MAY 2017

TERRORIST USE OF VIRTUAL CURRENCIES

Containing the Potential Threat

Zachary K. Goldman, Ellie Maruyama, Elizabeth Rosenberg,
Edoardo Saravalle, and Julia Solomon-Strauss

CNAS
Celebrating 10 Years

About the Authors

ZACHARY K. GOLDMAN is the Executive Director of the Center on Law and Security and an adjunct professor at NYU School of Law. He is also an Adjunct Senior Fellow with the Energy, Economics, and Security Program at the Center for a New American Security (CNAS). Previously Mr. Goldman served as a Special Assistant to the Chairman of the Joint Chiefs of Staff at the U.S. Department of Defense, and as a policy advisor in the U.S. Department of the Treasury's Office of Terrorism and Financial Intelligence, where he was the subject-matter expert on terrorist financing in the Arabian Peninsula and Iran sanctions.

ELLIE MARUYAMA is a Research Associate in the Energy, Economics, and Security Program at CNAS. Previously she worked at the World Bank and interned with the EU Delegation in Washington. She holds a bachelor's degree in international studies from the University of California, San Diego; and a master's in international affairs from Columbia University's School of International and Public Affairs.

ELIZABETH ROSENBERG is a Senior Fellow and Director of the Energy, Economics, and Security Program at CNAS. From May 2009 through September 2013, she served as a Senior Advisor at the Department of the Treasury, helping senior officials formulate anti–money laundering and counterterrorist financing policy and develop financial sanctions. In this capacity she also helped to oversee financial regulatory enforcement activities.

EDOARDO SARAVALLE is a Joseph S. Nye Jr. Research Intern for the Energy, Economics, and Security Program at CNAS. Previously he worked as an investment banker at Moelis & Company.

JULIA SOLOMON-STRAUSS is a Program Associate at the Center on Law and Security at NYU School of Law. Previously she worked at Harvard Business School's Europe Research Center in Paris and the Chicago Council on Global Affairs. She holds a bachelor's degree in social studies from Harvard College and a master's of philosophy (history) from the University of Cambridge.

Cover Photo
Chris McGrath/Getty Images (modified by CNAS)

Acknowledgments

The authors would like to acknowledge Loren DeJonge Schulman, Frederick Reynolds, Cari Stinebower, and Jenny Cieplak for their comments and insights on this paper. They would also like to thank Bogdan Belei for his extraordinary assistance in the initial research for and drafting of this report. The authors thank Kelsey Hallahan, Ushaia Kappen, and Abigail Van Buren for their research support. Finally, they are grateful for the assistance of Melody Cook and Maura McCarthy in producing this report.

TERRORIST USE OF VIRTUAL CURRENCIES

Containing the Potential Threat

Executive Summary

This paper explores the risk that virtual currencies (VCs) may become involved in the financing of terrorism at a significant scale. VCs and associated technologies hold great promise for low cost, high speed, verified transactions that can unite counterparties around the world. For this reason they could appear appealing to terrorist groups (as they are at present to cybercriminals). Currently, however, there is no more than anecdotal evidence that terrorist groups have used virtual currencies to support themselves. Terrorists in the Gaza Strip have used virtual currencies to fund operations, and Islamic State in Iraq and Syria (ISIS) members and supporters have been particularly receptive to the new technology, with recorded uses in Indonesia and the United States.

Most terrorist funding now occurs through traditional methods such as the *hawala* system, an often informal and cash-based money transfer mechanism, and established financial channels.[1] If VCs become sufficiently liquid and easily convertible, however, and if terrorist groups in places such as sub-Saharan Africa, Yemen, and the Horn of Africa obtain the kinds of technical infrastructure needed to support VC activity, then the threat may become more significant.

The task of the law enforcement, intelligence, regulatory, and financial services communities, therefore, must be to prevent terrorist groups from using VCs at scale. The use of VCs by "lone wolf" terrorists—a much bigger potential threat because of the small scales of funding needed to execute an attack—represents the kind of problem in intelligence and digital forensics that law enforcement agencies are well equipped to handle, even if they tax existing resources.

Attacking terrorists' use of virtual currency at scale is a challenging task for many stakeholders. New financial technology firms often lack the resources to comply effectively with oversight obligations, while regulators have tended to devote few resources to non-bank institutions. At the same time, different countries have adopted varying approaches to the regulation of virtual currencies, posing an enforcement challenge in a globalized field that requires a unified response. Finally, the privileging of prevention over management of illicit finance risk in the compliance world has created an incentive structure for banks that does not, ironically, push them toward innovative approaches to countering terrorist financing, including via virtual currencies.

The counterterrorist financing community should adopt three guiding principles that will provide the foundation for policies aimed at countering both the new virtual currency threat and the broader illicit finance danger. First, policy leaders should prioritize the countering of terrorist financing over other kinds of financial crime. Second, the policy and regulatory posture should be oriented toward rewarding and incentivizing innovation. Third, policymakers should emphasize and create a practical basis for strengthening coordination between the public and private sectors on terrorist financing. These approaches form the foundation of an effective response to existing and emerging terrorist financing threats and will balance the burden of regulatory compliance with the policy need to support innovative new virtual currency technologies.

01 CHAPTER

Introduction

In the past several years, terrorist groups in Gaza have solicited support in Bitcoin; there are isolated reports that ISIS has used the cryptocurrency; and cybercriminals use it and other virtual currencies in a range of circumstances. We cannot yet know whether the uses of virtual currencies by terrorist groups amount to isolated incidents or foretell a broader and more pernicious trend.[2] Individual incidents in which lone terrorists or terrorist groups use VCs of course pose a challenge. This is particularly so because the funding requirements for disruptive lone wolf acts of terror are small enough to pose a risk because they may slip through a counterterrorism financing system that struggles to stop small-scale acts of such financing regardless of the medium. But VCs become a strategic threat in the counterterrorism context only when they can compete with cash and other readily available means of financing and achieve "scale," which in this paper signifies a combination of market capitalization, liquidity, convertibility, and network effects that add up to ease of use. Scaled use of VCs by illicit actors poses a particular challenge and exacerbates the underlying threat posed by criminal or terrorist activity because it makes illicit funding networks harder to disrupt. And the larger the stable funding supply for terrorist groups, the greater the scale at which the groups themselves can operate and the more they can engage in acts of violence.

While VCs have many very important legitimate uses, certain characteristics also make them susceptible to abuse. Many, especially cryptocurrencies, protect or obscure identities, thereby making it more difficult for law enforcement to reveal and track those identities than traditional mechanisms of value transfer. Should terrorists adopt VCs at scale, therefore, it could become much more difficult to track and disrupt them.

A second reason it is important to understand the circumstances in which terrorist groups may wish to use VCs at scale is the global reach of such currencies. With certain virtual currencies, it is possible to transfer money instantly around the world without making use of institutions like banks, which require more transparency and have obligations to report suspicious transactions. Even centralized VCs may be accessible online anywhere in the world, so terrorists and criminals can take advantage of these currencies that have been set up in jurisdictions with less scrutiny. Potentially, such characteristics could effectively build a digital platform on top of established systems that currently allows terrorists, and others, to transfer cash on an international scale. Such an architecture would make it easier for terrorist groups to amass larger amounts of money than has generally been possible previously.

Finally, the novelty and some particular attributes of VCs, such as decentralization, make them a particular regulatory challenge. Decentralized cryptocurrencies such as Bitcoin lack concentrated repositories of identifying information on account-holders, which law enforcement agencies typically use in financial crimes and counterterrorism investigations, but which are unavailable when dealing with many VCs. A more precise understanding of the threats and risks posed by VCs will help regulators to develop an effective and efficient governance framework to monitor for potential abuse. In turn, a successful framework will ultimately strengthen the global fight against terrorist financing and terrorism as a whole.

