure for running secure software programs on an open network of distributed machines, which supports "applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference."[129][130] This platform is fueled by a token

[126] In the case of Appcoins, the blockchain serves as the record of coin issuance and of coin transfers. This can be recorded on an existing blockchain (like Bitcoin or Ethereum) or on a new one, made especially to support the Appcoin. The new blockchain needs some mechanism for security and consensus.
[127] "ICOs: Why Tech Investors Love ICO's -- and Lawyers Don't," 25 Jul. 2017, http://fortune.com/2017/06/26/ico-initial-coin-offering-investing/ . Accessed 17 Aug. 2017.
[128] In computing, a virtual machine is an emulation of a computer system. Virtual machines are based on hardware and software that provide distributed machines with the ability to behave like a single, physical computer.
[129] "Ethereum." https://www.ethereum.org/. Accessed 27 Feb. 2017.

called ether. Along with Bitcoin, Ethereum is one of the most prominent cryptocurrency projects in existence, with the second highest market capitalization of its token.[131] Smart contract scripts can coordinate the holding and release of tokens, according to parameters delineated in the contracts. [132]

Ethereum enthusiasts hope that smart contracts will enable the disintermediation of a wide range of activities that today we rely on organizations to handle for us. This disintermediation comes in the form of automated execution via smart contracts. As the Ethereum website describes, "[smart contracts] enable developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet, all without a middleman or counterparty risk."[133] The key capability that Ethereum offers for issuing Appcoins is ERC20, an interoperable standard which makes it possible for people to create their own digital token. This widely used standard makes it easier for people to issue, distribute and control new tokens via smart contracts on the Ethereum platform.

These tokens serve as a form of equity in the network. In many cases, Appcoin tokens also serve as the basis for accessing services built on top of the network, for example in the form of fees that are paid in the application's native token. Early supporters of a new project can buy tokens in an initial crowdsale, which infuses a project with the funds necessary to support full-time development.

Rather than seeking private funding or working for free, developers who work on an Appcoin project can take a certain percentage of the newly released Appcoin supply. For example, Zcash, a new cryptocurrency with built-in privacy, set aside 10% of the

---

[130] The challenges of creating programs that run "exactly as planned" have been illustrated recently in a project called, "the DAO" (short for Decentralized Autonomous Organization), which used ethereum to set up an organization that enabled DAO token holders to collectively invest in projects they wanted to support. As we will discuss later in the AppCoins section, someone exploited a known security vulnerability in the DAO code and drained millions of dollars worth of DAO tokens from accounts. This is a specific instance in which the code did not work as intended.

[131] "CoinMarketCap." https://coinmarketcap.com/. Accessed 27 Feb. 2017.

[132] For a more detailed explanation of how Ethereum works under the hood, please see the Ethereum white paper and code repository at: https://github.com/ethereum/wiki/wiki/White-Paper

[133]"Ethereum." https://www.ethereum.org/. Accessed 7 Mar. 2017.

total supply of coins for founders, employees, investors, and advisors -- the remaining 90% is to be distributed to the miners.[134] If the project achieves sufficient adoption, the token will grow in value and developers can receive compensation for their work by selling the tokens on the open market. The more demand there is to use the network, the more valuable these tokens could become.

Joel Monegro, of the venture capital fund Placeholder Capital, characterizes Appcoins as a means of redistributing the way value can be captured along the stack of the web. Until recently, Monegro claims, it was impractical for tech venture capitalists like himself to invest in the development of protocols, because one couldn't yield a return from them. It made more sense to invest in an application that would ultimately capture and monetize data. However, Appcoins provide an opportunity to think about building business models around open source technology. As Monegro argues, "The relationship between protocols and applications is reversed in the blockchain application stack. Value concentrates at the shared protocol layer and only a fraction of that value is distributed along at the applications layer."[135] Another venture capitalist, Naval Ravikant, argues that this redistribution of value capture can fuel a healthy cycle of speculation that drives early adoption of open protocols. Early adopters who think that a protocol will provide a lot of utility can speculatively purchase that protocol's Appcoin. The money raised through speculative investment can enable a community of developers to contribute to open source work in a way that was not possible before.

At the same time, this new method of fundraising has raised some interesting legal questions, particularly with regard to whether or not ICOs should be regulated as securities under the Securities Exchange Commission. The purpose of securities

[134] In addition, Zcash set up a foundation and the founders agreed to donate 10% of their coins to the foundation (so a little over 1% of all Zcash coins). Zcash hopes the foundation will be a "natural locus for voluntary governance." https://z.cash/blog/funding.html

[135] "Fat Protocols | Union Square Ventures." 8 Aug. 2016, http://www.usv.com/blog/fat-protocols. Accessed 28 Feb. 2017.

regulation is to ensure that issuers of securities honestly disclose the value of their company's shares, so that investors can make informed investment decisions.[136] This is a particularly salient concern in the cryptocurrency market, where a wave of altcoin projects (short for "alternative coins," or crypto-currencies besides Bitcoin) have resulted in pump and dump schemes, whereby instigators of a new project mint a new token, pump up the price in a pre-sale and then dump their holdings into the market.[137]

These schemes tend to result in a short-term profit for the instigators of the project, and net losses for those who invest later. As Brito and Van Valkenburgh capture in their discussion of this legal gray space, "When new or as-of-yet undeveloped coins with an uncertain future value are offered by developers in exchange for money, users are at the greatest risk of loss, and unscrupulous developers have the best chance of finding short-term gains (e.g. the windfalls of a pre-sale or the profits from selling a pre-mined token) with little concern over long term obligations (*i.e.* the developer can easily walk away from the effort, pocketing the funds)."[138]

In July 2017, the SEC ruled that tokens issued via ICOs are indeed securities, which makes them subject to SEC regulation. As the SEC argued in their recent announcement, "the automation of certain functions through this technology, "smart contracts," or computer code, does not remove conduct from the purview of the U.S. federal securities laws."[139] While the SEC stated that they did not intend to take enforcement action against the organizers of some of the earliest ICO experiments in this space, it is likely that future purveyors of Appcoins will be subject to stricter scrutiny from regulators.

---

[136] For a comprehensive discussion of if and when cryptocurrencies are subject to regulation under the SEC, see Coin Center's report: https://coincenter.org/wp-content/uploads/2016/01/CoinCenterSecuritiesFramework1.pdf

[137] Alternative coins (aka altcoins) is a term frequently used to describe the cryptocurrency projects that came after Bitcoin. There were dozens of these projects in early years of Bitcoin. Many of these projects were profit-making pump and dump schemes, whereby an altcoin creator would generate interest in their new token on message boards and in forums, causing the speculative price of their token to inflate. They would then sell their tokens for Bitcoin or cash before the price of the currency plummeted to zero.

[138] "Framework for Securities Regulation of Cryptocurrencies - Coin Center." 22 Jan. 2016, https://coincenter.org/wp-content/uploads/2016/01/CoinCenterSecuritiesFramework1.pdf. Accessed 28 Feb. 2017.

[139] "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO." 25 July 2017, https://www.sec.gov/litigation/investreport/34-81207.pdf. Accessed 11 Aug. 2017.

Despite these early challenges, this new method of fundraising has raised the interest of software developers, venture capitalists, speculators and cryptocurrency enthusiasts alike, and a rapidly growing number of open source software projects have begun to pursue this path towards funding. Much of this interest has been fed by the headline grabbing figures that ICOs have generated as of late. A slew of projects with Silicon Valley names like Bancor, Tezos, and Filecoin, have raised hundreds of millions of dollars in a matter of minutes.[140] However, it should be noted that, for all the rhetoric around the potential for ICOs to support open source software development, very few of the most successful projects to date have an explicit goal to support open source software.

