Blockchain Empowers Social Resistance and Terrorism Through Decentralized Autonomous Organizations

Author(s): Armin Krishnan

Source: *Journal of Strategic Security*, Vol. 13, No. 1 (2020), pp. 41-58

Published by: University of South Florida Board of Trustees

Stable URL: https://www.jstor.org/stable/10.2307/26907412

Journal of Strategic Security

Volume 13 | Number 1 Article 3

Blockchain Empowers Social Resistance and Terrorism Through Decentralized Autonomous Organizations

Armin Krishnan
East Carolina University, krishnana@ecu.edu

pp. 41-58

Recommended Citation
Krishnan, Armin. "Blockchain Empowers Social Resistance and Terrorism Through Decentralized Autonomous Organizations." *Journal of Strategic Security* 13, no. 1 (2020) : 41-58.
DOI: https://doi.org/10.5038/1944-0472.13.1.1743
Available at: https://scholarcommons.usf.edu/jss/vol13/iss1/3

Blockchain Empowers Social Resistance and Terrorism Through Decentralized Autonomous Organizations

Acknowledgements

I want to thank the anonymous reviewers of the article for their encouragement, insights, and constructive criticism that has helped to improve the quality of the article.

Introduction

Blockchain Technology (BT) or Distributed Ledger Technology has entered the public consciousness. Cryptocurrencies such as Bitcoin have also sparked growing government concerns about potential negative social consequences of the technology, especially as it relates to facilitating crime and terrorism.[1] For example, Treasury Secretary Steve Mnuchin has recently declared that cryptocurrencies pose a national security threat, as malicious actors may use them to fund illicit activities.[2] Unfortunately, this narrow focus on money laundering in the growing national security debate of BT and other virtual currencies is not helpful in terms of understanding the true potential of blockchains or how this technology could change the organization and practices of social, civil, nonviolent and violent resistance to government and other authorities. Gene Sharp suggested that "nonviolent action is a generic term covering dozens of specific methods of protest, noncooperation and intervention. In all of these, the resisters conduct the conflict by doing – or refusing to do – certain acts by means other than violence."[3] These acts can range from political activism, to acts of civil disobedience, and to mass protests and strikes. What begins as nonviolent resistance may later turn into terrorism, rebellion, and revolution. Social or civil resistance is often leaderless and relies on voluntarism: individuals can choose to join a cause by participating in collective actions that signify resistance or by supporting resistance acts of others.

The Internet has become a powerful enabler of social resistance and hence a threat to authority due to its decentralized nature. John Arquilla and David Ronfeldt argued already in the 1990s that the Internet "disrupts and erodes the hierarchies around which institutions are normally designed. It diffuses and redistributes power, often to the benefit of what may be considered weaker, smaller actors. It crosses borders and redraws the boundaries of offices and responsibilities. It expands the spatial and temporal horizons that actors should take into account. And thus it compels closed systems to open up."[4] Arquilla and Ronfeldt claimed that the Internet encourages network organization and enables new modes of conflict centered on communications and networks.

Arquilla's and Ronfeldt's analysis from the 1990s was extremely prescient, considering the rise and weaponization of social media that has enabled

numerous digital insurgencies by pro-democracy movements that have threatened and have sometimes even overthrown established corrupt power elites in the color revolutions of the Arab Spring and in Ukraine. According to Eric Schmidt, the former Google CEO, and Jared Cohen, a former State Department official, "[t]here can be little doubt that the near future will be full of revolutionary movements, as communication technologies enable new connections and generate more room for expression."[5] They claim that technology will make revolutionary movements more efficient as activists around the world can exchange their ideas, as technology will provide more anonymity to them and as people can join and assist revolutionary movements with limited commitment and risk for themselves, "making revolutionary gestures permanent."[6]

This article aims to investigate how diverse social movements and resistance organizations can utilize BT to further their social, political, or criminal objectives. In particular, this article will explore how transparency advocacy groups, pro-democracy groups, hacktivists, revolutionary movements, as well as terror organizations, and even criminal syndicates can leverage BT and associated organizational innovations such as Decentralized Autonomous Organizations (DAOs). The article argues that BT and DAOs could change the dynamics of social or civil resistance, its effectiveness, and its resilience in the face of countermeasures by governments. It will also provide policy recommendations.

Part I: Cryptocurrency

Satoshi Nakamoto proposed BT in his White Paper in 2008, where he described Bitcoin as a "peer-to-peer version of electronic cash."[7] The White Paper forms the basis of Bitcoin and many other cryptocurrencies. Bitcoin likely emerged from the cypherpunk movement and its inventor(s) clearly intended it to offer an alternative to the global financial system that came close to collapse in 2008.[8] Due to its opposition to the fiat currency system Bitcoin is plausibly itself a form social resistance as many early cryptocurrency enthusiasts are not afraid to acknowledge. For example, VC entrepreneur Naval Ravikant suggested, "Bitcoin is a tool for freeing humanity from oligarchs and tyrants, dressed up as a get-rich-quick scheme."[9] Similarly, cryptocurrency developer Amir Taaki stated:

https://scholarcommons.usf.edu/jss/vol13/iss1/3
DOI: https://doi.org/10.5038/1944-0472.13.1.1743

"Bitcoins aren't a f… payment innovation… Bitcoins are a political project."[10]