In the post-9/11 era, the international community has made significant progress in the struggle against terrorism generally, and in the struggle against terrorist financing specifically. In the counterterrorism context, "following the money" has been a particularly effective component of an overall strategy to degrade the capabilities of terrorist groups.[3] One of the most significant victories has been the establishment of a global legal and policy framework—grounded in U.N. Security Council Resolutions, national legislation, and global standards—that, by blocking terrorist groups' access to the formal financial system, has made it significantly more difficult for them to raise, move, store, and use funds.

However, recent evolutions in the terrorist threat, including the rise of ISIS and the continued importance of al Qaeda and its affiliates, have led the Financial Action Task Force (FATF), the intergovernmental standard–setting body for combating money laundering,

The hawala system of person-to-person money transfer, pictured above, allows terrorists to transfer cash on a global scale outside the regulated financial system, escaping anti-money laundering and combating the financing of terrorism oversight. (Institute for Money, Technology and Financial Inclusion/Flickr)

terrorist financing, and other threats to the integrity of the international financial system,[4] to note that "further concerted action urgently needs to be taken . . . to combat the financing of . . . serious terrorist threats" that have "globally intensified."[5]

Specifically, a number of challenges regarding terrorism and its financing remain. First, terrorist groups that control territory pose one of the most difficult strategic challenges that the counterterrorism community faces. When groups control territory, it is easier for them to plan and train without disruption. It is also easier for them to derive financial and material support from the local population (through taxation, extortion, or the extraction of natural resources) without having to rely on transfers of funds from external sources that are inherently more vulnerable to disruption.

A second strategic challenge pertains to individual lone wolf terrorists or cells that lack formal ties to any established group. This dynamic makes it more difficult to anticipate attacks with intelligence, because it is difficult to determine which unaffiliated individuals will perpetrate attacks. And because these attacks are relatively inexpensive to execute, it is more difficult to identify and choke off their sources of support. Terrorists such as those who carried out attacks in Orlando, Florida; San Bernardino, California; or Nice, France do not rely on associations with larger groups that require significant funds to sustain themselves. Therefore, they leave only trace financing "signatures" and are not easy to detect and disrupt under a global framework built for more established and less nimble threats.[6] Addressing lone wolf attacks is a significant intelligence challenge for the counterterrorism community. And identifying the ways in which such attackers may use VCs to fund themselves is similarly a significant forensic and intelligence issue that may require the government to invest in new capabilities and to work more closely than it has in the past with private entities.

Despite significant progress in the global counterterrorist financing regime, gaps remain in implementation and coverage. The charitable sector, for example, is still vulnerable to abuse, and unlicensed money transmitters, cash smugglers, and criminal activity of all kinds are a source of support for terrorist groups, both in the United States and abroad.[7] Furthermore, the global counterterrorism financing regime is more oriented toward identifying and degrading the ability of organized groups to function than toward the rising threat of independent attacks. When a terrorist in Nice, for example, can kill 86 people simply by renting a truck and driving it through crowds of revelers on Bastille Day, policy leaders must rethink the approach to counterterrorism that has been oriented primarily toward well-defined groups, as al Qaeda was before the 9/11 attacks.

Looking specifically at the counterterrorist financing risk for VCs, it does not appear that terrorist groups have yet used these currencies at scale, even while other criminal groups (specifically cybercriminals) have done so. Indeed, the U.S. government's 2015 "National Terrorist Financing Risk Assessment" cited cash and the banking system as two of the most significant terrorist financing risks that the United States faces.[8] The assessment described virtual currencies only as a "potential emerging TF [terrorist financing] threat,"[9] and noted that "the possibility exists that terrorist groups may use these new payment systems to transfer funds collected in the United States to terrorist groups and their supporters located outside of the United States."[10] At the same time, the European Banking Authority classified as a high priority risk terrorist use of VC remittance systems and accounts.[11] More troubling is the potential for virtual currencies to "democratize" the funding of terrorism, allowing far-flung, disconnected individual donors to participate in TF networks.[12] So while terrorist groups are not yet using VCs at scale, a key goal of the policy and financial regulatory communities is to prevent that from happening by adapting measures to better track and prevent this threat. A more forward-leaning posture on financial information sharing and disclosure would benefit all stakeholders involved in addressing terrorists' use of VCs and illicit financial activity more broadly.

While terrorist groups are not yet using VCs at scale, a key goal of the policy and financial regulatory communities is to prevent that from happening.

Terrorist groups have not yet adopted VCs at scale, but cybercriminal networks have. There are several reasons criminal and terrorist groups have behaved differently with respect to the adoption of virtual currencies. One important factor surely is the degree of technological sophistication needed to use such currencies at scale. The criminal enterprises that have made extensive use of VCs are generally engaged in technically complex crimes such as the remote theft and sale of data (or significant narcotics trafficking), and they operate in areas that have at least reasonably well-developed financial and telecommunications infrastructures.

Many terrorist groups, by contrast, operate in areas with poor infrastructure and low penetration of modern technical and telecommunications tools. This is true, for example, of al Qaeda in the Islamic Maghreb (AQIM) in the Sahel, al Qaeda in the Arabian Peninsula (AQAP) in Yemen, and, in some measure, ISIS in Iraq and Syria. And this dynamic illuminates a major obstacle to the adoption of VCs, even while terrorist groups take advantage of sophisticated technology in non-financial contexts. ISIS's use of social media to recruit and propagandize[13] and Hezbollah's use of drones stand out as two prominent examples.[14] Technologies like drones do not rely on network effects to be useful and can be provided (nearly) off the shelf and ready to use. Similarly, social media is available on the kinds of smartphones and websites that have been commoditized. Virtual currencies, by contrast, are more difficult to create (should a terrorist group try to do so), employ, and maintain.

Of course, not all terrorist groups or their supporters contend with limited Internet access, computing capabilities, or knowledge of sophisticated tactics to evade regulatory detection of electronic money movements. This is one reason for the instances of terrorist groups using VCs, albeit in more limited ways.

Terrorist networks, by contrast, have a different "business model." They often seek to move money from places outside the locations where they operate to the areas in which they plan and from which they launch attacks. Often they use many layers of intermediaries so that donors and ultimate recipients may not be known to one other. Or, in the case of lone wolf attackers, they scrape together funding from a wide range of sources. In either case, terrorists use the funds to buy things they need to sustain the group or to conduct attacks. And because they do so from the general economy, they often would need to reconvert the VCs they receive into fiat currency. This final step introduces both an unnecessary layer of complexity and an increased vulnerability to the disruption of their operations by adding additional actors and entities into the fundraising matrix.

Moreover, the virtual currency that has achieved the greatest market capitalization and penetration—Bitcoin—is only pseudonymous, not fully anonymous, as is commonly and incorrectly understood. The cryptographic addresses of the sender and the recipient of transactions are recorded; although they may not be linked to real-life identities, with enough investigative resources it may be possible to uncover the true identity

Many terrorist groups operate in areas with poor infrastructure and low penetration of modern technical and telecommunications tools.

Terrorist networks and criminal groups also have different financial structures in which they do or may take advantage of virtual currencies. Cybercriminals often use VCs to buy or sell stolen data, for their exploits in online "dark web" markets,[15] or for commercial transactions in illegal activities such as drug or weapons trafficking.[16] There is less of a need for VCs to be convertible in that context because their users can simply recycle them for the next purchase. Cybercriminals located in Eastern European countries with poor records of law enforcement cooperation with the West can exchange VCs for fiat currencies in unregulated exchanges.[17] Cybercriminals also often engage in extensive vetting of other purported criminals who wish to join online forums in which cybercrime activities take place; therefore they have some degree of confidence that their transaction counterparties can be trusted.[18] This dynamic stems from the fact that the criminals are often repeat players who depend on the continued operation of the network for their activities.

of senders and recipients of Bitcoin transactions. This of course diminishes the allure of that means of transferring funds to terrorists. Notwithstanding its incomplete anonymity, Bitcoin remains dominant in the space. For example, Monero, a cryptocurrency that is more anonymous than Bitcoin, has a market capitalization of about $340 million; Bitcoin's market cap is $17 billion.[19]

But the final—and most important—reason that terrorist groups have not adopted virtual currencies at scale is that these groups, and individual terrorist operatives, have not yet perceived the need to do so. They still find it possible to circumvent global rules governing terrorist financing with sufficient ease and frequency that using VCs is unnecessary. They exploit incomplete implementation of regulatory requirements and global standards at banks, use unlicensed and undersupervised money services businesses (MSBs), or simply cart around cash. As long as these value transfer methods are readily available, there is no great need to invest in new, complicated techniques to transfer value.