Bootstrapping a minimal viable network

In addition to supporting developer talent, Appcoins can also be used to incentivize early adopters to contribute the resources necessary to make an Appcoin network functional and valuable. Rather than needing a large company to invest in the underlying infrastructure, Appcoins can fuel an incentive system that economically rewards anyone who contributes resources to the underlying infrastructure that powers the service. This could help to address performance issues that other open source software projects have struggled with in the past. For example, Tor (a network that enables anonymous communication online) can be slow because it depends on volunteers to relay traffic. If there were a market incentivizing participation in the Tor network then the service would likely perform better. As Ravikant argues, “Any time we see a line, the product in question is underpriced.”[141]

Appcoins can serve as a means of bootstrapping resources to young, open networks. These resources can vary according to what the open protocol is designed to support. For example, in Bitcoin the most important resource needed to make the

[140] “ICO Bubble? Startups are Raising Hundreds of Millions of Dollars via Initial Coin Offerings.” 14 Jul. 2017, https://www.inc.com/john-koetsier/ico-bubble-startups-are-raising-hundreds-of-millio.html. Accessed 17 Aug. 2017.
[141] "The Bitcoin Model for Crowdfunding - Startupboy." 9 Mar. 2014, https://startupboy.com/2014/03/09/the-bitcoin-model-for-crowdfunding/. Accessed 28 Feb. 2017.

network secure is hashing power, needed to validate and process new transactions through mining, which requires an investment in specialized hardware and electricity. Those who mine in the system are rewarded in Bitcoins, in an amount that is roughly proportional to the percentage of hashing power they are contributing to the network. Perhaps the most popular extension of this idea has been to use an Appcoin to bootstrap a network for distributed storage. In addition to IPFS and Filecoin, projects like Maidsafe, Storj and Sia are working to develop Appcoin systems that incentivize people to contribute extra storage space in a distributed network. Ravikant muses that Appcoins can be used to incentivize all kinds of important tasks that will give a network value:

"What else can we allocate in a network? NameCoin is already working on Distributed DNS. Can we build a striped, encrypted, high-availability data store using Boxcoin which pays for disk availability? Can we build a caching infrastructure using Cachecoin which pays edge nodes with unused resources to cache large, static content? A DDoScoin used by web servers to throttle incoming browser requests? A PKIcoin that provides a global, un-assailable encrypted and anonymous messaging network?"[142]

With Appcoins, contributions need not be limited to hardware. Appcoins can also be used to incentivize useful behaviors on the part of early adopters. For example, an Appcoin could be used to reward users who curate entertaining playlists of videos on a distributed Appcoin version of Youtube. Rewards for such behaviors are based on some quantifiable metric of usefulness, such as the number of "likes" or upvotes such a curated list receives from other users.[143] All of these interactions are encoded and recorded on a shared, open ledger: a blockchain. As Coin Center argues, "The [Appcoin] is used not only as a means of exchange or payment but also as a means to account for, judge, and verify valuable community participation through provable

[142] Ibid.
[143] "Framework for Securities Regulation of Cryptocurrencies | Coin Center." 25 Jan. 2016, https://coincenter.org/entry/framework-for-securities-regulation-of-cryptocurrencies. Accessed 7 Mar. 2017.

viewership and payment statistics."[144] This process of maintaining auditable records on a public ledger provides transparency to the ways participation is rewarded.

Enabling greater competition

Appcoins open up new business models for the web, ones that no longer depend on monopolizing control over the data that is generated on the network. As such, Appcoins could fund the development of open data sets, on top of which a variety of different services can be built. For example, in Bitcoin all the transactions that happen on the network are recorded in the public blockchain ledger. Anyone can access this transaction data to build new services. In the case of Bitcoin, the most prevalent value-added services to date are coin exchanges, where users can buy and sell Bitcoin in exchange for other types of currency. Exchanges exist all over the world, and competition between them is strong. Since the exchanges are all built on a shared data set, it's easy for customers to switch between them.

By enabling the emergence of new business models that are not based on data captured at the application layer, Appcoins shift value capture down towards the underlying protocols, on top of which applications are built. One can imagine how this might fuel a healthy feedback loop that drives further development and adoption of the underlying Appcoin protocol. As the combined value of the applications built on top of the Appcoin grows, so does the value of the underlying infrastructure. As the protocol gets more robust and adoption spreads, more businesses are built on top of it, which drives greater competition at the application layer. Because these services are built on a shared data layer, they are more likely to interoperate, and their business models could also shift accordingly–perhaps to fee or subscription based models.

Tool for collective governance

Finally, Appcoins can serve as the basis for new governance models that shape how the network evolves over time. In some governance models, application tokens are

[144] Ibid.

considered vested “stake” in the network. When users buy or earn Appcoins, they might gain access to certain non-legal rights, such as the right to vote on key decisions about how the network is managed over time. The more stake a user has, the more influence they have over key decisions and software upgrades, via a weighted voting system.[145] Proponents of this idea claim that Appcoins enable more balanced evolution of these protocols–the assumption being that those who are most invested in a network will be the most interested in ensuring its long term well-being.[146]

This stands in stark contrast to the way many protocols are maintained today, via committees of technocrats in organizations like the W3C and IETF. Proponents of Appcoins hope to enable more decentralized decision making processes that require no formal coordinating entity. As De Filippi and Wright argue, “As opposed to traditional organizations, where decision-making is concentrated at the top (*i.e.*, at the executive level), the decision-making process of a decentralized organization can be encoded directly into source code. Shareholders can participate in decision-making through decentralized voting, distributing authority throughout the organization without the need for any trusted centralized party.” In theory, this might offer solutions to the problem Rebecca MacKinnon proposes in *Consent of the Networked*, where those who create value for platforms have no control over their operation.[147]

In recent years, there has been much discussion in the cryptocurrency world about “disintermediating” governance through a combination of automated code and stake-based voting. Early proponents of Appcoins framed tokens as a means of achieving cooperation on a large scale, without the need for governments or corporate organizational structures. These ideas were frequently extended to issues of ownership

---

[145] This concept does not map cleanly onto the Bitcoin example. Bitcoin tokens are not used as a means of voting for new software updates to the system. However, miners are viewed as an important stakeholder in the system, one that can “vote” through their decision to upgrade or remain with the status quo Bitcoin client. The more invested the miner is in the Bitcoin system (as measured in terms of the amount of hashing power they can wield), the more significant their vote is.

[146] "Continuations : Crypto Tokens and the Coming Age of Protocol...." 28 Jul. 2016, http://continuations.com/post/148098927445/crypto-tokens-and-the-coming-age-of-protocol. Accessed 28 Feb. 2017.

[147] MacKinnon, Rebecca. *Consent of the networked: The worldwide struggle for Internet freedom*. Basic Books, 2013.

and control on the web. For example, a project called Backfeed urges readers to, “Imagine...Facebook owned by its users, decentralized transportation networks independent of Uber, markets dominated by open-source communities where contributors are also shareholders, and where the value created is redistributed both fairly and transparently. Imagine the innovative potential of such organizations decoupled from the rigidities of hierarchical structures.”[148]

But for all the enthusiasm that the concept of Appcoins has generated, there is good reason to be skeptical of how these new organizational models actually play out in real life. In recent months there has been explosion of interest in fundraising via “initial coin offerings,” or ICOs. Most of the projects pursuing ICOs today are structured very much like traditional companies or organizations. The development of decentralized decision making structures has simply not been a priority. Moreover, the value of Appcoins is highly speculative, which means that there can be very large swings in the price of the tokens over time. This can make it challenging to adequately budget and make project plans based on funds from crowd sales. A distributed cloud storage project, Maidsafe, recently announced it was pursuing alternative fundraising strategies after the value of their tokens dramatically fell, cutting their revenues from over $8 million to around $2 million.[149] Moreover, as we discussed earlier, projects like the DAO have faced serious ethical dilemmas when security vulnerabilities in their token-based voting procedures were exploited to drain millions of dollars worth of user shares into a separate account.[150] The world is a messy place, and it’s unclear whether a “decentralized autonomous organization” via an Appcoin can really handle the complexity of real world contingencies solely within their self-contained code and token distribution structures.

