Axis of Resistance:
Democracy and the P2P Technologies of Cyberspace

Darrell Whitman\textsuperscript{a} and Toya Milano\textsuperscript{b}

\textsuperscript{a} Independent scholar and community activist living and working in the San Francisco area. E-mail: whitmandarrell45@gmail.com
\textsuperscript{b} Communications technology specialist and political activist who is also living and working in the San Francisco area.

Journal of Global Faultlines/ Volume 1/ Issue 1/ September 2013, pp. 136-150
Published online: 10 October 2013.

To cite this article:


PLEASE SCROLL DOWN FOR ARTICLE
Technology has always been important to politics because it helps define the capacity to interact and share political relationships. However, technology by itself is not political until someone chooses to employ it for political purposes. Electronic media technologies are among those technologies with the greatest potential in the modern era to be political because they are the primary means through which people gain information and exchange ideas, which in turn become political either by shaping political beliefs or by contributing to political action. Of these new media technologies, computers and the internet have proven the most political as they have insinuated themselves into almost all areas of mass communications and now represent the primary means through which global communications of all kinds are exchanged.

Beginning even before the so-called “Arab Spring”, the internet was gaining critical notice for the way that it influenced political action beyond national borders. Yet, while social media, like Facebook and Twitter have become ever-present tools for political organizing and transmitting real time political information, other communication technologies have grown to be equally important but far less well known. Axis of Resistance is offered as an introduction to one of these “other” technologies, known as “peer-to-peer” (P2P) networking, asking whether and to what extent it influences the democratic nature of the internet and offers an axis of resistance to the efforts of governments and corporations to control this essential form of exchange. In some cases, P2P technology appears to enhance democratic potential because it allows for unmediated interpersonal exchanges. However, that potential is contested and remains substantially under developed, and P2P technologies also reflect rather than replace other critical forms of political discourse that may or may not be democratic in character or effect. One of the more interesting applications of P2P technology has been in the creation of virtual currency, with Bitcoin being the most developed and widely used. At the moment, the democratic virtues of Bitcoin are rather murky in that while it appears to contradict the traditional control of governments over currency, it also is slowly being captured for the Capitalist marketplace. Who manages it and for what purposes will ultimately determine its democratic credentials, but it has opened a space for a serious discussion of how the internet and P2P technology may at some point displace corporate control over global economics.

* Dr. Darrell Whitman is an independent scholar and community activist living and working in the San Francisco area. E-mail: whitmandarrell45@gmail.com
Toya Milano is a Brazilian communications technology specialist and political activist who is also living and working in the San Francisco area.
In discussing P2P technologies and the contest for control of the internet, this writing draws on the work of cultural-political theorists, and particularly Robert McChesney (1999, 2013), who are attempting to grasp how this technology of the 21st Century influence democratic participation. As will be apparent, there is a strong debate among theorists (Castells 2012) as to just what internet communications mean and how they “interfaces” with other forms of democracy. The threads of this debate appear as a subtext throughout this writing, pointing to an inherent contradiction in the way that the internet on the one hand is promoted by governments and corporations, while at the same time governments and corporations are attempting to restrict how the internet can be used. Ultimately, these authors believe that this contradiction will be resolved, as are all contradictions in political systems are resolved, by the historical context within which the contradiction exists, with a growing paranoia by governments and corporations over their seeming loss of control to a profound desire by people globally to have a meaning role in the conditions that touch upon their lives, and particular with regard to their ability to share information openly with family, friends, and associates.