Therefore, the crux of the challenge that financial regulators and the counterterrorism community must confront with regard to virtual currency is one of monitoring and prevention: How will they know if and when terrorists begin to use VCs at scale? And how can they design the financial regulatory framework governing VCs to harness the positive uses to which they can be put while preventing them from abuse?

One of the most important factors in the ability of governments and other stakeholders to manage the risks posed by VCs is effective collaboration and communication. Three main categories of actors make up this ecosystem—financial institutions, the regulatory agencies that supervise them, and the law enforcement and intelligence community that target criminals and security threats.

At present, tension among these constituencies prevents them from optimally monitoring and governing the use of virtual currencies. Fundamentally, law enforcement agencies and bank regulatory agencies have different authorities and use information from the private sector in different ways. They also have different approaches to the terrorist financing challenge. Whereas the mission of law enforcement officials is to halt terrorism, regulators are charged with ensuring that financing does not occur in banks that they supervise. Law enforcement agencies take data that they get from banks (often via the government's financial intelligence unit, the Financial Crimes Enforcement Network, FinCEN, in the United States), combine it with other intelligence or evidence to improve their understanding of the threat landscape, and engage in further intervention—often a prosecution—to address it.[20] Regulatory agencies such as the Federal Reserve Bank or the Office of Comptroller of the Currency (OCC) and state-level regulators such as the New York State Department of Financial Services (NYDFS), by contrast, use information from the private sector to assess compliance with existing rules, and then undertake enforcement actions if necessary. These regulators also use private sector information to inform their view of changes that they or others may need to make to manage risk in the financial sector.

In the past decade, financial regulators responsible for supervising banks have imposed significant fines for violations of laws designed to counter illicit finance.[21] As described later in this paper, these enforcement actions have inhibited the development of effective public-private collaboration in the governance of VCs, because they have generated a significant amount of uncertainty within banks. Such collaboration is critical to prevent virtual currencies from being abused for illicit purposes at greater scale, particularly by terrorist groups.

Two main trends stand in the way of greater incorporation of VCs into the formal financial system, which would help manage the risks inherent in the near-instantaneous and anonymous global transfer of funds. The first trend in the financial sector is the desire of banks to avoid high compliance-cost business activities, including in jurisdictions with poor regulation and a relatively high occurrence of illicit financial activity or sanctions evasion, or in dealings with high-risk types of clients.[22] This trend has led many financial institutions to shed expensive-to-service accounts, correspondent relationships, and clients, and is commonly referred to as "de-risking."[23] Virtual currencies have been caught in this trend. Businesses that deal extensively in VCs have found it difficult to establish relationships with the largest global banks because the businesses are often perceived as relatively risky and therefore too costly to take on.[24] As a result, VC businesses have had to conduct their banking operations at smaller financial institutions that do not devote as many resources to compliance as do large global banks, and that are less well regulated than large money center banks. This dynamic, in turn, increases the likelihood that VCs will be used for the conduct of illicit activity at a scale, posing a security threat.

Businesses that deal extensively in VCs have found it difficult to establish relationships with the largest global banks.

Virtual currency firms are also stepping into lines of business—such as cross-border remittances—that some large global banks are abandoning because of the perceived risk.[25] And the anti–money laundering (AML), combating-the-financing-of-terrorism (CFT) and sanctions-compliance system requires companies to establish customer identification programs, screen for sanctions compliance, and establish suspicious activity reporting systems. This rigor may be too expensive for small VC startup companies, which may therefore either collapse before they get off the ground or operate in an unregulated manner, thereby increasing the risk that bad actors may use VCs without detection.

The second broad trend that has made it more difficult to govern virtual currencies is the libertarian ethos that animates many of the individuals and entities involved in the creation and growth of the VC movement.[26] For many people, the most attractive dimension of VCs such as Bitcoin is the same one that makes it most difficult to

govern—it serves as a store of value, unit of account, and medium of exchange that does not require the involvement of any large centralized government institutions or banks.[27] That means these kinds of VCs lack many of the features of national currencies that make them secure and trusted, and it makes them susceptible to abuse by criminals, terrorists, and fraudsters who want their financial transactions to be opaque. It also makes the currency volatile. A recent dispute among developers about one of the technical characteristics of the virtual currency led to a 20 percent decline in the value of Bitcoin over a single weekend.[28] Any system of regulation and governance for virtual currencies must contend with the fact that the developers who create many VCs do so in a manner designed to avoid control by centralized institutions of authority.

So what is the way forward for the governance of virtual currencies? How do policy leaders ensure that terrorist groups do not migrate to them and simultaneously support their innovative contributions to the financial system? Part of the answer requires changes to the current AML regulatory system—reforms to be discussed in greater detail in this paper. Another path is to create incentives for VC businesses themselves to see that preventing abuse is in their commercial interests. This is because a greater number of people will participate in a market in which they have confidence—which, in turn, requires that the public perception of VCs be positive. It also requires ordinary people to feel as though VC exchanges—the gateways between the fiat

What is the way forward for the governance of virtual currencies?

currency systems and new systems—will protect them against fraud. As described in this paper, this dynamic is what ultimately induced PayPal to develop one of the most sophisticated fraud prevention systems available. Ultimately it is the way in which any disruptive new technology may achieve scale.

The paper first describes contemporary methods of terrorist financing and the emerging virtual currency marketplace. Against this backdrop, the paper lays out strategies to better monitor terrorist use of VCs and adapt policies and regulations to guard against broader use. It concludes with specific policy recommendations to stakeholders.

02 CHAPTER

Setting the Stage: Contemporary Terrorist Financing and the Evolving Virtual Currency Landscape

Tracking and disrupting terrorists' financial networks is an important way to follow and impede their overall operations. Intelligence agencies, financial intelligence units including FinCEN, and law enforcement officials work to stay ahead of the evolving threat of terrorist financing, which is influenced by changes in the global financial system and the emergence of new financial technologies, among other factors. This chapter briefly summarizes the vulnerability of VCs to abuse by terrorists, and how terrorists have used this value transfer method in the past. To provide context, the chapter describes the general landscape of contemporary terrorist financing, as well as some of the important innovative uses to which VCs are being put. This framing underlies the challenge and need for financial policymakers to support innovation in VCs and new payment technologies while simultaneously guarding against their abuse.

Contemporary Terrorist Financing

Although terrorist financing requirements vary depending on the organization, they generally consist of funding specific operations and/or providing for the broader costs needed to maintain the viability of the terrorist organization and promote its ideology and objectives.[29] Large organizations require significant funding. Al Qaeda's pre-9/11 annual budget was an estimated $30 million,[30] while ISIS approved a $2 billion budget for 2015.[31] These large organizations often support operatives, some with dependents, who require income, training, and travel support.[32] Costs of specific attacks can vary greatly, from an estimated $10,000 for the 2015 Paris attacks to $400,000–500,000 for the 9/11 attacks.[33] Terrorist groups exhibit a great deal of variation, adaptability, and opportunism when it comes to their funding and are essentially willing to raise and move money any way they can.[34] Although traditional methods of doing this are still in use, including through criminal activities and by relying on banks, MSBs, and cash couriers, innovations unfolding in the 21st century digital economy are introducing changes.