Some Characteristics of Bitcoin

The Bitcoin blockchain is a decentralized digital ledger that updates in fixed time intervals according to a process called consensus. Bitcoin uses a proof-of-work algorithm that requires miners to perform complicated mathematical calculations that are energy-intensive and require specialized mining (ASIC) computers. Several Bitcoin transactions form a bundle or block and several blocks form a chain. The miners represent the nodes in the Bitcoin network, and they have to confirm any change to the encrypted ledger by adding or not adding a proposed new block. All nodes possess a complete copy of the entire blockchain, which includes all transactions since block 1. Anybody can connect a computer to the Bitcoin network to mine Bitcoin by making computing power available. Miners receive rewards in two ways: they receive a transaction fee in Bitcoin that the user can set (a high fee means fast transactions) and they compete over a block reward of currently 25 Bitcoin per block. The computer that is first to complete a block, which takes in average ten minutes, receives the block reward. The mining difficulty increases as the network grows over time. This means that miners have to commit more and more computing power and electricity in order to have a reasonable chance of getting the block reward. The transactions also contain a cryptographic hash or a digital fingerprint that is in theory impossible to forge. The proof-of-work algorithm makes it near impossible for a malicious actor to reverse transactions since the malicious actor would need to redo all the work from block 1 to the current block, which is prohibitively expensive. Hackers also cannot simply distribute a new block with fraudulent transactions that double-spend a Bitcoin, unless a majority of miners are cooperating in the attack, which is called a 51 percent attack.[11]

Users can interact with the blockchain through a digital signature or private key that gives them control over the record associated with that key. When a user installs a cryptocurrency wallet on a computer or mobile phone the wallet randomly creates a public and private key. The public key becomes the public address that allows a user to receive cryptocurrency. Possession of the public key does not enable a hacker to infer the private key due to asymmetric encryption. Transactions are time-stamped and are

in theory irreversible. More importantly, BT makes the existence of a trusted intermediary like an escrow or notary, typical for many business arrangements, unnecessary as all transaction are retained on an immutable public blockchain. In other words, the blockchain eliminates the need to trust any individual within a trusted network. William Mougayar asserts, "Trust can be coded up, and it can be computed to be true or false by mathematically backed certainty, that is enforced by powerful encryption to cement it."[12] The trustless nature of the blockchain and its ability to enforce any kinds of rules through the consensus mechanism makes the blockchain a revolutionary and potentially a socially disruptive technology.

Critics of Bitcoin have frequently dismissed the significance of the innovation of BT by calling Bitcoin and other cryptocurrencies worthless. For example, President Trump claimed that cryptocurrencies "are not money" and are "based on thin air."[13] Although Bitcoin has undergone many severe crises since its inception with massive price fluctuations, it has proven to be anti-fragile. After each crisis Bitcoin emerged much stronger than before, benefitting from network effects: The more user it has, the more valuable it becomes and the more valuable it is, the more users it will attract. Its main value proposition is its use-case of permissionless peer-to-peer value transfers and its guaranteed limited supply, capped at 21 million units. Up to now, most owners of Bitcoin and other cryptocurrencies use them merely as a speculative investment, although there are already some limited real-world applications other than financial speculation.

Bitcoin, Crime, and Terrorism

Criminal and terrorist organizations might be interested in cryptocurrencies because it might be more difficult for law enforcement agencies and counterterrorist professionals to track cryptocurrency assets.[14] Early on, criminals have turned to Bitcoin as a way of making anonymous payments. For example, Bitcoin was the standard method of payment for buying illegal drugs on the infamous dark web platform Silk Road, which Ross Ulbricht had launched in July 2010.[15] Silk Road processed sales worth 9.5 million Bitcoin out of 12 million in circulation between 2010 and 2012.[16] Hackers have used Bitcoin in ransomware attacks such as WannaCry, where a malware like CryptoLocker encrypts all

https://scholarcommons.usf.edu/jss/vol13/iss1/3
DOI: https://doi.org/10.5038/1944-0472.13.1.1743

data on compromised computers. The hackers then offer the encryption key in exchange for a specified amount of Bitcoin.[17] Not surprisingly, government studies and academic research regarding the dangers of BT have mainly discussed criminal and terrorist uses of cryptocurrency and money laundering. However, Bitcoin itself is not actually anonymous but pseudonymous: Bitcoin transactions are recorded with the sending and receiving wallet addresses that are visible to everybody on the public ledger.[18] Any transaction linked to a particular cryptocurrency wallet (a software or hardware that stores private keys) can be tracked and the owner may be unmasked by using special methods of analysis and computer forensics.[19]

Still, Bitcoin offers a couple of advantages to dissidents, criminals, and terrorists. First, a government cannot stop transactions or freeze crypto-assets as would be the case with regular bank transfers and bank accounts (unless a user holds the cryptocurrency in a cryptocurrency exchange account within the government's jurisdiction). Second, an individual can store a theoretically infinite amount of value in his head simply by memorizing a private key that gives access to funds on the blockchain. This makes cryptocurrency hard to confiscate and hard to enforce capital controls on, even if governments can arrest an individual or seize other physical assets.[20] Third, a resistance group can easily raise funds by accepting cryptocurrency donations from anywhere in the world and from anybody by simply by publishing their public cryptocurrency addresses on a website with no need to rely on third parties, such as front organizations and credit card companies or PayPal. For example, the Islamic State reportedly solicited donations by posting a Bitcoin address.[21]