Background – the design of P2P technology

Many of us use P2P systems without recognizing them as such. The popular Skype internet telephone system, instant messaging, online chat networks, and other widely-used file-sharing programs, such as Gnutella and Ignite all employ P2P technologies. What P2P stands for are forms of computer software that facilitates access to decentralized and distributed computer network in which individual nodes in the network (called "peers") act as both suppliers and consumers of resources. In this way, P2P networks interconnect peers directly to other network participants without any centralized server, and these connections are made possible by the sharing between peers of encrypted connections, meaning that without that encryption another "peer" cannot access the information being shared. The process is made possible by a File Transfer Protocol (FTP), in which the client and server programs are distinct: the clients initiate the transfer and the servers satisfy these requests. P2P networks generally use some form of a virtual “overlay network” on top of the physical network topology, where the peers form a subset of nodes in the physical network. Data is then exchanged directly over the underlying TCP/IP network but at the application layer peers are able to communicate with each other directly via the logical overlay links. Overlays are then used for indexing and peer discovery, making the P2P system independent from the physical network. Depending on how the peers are linked to each other within the overlay network, and how resources are indexed and located, networks are classified as either unstructured or structured or as a hybrid between the two. This contrast to centralized client-server models, such as those used in internet commerce, that require that peers request access to resources provided by central servers.²

While the technical details of P2P networks can be dense for those of us who aren’t computer engineers, the basic idea that P2P exchanges are democrat comes from the way that these networks offer enhanced privacy and protect information exchanges from the prying eyes of governments and corporations. However, while P2P networks do enhance privacy by creating direct connections between users, they also require considerable management to ensure their integrity, which in turn requires a cooperative and mutually supportive relationship between users. For example, anonymity, which is the primary
strength of P2P transmissions, requires the use of carefully constructed encryptions that protect the point of P2P connection from being randomly accessed. These encryptions are much more than the typical password that most people assume provides them security, and knowledgeable P2P users spend considerable time constructing encryption codes that are difficult to decipher. Sharing such an encryption with another user is a question of trust, and trust is the democratic touchstone of P2P networks. Unfortunately, trust alone is not sufficient to protect the integrity of P2P networks, as these networks are vulnerable to disruptions by viruses and malware at the point where individual peers connect to a non-P2P network. Thus, participating in a P2P network implies a higher level of vigilance in protecting against these intrusions to avoid inadvertently transmitting a computer virus or malware to an unsuspecting peer during the file sharing process.

As with all systems of technology, P2P systems are always under development in an effort to overcome its vulnerabilities and limits. As people join P2P networks they are invited to become part of this development process by sharing experiences about their P2P network use. This sharing provides the basis for a virtual democratic community with opportunities to acquire democratic skills, take leadership roles, and advocate for change on the basis of this virtual democracy. Participation in P2P communities comes with the additional incentive in that the value of a P2P system increases with the number of users, which in turn encourages P2P network members to recruit new members and P2P developers to find ways to make a P2P system more accessible. In this way, a P2P network has the potential to become a collective enterprise, with shared language and concerns for protecting a P2P system, and a sense of personal investment for P2P network members. One of the most successful early P2P networks was Napster, which allowed its members to exchange music files over the Internet for free. Unfortunately, Napster generated considerable opposition from the music industry which, rightly or wrongly, believed that the music file sharing was reducing demand for its products. With a resort to Capitalist property law, the industry finally shutdown Napster as a P2P network, but the millions of loyal Napster came away from the experience with a sense of the democratic possibilities of P2P networking, generating a built-in receptive audience for the P2P ventures that followed.

**Cyber warfare and the fight for democracy in cyber space**

The basic idea of a system of electronic communications that would directly link users is at least a half-century old. In the beginning, it did not have a global or even national reach, but was confined to small networks that were linked through telephone communication systems. Beginning in the early 1980s, potential commercial value of the internet pushed development of a much larger system of interconnections that could broadly reach to diverse communities of potential users, which led to the creation of the “world-wide web” by a university-based group of researchers organized as the World Wide Web Consortium (W3C), which led to a global system of internet exchange. Thus, the evolution of the internet moved from viewing it as a research tool to developing it as a commercial hub redefined how it would develop and for what purpose.

Once the internet became established as a central feature in everyday life, questions about its effects on democracy began to be raised. These questions were commonly answered by opining that the internet could/would increase democracy by
providing a space within which ideas could be disbursed to wide audiences and invite wide participation. On closer examination, however, there was a considerable gap between democratic potential and democratic realization because, as Robert McChesney recently observed the internet exists within a Neo-liberal Capitalist system that is inherently hostile to any use of the internet that does not contribute to its potential for generating profit. What McChesney and other critical cultural-political theorists are saying is that any consideration of democracy in cyber space must account for how democracy is affected by the control of Capitalism over the internet itself. In this context, the fight between governments, corporations, and political activists to control cyber space becomes a war to control the technology that creates it.