---

[148] "Backfeed." http://backfeed.cc/. Accessed 16 Feb. 2017.
[149] "MaidSafeCoin Announcement | MaidSafe - MaidSafe's blog." 31 May. 2016, https://blog.maidsafe.net/2016/05/31/maidsafecoin-announcement/. Accessed 28 Feb. 2017.
[150] "A $50 Million Hack Just Showed That the DAO Was All Too ... - Wired." 18 Jun. 2016, https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/. Accessed 28 Feb. 2017.

Steemit

Steemit gives us the most direct insight into how Appcoins might fuel a different kind of experience for publishing and dissemination of personal speech online. Projects like Steemit, Backfeed and Synereo all aim to build a "decentralized social network" on top of a cryptocurrency token. Steemit is the most advanced of these projects, as it has launched an application that supports a growing base of users. The site is supported by a token called STEEM, which is trading at about $0.16 per token, with a market capitalization of approximately $37M.[151] The platform's stated mission is to foster high-quality online communities with the help of a monetary incentive system that rewards users who share, curate and comment on content that other members of the community appreciate. This system of rewards supports a new model of collective ownership of networks whose value is largely derived from the creation and curation of user-generated content.

Steemit is an open-source, Reddit-like application that lets users post and engage with content, and is organizationally distinct from the Steem blockchain, which maintains the STEEM token.[152] Steemit is a private company, whereas the Steem blockchain is operated by an open network of independent computers that maintain a chronological list of all the activity taking place on the Steemit site. These computers update and maintain the sanctity of project's public ledger, similar to the role of miners in Bitcoin, and are known as *witness nodes.*[153] The Steem blockchain serves as a timestamped, ordered, public data store of everything that happens on the network.

As the Steemit web site explains, "Collectively, user-generated content has created billions of dollars worth of value for the shareholders of social media

---

[151] "CoinMarketCap." https://coinmarketcap.com/. Accessed 28 Feb. 2017.
[152] Nomenclature in the Steem world can be tricky. "Steemit" refers to the social media platform and "Steem blockchain" refers to the shared ledger that keeps track of "STEEM" tokens. We provide more detail about the legal distinctions between these three Steem entities in subsequent sections.
[153] The Steem blockchain does not operate the same way as Bitcoin. Steem uses "Delegated Proof of Stake" (DPOS). DPOS is a variant of Proof-of-Stake consensus models, which were developed in order to reduce the cost and inefficient electricity usage associated with Proof-of-Work systems such as the one used by Bitcoin. For more information on how DPOS works, see "Steem Whitepaper." https://steem.io/SteemWhitePaper.pdf. Accessed 28 Feb. 2017.

companies, such as Reddit, Facebook, and Twitter. Steemit supports social media and online communities by returning much of its value to the people who provide contributions by rewarding them with virtual currency."[154] In the following sections, we will take a closer look at how the Steem token system is used to address the areas we outlined above, regarding crowdfunding, the bootstrapping of network resources, interoperability via shared data, and collective governance.

Crowdfunding into Existence

The Steemit platform used the creation of the STEEM token as a key mechanism for remunerating the team of full-time developers who were hired to work on the project. Initially, Steemit's founders, Ned Scott and Dan Larimer, raised enough money from an angel investor to pay a small team of developers to implement the first blockchain infrastructure and front-end website. The company launched in February 2016, and the first STEEM tokens began trading on currency exchanges by the end of March. At that point in time, Steemit the company had mined about half of all STEEM tokens in existence, and it split those tokens amongst the core group of developers working on the project.

These STEEM tokens were mined into existence when Steemit made a soft launch of its platform, recruiting individuals to host witness nodes. In the early days, Steemit recruited witness nodes via announcements made on a couple of popular cryptocurrency discussion sites and podcasts, such as Bitcoin Talk.[155] Steemit's founders viewed the cryptocurrency community as a natural starting place for these activities because it is a home for many individuals who might be interested in both the technical design of the platform, as well as the speculative value of new currency types.

In essence, the Steemit platform operates like Reddit with a digital wallet. In contrast to other Appcoin models, a new user on Steemit does not need to buy STEEM in order to access the site. In fact, when a new user opens an account they are

[154] "Steem." https://steem.io/. Accessed 28 Feb. 2017.
[155] Steem initially launched mining as a Proof-of-Work algorithm, similar to Bitcoin, but after a month of operation they switched over to Delegated Proof of Stake.

automatically given a digital wallet with $3-4 worth of STEEM tokens to experiment with.[156] The initial seeding of a user's account with a small amount of STEEM is designed to give them a sense of shared ownership in the network, which they can grow by participating on the site. Starting in March 2016, new users could sign up for an account and start posting content.

Activities on the network are recorded on the Steem blockchain, which keeps track of the interactions users have on the platform, such as posting, sharing and liking content. By design, users receive a payout of freshly minted STEEM tokens every day, distributed continuously according to how much value (posts, up-votes, etc)[157] each user is contributing to the network. In the early months of the Steem blockchain launch, rewards were withheld as the developer team stress tested the network and made sure that their blockchain was secure. On July 4th, Steemit did its first official payout of STEEM, based on the prior three months' activities on the site. The payout was estimated to value $1.3 million, causing a spike in attention from both the media and the currency markets. This, in turn, sparked a dramatic 1,000% increase in the market price of the token, from $13m to $150m market capitalization in the two weeks following the initial payout.[158]

Today, the market cap for STEEM is valued at over $287 million.[159] This value is derived largely from the speculative rate of exchange for the token on cryptocurrency exchanges like Poloniex, where STEEM holders can sell their tokens for Bitcoins or other fiat currencies like the USD or the RMB.

Bootstrapping a minimal viable network

At its heart, the Steemit platform aims to redistribute value and promote a sense of collective ownership through the distribution of new STEEM tokens each day. These

[156] Steemit issues the same dollar value of STEEM to all new users, which means that the actual amount of STEEM tokens issued varies according to the token's valuation at any given time.
[157] We provide a more i- depth discussion of how value is defined and measured in the following section.
[158] "Digital currency Steem soars 1,000% in value in two weeks ...." 12 Jul. 2016, https://www.theguardian.com/technology/2016/jul/12/steem-digital-currency-steemit-value-soars. Accessed 28 Feb. 2017.
[159] "CoinMarketCap." https://coinmarketcap.com/. Accessed 11 Aug. 2017.

tokens are minted and distributed at a constant rate, according to a set of specific rules. These rules are intended to incentivize users to actively contribute and curate engaging content that other users find valuable. Each day a new set of coins is minted and distributed to users according to an algorithm that apportions the rewards based on a range of activities, such as how popular a user's published content is, or how well they are able to predict what other users in the system will like. Those rewards are divided evenly into two types of tokens that are derived from the STEEM base currency–Steem Power (SP) and the Steem Backed Dollar (SBD).[160]

SP and SBD are designed to strike a balance between the need for users to receive instant gratification for their contributions, while also fostering long-term investment in the Steemit network. Steem Power is essentially an influence token–the more SP a user has, the more weight their votes have in the system. In addition to earning SP through posting and curation, users can accumulate more SP by committing some of their STEEM tokens in an escrow, effectively investing that value into the system. When a user wants to cash out, they "power down" their SP, triggering a release of STEEM in equally proportioned weekly increments over the course of two years. The two-year payout schedule is designed to align users' economic interests with the long-term stability of the Steemit platform, and thus incentivize them to behave in a way that maximizes the value of the platform to the Steemit community. If the price of STEEM falls, the value of one's weekly power down payout will fall as well. As such, the more SP a user has in the system, it is assumed, the more aligned the user's preferences are with the broader community and, therefore, the more influence they should have over what content is surfaced on the site.