Despite these advantages, numerous disadvantages have resulted in a slow adoption of cryptocurrency by terrorist groups. Major problems are the great volatility of crypto-assets, which creates organizational uncertainties, the reduced ability of terror leaders to exercise control over funds entrusted to agents, and the problem of exchanging crypto-assets back into fiat currencies.[22] A recent RAND study therefore found that "there is little indication that terrorist organizations are using cryptocurrency in any sort of extensive or systematic way."[23] In the future criminals and terrorists may turn to privacy coins such as DASH, ZCASH, and Monero, which have achieved important innovations such as anonymization through coin-mixing, the encryption of transaction values, and a 'zero-

knowledge-proofs' protocol where transactions can be confirmed without revealing the address of the sender or recipient on the blockchain.[24]

Part II: Decentralized Autonomous Organizations

It has been pointed out that leaderless organizations are much more resilient and sometimes more successful than hierarchical organizations. Ori Brafman and Rod A. Beckstrom argued that hierarchical organizations are like spiders: Cut their head off and they will die while leaderless organizations are like starfish: Cut a leg off and it will regrow and the cut-off leg may itself grow into a new starfish.[25] They observed "Decentralized organizations are…trickier to understand. In a decentralized organization, there's no clear leader, no hierarchy, and no headquarters. When a leader does emerge, that person has little power over others. The best that person can do to influence people is to lead by example."[26] Analysts have described jihadist organizations such as al Qaeda and the Islamic State as leaderless organizations that encourage others to take the initiative to advance a shared ideological goal.[27] In recent years, terrorism experts have noted the growth of lone wolf attacks and other forms of leaderless resistance. For example, George Michael has claimed, "[T]he increased frequency of these lone wolf attacks indicates a shift from terrorism by organized groups to terrorism by unaffiliated individuals."[28] There have been concerns over the online radicalization of individuals and the possibility of terror organizations providing virtual training in terror tactics to interested individuals, which may have facilitated this recent rise in lone wolf terror attacks. BT could add new dangers by enabling new forms of organization, of social resistance, and of terrorism. Decentralized Autonomous Organization (DAO) is a term that can describe this new model of a blockchain-based leaderless organization.

The Concept of the Decentralized Autonomous Organizations

As of 2019, there are two generations of blockchains: 1) the Bitcoin protocol and derivatives of it (blockchain 1.0), and 2) smart contract platforms (blockchain 2.0).[29] Particularly important for the further discussion are smart contract platforms. Ethereum is the first of its kind when it launched on July 30, 2015.[30] It enables programming hard rules into a blockchain for governing transactions. Ethereum is programmable money that allows two parties to enter a contract (via software) and that,

https://scholarcommons.usf.edu/jss/vol13/iss1/3
DOI: https://doi.org/10.5038/1944-0472.13.1.1743

for example, holds funds in escrow until objective conditions trigger a transaction. The most common smart contracts use today is the issuance and governance of unique digital tokens that are freely transferable and tradeable.[31] However, the most promising future application relates to the Internet of Things For example, a smart contract may govern the use of a rental car: If a rental car user makes a payment, the software can verify the payment on the blockchain and will then automatically unlock the car.[32] Furthermore, smart contracts can enable new forms of organization and new ways of cooperation that do not require any fixed hierarchical organizational structures. Smart contracts make it possible for a large number of unconnected contributors or volunteers to spontaneously enter into a collaborative arrangement and to form a leaderless organization.

The first experiment with a DAO for crowdfunding was a project by the Berlin-based blockchain company Slock.it.[33] The company intended the DAO to function as an investment vehicle for Ethereum-based software development projects. The DAO White Paper stated that a DAO "can be used by individuals working together collaboratively outside of a traditional corporate form. It can also be used as a registered corporate entity to automate formal governance rules contained in corporate bylaws or imposed by law."[34] The original DAO was thus a company without CEO or management that was based entirely on a community of developers, who cooperated by submitting proposals and making decisions via voting on the blockchain.[35] Slock.it issued Ethereum-based DAO tokens that anybody could buy. Token-holders could then vote on proposals by initiating a token transaction. Smart contracts then automatically enforced the votes on the blockchain with nobody being in control of the process. For example, DAO token-holders could vote on whether to reinvest any generated profits or disperse them in Ethereum to token-holders in proportion to their original investment.[36] The management of the DAO was therefore democratic and was based on a trustless technical system. The DAO failed weeks after its launch in June 2016 when a technical flaw enabled hackers to gain control over $50 million worth of Ethereum tokens. Ethereum founder Vitalik Buterin took the radical step to reverse the transactions on the Ethereum blockchain. Most Ethereum miners supported Buterin's decision to exclude the compromised transactions in order to prevent the hackers to profit from the attack on the DAO, but some Ethereum miners decided to maintain the original Ethereum blockchain, which has become a separate cryptocurrency with the name

Ethereum Classic.[37] Although the first DAO was a spectacular failure, the underlying concept is sound.[38] Bitcoin itself operates like a DAO, as it compensates miners, manages transactions, and improves its features with no owners, no CEO, and no employees, which is in itself remarkable.[39] A government cannot arrest the CEO of Bitcoin or order the Bitcoin organization to cease and desist in order to stop Bitcoin's usage.