The war now raging in cyber space is rarely visible to the average person, and even those who are regular users of the internet. Recently, however, the public got a rare look inside this war through documents leaked by Edward Snowden, which reveal how in 2011 U.S. intelligence services carried out 231 offensive cyber-operations, including a $652 million program code-named GENIE in which a staff of 1,870 U.S. computer specialists broke into foreign computer networks and put them under surreptitious U.S. control. According to the documents, the U.S. covertly inserted sophisticated malware into computers, routers and firewalls on tens of thousands of machines every year, and had plans to expand those numbers into the millions. There was no information about what kinds of computers were targeted, but most of those who use computers understand the implications of GENIE, whether or not their computers were targeted, and the knowledge that GENIE exists will have a chilling effect on how they use our computers in the future. The fact that the U.S. government has invaded and manipulated computers from a remote location means that it is willing to violate international norms regarding cyberspace, if not laws, and ignore privacy rights in the pursuit of what the U.S. government defines as its national interests.

While cyber warfare is poorly understood public, it has serious consequences, and not just for its intended targets. For example, in 2009, the U.S. and Israel collaborated in the development of Stuxnet, a computer worm that was unleashed in 2009-2010 on Iran intended to destroy Iranian nuclear centrifuges. Unfortunately for many internet users, Stuxnet escaped from the control of its creators and spread through the world-wide web to infect millions of personal computers, revealing the quixotic nature of how the internet actually works and the lack of concern that governments have for the collateral damage that these attacks may cause. However, once revealed public knowledge of this war and its consequences for their personal privacy and interests undermines the public trust in government, which explains the almost hysterical reaction of governments to the disclosure of information about its activities in cyber space.

In some ways, the present cyber war orchestrated by governments reflects the decline of the old nation-state system that has become evident as Neo-liberal Capitalism has spread globally. Modern governments are at best complex organizations with internal bureaucratic dynamics that do not lend themselves to sophisticated and fast-changing circumstances, such as those present in the dynamics of cyber space. This is forcing governments to increasingly rely on collaborations with non-state actors, which weakens government control over this cyber war. Edward Snowden is an example of that weakness and how these collaborations introduce challenges to government control. Snowden was not an employee of the U.S. government, as was Chelsea Manning, and lacked the implicit loyalty and legal burdens that would come with being a government employee. Thus, the
barriers to Snowden’s release of documents occurred in the context of Snowden as a citizen concerned with crimes against the public interest, rather than Snowden as an extension of the culture of government secrecy. It is also the case, that governments now rely on a cadre of computer specialists many of whom have grown up within a culture that encourages, rather than discourages, collaboration and disclosure and which has always included certain anarchist tendencies. The reaction of the U.S. government and other governments to the Snowden affairs thus reflects a deep anxiety that only extreme punishments can counteract this culture.

Another weakness in government efforts to control cyber space comes from the nature of P2P technology, which allows for direct information exchanges that are nominally outside the control of governments. Anonymous, a loose confederation of international computer software experts represents perhaps the greatest threat because its membership is composed of highly sophisticated experts who have thus far managed to escape identification while engaging in a cyber war of their own. A visit to any social website where Anonymous posts its messages provides some idea of their politics and how they work.9 The scope of cyber attacks launched by Anonymous is impressive, including an attack on Israeli government sites and banks in retaliation for Israeli attacks on Palestinians in Gaza. However, the greater part democratic work of Anonymous has been to act as a facilitator for various radical groups that challenge government environmental and police practices that are shared globally, creating networks of resistance among groups involved in different struggles. At the same time, because membership is anonymous, Anonymous is exposed to eventual infiltration by individuals and groups that have less than democratic intentions.