The other half of Steemit's daily payout is distributed in the Steem Backed Dollar (SBD), which is pegged to the value of the US dollar. The Steem network maintains this peg by paying out interest to holders of SBD.[161] The goal of SBD is to reduce the

[160] Steem is the fundamental unit of account on the Steem blockchain. SP and SBD derive their value from the value of STEEM. Generally speaking STEEM is only held for short periods of time, as an exchange currency - someone looking to enter or exit the Steem platform will have to buy or sell STEEM.
[161] "Savings Rewards - Steem." https://steem.io/getinvolved/steem-backed-dollars/. Accessed 7 Mar. 2017.

monetary and cognitive costs of frequent price swings in STEEM. This is particularly important for attracting users who are drawn to the Steemit platform by the prospect of making money for their contributions to the site -- so when a user is rewarded 20 SBD, they know they have earned $20 of value that day. If users want to cash their SBD into USD, then they can initiate a 7-day cash out process and get their payout in dollars, or another currency of their choice.[162]

This rewards structure was designed as a mechanism for overcoming the high switchover costs of getting users to engage with a new social media platform. User generated content is arguably the most important resource for a social media network to bootstrap in the early days of its existence. This can be challenging due to high switchover costs and the impact of network effects for social media sites. Even when functional alternatives to a dominant social media site are created, it can be hard for them to attract a sufficient user base to render them useful. In spite of growing evidence that sites like Facebook and Twitter are important vectors for surveillance and controlled speech online, there does not appear to be a large demand for alternatives.

Steemit's founder, Ned Scott, was well aware of these constraints as he and his team designed Steemit. "You can't just make a platform that is as good as Facebook," he said in an interview for this report, "You have to provide a clear value add that will draw new users in." Ned envisions cryptocurrency as a driver for the creation of a diversity of platforms that support different incentives to achieve distinctive user experiences online. Steemit's model of economically rewarding users for their contributions has been a particularly enticing value proposition for semi-professional content creators who are looking for more lucrative ways to monetize their work.[163] Perhaps unsurprisingly, the other large group of early adopters has been cryptocurrency enthusiasts, interested in supporting and speculating on new token projects like STEEM. In some ways, it appears that Steemit's novel model for value distribution on

[162] It takes seven days to convert Steem Backed Dollars into STEEM, after which, users can buy and sell STEEM on a cryptocurrency exchange like Poloniex or Bittrex.
[163] "My First Steemit Post Made $545.75 Here's Why - YouTube." 17 Aug. 2016, https://www.youtube.com/watch?v=YpCAp69NuSY. Accessed 28 Feb. 2017.

their site has been a hit -- the platform is supporting over 100,000 accounts after just six months of operation[164] and has a steady stream of new content running at all times.[165]

However, in addition to the number of new and active users, it's important to also examine how economic incentives shape the quality of the content that is generated on the site. In the first few months of Steemit's operation, content about the platform itself dominated the Steemit feed. These included how-to explainers for beginners who were interested in strategies for making money on the site, as well as promotional content that highlighted the positive impact that Steemit has had on user's lives. It is not uncommon for posts to embed the Steemit logo into their banner at the top of their posts.[166] Ned Scott likens this behavior to a form of patriotism -- users wave the Steemit flag to rally around an idea, a new social structure that they believe their currency enables. According to Scott, early adopters are like the founding fathers -- because of the token distribution structure, they feel a strong sense of pride and ownership in the site.[167] However, an alternative explanation for this behavior might be that Steemit is operating like a pyramid scheme, whereby members of the scheme expend their resources on recruiting new members to the site, in the hopes that additional users will mean additional payouts for them as the network grows over time.

One way to differentiate between scams and legitimate projects in this space is based on the level of transparency the initiators of the project provide around how many tokens they hold, and when they sell them. Scott says that Steemit has made efforts to ensure that it is very easy to track the amount of STEEM each user on the site holds. Top holders of STEEM are listed on a "Rich List" which updates in real time and is

---

[164] "Distribution - Steem." https://steemd.com/distribution. Accessed 28 Feb. 2017.

[165] To put this number into context, Facebook had over 1 million users by the end of their first year in operation. Twitter had approximately 120,000 users in their first 18 months of operation.

[166] Some of this logo embedding might have been part of a gamified incentive program the Steemit team was experimenting with: if the Steemit logo was placed next to the title of a post, then it meant that the author had pledged to commit his or her entire earnings from that post in SP, rather than cashing out of the system.

[167] In many ways, the Steem community looks like other communities that form around cryptocurrencies. Hardcore "Steemers" even meet outside the platform for gatherings like "Steemfest" which happened in the fall of 2016 in Amsterdam. See William Mougayar, "Steemit's First 'Fest' Reveals the Power of Blockchain Community ...." https://steemit.com/steemfest/@wmougayar/steemit-s-first-fest-reveals-the-power-of-blockchain-community. Accessed 28 Feb. 2017.

publicly available.[168] At the same time, the individuals listed on this page are only known by their Steemit handles. There is no obvious way to connect the identities of the Steemit team to their Steemit handles, which makes it more challenging to audit the team's token holdings. The Steemit team could improve this tool by explicitly identifying the handles of the individuals who work for the company.

While much of the early content and user base drew heavily from a community of cryptocurrency enthusiasts, Scott expressed a desire to expand and diversify the user base. After six months of observation, it appears that the Steemit team has made some progress in diversifying their content. Today the platform's stream of trending content is increasingly varied, ranging from discussions on recent sporting events to cannabis reviews and journal entries of users' travels around the world. One strategy the platform adopted to diversify posts was to highlight creators of content that has proven to be viral on other sites like Youtube and Tumblr. This includes video tutorials for makeup application and how-to's for various hobbies, like gardening.

Steemit is not the only instance in which we've seen economic incentives impact the quality and quantity of the content users post online. Last year a Spanish-language social media site called Taringa! launched a new program called Creadores, a revenue sharing program that targeted the site's most prolific content creators. Because many of the site's customers are young and do not have bank accounts, Taringa! decided to distribute its payouts in Bitcoin. The goal of this program was to incentivize high quality content that the Taringa! community appreciated.[169] However, the initial pilot of the program appears to have had the opposite effect -- rather than posting original content, members of the Creadores program started posting copied content in significantly higher volume (around 30% more content).[170] These posts were often copied directly from articles on other social media sites. As might be expected, the presence of economic incentives changed the nature of the posts shared on the site, in a way that favored spam over high quality content.

---

[168] "Richlist - Steemd." https://steemd.com/richlist. Accessed 28 Feb. 2017.
[169] "Taringa Creadores!." http://www.taringa.net/creadores. Accessed 28 Feb. 2017.
[170] Gino Cingolani, interview by Chelsea Barabas, August 10, 2016, interview 2, transcript.

The case of Taringa! illustrates the challenge of relying on economic incentives to bootstrap user generated content to new social media sites. In traditional social media platforms, users tend to organically generate and share content that they enjoy and that they think their friends will also appreciate. The motivation for sharing is social at its foundation. Economic incentives change the nature of engagement on a self-publishing platform, from one of social interaction to one of profit-seeking. Depending on how "quality content" is defined and measured on the platform, these economic incentives can have a significant impact on the nature of the content that is produced (i.e. to optimize for click bait over more niche interest stories). Further on, we will explore complicated interactions between Steemit's algorithm for defining "quality" content and the types of media that end up succeeding on their platform.

In addition to incentivizing content production, Steemit uses its token system to partially bootstrap resources for the witness nodes, the underlying infrastructure that supports the Steem blockchain and the social network. All of the witness nodes that process and store user data in the Steem blockchain are owned and operated by individuals outside of the Steemit company. A variety of tools have been developed to support people who want to build applications on top of the Steem blockchain.[171] Witness nodes receive rewards in the form of SP, which serve as an incentive for contributing computational resources to the network. These witnesses play a critical role in updating the log of activities and content posted to Steemit. In the following section, we will go into greater detail about the role that witnesses play in maintaining an open publication system that enables competition and supports censorship resistance in publishing.

Supporting Competition

It is important to note that Steemit is organizationally distinct from the Steem blockchain, though Steemit relies on the Steem blockchain as a public data store. Steemit is a private company, whereas the Steem blockchain is supported by an open

[171] "SteemPower.org." https://steempower.org/. Accessed 28 Feb. 2017.

network of computers. The Steem blockchain developers (who are also Steemit's developers) describe Steemit as a practical example of the many applications that can be built on the STEEM token system. Today there is a steadily growing number of other applications that use the Steem blockchain data.[172] For example, tools like Steemstream provide a live feed of all the activity on the site in real time.[173] Steemd.com provides a daily analysis of the number of active users on the site. Some applications are designed to enhance the user experience on the Steemit social media platform -- they help users to find new and interesting people to follow, or to serendipitously discover random new posts.