Decentralized WikiLeaks

WikiLeaks is an excellent example for a social resistance organization that has been transformed by the blockchain revolution. The organization exposes government and corporate corruption by leaking original and often sensitive documents on the Internet in a publicly available database that is easily searchable. WikiLeaks procures these documents from insiders, who want to expose wrongdoing on part of their own organization by anonymously providing them to WikiLeaks, which may then decide to publish them. Former CIA Director Mike Pompeo even called WikiLeaks a "non-state hostile intelligence service."[40] According to a report from the U.S. Army, "Wikileaks.org was founded by Chinese dissidents, journalists, mathematicians, and technologists from the United States, China, Taiwan, Europe, Australia, and South Africa" and its website became active in early 2007.[41] The front person of WikiLeaks is the Australian Julian Assange, who is also the co-founder and driving force behind WikiLeaks.

After WikiLeaks published the State Department cables in 2010, the U.S. government urged banks, credit card companies, and other payment processors to close accounts and to refuse payments to WikiLeaks, which put enormous financial pressure on the organization. Amazon terminated services to host the WikiLeaks website and the DNS service to the WikiLeaks.org domain was unavailable by December 2010. Thousands of WikiLeaks supporters around the world managed to restore the website by mirroring it and by distributing the IP address through social media.[42] Amir Taaki advocated for using Bitcoin to support WikiLeaks in 2010, but Satoshi, who was still actively involved at the time, made the appeal to WikiLeaks not to use Bitcoin, as it "is a small beta community in its infancy. You would not stand to get more than pocket change, and the heat you would bring would likely destroy us at this stage."[43] However, from June 2011 WikiLeaks accepted donations in Bitcoin and made a strategic

https://scholarcommons.usf.edu/jss/vol13/iss1/3
DOI: https://doi.org/10.5038/1944-0472.13.1.1743

investment in the digital currency.[44] Assange has since been an outspoken promoter of Bitcoin and the blockchain. When the price of Bitcoin rose steeply in November 2017 to over $7,000 (and eventually to over $20,000), WikiLeaks had already accumulated 4,000 Bitcoin, which were worth some $29 million.[45] After British authorities arrested Assange on April 11, 2019 Bitcoin dropped $300 from $5,300 to about $5,000. Observed movements of funds from known WikiLeaks wallets led to widespread Internet speculations that WikiLeaks may be selling off its Bitcoin fortune to finance Assange's legal defense.

In order to prevent an official takedown of the WikiLeaks website from the Internet and the removal, censoring, or alteration of the leaked documents a developer for Bitcoin Cash, Chris Troutner, decided to upload the entirety of the WikiLeaks document collection, some 30 GB of data, on the Inter-Planetary File System (IPFS). The IPFS is a peer-to-peer decentralized network not on the worldwide web. Troutner has protected the files with a cryptographic hash to ensure the integrity of the originally uploaded files. Even if authorities shut down the website WikiLeaks.org the original content remains available through https://wikileaks.cash or by using the IPFS protocol directly. Troutner has also embedded he links to the files in the Bitcoin Cash blockchain. As long as the BCH and IPFS networks exist, everybody in the world with Internet access will be able to view the documents and will be able to check that they are authentic (in the narrow sense of as originally published by WikiLeaks).[46] It is likely that WikiLeaks supporters will also archive future WikiLeaks documents in this manner. This could indicate that WikiLeaks could re-emerge as a more decentralized, resilient, and successful organization after the demise of its original leader.

Decentralized Illicit Marketplaces and Assassination Markets

New forms of criminal syndicates may emerge that rely on DAOs as their main mode of organization. Criminals could cooperate on the Internet in a leaderless, anonymous, decentralized, and trustless fashion, which could create tremendous challenges to identify perpetrators or disrupt their illicit activities. The main weakness of Silk Road was that it required Ulbricht to be the webmaster and to sort out disputes between customers and sellers with each login onto his site being potentially trackable. Eventually the FBI could find him through an e-mail address linked to his

real name that he had once used on a forum to post a job ad related to Silk Road.[47]

A new decentralized Silk Road for illicit goods and content could appear at any time that uses smart contracts to manage orders, to accept and release payments, and to deduct a founders' fee, without the need of the operators to leave behind many digital fingerprints, if any at all. It might be impossible to shut down a blockchain-based Silk Road, especially if its nodes were numerous and spread across multiple jurisdictions.[48] Obviously, blockchain and smart contracts would also lend themselves to the use for blackmail and for dead hand switches that automatically release content based on pre-programmed conditions. For example, if a certain transaction on the blockchain has not taken place at a specific point of time, it can trigger the smart contract function, which executes a program.

One can also imagine the use of a DAO to facilitate an anonymous assassination market, which is a concept originally proposed by anarchist Jim Bell in his 1994 essay "Assassination Politics." Bell wrote, "While it's comparatively easy to "get away with murder," it's a lot harder to reward the person who does it, and that person is definitely taking a serious risk.' [49] His solution is an anonymous assassination market, where individuals can anonymously contribute funds for the assassination of a celebrity to a legal organization and whoever guesses the correct death date of the celebrity receives all the money donated. A high enough fee for making a bet would discourage contributors from making random guesses. As the contributions increase, so would the incentives for somebody to kill the unpopular celebrity and collect the money.