The obsession of governments, and particularly the U.S., with security and control over cyber space has had serious consequences for individuals caught up in this cyber war, and generated a push back from within the cyber community. In generating victims like Aaron Swartz,9 who simply sought to challenge narrow interpretations of what should be protected, Chelsea Manning,10 who believed it their civic duty to disclose wrongdoing by government, and Julian Assange11, who broadly challenged the anti-democratic practices of governments everywhere, governments have widened the gulf between themselves and their citizens. In turn, this paranoia has been reflected inward and begun to infect critical functions of government, such as the legitimacy of elected representation and the ability of government employees to function where elected representatives and government employees become targets of surveillance. From the author’s direct experience, the U.S. government informed its employees in 2012 that they would be terminated if they accessed the WikiLeaks even on their personal computers, and staffers with at least one U.S. Congressperson have reported having their offices bugged and telephones tapped by other federal agencies.

The revelations from the Snowden affair are likely to continue as the massive collection of documents sorts itself out. However, from what is already known, and from has previously been posted by WikiLeaks, the conduct of intergovernmental relations has been seriously disrupted. Further, the revelations have increasingly defined a new global fault line with governments and corporations estranged from the publics they wish to influence, and organizations of so-called “hacktivists”, which is a pejorative term used in government circles to stigmatize cyber-activists.12 In response, so-called hacktivists have formed international links to push back against government invasions of the internet. Some argue that these revelations are “changing statecraft for the better”, in that open
internet access ensures that the workings of government do not remain behind closed doors. However, to the extent that Robert McChesney’s argument that Capitalism is undermining internet democracy because a shared truth, the fault line that is appearing is also likely to represent a new front in the struggle against Capitalism itself.

While it is quite clear that the intergovernmental cyber war will continue and intensify as computer technology comes to dominate modern warfare and the global economy. However, it is far less clear that there can be any winners in this intergovernmental cyber war or that this intergovernmental war can be confined to state-to-state combatants. Recently, stories have appeared in the media reporting efforts by governments to penetrate the security systems in everyday use on the internet by cracking the encryption codes that have been created to protect personal privacy, which when coupled with the ongoing effort of corporations spy on consumers, paints a picture of a convergence between governments and corporations on the proprietary treatment of cyberspace as wholly theirs. This unmasking of intentions by actions reveals how little democracy matters in the Neo-liberal reconstruction of the world, and how the line between governments and corporations has become thin to the point of disappearing. Yet, so long as governments and corporations cannot control cyber space as dynamic and evolving sets of technological and human relationships, the possibilities for democracy in cyber space will remain.

### Bitcoin and the struggle for economic democracy in cyber space

The struggle for political democracy in cyber space has an economic ally in the struggle to develop a virtual currency that lies beyond the control of governments and corporations. *Bitcoin*, which is the most recent iteration of this effort, offers both promise and caution as it is both more and less than the claims made by its advocates. Yet, to the extent that economics lies at the heart of systems of political economy, *Bitcoin* offers interesting insights into how Neo-liberalism attempts to capture all forms of economic activity within its embrace.

Functionally, Bitcoin operates through a P2P program casually created by a Japanese software engineer in the 1990s for the limited purpose of testing the viability of a virtual financial market in Cyberspace. The program may have languished in obscurity, except that it attracted the attention of Amir Taaki, who describes himself as a crypto-anarchist, which provides a running account of developments concerning virtual currencies such as Bitcoin. While the general political flavor of Bitcoin is decidedly anarchist, it has attracted a wide following among both leftist groups, who see in it the potential to disrupt and potentially displace existing systems of economic exchange, and mainstream capitalists who are intrigued by the way that it presents new opportunities to expand global commerce. However, according to *Bitcoin Magazine*, the official source of information about *Bitcoin*,

Bitcoin is a new kind of digital currency originally created by Satoshi Nakamoto in 2009. Of course, the idea of digital money is not new; for many years now we have had Paypal, credit cards, WebMoney dollars and even the virtual gold in video games like World of Warcraft. What makes *Bitcoin* different from anything that came before it, however, is that *Bitcoin* exists only on the internet, and is not
dependent on any government or corporation. Instead, the Bitcoin system is collectively maintained by thousands of computers owned by various individuals around the world.\footnote{9}