SOLICITING AND RAISING MONEY

Terrorist groups' sources of revenue and fundraising activities combine traditional and new methods. According to FATF, these organizations depend on numerous sources of income derived from both criminal activities and the abuse of legitimate activities.[35] Examples of criminal activities include arms trafficking, kidnapping for ransom, extortion, racketeering, and drug trafficking.[36] Terrorist organizations and their associates also divert funds from legitimate sources such as charities and businesses.[37]

ISIS, described by senior U.S. officials as one of the world's best-funded terrorist organizations,[38] counts on a diverse array of sources.[39] According to U.S. Department of the Treasury estimates, ISIS earned approximately $1 billion in total revenue in 2015, $500 million of which came from the sale of oil and about $350 million from extortion.[40] Unlike most terrorist organizations, ISIS controls tracts of territory across Syria and Iraq.[41] It derives the most significant portion of its revenue from a range of illicit proceeds generated in areas where it operates.[42] This includes theft of cash, as well as assets stolen from banks, black market sale of natural resources such as oil and agriculture, and sale of stolen antiquities from within its controlled territory.[43] In 2014 and early 2015, ISIS obtained a windfall of between $500 million and $1 billion in Iraqi currency from bank vaults, while it made less than $10 million in trafficking antiquities.[44]

Apart from funding derived from the territory under its control, ISIS also has other prominent sources of funding. In 2014, ISIS earned between $20 and $45 million from kidnapping-for-ransom (this figure has since declined substantially, due to the reduced presence of potential Western hostages in or near ISIS-controlled territories).[45] The organization has received funding from wealthy, private, regional donors as well as foreign terrorist fighters who collect money for travel, travel with funds, and/or receive funding from external supporters.[46] ISIS's financial picture is dynamic, depending on the availability of resources and the status of coalition military operations.[47] For instance, oil and gas sales to the Assad regime have recently been an important source of the group's funds.[48] In fact, despite the Syrian regime's insistence that it is fighting ISIS with the cooperation of Russia and Iran, it purchases oil from the terrorist group, which sustains it in the face of military pressure.[49]

Unlike most terrorist organizations, ISIS controls tracts of territory across Syria and Iraq. It derives the most significant portion of its revenue from areas where it operates.

Terrorist groups have begun to view social media and crowdfunding networks as innovative and expansive new mechanisms for soliciting funds. In one case, a user placed a call for funds for a fighter in Syria on a Facebook page that provided recipes. The fighter supposedly needed "equipment, food, and pharmaceuticals," and the

user gave details of an account with a German bank.[50] This illustrates the ease with which anyone with access to the Internet can fundraise for a terrorism-related cause outside of traditional platforms.

Similarly, crowdfunding websites enable terrorists to set up a page and collect donations.[51] While these crowdfunding platforms have cooperated with investigations in the past, FATF has called for further study about their role in terrorist financing activity.[52] ISIS has made effective use of crowdfunding campaigns to garner support.[53] The group—along with other terrorist organizations in the area—has provided a menu of options for prospective crowdfunding donors to choose from, ranging from covering the cost of a weapon to financing an entire operation.[54] In some instances, the true purpose of a crowdfunding campaign is masked, so an individual may end up inadvertently contributing to a terrorist organization that claims to be engaging in charitable or humanitarian activities.[55]

MOVEMENT OF TERRORIST FUNDS

Traditionally, to move money terrorist groups relied on banks, money transfer systems, and cash couriers. These methods are still in use today. However, terrorist organizations continue to adapt to the pressure placed on their financial networks since 9/11, and they rely on means and resources that are now more varied and localized.[56] New, alternative methods to move money include the use of prepaid cards and digital payment systems.[57] These new methods facilitate transactions that are faster, more anonymous, and capable of global movements.

The formal financial sector remains attractive to terrorist organizations due to its reliability, vast size, and the speed and ease with which money can be moved.[58] To orchestrate the 9/11 attacks, al Qaeda extensively used banks in the United States.[59] Hijackers opened accounts in their own names and conducted small transactions that could pass unnoticed amid billions of dollars flowing through the formal financial sector.[60]

In 2010, for example, St. Louis resident Mohamud Abdi Yusuf was indicted and arrested for sending funds to al Shabaab supporters in Somalia from licensed MSBs, using fictitious names and phone numbers to conceal the purpose of his activities.[62] He was also charged with structuring financial transactions to avoid record-keeping requirements.[63]

Some terrorist organizations resort to physically moving cash across international borders.[64] This method is particularly common in regions where the electronic banking system is nascent or little used by the population.[65] An October 2016 FATF report noted that large, informal, cash-based economies in countries of West and Central Africa with porous borders and lack of financial controls create opportunities for the anonymous movement of money that leaves no paper trail.[66] According to captured internal al Qaeda in Iraq documents, between 2006 and 2007, funds brought by foreign fighters were estimated to make up more than 70 percent of the budget in the group's Border Sector 1 near Sinjar.[67]

Digital payment services such as PayPal, Amazon Pay, and Google Wallet may also be susceptible to abuse.[68] In 2015, Mohamed Elshinawy of Maryland was arrested and charged with attempting to aid ISIS. According to a criminal complaint filed by the Federal Bureau of Investigation (FBI), he received about $8,700 through Western Union and PayPal accounts from individuals abroad he believed had connections to ISIS, and the money was intended for "nefarious purposes."[69] Terrorism suspects have used multiple online payment accounts—both verified and guest accounts—to purchase equipment and clothing before traveling to conflict zones.[70] Some online payments companies such as Venmo have deployed scanning technologies to flag words and symbols associated with terrorism.[71] The prevalence of online payment services and purchases, of low-value transactions often involved, and the ease with which one is able to create accounts are the basis of the difficulty involved in definitively linking to terrorism transactions on these new payment platforms.

Large, informal, cash-based economies in countries of West and Central Africa with porous borders and lack of financial controls create opportunities for the anonymous movement of money that leaves no paper trail.

Terrorist organizations have also used MSBs and alternative remittance systems, financial services providers that often do not register themselves in order to avoid oversight within the regulated financial system.[61]

Counterterrorism officials are also focused on prepaid cards. Following the November 2015 Paris attacks, French government officials reinvigorated their scrutiny of prepaid cards because of their involvement in

financing the terror attacks.[72] Searches of the homes of individuals belonging to terrorist networks have turned up prepaid cards.[73] Last year the European Commission proposed stricter rules on the use of prepaid cards, including reducing the threshold for making anonymous payments from 250 to 150 euros.[74] Although policy-makers struggle to know the full extent of terrorists' use of prepaid cards, the amount of money each card can carry as well as its ease of use pose a significant threat in the terrorist financing context.

Terrorist Groups' Use of Virtual Currency

Virtual currencies may be appealing to terrorist groups for the same reason they appeal to legitimate actors. VCs are mainly distinguished by their global reach, often a decentralized structure, varying degrees of anonymity, rapid transactions, and minimal costs. The rapid, efficient, and less costly financial transactions that VCs enable account for their appeal to an array of actors.

The detection of illicit transactions conducted via VC rather than fiat currency is inherently challenging. Law enforcement officials and regulators may have difficulty accessing customer and transaction records that are distributed across different jurisdictions,[75] or that do not exist at all. Centralized VC systems may deliberately be located in jurisdictions with weak AML/CFT regimes.[76] The diffusion of infrastructures, entities, and services involved in transferring or executing payments in these currencies makes it challenging to assign jurisdictional responsibility for compliance and enforcement, while the evolving nature of VC technology and business models compounds the difficulty of tracking their use.[77]

Amid these forces, anecdotal evidence points to episodic terrorist use of VCs. According to Yaya Fanusie, the first publicly verifiable instance of a terrorist group using Bitcoin entailed a social media fundraising campaign run by the media wing of the Mujahideen Shura Council in the Environs of Jerusalem, a collection of Salafi-jihadist groups in Gaza designated by the U.S. State Department as a foreign terrorist organization. The campaign began in July 2015, and it added the option for donors to pay in Bitcoin in June 2016. As of August 2016, the campaign had received roughly 0.929 bitcoins (around $540) through two transactions that occurred six days apart in July 2016, despite seeking at least $2,500 per fighter. The identity of those responsible for making the deposits is unclear, but Fanusie suggests they are proficient Bitcoin users and employed techniques to preserve their anonymity.[78]