In the blockchain age a smart contract can govern such an arrangement. The assassin could be confident that the sponsoring organization will make the payment for a correct bet and would be able to collect the money in an anonymous fashion. An anonymous vote by all contributors could establish whether the celebrity has died and could automatically release accumulated funds to the correct guesser. According to a report by *Vice*, people already use the prediction platform Augur to make bets on "the deaths of public figures, including Betty White, Donald Trump, Jeff Bezos, and Warren Buffett."[50] The practical advantage of an assassination market for those participating is that it creates legal challenges as to whether

https://scholarcommons.usf.edu/jss/vol13/iss1/3
DOI: https://doi.org/10.5038/1944-0472.13.1.1743

making a bet constitutes the incitement of murder and also who could be charged with it in case of a large number of people contributing money to the cause of compensating somebody who makes a correct prediction.

Blockchain-Enabled Political Revolutions

During the Arab Spring small groups of activists could mobilize the masses against the respective government through tweets, Facebook posts, and text messaging. The Egyptian government became so desperate at one point that they temporarily shut down the Internet and mobile services nation-wide on January 28, 2011 to prevent the coordination of anticipated mass protests.[51] After the Arab Spring, many authoritarian governments cracked down on social media and NGOs. Major social media platforms and search engines, most importantly Facebook, Twitter, and Google now face strong political demands to police content under the threat of onerous regulation and fines. Peter Singer and Emerson Brooking have pointed out that the social media companies have assumed the functions of government and that "they are now grappled with intractable political problems," adding that the problems are of "the kind [that are] always destined to leave a portion of its constituents displeased."[52]

As more users of social media become dissatisfied with censorship of content, they will look towards new platforms that are censorship-free. Many blockchain-based solutions to Internet censorship are readily available. A good example is the Twister microblogging platform invented by Miguel Freitas in 2014, which can be freely downloaded and which uses a BitTorrent-like protocol to distribute data amongst users. The users can contribute computing power to the network in exchange for free adverts that they can send across the network.[53] A San Francisco-based start-up with the name Unstoppable Domains launched in 2018. The company wants to create a platform that allows human-readable blockchain addresses and to host and maintain censorship-resistant websites.[54] VC investor Tim Draper funded the start-up with $4 million. Website domains and content would be stored on the Zilliqa blockchain and would have *.zil* addresses that are not part of the Internet Domain Name System (DNS). Since the blockchain domain does not require an entry into the centralized registry of the DNS there is no way that a government can remove the website or that an ISP can block access to the website. Anybody who has

the domain blockchain address can view the contents. Owners of the blockchain domain also get an integrated cryptocurrency wallet that allows them to send a variety of cryptocurrency to other users or receive cryptocurrency using a memorable name or phrase as address.

In the future governments will be struggling to suppress content or prevent coordinated resistance by dissatisfied populations, as online-based communications services become much more decentralized and resilient. As a general rule, no ISP is able to block user access to blockchain-based media and messaging. Even if a government takes, the extreme step of shutting down the Internet and mobile services there is already a work-around for groups and individuals to maintain communications locally or nationally. A blockchain developer from New Zealand has demonstrated that blockchain transaction can occur in a (partial) off-grid situation. The developer managed to send a signed Bitcoin transaction over 19 km, using a Samourai Cryptocurrency wallet and a mesh of several goTenna radio devices that were attached to smart phones that had no Internet connection.[55] Obviously, the transaction must synchronize with the Internet at some point to avoid double spending, but it demonstrates that off-grid transactions on the blockchain can occur with inexpensive technology. Activists (or terrorists) could communicate via a short-range radio mesh, send or receive cryptocurrency, or otherwise interact with blockchains even when the Internet or telephone services are temporarily down.

Part III: Government Regulation

Blockchain Technology is not limited in its utility to facilitating financial transactions and enabling transfers of value, but has sparked a large industry around many other potential applications, such as “inviolable property registries,” “real-time, direct, bank-to-bank settlement of securities exchanges,” “self-sovereign identities,” “decentralized computing,” “decentralized Internet of Things,” “blockchain-based supply chains,” and “decentralized media and content.”[56] According to a new market research report, companies in the United States spent $1.6 billion in 2018 on BT and according to some projections this could increase to $41 billion in 2025.[57] Major financial institutions and IT companies have invested in BT, including JP Morgan, UBS, IBM, Intel, Facebook, and Microsoft. Most notably, Facebook announced that it intends to launch a

https://scholarcommons.usf.edu/jss/vol13/iss1/3
DOI: https://doi.org/10.5038/1944-0472.13.1.1743

global cryptocurrency name *Libra* that would allow Facebook users to send or receive cryptocurrency on Facebook to make purchases or to transfer money.[58] The realization that cryptocurrency is here to stay is slowly sinking in with lawmakers and regulators. Governments are no longer able to ignore BT and they have to find regulations that allow them to leverage the technology while also minimizing the potentially destabilizing effects.

Identity Authentication

China is a leader in BT and the Chinese is already facing many of the challenges outlined above. Chinese dissidents have used blockchains to expose corruption and to distribute scandalous information on officials.[59] The Chinese government is now requiring all blockchain operators to register their code with the government, as well as all their server IPs, and record and provide all information on their users.[60] The government threatens any Chinese blockchain company that violates these regulations with high fines and prison sentences. Chinese Internet users who access social media platforms or other Internet services with a VPN to hide their online identity are also subject to punishment.