Seen through its own lens, Bitcoin appears to be a currency that is democratic in that it is wholly under the control of those who participate in the Bitcoin P2P network. On closer inspection, that claim does not entirely stand up as Bitcoin has over the last 2-3 years moved closer to a corporate model of governance and closer to government control over the network. For example, as an organization, Bitcoin is presently consumed with an effort to establish itself as a viable currency for internet commerce, which has led it to evolve an elaborate structure of governance that includes a Bitcoin Foundation, initiate a Bitcoin Gambling enterprise, and seek legitimacy from U.S. federal regulators. In fact, Bitcoin now appear quite mainstream and has gained the support of Capitalists who see in Bitcoin an opportunity to conduct international transactions outside of traditional venues and thus avoid various transaction costs. Further, as Bitcoin itself acknowledges, the possibility for government regulation exists because the “miners”, who manage Bitcoin exchanges, can be identified regulated and taxed. All of this raises the question of whether Bitcoin has any actual potential for democratizing economic exchange, or whether it is merely the newest in a string of Neo-liberal initiatives designed to further remove Capitalist economic activity from government control. To answer this question, we need to look back on the development of currency itself.

While the emergence of Bitcoin as a viable virtual currency is a direct challenge to government control over money, it follows from a history of Capitalism developing new forms of currency that allow currencies to adapt to Capitalist interests. Historically, paper currency emerged in the 19th Century as a response to the development of internal national capital markets that required forms of wealth that were easily transferred and collected. David Ricardo, the noted Capitalist political economist of that time, pointed out that a system of financial exchange based on paper money was inherently unstable because it invited manipulation by capitalist bankers and governments who would periodically debased the value of paper money for their own interests.\footnote{8} This led Ricardo to advocate for a currency tied to gold, a commodity that had an agreed, wide-spread inherent use value and as the 19th Century proceeded with reoccurring economic crisis tied to paper currency, capitalist economists and governments seized on Ricardo’s idea to create the gold and later the silver standard to protect the wealth of Capitalists and the legitimacy of Capitalist governments. Of course, the assumptions of the 19th Century did not hold into the 20th Century, and the process of evolving a new monetary system was repeated with various schemes that attempted to somehow create permanency in a monetary system that was tied to a dynamic economic system.

Most recently, in 1971, all previous efforts at fixing the value of currency to a commodity, such as gold or silver, were abandoned in favor of a paper currency whose value was tied to the ability of the U.S. government to command its value in various ways. The development of this “dollar standard”, however, carried with it inherent contradictions as it worked only as long as the U.S. maintained control over the global financial system, which ensured that the U.S. would act as the world’s “policeman”, which became a very expensive proposition as the cost of foreign economic and military adventures mounted and the U.S. economy aged and became less competitive in the global marketplace. Arguably, the adoption of Neo-liberalism within the U.S. in the 1970s
represented an acknowledgement that the dollar standard was no longer viable and that managing the global economy required that power over financial transactions be passed to private banking interests and the corporations they served.

As before, by the early 1990s, changes in the global economy demanded a reformulation of the Capitalist system. One of the changes that generated this demand was the emergence of the internet and global communications technology that allowed for the rapid and largely unregulated exchange of value in the global Capitalist marketplace. The truth of this can be found in the way the 1998 Asian currency crisis, which was triggered by the internet speculation of a single currency trader, nearly sank the international financial system. Evidence that the problem was not solved by any reform of the international economy surfaced during the U.S. recession of 2000-2002, known as the bursting of the Dot.com bubble, which came from speculation enabled by complex computer trading programs that concealed the risks involved in various investments. Then, in the 2007-2009 financial panic that led to the 2009-2013 global economic crisis the problem of unregulated global internet trading and investment exploded, further eroding the credibility of government management of currency and the global economy.