Many tools are intended to help users maximize the monetary value they are able to extract from the system, by providing analysis and data visualizations on what posts are gaining momentum, or what authors are the most up and coming. Still others seek to leverage the STEEM token system to support new collaborative applications, such as Radio Steem, which supports crowdsourced music playlists.[174] Another tool, SteemSpot, helps users connect with other Steemers around the world when travelling.[175] Even alternatives to the Steemit social media platform have been built on top of the Steem blockchain -- sites like Busy.org leverage the STEEM token system in order to create a different social network.[176]

These applications are built on top of the Steem blockchain, which provides a reliable account of transactions on the network, in chronological order. This chronological account of activity is important because it serves as the basis for determining how payouts are distributed at the end of each day. The Steem blockchain is managed through a process termed "delegated proof of stake," whereby activities are recorded in rounds of new blocks generated and signed every 63 seconds. Each round is comprised of signed blocks produced by each of the 21 "witness" nodes in the

---

[172] These tools tend to be made by users and enthusiasts of the platform, not Steemit the company. A list of these tools can be found on a site called Steemtools.com

[173] "SteemStream.com - realtime blockchain stream visualisation." http://steemstream.com/. Accessed 28 Feb. 2017.

[174] "RadioSteem.com - Consensus Radio." http://radiosteem.com/. Accessed 28 Feb. 2017.

[175] "Steemspot." http://steemspot.com/. Accessed 28 Feb. 2017.

[176] "busy.org — Steemit." https://steemit.com/@busy.org. Accessed 28 Feb. 2017.

network. 19 of these witnesses are elected by STEEM token holders (votes are weighted in proportion to the amount of SP a given user holds). Ned Scott characterizes witnesses as politicians -- each witness must demonstrate to the broader community why they are worthy of the job.

Scott claims that many witnesses are also active and well-known members of the Steemit community, arguing that it is common practice for witness candidates to post links explaining who they are and why they would like to serve as a witness. Some even make pledges to redistribute their SP rewards back to the community. In addition to these personalized narratives, sites like steemd.com keep track of key performance metrics, such as the amount of up-time for each node. Those witnesses who are not voted into the top 19 positions are included in a lottery, and one is selected every round to sign a new block. Their likelihood of being selected is proportional to the number of witness votes they received. Finally, one witness is selected based on a proof-of-work algorithm.[177]

Witnesses are continuously rated and reshuffled according to user votes. According to Ned Scott, about 30% of the current STEEM stake is actively engaged in voting. This is quite a high percentage, given that developers on the Steemit team own about half the stake in the network. For the moment, the Steemit team has opted to withhold from voting on witnesses, which means more than half of all user stake in the system is participating in witness election. However, it's tough to gauge how active this voting process is. To date, we have not been able to surface a specific instance in which incumbent witnesses have been kicked out in favor of new candidates.

Moreover, it remains unclear how necessary it is to manage this somewhat convoluted process of voting and delegation across the twenty-one witnesses. According to Scott, this detailed election process was created in an effort to ensure that the Steem network provides robust censorship resistance guarantees for published content. The only way for content to be censored from the Steem network is if every

[177] By diversifying the paths to becoming a witness, Steem aims to "provide a high reliability while ensuring that everyone has the potential to participate in block production, regardless of whether they are popular enough to get voted to the top." For more details see the Steem white paper at: http://steem.io

single witness refuses to include it in a block that they sign into the blockchain data structure. If users suspect that witnesses are censoring content, they can elect a new group to sign blocks.

Even if those witnesses somehow collude to collectively censor a given file, the random selection of the final two witnesses will make it challenging to make that exclusion airtight. “If you have written something down that is logged in the Steem blockchain, it is always in the Steem blockchain. So it never can truly be censored,” claims Scott. What he means is that, even if content is removed from the Steemit website, it can easily be found and republished via an alternative website that builds on top of the open Steem blockchain.

However, while Steem’s blockchain may make it easier to publish content, it doesn’t necessarily mean that the content will be easily surfaced by other clients. Currently, whenever Steemit receives a takedown notice under the Digital Millennium Copyright Act (DMCA), they take down the content and post the notice in the Steem blockchain so that other websites are aware of the content’s legal status. Ultimately, every site is held responsible for ensuring illegal content (i.e. copyrighted material, pornography, etc.) are not published on their site. Hypothetically that content is still available to anyone who downloads the entire Steem blockchain, but this seems like an impractical way to safeguard against censorship. According to Scott, the blockchain takes about half a day to download today. As it grows in size, it will eventually become too large for run-of-the-mill consumer hardware to support.[178]

Regardless of these limitations, the Steem blockchain offers a very different model for thinking about the role of data in supporting revenue generation and competition for the platform. Rather than locking user data away in a private silo that can only be accessed via API, the Steem blockchain serves as comprehensive and

[178] The Steemit team has expressed aspirations to migrate over to a more distributed data storage system, like IPFS. This is important, Scott says, because Steemit doesn’t want to be subject to pressures from government to take down content. Scott says they may eventually integrate with a distributed storage service so that they can provide strong protections against censorship for their users. If Steemit is forced to take down content, at least it can be rendered via a different service if the content is hosted on IPFS. However, integration with IPFS is not something that Steem would directly support via their Appcoin.

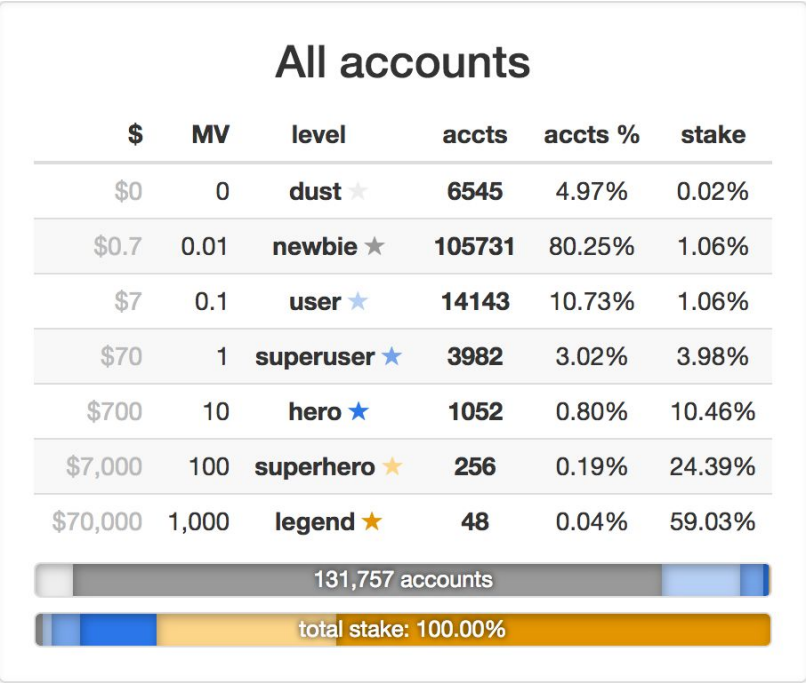
open API, one that gives third parties and users the opportunity to develop value-added services and competitor products on top of it. As Ned Scott explains, “For the first time, all the data is publicly available. There’s no walled garden of information anymore.” This stands in stark contrast to the major social media platforms of today, whose data sharing policies make it challenging for competitor services to bootstrap a user base. This, in turn, exacerbates risks of censorship on mega-platforms.