Although the extremely repressive approach of the Chinese government is not consistent with democratic practices, there is nothing wrong in principle with requiring robust identity authentication for accessing Internet services, including microblogging or messaging services. Instead of playing whack-a-mole with the Islamic State, removing fake accounts that the terrorists can quickly reopen under a slightly different name, the time has come for a new approach.[61] The immutable nature of the blockchain combined with the use unique cryptographic keys makes it suitable as a method of verifying the identity of users in a number of contexts. This provides a more convenient and secure solution than passwords and other methods of authentication. For example, the Civic project offers blockchain-based identity verification: Users can submit their personal information in exchange for Civic tokens and others can pay with Civic tokens for validating information (with the permission of the owner of the information).[62] This way a user could not easily change their digital identity or otherwise hide their identity when they access online services, which also reduces all kinds of identity fraud and illicit activity online.

Crowdsourced Counter-Messaging

Counter-messaging has been a reasonably successful approach used against radical groups such as ISIS. Gareth Mott pointed out "[w]hile violent extremist content hosted in an encrypted peer-to-peer manner may have the potential to be technically resilient, this does not necessarily make it socially resilient." He suggests "When violent extremists elect to use social media to further their agenda…they give their narrative(s) visibility and open a space for them to be critiqued."[63] Suitable strategies for dealing with problematic social messaging is to debunk false information, to demonstrate faulty logic, to expose immoral arguments for what they are, and to ridicule extremist positions. Instead of trying to censor speech by removing unwanted content governments would need to encourage virtual communities to police themselves. A moderate majority can marginalize radical positions by voicing disagreement. Effective counter-messaging can bury distasteful information by making it harder to find, even if it is not possible to remove it. Most importantly, a free society should foster a critical mindset with respect to online information to enable people to better navigate and evaluate the information available to them.[64]

Co-opt Blockchain Development

Governments may choose to support blockchain companies that build technology more consistent with the concerns of regulators. A RAND study pointed out that there is a middle ground between completely decentralized and centralized ones, namely semi-centralized systems, "where the authority mechanism is distributed among a restricted set of participants."[65] For example, the Chinese government has chosen to promote blockchains with a few 'super nodes' that are much more centralized, as they are easier to control by the government. In this model, transactions have to be approved or validated by a small number of consensus nodes (21 nodes for EOS, 9 nodes for Ontology, and only 7 in the case of NEO), which makes it effectively a closed permissioned system, where certain users can be excluded and certain transactions can be stopped.[66] Most strikingly, EOS has already demonstrated the capacity to reverse confirmed transactions and to freeze user accounts, which is supposed to be impossible on a real blockchain.[67]

https://scholarcommons.usf.edu/jss/vol13/iss1/3
DOI: https://doi.org/10.5038/1944-0472.13.1.1743

Interestingly, Facebook is following the Chinese model as indicated in its White Paper. The Libra Association originally planned to have one hundred Founding Members comprised of various organizations, who would run geographically dispersed validator nodes. It is a permissioned system that would allow cryptocurrency transactions of a stable coin called *Libra*, which would be also a hundred percent backed by a basket of currencies and bonds.[68] Despite the enormous strides Facebook made to accommodate government concerns over regulation, the company faced outright hostility and skepticism from U.S. legislators.[69] Regardless, Facebook is a company that is well-positioned to dominate the cryptocurrency space since it has already a user-base of over 2 billion.

Conclusion

Senator Mike Crapo recently suggested: "If the United States were to decide, and I'm not saying it should, if the United States decided we didn't want cryptocurrency to happen in the United States, and tried to ban it, I'm pretty confident we couldn't succeed in doing that because this is a global tech, a global innovation."[70] He is right: Bitcoin has over 10,000 full active nodes in over a hundred countries.[71] No single government or group of governments could hope to shut down the self-organizing and self-sustaining Bitcoin network or a similarly large blockchain network (Ethereum). The most important feature of BT is censorship-resistance: A government cannot remove information that resides on a decentralized autonomous network through a court order or through pressuring the company that originally developed the blockchain. However, this feature does not necessarily equate in the triumph of malicious actors, who could take advantage of the technology. As Kevin Werbach has argued, "The global scale of blockchain networks does not prevent nations from enforcing their laws. Coordination among law enforcement and mechanisms such as extradition can be used to bring criminals to justice."[72] However, what could be an even bigger challenge than BT-related cybercrime is BT-enabled social or civil resistance that could make opposition to authority much easier to join and to sustain in the end through the self-organizing trustless mechanism of a DAO. Governments and regulators need to have a more nuanced understanding of the technology, so that society can take advantage of the innovative potential

of the technology while mitigating some of the politically destabilizing effects.