The appearance of Bitcoin in the midst of the series of crises that began in 2007-2009 offered Bitcoin a prominent role during the Cyprus crisis in early 2013. When the decision was taken by the European banks to seize personal deposits to repay a national debt, bank depositors in other parts of Europe rushed to find a secure haven for their own bank deposits and found it in Bitcoin, which doubled in value almost overnight. The value of Bitcoin has since retreated to a more normal range, but the lesson has not been lost on Capitalists who have always wary of the intentions of governments, as was David Ricardo almost two centuries past. Their embrace of Bitcoin, however, is not necessarily a permanent marriage, but may represent something more of an infatuation with the prospect of escaping government control while maintaining Capitalist control of the value of currency.

Whether or not Bitcoin becomes captive to Capitalism, the emergence of the possibility of constructing a system of exchange through P2P technology suggests that a more democratic economics may be possible. This possibility is implicit in the way that governments acknowledge the importance of their control over the economics of cyberspace as a matter of national security. Yet, once unleashed the power of Neo-liberalism may prove to be the contradiction that undermines these efforts by governments by pursuing any means to avoid effective government regulation, which to some extent it already has. In that way, the insinuation of Capitalism into the Bitcoin system may ultimately prove to be the undoing of Capitalist governments, proving the functionality of an unregulated virtual currency while also opening the door to future runs on what would become an unstable world of national paper currencies.

P2P systems and the future of the Axis of Resistance

The remarkable feature of P2P cyber systems is their ability to level the political and economic playing field in which they operate. Banks and governments that were once seen as all powerful and all knowing have shrunk considerably in status as the global economic crisis of Capitalism continues to attack the middle and working classes. Similarly, in the battle for control over cyberspace it is governments who are losing out to the ability of
small groups of skilled and dedicated cyber warriors to disrupt and disarm them almost instantaneously, and even where they do find small victories governments have become increasingly dependent on the expertise of those have become the subject of its attacks.

As Karl Marx argued some 150 years ago, as material conditions change they change the terms of politics, newly empowering those who can access and use these new circumstances and disempowering those who fail or cannot adapt. Cyber technologies represent a material change in the organization of economic and political life in the modern era because they limit possibilities for monopoly control while increasing possibilities for broad popular participation. Access to the internet, and thus to opportunities to know and act, has spread rapidly and has reached into the far corners of the globe and into areas where governments have only limited powers of control. In this way, centralization is giving way to decentralization and new groups are appearing with the ability to share information through P2P technologies which previously was mediated and thereby controlled by governments and corporations. As these P2P technologies spread and engage ever larger audiences, the question is less whether democracy in the world of cyber space can grow and more how it will develop.

There are three possibilities for P2P systems and the future of the axis of resistance: they can become captive to Capitalism and assist in the evolution of Capitalism; they can be compromised and disrupted, leading to further and more intense confrontations with Capitalism; or they can steadily displace the architecture of control developed by Capitalist governments and corporations. Looking at these alternative futures, none can be fully discounted because the future of P2P systems has yet to be determined either technologically or politically. There are, however, characteristics that can be extrapolated from the present and projected into the future as a guide to what elements might prove decisive. As was noted earlier, current P2P technologies have their vulnerabilities and considering the interest that they have already attracted more vulnerabilities are likely to appear. These vulnerabilities themselves have attracted the attention of P2P advocates and contests over P2P vulnerabilities are likely to be resolved in favor of advocates simply because they have the stronger motive and organization to adapt these technologies to make them less vulnerable. Ultimately, the outcome of the cyber war that P2P technologies have generated depends on the politics of its defenders, which are many, complex, and overlapping.

Presently, P2P systems and the axis of resistance are dominated by political anarchists in Europe and North America, most of whom who believe that resistance alone is sufficient to guarantee a democratic victory. Given their experience with Capitalist governments and corporations, that belief is understandable. But the jury is still out on whether these Euro-American political anarchists can by themselves account for the democratic impulses that are being realized around the globe by other groups with different political experiences and perspectives. Representative of this anarchist perspective is Amir Taaki, the co-founder of Bitcoin and a self-identified crypto-anarchist. Taaki’s view is that, “We need a world of entrepreneurs and small businesses. Creating your own business to challenge the power of a corporation is the most subversive thing you can do.” Taaki mixes his pro-Capitalist rhetoric with other anti-Capitalist observations, such as “Workers will never be free. Bosses will always rule,” and “Employees, don’t be slaves! The boss will always reap the rewards of your work. You will never own the products of your work. You will never own your dignity. You will always be
owned”, leaving the impression that he has not clearly thought out the political implications of Bitcoin or P2P technology.