ISIS supporters' activities have also shown the potential for terrorist groups to use virtual currencies on a global scale. Most recently, Indonesia's financial-transactions agency announced that Bitcoin and online payment services had been used by Islamic militants in the Middle East to fund terrorist activities in Indonesia.[79] In August 2015, a computer intruder with ties to ISIS who went by the user name "Albanian hacker" demanded payment of two bitcoins from an Illinois Internet retailer in exchange for removing bugs from their computer. Using data extracted from the server, the Albanian hacker put together a "kill list" for ISIS with identities of 1,351 U.S. government and military personnel.[80] In June 2015, Ali Shukri Amin, a 17-year-old in Virginia, pled guilty to conspiring to provide material support and resources to ISIS. Among other wrongdoings, including facilitating the travel of ISIS supporters to Syria, he used social media to instruct donors on the use of Bitcoin to provide untraceable financial support to the group.[81] In May 2015, "Abu Ahmed al-Raqqa" appealed to supporters of ISIS for donations in the form of Bitcoin on the dark web.[82] In January 2015, *Haaretz* reported on the first instance of an ISIS cell fundraising using Bitcoin on the dark web. The fundraiser was a man identified as Abu-Mustafa, and his Bitcoin account number indicated that he had managed to raise five bitcoins (approximately $1,000) before the FBI shut down his account.[83] More broadly, a number of forum discussions on websites affiliated with the group show efforts by more technical members to educate their peers on the use of virtual currencies.[84] Participants have also referenced using VCs to transfer money to countries where traditional transactions are difficult due to lack of network capacity or surveillance and regulation.[85]

Participants have also referenced using VCs to transfer money to countries where traditional transactions are difficult due to lack of network capacity or surveillance and regulation.

Selected Episodes of Terrorists Using VCs[86]

January 2015

Haaretz reports first ISIS use of Bitcoin in the dark web. Supporter Abu-Mustafa is able to raise **five bitcoins** (approximately **$1,000**) before his account was shut down by the FBI.

May 2015

"Abu Ahmed al-Raqqa" appeals to supporters of ISIS for **donations** in the form of **bitcoins** on the **dark web**.

June 2015

Seventeen-year-old Virginian Ali Shukri Amin **pleads guilty** to conspiring to provide material support and resources to ISIS. Amin used **social media** to instruct donors on the use of Bitcoin to provide untraceable financial support to **ISIS**.

August 2015

ISIS-linked computer intruder "Albanian hacker" **demands** two bitcoins (approximately $500) from an Illinois internet retailer **in exchange** for removing bugs from its computer.

July 2016

The **media wing** of the Salafi-jihadist group Mujahideen Shura Council in the Environs of Jerusalem receives about 0.929 bitcoins (approximately $540) in two separate transactions after adding the option of **Bitcoin donation** in June 2016.

January 2017

Indonesia's financial-transactions agency announces that **Bitcoin** and online payment services were used by Islamic militants in the Middle East to fund **terrorist activities in Indonesia**.

These instances of terrorist groups using virtual currency indicate that the phenomenon is, at the moment, episodic and not widespread. The "firsts" of terrorist groups using VCs are fairly recent; they appear to still be familiarizing themselves with this new form of value transfer. Where the amount of virtual currency involved has been reported, it has tended to be small. The U.S. government is not inordinately concerned about this threat; David Cohen, former Undersecretary of the Treasury for Terrorism and Financial Intelligence, noted in 2014 that terrorists generally need "real" currency to pay their expenses, rather than employing VCs.[87] A 2015 RAND report posited that there was little evidence terrorists were developing their own VCs.[88] According to a January 2016 Europol report, "Despite third party reporting suggesting the use of anonymous currencies like Bitcoin by terrorists to finance their activities, this has not been confirmed by law enforcement."[89] Scholars generally agree that while virtual currencies have gained in popularity, their expansion among terrorist organizations has been slow and has lagged behind transnational criminal uses of the technology.[90] The following chapter explores some of the reasons for which terrorist groups have been slow to adopt virtual currencies.

Scholars generally agree that while virtual currencies have gained in popularity, their expansion among terrorist organizations has been slow and has lagged behind transnational criminal uses.

The Evolving Virtual Currency Landscape

Information technology and the spread of the Internet have revolutionized the financial system. Populations previously excluded from financial markets can now save, transfer, and exchange money with more ease, at greater speed, and with fewer costs. A 2015 U.S. study found that Internet access reduced the probability of not having a bank account by 9.8 percent for individuals in the lowest income decile and by 7.1 percent for the whole population.[91]

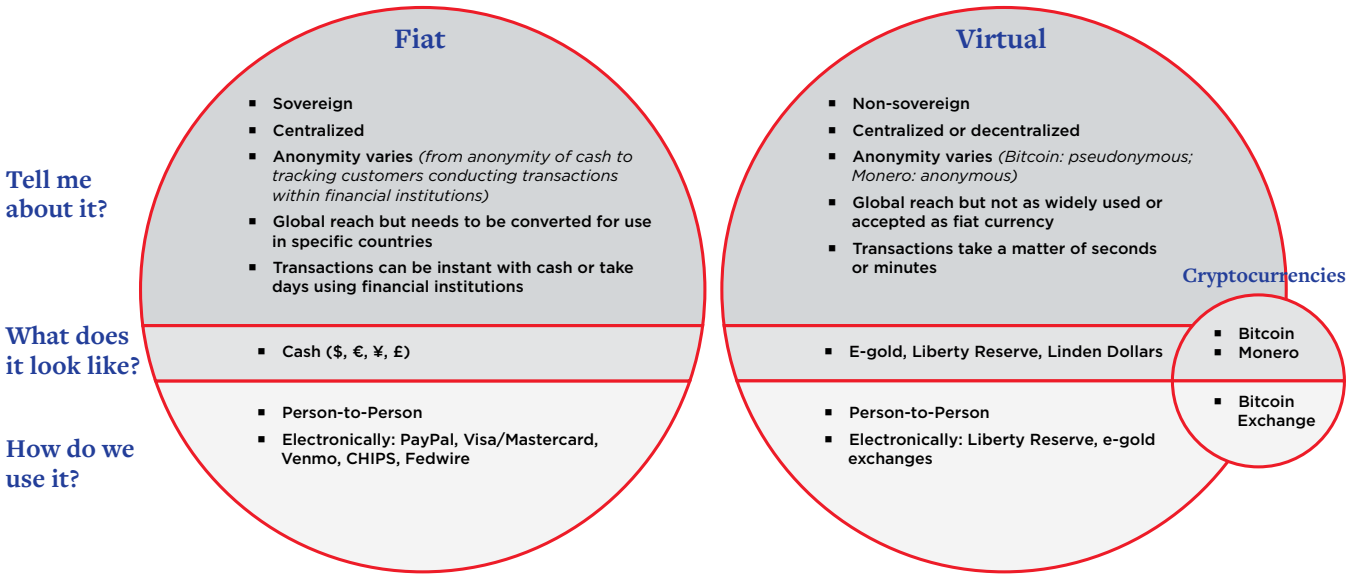
Mobile technologies allow people in developing economies to make small-value electronic payments from mobile phones. Kenya's M-Pesa and similar mobile money systems—used by 86 percent of Kenyans[92]—show how mobile technology makes financial services accessible in a country with almost 25 times fewer ATMs per person than in the United States.[93] Although this mechanism of transferring money does not serve as a primary medium of illicit finance,[94] some experts believe it is simply a matter of time and proper regulatory oversight before violations are discovered.[95] These technologies are more prolific, and therefore potentially more of an immediate security threat, than virtual or cryptocurrency technology such as Bitcoin. According to a study tracking growth during the months since their respective releases, Bitcoin grew at about 5 percent of M-Pesa's rate.[96] The widespread nature of M-Pesa, combined with limited oversight, has led some experts to be concerned. One analyst argued that SMS systems "fail to provide the protections needed by financial services."[97] Another explained, "Simply put, mobile payment systems can be considered the 'Wild West' for savvy criminal organizations."[98]