Endnotes

[1] Angela S.M. Irwin and George Milad, "The Use of Crypto-Currency in Funding Violent Jihad," *Journal of Money Laundering Control* 19, no. 4 (2016): 411, https://doi.org/10.1108/JMLC-01-2016-0003.
[2] Alan Rappaport and Nathaniel Popper, "Cryptocurrencies Pose National Security Threat, Mnuchin Said," *New York Times*, July 15, 2019, https://www.nytimes.com/2019/07/15/us/politics/mnuchin-facebook-libra-risk.html.
[3] Gene Sharp, *Waging Nonviolent Struggle: 20th Century Practice and 21st Century Potential* (Boston: Porter Sargent, 2005), 41.
[4] John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" in Arquilla, John and Ronfeldt, David, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND, 1997), 26.
[5] Eric Schmidt and Jared Cohen, *The New Digital Age: Reshaping the Future of People, Nations and Business* (New York: Alfred A. Knopf, 2013), 121.
[6] Schmidt and Cohen, *The New Digital Age*, 124.
[7] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (Bitcoin.org, 2008), https://bitcoin.org/bitcoin.pdf.
[8] Max Border, *The Social Singularity: A Decentralist Manifesto* (Austin, TX: Social Evolution, 2018), 49.
[9] Kevin Werbach, *The Blockchain and the New Architecture of Trust* (Cambridge, MA: MIT Press, 2018), 4.
[10] Jamie Bartlett, *The Dark Net: Inside the Digital Underworld* (New York: Melville House, 2015), 75.
[11] William Mougayar, *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology* (Hoboken, NJ: Wiley & Sons, 2016), 3.
[12] Mougayar, *The Business Blockchain*, XXIII.
[13] Donald Trump (@realDonaldTrump), "I am not a fan of Bitcoin and other cryptocurrencies…," Twitter, July 11, 2019, https://twitter.com/realdonaldtrump/status/1149472282584072192?lang=en.
[14] Christopher Whyte, "Cryptoterrorism: Assessing the Utility of Blockchain Technologies for Terrorist Enterprise," *Studies in Conflict and Terrorism* (2019): 2, https://doi.org/10.1080/1057610X.2018.1531565.
[15] Nathaniel Popper, *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money* (New York: Harper, 2015), 69-73.
[16] Werbach, *The Blockchain*, 49.
[17] Popper, *Digital Gold*, 347.
[18] Whyte, "Cryptoterrorism," 4.
[19] Werbach, *The Blockchain*, 179.
[20] Whyte, "Cryptoterrorism," 14.
[21] Joshua Baron, Angela O'Mahoney, David Manheim, and Cynthia Dion-Schwarz, *National Security Implications of Virtual Currencies: Examining the Potential for Non-State Actor Deployment* (Santa Monica, CA: RAND, 2015), 19-20.
[22] Whyte, "Cryptoterrorism," 14.
[23] Cynthia Dion-Schwarz, David Manheim, Patrick B. Johnston, *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats* (Santa Monica, CA: RAND, 2019), 21.
[24] Michael C. Casey, and Paul Vigna, *The Truth Machine: The Blockchain and the Future of Everything* (New York: St. Martin's Press, 2018), 33.
[25] Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (London: Penguin, 2007).
[26] Brafman and Beckstrom, *The Starfish and the Spider*, 19-20.

https://scholarcommons.usf.edu/jss/vol13/iss1/3
DOI: https://doi.org/10.5038/1944-0472.13.1.1743

[27] Brafman and Beckstrom, *The Starfish and the Spider*, 140-143.
[28] George Michael, *Lone Wolf Terror and the Rise of Leaderless Resistance* (Nashville, TN: Vanderbilt University Press 2012), 2.
[29] A third generation is emerging with respect to new blockchains that have either interchain functionality (for example Dragonchain, Aion, and Cosmos) or that use a Directed Acyclic Graph protocol that makes mining unnecessary (for example Algorand, Hashgraph, and IOTA).
[30] Don Tapscott and Alex Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World* (New York: Penguin, 2016), 87.
[31] The Ethereum ECR-20 tokens were the primary vehicle for fund-raising during the 2017 Initial Coin Offering (ICO) craze.
[32] Mougayar, *The Business Blockchain*, 42.
[33] Werbach, *The Blockchain*, 67.
[34] Christoph Jentzsch, "Decentralized Autonomous Organization to Automate Governance," Slock.it White Paper (2016), https://download.slock.it/public/DAO/WhitePaper.pdf.
[35] Casey and Vigna, *The Truth Machine*, 56.
[36] "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO," Securities and Exchange Commission, July 25, 2017, 6, accessed December 4, 2019, https://www.sec.gov/litigation/investreport/34-81207.pdf.
[37] Casey and Vigna, *The Truth Machine*, 85.
[38] Werbach, *The Blockchain*, 110.
[39] Ying-Ying Hsieh, Jean-Phillipe Vergne, Phillip Anderson, Karim Lathani, and Markus Reitzig, "Bitcoin and the Rise of Decentralized Autonomous Organizations," *Journal of Organization Design* 8, no. 3 (2019): 2, https://doi.org/10.1186/s41469-018-0038-1.
[40] Martin Matishak, "CIA Director Labels WikiLeaks a "Hostile Intelligence Service,"' *Politico*, April 13, 2017, https://www.politico.com/story/2017/04/mike-pompeo-wikileaks-hostile-intelligence-service-237206.
[41] U.S. Army, "Wikileaks.org – An Online Reference to Foreign Intelligence Services, Insurgents, or Terrorist Groups?" U.S. Army Counterintelligence Center, March 18, 2008, https://www.wired.com/images_blogs/threatlevel/2010/03/wikithreat.pdf.
[42] Julian Assange, *Freedom and the Future of the Internet* (New York: OR Books, 2016), 13-14.
[43] Popper, *Digital Gold*, 58.
[44] Nermin Hajdarbegovic, "Assange: Bitcoin and WikiLeaks Helped Keep Each Other Alive," *Coindesk*, September 16, 2014, https://www.coindesk.com/assange-bitcoin-wikileaks-helped-keep-alive.
[45] Greg Synek, "WikiLeaks Thanks US Government for Blocking Credit Card Transactions," *Techspot*, November 17, 2017, https://www.techspot.com/news/71764-wikileaks-thanks-us-government-blocking-credit-card-donations.html.
[46] Jamie Redman, "WikiLeaks Cache Now Hosted on IPFS Thanks to This Bitcoin Cash Developer," *Bitcoin.com*, April 13, 2019, https://news.bitcoin.com/wikileaks-cache-now-hosted-on-ipfs-thanks-to-this-bitcoin-cash-developer/.
[47] Popper, *Digital Gold*, 248.
[48] Itai Damti, "The Dark Side of the Chain: Blockchain Viruses and Decentralized Autonomous Crime Organizations," Hackernoon.com, October 21, 2018, https://hackernoon.com/the-dark-side-of-the-chain-blockchain-viruses-and-decentralized-autonomous-crime-organizations-6e44bc9a4c54.
[49] Jim Bell, "Assassination Politics," (1994), http://www.outpost-of-freedom.com/jimbellap.htm.
[50] Daniel Oberhaus, "Assassination Markets for Jeff Bezos, Betty White, and Donald Trump Are on the Blockchain," *Vice*, July 25, 2018, https://www.vice.com/en_us/article/gy35mx/ethereum-assassination-market-augur.
[51] Schmidt and Cohen, *The New Digital Age*, 138.
[52] Peter W. Singer and Emerson T. Brooking, *Like War: The Weaponization of Social Media* (New York: Houghton Mifflin Harcourt 2018), 233.