While Taaki spoke for the aspirations of many who want a sense of personal freedom, other cyber warriors have taken a wider political view of cyber space. Chelsea Manning, U.S. Army soldier whose decision to release classified documents is credited with helping to end the U.S. war in Iraq, took a very different approach to his act of resistance, observing:

I wanted the American public to know that not everyone in Iraq and Afghanistan are targets that needed to be neutralized, but rather people who were struggling to live in the pressure cooker environment of what we call asymmetric warfare. After the release I was encouraged by the response in the media and general public, who observed the aerial weapons team video. As I hoped, others were just as troubled - if not more troubled - than me by what they saw.21

The contrast between Taaki and Manning is striking not only in focus, but also in the way that each has brought to their views the particular characteristics of their life experiences: Taaki has devoted himself to the technological question involved with P2P networks, while Manning used cyber space to illuminate a world often beyond the apprehension of ordinary people. Ultimately, while Taaki’s views are mixed with admirable motives, they also expose a potentially fatal innocence about the politics of P2P technology that require far more organization and discipline than Taaki is unable to recognize, but which Manning does. The future for P2P technology will be democratically limited if it only serves to satisfy a sense of personal independence rather than actual democracy, which has a much larger agenda. That larger democratic agenda may be written by those outside of Europe and North America who are bringing already well-formed political experiences with Neo-liberal Capitalism and alternative forms of political organization that have roots beyond the cyber space community. If it is, the capture of P2P technology by Capitalism is unlikely as control of cyber space will be subordinated to the outcome of the war against Capitalism, with Capitalism’s instability and tendencies toward crisis limiting its power to control.

In spite of Taaki’s representations otherwise, governments are already moving to regulate Bitcoin with the cooperation of Bitcoin managers through FINCEN, which appears as a Neo-liberal arrangement that regulates Bitcoin exchanges, and provides for taxation of transactions but does not attempt to regulate Bitcoin possession.22 Thus, as Bitcoin drifts into the sphere of Neo-liberal influence it is less and less likely to act as anything other than an illusion of individual independence defended by people who are focused on economic opportunity and security rather than political democracy. But Bitcoin is only one of a growing number of P2P networks which, as Manuel Castells argues, are creating a network society where national borders disappear, along with national control.23 Drawing on observational research covering the global Occupy Movement, Castells found that cyber space is crowded with democratic users who not only exchange information, but who are also engaged in constructing common language and political analyses across traditional barriers of geography, language, and culture. His argument reaches beyond cyber space to claim that the ability to connect through electronic networks has undermined, and in some cases displaced, the ability of governments to manipulate perception and control behavior. In fact, Castells concludes that the social movements created in cyber space represent a new form of cultural politics
destined to defeat global Capitalism. Whether or not Castells argument eventually proves itself true, P2P technologies can claim an important role in providing an intimate space within which a new global politics can flourish. Because they are “peer-to-peer”, these technologies reestablish the value of direct personal communications in the formation of useful and powerful politics.

Conclusions

While the debate and contests over the internet continue, the final question is what would democracy in cyber space look like? Created in 2006, Twitter provides an example of a use of cyber space with democratic overtones. It offers social networking and micro-blogging using a P2P technology which allows registered users to determine who receives their posts.24 Currently, Twitter claims more than 200 million users who make more than 400 million posts each day. Twitter is unique in that it is presently part of a system of exchange of real-time video and comment between political activists locally, nationally, and globally, creating a sense of participation in events and discussions that would otherwise appear as arms length, after-the-fact communications. As P2P technology and cyber space evolves, other and even more powerful forms of communication will emerge that will further enhance the democratic potential of cyber space.