Collective Governance for Curation

Steemit uses its token system as the basis for offloading some critical aspects of governance to the community, particularly with regard to curation of content. As discussed earlier, Steemit uses a weighted voting system to curate content on its site. Economic incentives play a critical role in how Steemit conceives of filtering for high quality posts. In order to ensure that users don’t simply upvote their own publications, the developers of Steemit split the payout for new content between the person who posted it and those who subsequently vote for it. The idea is that users are incentivized to invest in content that they think others in the network will appreciate. In theory, the more up-votes a piece of content garners, the higher the reward they will receive. Thus, ideally, users are economically rewarded in proportion to how much their content is appreciated by other users.

However, in reality, rewards are not distributed directly in proportion to the raw number of up-votes it receives. The economic success of a post depends greatly on how influential the voters are who vote on their post are, as determined by the amount of SP they hold in the system. Right now, the distribution of SP across users in the system is very unequal -- more than 90% of SP tokens are held by less than 2% of account holders in the system.[179]

[179] "Distribution - Steem." https://steemd.com/distribution. Accessed 28 Feb. 2017.



https://steemd.com/distribution

This immense disparity in voting power complicates Steemit's narrative around democratized content curation -- it means that a very small number of users are extremely influential and that the vast majority of users' votes are virtually inconsequential. This begs the question: do we really think that those who have the most stake in the system are going to handle the job of content curation in a more fair and balanced way than, say, Facebook currently handles it?

When pressed on this issue, Ned Scott points to the market as the solution. He envisions curation evolving through the formation of "curators guilds" that are funded by large stakeholders in the system, known as "whales." Whales could delegate their voting power to editors and curators, whom they hire to do the hard work of high-quality curation. Ideally, the rewards garnered through curation activities would cycle back through the guild to fuel future work. All the accounting and management of curation

would be handled on the blockchain, and as the guild grows it can "harness the wisdom of the crowds" to surface the best content in a more democratic way.[180]

According to Scott, the whale model is more appealing than implementing, say, a one vote per one account rule, because it doesn't require strict monitoring of accounts. If every account had an equal amount of influence in the system, then users would be incentivized to figure out ways to open multiple accounts that can be controlled by one person. This opens the platform to sybil attacks.[181] Moreover, Scott argues that it's not socially desirable to give one equally weighted vote to each user, because people are not equally invested in the site. Shouldn't those who know and contribute to the site the most have more say in how it is operated?

But this idea is problematic for a variety of reasons. After all, the biggest financial stake holders of the *New York Times* are not also the people held responsible for deciding what is placed on the first page of the publication each day. Moreover, this scheme does not address the underlying assumption that the highest grossing articles (in terms of STEEM rewards) are the highest quality content. For a variety of reasons, that might not be true. The Steemit incentive scheme turns user generated content into a commodity that others can speculate on. The goal of speculation is to make money, not to curate the front page of Steemit for relevant current events.

In this speculative market for content, there tends to be big winners and a long tail of losers. Due to the massive consolidation of tokens into the hands of just a few, the likelihood of a post's success has more to do with *who* voted on it than how many people actually read and enjoyed it. This, in turn, continues to perpetuate inequality, as incumbent winners are more likely to continue winning for their posts, while unknown newcomers struggle to get noticed on the sidelines. This problem is exacerbated by

[180] This is a phrase that Ned Scott used frequently during our conversations. As someone who had formerly worked in finance, he argued that economic incentives and free market forces could be relied upon to surface more "ideal" content on social media.

[181] In computer security, a Sybil attack is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks.

bots, which tend to pile on votes for a small number of well-known authors in order to win curation rewards fast.[182]

Second, Scott's concept of curation guilds looks very similar to the privatized, profit seeking models we are already struggling with on social media sites like Facebook. Rather than supporting a group of engaged users who are expending their personal collateral to influence content curation, SP would consolidate around something that looks more like a private company that hires professional content curators, whose goal is to earn more SP through their activities. Therefore, the logic of operation for one of these guilds is likely to be consistent with the profit-seeking motives of Facebook, who has been criticized for prioritizing dubious click bait over traditional news media in an effort to optimize revenues, rather than high-quality civic discourse. Without directly adjusting the goals and logic of curation to prioritize certain social values (i.e. accuracy), it's unclear how this guild model would enable surfacing high-quality content. In this sense Steemit faces some of the problems journalism faces with clickbait–projects may require a double bottom line of fiscal sustainability and civic impact to provide socially valuable content.

Appcoins: Concluding Thoughts

Underlying Steemit's Appcoin approach is a deep faith in market-driven solutions to solve tough social problems. As founder Ned Scott summarized to me, "This is a free market system. This is a swarm of people. There's no puppeteer at the top of this thing. There's many many people, and that's what gives us the wisdom of the crowd."[183] For Scott, the market is a natural, constantly adapting force that shapes user behavior through a framework of economic incentives which users can voluntarily opt-in to.

At a high level, the Steemit system does provide a compelling way to support collaborative co-creation of a shared social network, one that delineates clear ways for

[182] Bots have posed an ongoing challenge for Steemit. We think the economic incentive framework that Steemit has created plays a large role in this - people have clear incentives to game the system, through automated "bots" that can constantly be online, waiting for opportunities to vote or post content that might be lucrative.
[183] Ned Scott, interview by Chelsea Barabas, December 4, 2016, interview 2, transcript.

users to gain ownership and influence into the system. It provides an alternative funding model for open source projects and lowers switching costs by rewarding people for their participation and making it easy for competitor services to be built on the same body of data.

The Steem blockchain also provides some assurances around data transparency and censorship of published material -- even if one particular site is pressured to take down content, the data is still discoverable on the distributed Steem blockchain. In these ways, we could imagine the Steem model enabling a greater diversity of choice in how users publish and disseminate their content, while also providing a vision for alternative business models that do not necessitate the enclosure and lock-in of user data.

Yet, upon closer scrutiny this narrative quickly gets complicated. Much of the value and activity generated on Steemit is based on speculation and convoluted economic policies.[184] These schemes have not worked well for most Appcoins, since in the last several years the cryptocurrency world has been riddled with pump and dump scams that seek profit from speculation. Even in scenarios where Appcoins are not created for the sake of blatant fraud, most tokens' trajectories are downwards, towards exponential decay.[185] In this sense, they exhibit the symptoms of any speculative venture–failing projects lose user bases–compounded by the loss of incentive to participate from a falling currency.

There are open questions about how to regulate these types of projects to ensure that consumers are treated fairly. Like in many Appcoin schemes, early adopters tend to accumulate an outsize amount of stake in the system, which gives them outsize influence and control. This fuels significant disparities between early and late comers, in terms of influence and profit over time. However, this accumulation of influence is not

[184] The economic policies underlying Steem have been tweaked and changed a number of times. The most significant set of changes came at the end of 2016, in a software upgrade that had significant implications for the ways the economic mechanics of the sited worked. For example, the upgrade decreased the amount of time it takes to "power down" SP from 104 weeks to just 13 weeks, and inflation rates were adjusted. For a more detailed sense of these changes, see: https://steemit.com/steem/@steemitblog/final-review-of-steem-economic-changes.

[185] However, this has not been the case for Bitcoin, because the BTC token arguably has some inherent value as a censorship-resistant means of value exchange. Because there are a large number of people who, say, want to buy illegal goods on the the dark web, the price of Bitcoin is likely to retain value.

necessarily inherent in these token-based systems. Steemit and similar platforms might be able to learn from ongoing work of people in the platform cooperativism movement. The concept of platform cooperativism was first introduced in 2013 by Trebor Scholz and Nathan Schneider, in response to the growing concern around worker rights and user protections on online service platforms, such as Uber and Airbnb. Like Steemit, a large focus of platform co-op efforts are around developing new models of collective ownership and governance for digital platforms.

Indeed, advocates of platform cooperativism have expressed keen interest in exploring the possibility of using digital token systems to experiment with new ownership and governance models.[186] Most of these projects, such as the Economic Space Agency (ECSA) are brand new, but they espouse values that are aligned with the ideas of equitable, collective ownership of digital platforms. As ECSA explains in their mission statement as "[we] give individuals, communities, organizations and networks innovative instruments to create new economic incentive structures that match their values and visions. Our tools provide ways to align economic value with social value by incentivizing cooperation and fostering a sense of community and shared purpose."