[53] Gareth Mott, 'A Storm on the Horizon? "Twister" and the Implications of the Blockchain and Peer-to-Peer Social Networks for Online Violent Extremism," *Studies in Conflict and Terrorism* (2019): https://doi.org/10.1080/1057610X.2018.1513986
[54] Zack Seward, "Decentralized Domain Registry Raises $4 Million from Draper, Boost VC," *Coindesk.com*, May 23, 2019, https://www.coindesk.com/decentralized-domain-registry-raises-4-million-from-draper-boost-vc.
[55] Matthew Beedham, "Dev Sends Bitcoin Without Using the Web or the Power Grid," *TheNextWeb.com*, October 16, 2018.
[56] Casey and Vigna, *The Truth Machine*, 8.
[57] "Blockchain in the United States: Forecast to 2025 - Spend on Blockchain is Expected to Record a CAGR of 44.5 percent, Increasing from $3.12Bn in 2019 to $41.11Bn by 2025," *Globenewswire.com*, March 25, 2019. https://www.globenewswire.com/news-release/2019/03/25/1760459/0/en/Blockchain-in-the-United-States-Forecast-to-2025-Spend-on-Blockchain-is-Expected-to-Record-a-CAGR-of-44-5-Increasing-from-3-12Bn-in-2019-to-41-11Bn-by-2025.html.
[58] Peter Holley and Rachel Siegel, "Facebook Launches Libra, Its Own Cryptocurrency Network," *Washington Post*, June 18, 2019.
[59] Nicole Hao, "China Moves to Restrict the Use of Blockchain Technology," *Epoch Times*, January 14, 2019.
[60] Hao, "China Moves to Restrict the Use of Blockchain Technology."
[61] Singer and Brooking, *Like War*, 236.
[62] Werbach, *The Blockchain*, 87.
[63] Mott, "A Storm on the Horizon?," 220.
[64] Mott, "A Storm on the Horizon?," 220.
[65] Baron e.a., *National Security Implications*, 18.
[66] Nir Kshethri, "Chinese Internet Users Turn to the Blockchain to Fight Against Government Censorship," *The Conversation*, February 25, 2019, https://theconversation.com/chinese-internet-users-turn-to-the-blockchain-to-fight-against-government-censorship-111795.
[67] William Suberg, 'EOS "Reverses" Previously Confirmed Transactions as Pundits Decry Centralization,' Cointelegraph.com, November 12, 2018, https://cointelegraph.com/news/eos-reverses-previously-confirmed-transactions-as-pundits-decry-centralization.
[68] Facebook, "Libra White Paper," Libra Association, July 23, 2019, https://libra.org/en-US/white-paper/#the-libra-blockchain.
[69] Renae Merle, "Facebook Cryptocurrency Libra Skewered on Capitol Hill," *Washington Post*, July 16, 2019, https://www.washingtonpost.com/technology/2019/07/16/facebook-privately-pitched-its-cryptocurrency-plan-last-month-regulators-they-were-left-even-more-scared/.
[70] Ben Brown, "U.S. Senator: Even If We Wanted to, We Couldn't Ban Bitcoin," *CCN.com*, July 31, 2019, https://www.ccn.com/us-senator-even-if-we-wanted-to-we-couldnt-ban-bitcoin/.
[71] "Global Bitcoin Nodes Distribution," *Bitnodes*, https://bitnodes.earn.com/?The, accessed July 2, 2019.
[72] Werbach, *The Blockchain*, 179.

https://scholarcommons.usf.edu/jss/vol13/iss1/3
DOI: https://doi.org/10.5038/1944-0472.13.1.1743