Yet, there is a dark side to the free-wheeling participation in cyber space communications. As Twitter recently demonstrated, open and unregulated access comes with no guarantees for the quality of participation, as racist posts flooded Twitter following the nomination of an Indian-American as the new Miss America.25 What this episode demonstrates is that standing alone democracy can only open doors to participation in public life and thereafter the nature of public life is determined by the deeper cultural politics that shape it. It is an open question as to how a popular democratic cultural politics of toleration can emerge in cyber space with all its limits on direct experience.

Democracy in cyber space is the beginning not the end of the process of creating a new and sustainable politics of inclusion and much attention needs to be paid to how democracy in cyber space is constructed, which implies that the construction itself must be democratic. The good news is that there are legions of sophisticated cyber space users among the generations born after 1980 into the age of the internet. The bad news is that Neo-liberal Capitalism has deployed powerful ideological messages about self-interest and individualism that are barriers to the politics of inclusion. Thus, the real axis of resistance is at one pole technological and at the second pole ideological, and only where these two poles meet can be the possibility for a genuinely democratic cyber space.

Notes

1 “P2P” refers to peer-to-peer internet communication systems that occur outside of a mediated computer programs.
2 Schollmeier, R., “A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications”, *Proceedings of the First International Conference on Peer-to-Peer Computing*, IEEE, Detroit, MI.
8 See, e.g., Twitter, available from <https://twitter.com/YourAnonNews>.
9 Swartz, John, 2013. Internet activist and creator of RSS, is dead at 26, an apparent suicide, The New York Times, 12 January, available from <http://www.nytimes.com/2013/01/13/technology/aaron-swartz-internet-activist-dies-at-26.html?pagewanted=all&_r=0>. As a teenager Aaron Swartz helped develop code that delivered ever-changing Web content to users and later became a steadfast crusader to make that information freely available, was found dead at the age of 26 in January 2013, an apparent suicide. In July 2011, Schwartz was indicted on federal charges of gaining illegal access to JSTOR, a subscription-only service for distributing scientific and literary journals, and downloading 4.8 million articles and documents, nearly the entire library. Charges in the case, including wire fraud and computer fraud, were pending at the time of Mr. Swartz’s death, carrying potential penalties of up to 35 years in prison and $1 million in fines.
10 Abrams, Floyd, and Benkler, Yochai, 2013. “Death to Whistleblowers?”, The New York Times 13 Mar 2013, available at <http://www.nytimes.com/2013/03/14/opinion/the-impact-of-the-bradley-manning-case.html>. In this Op-Ed piece in the New York Times, the authors decry the potentially lethal legal attack on Manning for releasing government documents concerning revelations, including American forces’ complicity in abuses by Iraqi allies, underestimation of civilian casualties and abuses by contractors, observing that “If successful, the prosecution will establish a chilling precedent: national security leaks may subject the leakers to a capital prosecution or at least life imprisonment. Anyone who holds freedom of the press dear should shudder at the threat that the prosecution’s theory presents to journalists, their sources and the public that relies on them.
11 Assange and WikiLeaks have become international icons as symbols of resistance to government censorship. Assange studied physics and mathematics at the University of Melbourne. He wrote Strobe, the first free and open-source port scanner, and contributed to the book *Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier*. Currently, he is in involuntary residence at the Ecuadorian Embassy in London, resisting extradition to Sweden, and by inference to the U.S., where he like Bradley Manning would potentially face the death penalty for releasing official government secrets.

14 Clark, Richard A., 2012. Cyber War, Ecco, New York. As the former U.S. National Security Advisor cautions, there are very real cyber threats to battlefield computers and in the form of denial of service attacks on government computers.


16 Crypto-anarchism is a form of anarchism that grew out of the communications revolution that created Cyberspace, which recognized as early as 1992 that communication technology would shatter the comfortable control by governments over information and exchanges between individuals. See, Timothy C. May, The Crypto Anarchist Manifesto http://www.activism.net/cypherpunk/crypto-anarchy.html, and Mihail Issi, the founder of Bitcoin Magazine [http://bitcoinmagazine.com/]


References