Projects like ECSA draw from a long line of work in developing cooperative governance structures. They may be able to think more intentionally about how to structure token-based ownership models in a way that is more equitable and fair than what we currently see on Steemit. In coming years, we expect to see more AppCoin experiments that combine token-based incentives with more thoughtful collective ownership and value distribution models.

[186] "Platform Cooperativism - Rosa Luxemburg Stiftung NYC." http://www.rosalux-nyc.org/wp-content/files_mf/scholz_platformcoop_5.9.2016.pdf. Accessed 28 Feb. 2017.

Section V: Conclusion

The impetus for this research is the concern that consolidated publishing platforms have gained significant and possibly dangerous power over free speech online. As content curators, they have immense influence over civic discourse. As gatekeepers, their community governance policies have the potential to sideline important voices. In this report, we have explored two distinct, but interconnected meanings of the term centralization: 1) market centralization, where a handful of private companies now dominate personal publishing online and 2) structural centralization, where we see the consolidation in control over publishing infrastructure, such as data storage, identity authentication and data formats.

Market and structural consolidations are deeply interconnected. This is in large part due to the business model most successful platforms employ, advertising and targeting based on user data. Users seem comfortable giving up their content in order to get free access to applications. Platforms are motivated to capture, collect, and cordon off a growing set of user data to improve advertising targeting. In addition to being motivated by data capture, these platforms become more valuable through network effects as more people join and use them. The rise of large platforms has brought about and accelerated the privatization of the web's underlying infrastructure, shifting it out of the hands of users and into the control of a small number of private corporations. These trends pose a real problem for advocates of free speech -- they have created a world in which exclusion from a specific platform can practically silence one's ability to communicate with others online, a world in which opaque algorithmic practices shape how complex issues are framed, and what voices get heard.

In light of these trends, we began this work by focusing on technical interventions that would help us move towards a "re-decentralization" of the web. The key theory of change we wished to evaluate was the idea that the availability of decentralized infrastructure would enable the creation of compelling alternative platforms or directly provide users with greater variety and control over the means of publishing and

distribution online. Our primary concern was whether or not it was technically feasible to support a more peer-to-peer architecture for mass publishing online. Unfortunately, our analysis shows that the impact of structural interventions is often constrained by broader social and economic forces that regulate our behavior. The challenge is not just building decentralized software or creating alternative platforms, but creating options for users that are financially sustainable, usable and compelling.

Historically, open standards and other efforts to support interoperability have been abandoned because they impose significant constraints on the ability of platforms to be responsive to user needs and preferences. Moreover, if there is limited consumer demand for alternative publishing platforms, it doesn't matter if a more privacy preserving, user-controlled version of Facebook is created. People rarely adopt new platforms for abstract, ideological reasons, like "decentralization." Rather, they generally adopt technologies based on convenience, price, usability and where their friends are hanging out.

In light of these findings, it's not clear that these issues of centralization can be solved by simply pursuing the opposite trend, towards "re-decentralization" of publishing online. The concept of decentralization is closely tied to the values of individual empowerment and self-sufficiency, eliminating choke points in the system by placing key functions of publishing, discovery and curation directly back into the hands of users. Today's advocates of decentralization tend to view any third party intermediary as a threat, a choke point that could be used to censor speech. For them, the ideal web landscape is one of self-publishers, who can directly reach their online audiences without the need for a third party service to host and curate their content.

But as our case studies illustrate, values of individual empowerment and autonomy need to be balanced by a recognition that most people are going to experience the web through a set of trusted third party services. As the Freedom Box example illustrates, it is impractical to expect most people to run their own publishing hardware. Complete control over publishing infrastructure also means complete responsibility for ensuring your content is available, discoverable, verifiable, and, if

necessary, deletable. In a world where most of these processes are hidden to the average user, it is not reasonable to expect everyday people to take on complete responsibility of running these processes for themselves.

What is more likely – though far from guaranteed–to arise, we argue, is a small set of trusted service providers who compete for business in an open network, where users can opt in or out of services based on information about the platforms' performance according to well-defined metrics. For free speech die-hards, this may seem like an imperfect and partial solution. If the IPFS network isn't a literal peer-to-peer network of individuals offering up spare hard drive space, then it's not fully "decentralized" and there is still potential for censorship. But this perspective overlooks the potential for a system like Filecoin to enable a more competitive marketplace, one with greater transparency around storage provider's performance and reliability.[187] Reduced market centralization combined with increased transparency, rather than full "decentralization" of publishing infrastructure, might be what is needed to rebalance the current equation.

Rather than striving for censorship-proof technology, a better goal would be to pursue strategic structural, legal and normative shifts that support greater experimentation and user choice in the way platforms curate content and govern community interactions. We recommend two umbrella strategies for achieving this goal: 1) developing a robust set of tools and legal frameworks for establishing consumer rights over the content and data users generate on platforms and 2) increasing transparency and experimentation around methods of content curation and community governance on social media sites.

At the heart of many of the projects we examined in this report is the concept of providing users with greater ownership and control over the content that they publish on social media sites. For example, projects like Solid are building out the technical specifications necessary for users to port and plug in their data to a variety of

[187] In interviews with other Appcoin-based distributed storage projects, such as Maidsafe, Storj and Sia, the project's developer's site visibility into performance of service nodes is a key feature they are working to build out, as it will provide the basis for informed consumer choices on behalf of the consumer.

interoperable services. This would sharply lower barriers to entry for new platforms, enabling users to make change via market forces. If users can switch between services in a frictionless way, then it's possible for them to exert some influence over contentious or problematic policies that they wish to see changed.

Moreover, if users are able to access their data independent of a specific platform, then we reduce the risk of certain types of censorship. For example, if a government pressures Facebook to delete or hide content posted by an activist group, it is important that those individuals are able to access and re-publish that content elsewhere. Stronger consumer rights over data could also lay the groundwork necessary for thinking about more diverse ways of curating content from across a variety of content sources, using clients that can federate data from different platforms.

At this point, the most significant barrier standing in the way of user control over their data is legal, not technical, in nature. Laws such as the Computer Fraud and Abuse Act and the Digital Millennium Copyright Act bar users (or third party services acting on behalf of users) from circumventing access controls and digital rights management protections in order to access and repurpose the data they generate on third party platforms. Facebook has used these laws in order to raise lawsuits against companies that offer federated curation services to users across platforms. For example, in 2008 Facebook filed a suit against Power Ventures, a third-party platform that offered a single portal for users to view their content, by aggregating it from across their social media accounts (Facebook, Twitter, Instagram, etc).[188] Without a serious revision of these types of laws, users will have a hard time pressuring mega-platforms to modify policies by "voting with their feet."

In addition to these efforts, we recommend that foundations invest in the development of tools to support greater transparency and experimentation in the way platforms curate content and govern community norms. As awareness of the role that algorithms plays in curation and governance becomes more widespread, the concept of

[188] "Facebook's Ongoing Legal Saga with Power Ventures Is Dangerous ...." 11 Mar. 2014, https://www.eff.org/deeplinks/2014/03/facebooks-ongoing-legal-saga-power-ventures-dangerous-innovators-and-consumers. Accessed 7 Mar. 2017.

"algorithmic transparency" has been offered as a solution to some of our concerns.[189] In theory, if we had greater transparency into the way platforms were algorithmically surfacing our content, then we could check for blatant abuses of platform's curatorial power, as well as pave the way for users to make more informed decisions about which platform to use, based on their content consumption preferences.