Online and peer-to-peer money transfer services such as Xoom Corp. and Venmo are disrupting not only the remittance market,[99] one of the slowest and most expensive subsectors of consumer finance, but also traditional payment forms, for example cash and checks.[100]

VIRTUAL CURRENCY TYPOLOGY

Virtual currencies, and especially cryptocurrencies, are at the leading edge of this financial revolution. While they vary along three main axes, VCs lack sovereign backing. First, these currencies can be non-convertible or convertible. Non-convertible currencies operate within a closed virtual platform. Examples include currencies used in massively multiplayer online role-playing games, where no sanctioned mechanism exists to translate the virtual unit into fiat currency. In these systems, however, black market exchanges may spring up, effectively offering some degree of convertibility.[101] Convertible currencies, by contrast, have a defined equivalent value in fiat currency and can be exchanged, through either floating or pegged rates.[102] Second, VCs vary in their degree of anonymity. Generally they fall between the almost total anonymity of cash exchanges and the traceability and disclosure of online payments through the traditional banking system, making them appealing to legitimate users concerned about privacy.[103]

Currency Typology



Recently, new entrants in the VC space have focused on complete anonymity by developing techniques to obfuscate the true origins of Bitcoin transactions.[104] Cybercriminals are making use of new cryptocurrencies such as Monero, which has been called the "drug dealer's cryptocurrency of choice,"[105] because of its enhanced anonymity properties. In August 2016, Monero rose to prominence after AlphaBay, the dark web market, started accepting it as a Bitcoin alternative.[106] It attempts to ensure users' privacy by combining multiple transactions, hiding the amount of each transaction, and obscuring the recipient of the funds.[107] By January 2017, it had become 27 times more valuable due to its adoption in online criminal markets.[108] It is already drawing the attention of law enforcement for its facility of use by criminals on the dark web.[109] Similarly, Dark Wallet, which seeks to make de-anonymizing Bitcoin transactions impossible, disrupts the blockchain's potentially identifying aspects by combining random contemporaneous transactions and then encrypting recipients' information so it does not appear on the blockchain.[110] This method explicitly seeks to enable illicit finance; as one of its founders stated, "It's just money laundering software."[111] Dark Wallet has been commended on blogs supportive of ISIS.[112]

Decentralized VCs have no central administrator or oversight, and trust is based on consensus validation.

Finally, VCs may be centralized or decentralized. Fundamental to this distinction is the question of how to engender trust without government or central bank backing. For centralized VCs, an administrator issues the currency, maintains a unified central payment ledger, and retains the power to withdraw currency from circulation.[113] This central institution acts as the ultimate repository and guarantor of trust. Examples include Linden Dollars, available in the Second Life virtual reality world; Perfect Money; units of the now-defunct e-gold; and LRs, units used on Liberty Reserve.

As discussed above, decentralized VCs have no central administrator or oversight, and trust is based on consensus validation. They often rely on cryptography for their operations and use distributed ledger technologies to record transactions. As the most widespread decentralized VC, Bitcoin has also faced the most real-world vetting. It survived a software glitch in 2013 and a security breach and bankruptcy of its largest exchange in 2014. It has found acceptance as a currency among retailers including popular websites, for example Expedia and Overstock.com.[114] As circulation broadens and trading volume increases, it may become more stable.[115]

KEY ADVANTAGES OF VIRTUAL CURRENCIES

Virtual currencies such as Bitcoin offer two primary benefits compared with legacy financial technology—lower costs and faster transaction speeds.[116] Lower transaction costs were an important goal identified by an anonymous founder—or team of founders— known as Satoshi Nakamoto when conceptualizing Bitcoin.[117] As Nakamoto noted, requiring financial institutions to act as trusted third parties in transfers raises the overall costs.[118] In 2015 the global average cost of sending a $200 remittance, for example, was close to 8 percent.[119] Although diminished from the 9.7 percent average in 2009, this cost remains far above the 1 percent average fee, per Goldman Sachs estimates,[120] and even above the 3 percent fees associated with Bitcoin transfer systems popular in East Asia.[121]

VCs allow for improved speed of transactions by adapting the method of recording the value transfers with very low latency periods.[122] Increased transaction speeds unlock ancillary advantages as well. Faster transfers reduce settlement and credit risks involved in waiting for funds to transfer, and they enable parties to use capital more effectively.[123] Greater speed also reduces a user's exposure to exchange rate fluctuations, a source of concern given the volatility of many early-stage VCs.[124] The current concern over the scalability of Bitcoin highlights how important speed is to virtual currencies. As the scale and use of these currencies has increased, the time to validate each transaction has grown as well, leading supporters to search for technical solutions and skeptics to wonder whether the inability to process a growing number of transactions at sufficient speeds will impose a ceiling to the technology.[125]

The potential of VCs to bring about benefits can be seen in the remittance market. Payphil, Sentbe, and similar Bitcoin transfer services have halved remittance costs between South Korea and the Philippines, and they account for 20 percent of the total remittance flows between the two countries.[126] Circle Internet Financial, for example, provides free remittance services using blockchain. Circle is also registered as an MSB, enabling the company to provide many other financial services. The company is licensed in the United Kingdom and has partnered with Barclays Bank.[127] This partnership allows customers to exchange the British pound and U.S. dollar immediately for free.[128] It is worth noting, though, that unlike direct Bitcoin transfers, many Bitcoin remittance services and exchanges are more akin to payment systems,[129] benefiting from the ease of exchange of VCs without the risks of anonymity or pseudonymity.[130]

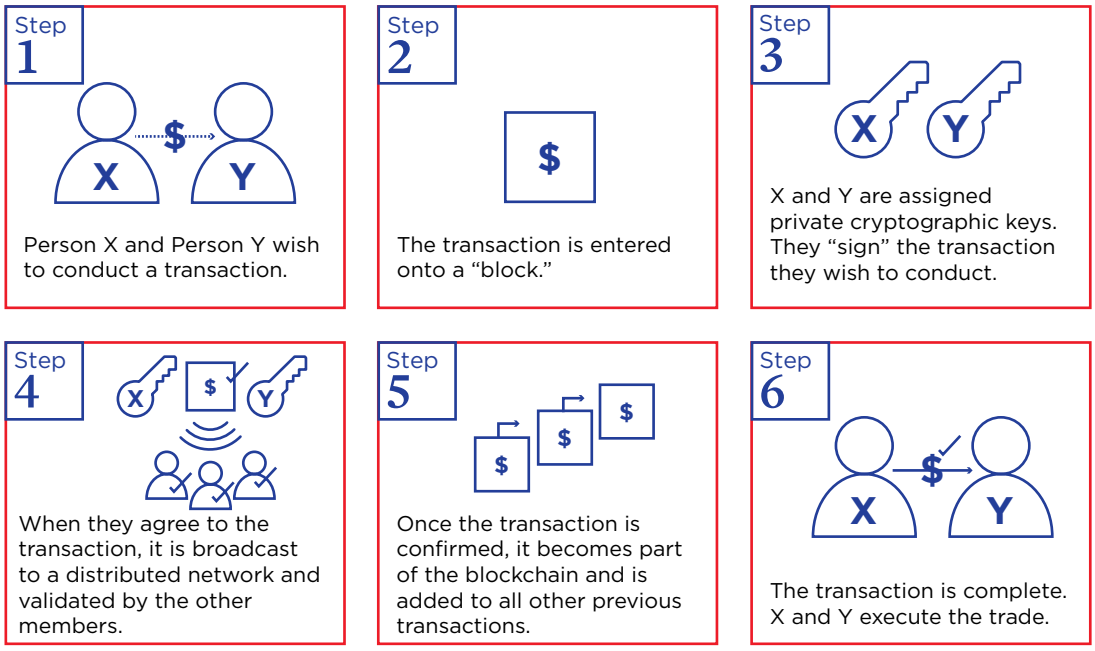
BLOCKCHAIN

A blockchain is a type of distributed ledger, a copy of which is stored on each instance of a distributed system. Each new entry (known as a block) is certified through the creation of a unique fingerprint that incorporates the previous block, forming a "chain" and cryptographically creating an indelible record of previous transactions.[131] All copies of the blockchain are updated with changes that take place. In the case of Bitcoin, the blockchain is public, records transactions, and enables the cryptocurrency to be decentralized.[132]

The blockchain's appeal as a secure, decentralized database has provoked speculation about its potential for applications across a range of fields. Blockchains can potentially be used to streamline financial transactions;[133] track the origins and legitimacy of precious gems;[134] improve the insurance industry;[135] create secure patient records across healthcare systems;[136] maintain accurate international customs, shipping, and distribution records;[137] secure voting;[138] and help protect property in unstable markets by creating a more stable non-state ownership record network.[139]

But potential obstacles remain to the blockchain's expansion, including because of its indelibility and irreversibility. Human error, hacks, and laws governing consumer rights to data deletion or correction pose challenges for the broad adoption of the blockchain. For example, after fraudulent Bitcoin transactions lost customers tens of millions of dollars in August 2016, the blockchain's irreversibility hindered the amelioration of the breach.[140] And in most of the blockchain's potential applications, the database would only be viewable by a select audience, unlike the public Bitcoin blockchain.