However, as Christian Sandvig has argued, algorithmic transparency efforts have proven to be much more challenging than they initially seem.[190] For one, the amount of code underlying algorithms like Facebook's news feed is massive, numbering in the millions of lines of code. Even the average iPhone application today runs on no less than 40,000 lines of code.[191] The sheer quantity of information that would need to be parsed in order to understand what's going on "under the hood" of a social media site renders the task nearly impossible. As Sandvig argues, historically, attempts to open source code in an effort to increase transparency and accountability have fallen flat, due to the sheer complexity of the software.[192]

At the same time, if one were to distill these immense code bases down to a few comprehensible rules for how content is prioritized, then we open up platforms to the vulnerability of massive manipulation by users who want to ensure their content reaches as many eyeballs as possible. As media scholar danah boyd points out in "Hacking the Attention Economy," the networked media sphere has given rise to various groups that "hack" traditional media distribution channels in order to get their ideas heard and seen by a wide audience.[193] As boyd argues, "A new form of information manipulation is unfolding in front of our eyes. It is political. It is global. And it is populist in nature. The

---

[189] "Algorithmic Accountability. Journalistic ... - Nick Diakopoulos." 7 Nov. 2014, http://www.nickdiakopoulos.com/wp-content/uploads/2011/07/algorithmic_accountability_final.pdf. Accessed 28 Feb. 2017.

[190] Sandvig, Corrupt Personalization: Algorithmic Culture in Media and Computing, forthcoming from Yale University Press.

[191] "Million Lines of Code — Information is Beautiful." http://www.informationisbeautiful.net/visualizations/million-lines-of-code/. Accessed 28 Feb. 2017.

[192] Sandvig, Christian, et al. "Auditing algorithms: Research methods for detecting discrimination on internet platforms." *Data and discrimination: converting critical concerns into productive inquiry* (2014).

[193] "Hacking the Attention Economy - Data & Society: Points." 5 Jan. 2017, https://points.datasociety.net/hacking-the-attention-economy-9fa1daca7a37. Accessed 28 Feb. 2017.

news media is being played like a fiddle, while decentralized networks of people are leveraging the ever-evolving networked tools around them to hack the attention economy." This situation could get worse if we were to increase the transparency around the algorithms used to prioritize content on these sites.

Alternatively, Sandvig advocates for the development of tools to support algorithmic auditing practices, similar to those conducted by social scientists looking to surface and understand the nature of bias in key decision making processes, such as hiring and loan decisions. The goal of an algorithmic audit is to surface problematic outcomes of an algorithmic system, as well as identify the magnitude and prevalence of the issues identified.[194] To achieve this, Sandvig proposes that we develop tools that transform black box decision making processes into "glass boxes" that we can engage with. We advocate a user-centered approach to building tools to support algorithmic audits, one the focuses on curation audits at the user level.

Some researchers have already begun to examine ways in which social media platforms can develop effective "peer encouragement designs," to shape an individual's behavior based on interactions with their peers.[195] We propose to build from this work by examining ways in which peer consumption practices can influence individual choices around personal curation of content online. By giving users the opportunity to optimize their media feeds based on specific preferences (i.e. more long reads or fewer cat videos) and values (i.e. "mostly liberal" perspectives or "across the political spectrum" perspectives), then we can introduce some diversity in the way media is curated for different users.

This will alleviate some of the concerns we have over the potential for large social media platforms to exert monolithic decisions over how content is curated on their site. Rather than calling for the Facebooks of the world to take on the responsibilities of mass media curation, we'd prefer to see a diffusion of that responsibility, across the

---

[194] Sandvig, Christian, et al. "Auditing algorithms: Research methods for detecting discrimination on internet platforms." *Data and discrimination: converting critical concerns into productive inquiry* (2014).
[195] Eckles, Dean, René F. Kizilcec, and Eytan Bakshy. "Estimating peer effects in networks with peer encouragement designs." *Proceedings of the National Academy of Sciences* 113.27 (2016): 7316-7322.

users who are on these sites. A personal media dashboard would give users the opportunity to exert greater agency over the information that they are exposed to.

Of course, this is no silver bullet solution to many of today's most pressing problems related to online content curation and civic discourse. Research has shown that we tend to self-segregate along ideological lines on social media, driven in large part by users' preferences for seeing content that aligns with their pre-existing beliefs and worldviews.[196] If we give users more decision making power over content curation, we run the risk of further fueling the propagation of misinformation, filter bubbles and biased reporting online. However, by giving people the opportunity to adjust and reflect on the outcomes of various personal preference settings, we create an opportunity for individuals to conduct a personal audit of their media consumption practices online.

One of the many challenges of this intervention is determining the factors that prioritize what content a user could see and designing a system that allows a user to experiment in a way that is understandable and user-friendly. This is not merely a technical problem, but a social and political one, involving debates over what aspects of media consumption are most important for citizenship. In order for this technical intervention to push us in the right direction, we will need to accompany it with broader cultural campaigns that nudge people towards embracing the diverse society we live in today.

In his examination of anti-facist media campaigns during World War Two, The Democratic Surround, Stanford historian Fred Turner documents the ways in which Americans were forced to wrestle with the plurality of American life in the context of massive museum installations such as "The Family of Man."[197] It is possible to imagine contemporary cultural campaigns that encourage people to encounter the wider world, beyond their comfort zone, in ways that get at the root of challenges we face today in

[196] Bakshy, Eytan, Solomon Messing, and Lada A. Adamic. "Exposure to ideologically diverse news and opinion on Facebook." *Science* 348.6239 (2015): 1130-1132.
[197] Turner, Fred. *The democratic surround: Multimedia and American liberalism from World War II to the psychedelic sixties*. University of Chicago Press, 2013.

the era of “fake news” and polarized civic discourse.[198] Similar cultural efforts could be central today if we ever hope to nudge people towards healthier media consumption habits with personal curation tools.

While personal curation tools may help us mitigate the monolithic influence of mega-platforms over curation, it won’t solve all the challenges we face with regard to free speech online. We would still benefit from having a bird’s eye view into how decisions are made about whose voices are amplified and silenced on social media sites. This involves understanding how community governance guidelines are developed and deployed to police speech on specific platforms. Community governance of speech is an extremely challenging task, one that sites like Facebook, Reddit and Twitter have been grappling with for many years. Historically, attempts to mitigate the dissemination of hate speech and harassment on these sites have been met with fierce resistance from free speech advocates, who characterize any proactive attempt to mitigate problematic content as censorship or a sell-out to advocates of political correctness.

However, as Alice Marwick argues, as long as we consider moderation of content to be censorship, then the voices of minority and marginalized populations will continue to be overwhelmed by aggressive interlocutors from the majority.[199] At the same time, earnest efforts to foster productive debates online can sometimes prove counterproductive. For example, research has shown that people tend to strengthen, not moderate, their perspective when presented with an alternative viewpoint on a given issue.[200] Developing effective ways to moderate content is not always a straightforward task. In light of these challenges, there are a growing number of researchers who are developing tools and methods to support online communities in running their own experiments on the effects of novel moderation practices.

---

[198] "Fake news is a red herring | World | DW.COM | 25.01.2017." 25 Jan. 2017, http://www.dw.com/en/fake-news-is-a-red-herring/a-37269377. Accessed 28 Feb. 2017.
[199] "Are There Limits to Online Free Speech - Data & Society: Points." 5 Jan. 2017, https://points.datasociety.net/are-there-limits-to-online-free-speech-14dbb7069aec. Accessed 28 Feb. 2017.
[200] Nyhan, Brendan, and Jason Reifler. "When corrections fail: The persistence of political misperceptions." *Political Behavior* 32.2 (2010): 303-330.

Nathan Matias has designed a project called Civil Servant, which aims to equip online communities with the tools necessary to conduct their own governance experiments, and to translate insights from those experiments into practical community governance policies online.[201] More work should be done to help communities carry out this kind of experimentation, as well as disseminate the knowledge that is generated from them.

We wish the problem of platform centralization and the power dynamics associated with it were as simple as the thorny technical problems the projects discussed here are wrestling with. Instead, we believe that protecting the future of speech online involves not only these ambitious experiments in decentralization, but the cultivation of an ecosystem of competing publishing platforms, diverse in governance strategies, interoperable and connected by a diversity of federated clients. We hope that those most concerned with the potential of the network public sphere will support not only experiments with decentralization, but the legal, normative and technical work necessary for these types of projects to thrive.

[201] "CivilServant." https://civilservant.io/about_us.html. Accessed 28 Feb. 2017.