What Is a Blockchain?[141]



03 CHAPTER

Evaluating the Potential for Terrorists to Abuse Virtual Currencies

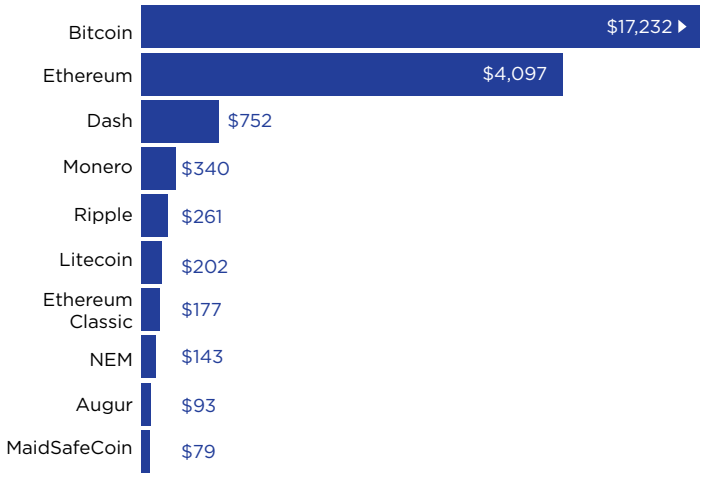
For policy and security leaders focused on countering terrorism, the core question about VCs is when they will reach the kind of scale at which both terrorist groups and their funders can use them with sufficient ease that it becomes a value transfer mechanism of choice. As the previous chapter demonstrates, there is anecdotal evidence that terrorist groups or terrorists working independently have used Bitcoin or have solicited donations in Bitcoin, although there is not yet public evidence that they have begun to do so at scale. Setting aside these more limited instances of terrorists' use of Bitcoin, as a general matter such cryptocurrencies have only really begun to achieve significant scale in a limited fashion, and not yet in the terrorist financing realm. Although scholars and experts are just beginning to rigorously study how and why VCs and payment systems grow and achieve scale and sustainability, policymakers must prioritize these questions to assess potential illicit finance threats prospectively.

To illustrate the importance of scale, Bitcoin, the largest and most widely used cryptocurrency, has an approximate market capitalization of $17 billion as of March 20, 2017.[142] Newer cryptocurrencies are far smaller; Monero's market capitalization for example, is approximately $340 million,[143] and that of ZCash about $22 million (as of early 2017).[144] By contrasting this to the scale of terrorist financing specifically and illicit financing more generally, it is clear that at present, the role that cryptocurrencies can play in illicit activities is structurally limited, especially in comparison with more common means of financing illicit activity. In 2014, in ISIS's most flush period, it brought in $2 billion.[145] The U.S. government estimates that illicit financing generates $300 billion per year,[146] while more than a trillion dollars' worth of illicit financing is raised and moved globally.[147]

> **Scholars and experts are just beginning to rigorously study how and why VCs and payment systems grow and achieve scale and sustainability.**

Studying previous instances in which new payment methods and VCs have scaled, and the ways in which they have been abused by criminal groups, offers a sense of the conditions that may be necessary for VCs to become vulnerable to abuse by terrorists. Such an analysis is useful even though there are fundamental differences between criminal groups and terrorists in the volume of money they move and their ultimate aims. This is because previously new payment technologies such as PayPal were trying to solve the same problems that VCs aim to address today—namely, moving money more quickly and more cheaply in an increasingly globalized environment, often with a commitment to escaping the control of centralized institutions. It also gives a sense of how the characteristics of VCs might change as the currencies grow in users and size, and how those changes may affect their potential for abuse by illicit actors. Thus, notwithstanding the important differences between how criminals have used new payment technologies and VCs in the past and the concerns about terrorist financing today, previous examples are instructive.

Virtual Currencies Market Capitalization *(in millions)*



"CryptoCurrency Market Capitalizations," CoinMarketCap.com, March 20, 2017, https://coinmarketcap.com/.

How New Payment Technologies Grow and Scale

Three of the key characteristics that determine the scale that virtual currencies can reach are their degree of centralization, their liquidity and convertibility, and the network effects—whereby a service becomes more useful to all users the more people use it.

CENTRALIZATION

As virtual currencies and payment systems expand, it is likely that they will become increasingly de facto centralized, even though they began as a deliberately decentralized system. Experts have observed that online peer production projects (e.g., Wikipedia) likely conform to the so-called iron law of oligarchy, which holds that even organizations set up in a distributed fashion will increasingly converge around a few institutions as they grow.[148] This is in part because as more people begin to use VCs and cryptocurrencies, investments in necessary infrastructure (such as exchanges) will become less expensive as economies of scale take hold. Additionally, users will have more confidence that a transaction will go through, which will reduce volatility and make currencies more consumer-friendly.

Bitcoin, for instance, shows incipient signs of behaving in a manner consistent with the iron law of oligarchy. As scholars have observed, although Bitcoin's founders emphasized its decentralized characteristics, this does not accurately describe how it functions today. Specifically, although the "Bitcoin protocol supports complete decentralization, . . . significant economic forces push towards de facto centralization and concentration" throughout the system.[149] This centralization manifests in several ways. For example, Bitcoin exchanges in well-supervised jurisdictions such as the United States are highly centralized because of regulatory requirements and the technical security requirements necessary to maintain the integrity of a Bitcoin exchange. Moreover, Bitcoin is generated by "mining," in which computers solve mathematically challenging problems (requiring more computing power) to create new bitcoins. These problems become more difficult over time, and miners have brought together their resources into large mining pools, threatening Bitcoin's decentralization.[150]

LIQUIDITY AND CONVERTIBILITY

Liquidity and convertibility are essential components for any currency, including virtual currencies, to become usable by large groups of people. A currency needs to be useful for purchasing a variety of goods or it will be challenging for that system to scale and gain prominence. It also needs to feature easy convertibility to fiat currency. Some liquid, highly convertible, nearly anonymous stores of value do exist and are extremely common. For example, gift cards to Amazon.com approach the liquidity of cash, are easy to obtain—and represent a growing money laundering threat.[151] In March 2016, the U.S. Department of Homeland Security filed a warrant application in which it alleged that 5dimes, an offshore gambling site, used Amazon gift cards to launder almost $2 million. The site offered incentives for gamblers to use Amazon gift cards over other methods of funding their accounts.[152]

For similar reasons, online gift cards are becoming increasingly appealing to terrorists. In January 2017, a Washington transit police officer was arrested for attempting to provide financial support to ISIS by using Google Play gift cards (he gave them to an FBI informant rather than a true supporter of ISIS).[153] Because online gift cards illustrate the kinds of characteristics—liquidity and convertibility—that are needed for a payment mechanism to be used by a large number of people, it is necessary to develop a strategy to avoid their becoming vehicles for illicit finance.

Bitcoin shows incipient signs of behaving in a manner consistent with the iron law of oligarchy.

Case Studies: Abuse of New Financial Technology by Illicit Actors

Exploring several case studies demonstrating how criminals and other illicit actors have employed new payment systems illustrates a number of the dynamics outlined above. Criminals may precede terrorists in abuse of VCs as they seek new pathways to avoid the restrictions of the formal financial system. Understanding how this may occur, and some of the methodologies that could be used, will help supervisors and regulators contemplate adequate protections against such abuse. With this information, they can better avoid the use by illicit actors of new financial technologies as they connect a larger network of people, and as the currencies themselves become easier to use.

PAYPAL

This payment technology met an important market need for easier payment methods and improved user interfaces. It achieved scale and broad market penetration while simultaneously protecting against illicit activity. PayPal was officially launched on October 22, 1999.[154] By April 2000, it had 1 million users,[155] and it developed a niche as a credit-card processing service.[156] In August 2002, eBay announced plans to buy PayPal after finding that the service was vastly preferred among eBay customers.[157] This is a prominent example of how network effects can contribute to exponential growth of a business, particularly in the payments space. As more eBay customers used PayPal, it was more advantageous for non-PayPal users to adopt the method, and PayPal was able to push out other competitors. This eventually led to a partnership with an enormous e-commerce merchant. In 2015, eBay spun off PayPal with a second initial public offering.[158] By the end of 2016, its revenue was $10.84 billion, processing 6.1 billion individual transactions, with 197 million active accounts.[159] Its early market strength allowed it to make acquisitions and engage in product development to retain a presence in the now-competitive new payments space.[160]

Importantly for regulatory purposes, PayPal has classified itself as an electronic money transmitter rather than a bank, although it performs bank-like functions, providing accounts, facilitating payments, and even giving loans to customers.[161]At this time, only 20 banks in the country hold more money than PayPal—as of March 2016, it held about $13 billion, just behind TD Bank and Capital One, in accounts that clients could use to buy things online or link to another account, for example a credit card or bank account.[162] Rather than competing with cash the way some virtual currencies do, it instead competes with credit cards, banks, and other payment transfer systems. This distinguishes PayPal from the VCs that are now emerging, which self-consciously seek to circumvent the formal financial system.

PayPal's early market strength allowed it to make acquisitions and engage in product development to retain a presence in the now-competitive new payments space.

PayPal's focus on fighting fraud was fundamental to its success because it allowed the service to distinguish itself from peers. As a major player in the payment space, PayPal's continued focus on fighting fraud must keep pace with evolving tactics used by terrorists. (Guruofsales/Flickr)

Because PayPal allowed (and continues to allow) chargebacks,[163] fraud had the potential to derail the business from the outset.[164] As a result, its founders deliberately focused on how to manage the fraud and crime risk attendant to an online, international payment system.[165] In the summer of 2000, when systematic fraud attacks from organized crime and cybercriminals hit PayPal, company executives realized they needed to tackle fraud head-on or risk significant harm.[166]

Immediately the company invested significant resources in detecting and preventing fraud. Among the most important tools they developed was a machine learning system named Igor, which used advanced analytical techniques to evaluate and understand patterns of fraud across the company. Igor would later become the basis for a new company, Palantir Technologies, spun off by one of PayPal's founders.[167]

Thus PayPal's fraud problem, instead of spelling doom for the company or becoming an inflection point into an illicit finance service, allowed it to distinguish itself from its competitors in a way that became a permanent

advantage. An early commentator noted that "the backbone of PayPal's success is its fraud squad."[168] This led to a cascade of business advantages, including charging customers a low transaction fee relative to credit card companies, which was only possible because of the aggressive and successful fraud detection and mitigation system.[169]

PayPal had other innovations that gave it its foothold in the digital payment market. It debuted novel Know Your Customer (KYC) techniques; for example, when a user requested that PayPal have direct access to an account to deposit or withdraw money, the company would make two small test deposits (a few or several cents each). The user would then have to confirm the exact amounts of the deposits with PayPal.[170] The company is also based around email; each account is limited to one email, and recipients are known by their email rather than name, physical location, or bank account information.[171] This was much easier than asking users to download software or employ complicated security systems, as competitors were doing at the time. PayPal solved both a convenience and a security challenge through this method. Payments themselves were not sent over email; only notifications of payments were transmitted over the Internet, while the money flowed between PayPal servers disconnected from the Internet.[172]

PayPal's fraud problem allowed it to distinguish itself from its competitors in a way that became a permanent advantage.

Instead of seeing counter-illicit finance protections as a burden and an obstacle to effective commerce, PayPal saw them as indispensable to the viability of its business. Yet although PayPal is generally a success story of corporate growth and sustainability without compromising integrity or ability to innovate, no system is perfect. In 2009, PayPal admitted to violating aspects of Australia's AML-CTF law and made an arrangement with the government to address its policies and avoid further issues.[173] More recently, in March 2015, PayPal agreed to pay the U.S. Treasury $7.7 million for violating sanctions by transacting with Cuba, Sudan, Iran, and Turkish nationals blacklisted for proliferation of weapons of mass destruction.[174] At the time of the settlement, the U.S. government explained that PayPal had failed to "implement . . . effective compliance procedures and processes to identify, interdict, and prevent transactions" that violated sanctions, "despite processing a high volume of transactions and maintaining an international presence."[175] In response, PayPal settled with the government and adapted its compliance system.[176]

Even after PayPal instituted procedures designed to ensure adherence to sanctions and anti-fraud measures, in December 2015, the cybersecurity journalist Brian Krebs detailed an incident in which his account information was involuntarily reset by hackers, and money from his account was transferred to terrorist-linked groups.[177] So while PayPal's early success in scaling could largely be attributed to its innovative anti-fraud tactics, now that it is a giant in the payment space, it needs to continue evolving as cybercriminals and terrorists become ever-more technologically advanced. Key for the purposes of evaluating the vulnerability of this technology to terrorist financing is that PayPal initially viewed investment in sophisticated anti-fraud techiques as the foundation of its business success.

E-GOLD

In contrast to PayPal's successful evolution, e-gold, a virtual currency and bespoke money movement system, failed as a business enterprise because it did not do enough to keep out illicit activity. Continued investigations by law enforcement ultimately made it non-viable. E-gold was created in 1996 as a monetary system based around a VC backed up by gold, independent from any government.[178] The founder of e-gold sought to create a "private, international currency," isolated from the market swings of ordinary currencies and instead linked to gold.[179] Other VCs that started around the same time failed, mainly because of customers' reluctance to pay fees to convert fiat currency into virtual currency.[180] But by 1999, commentators deemed e-gold "the only electronic currency that has achieved critical mass."[181] In 2001, an article argued that the "ideal e-currency might even be backed by gold," and praised e-gold's transparency to customers.[182] A 2002 profile in *Wired* lauded it for "quietly thriving" while other VCs and similar systems failed, describing its mission as "not simply better money but the best."[183]

To use e-gold, one had to open an account online; convert a fiat currency into e-gold by using an e-gold exchanger who facilitated getting money into and out of the system; use e-gold to transfer funds or purchase or sell a good or a service; and then exchange e-gold back into fiat currency through the same system of exchangers.[184] These elements of the system—its intentional self-containment, limited connections to the formal financial system, and creation of a novel way to

store and transfer value—would reappear in later financial networks. For example, Liberty Reserve and Silk Road were systematically abused by criminals.

E-gold differentiated itself from its competitors in a few ways, all of which contributed to its ability to scale. First, it was the first virtual currency to be backed by gold,[185] which gave customers a confidence that most VCs could not and appealed to customers who had concerns about the formal banking system.[186] This innovation was so appealing that it spurred the development of several similar currencies.[187] Such a use of gold meant the service was grounded in a formal, inherently trusted institution. Second, it was extremely cheap, at a cost of 1 percent per transaction up to $5 and 50 cents for every transaction after that.[188] Third, it intentionally did not have any identification verification procedures, purporting to protect the privacy of customers.[189] It differentiated itself from PayPal by having no consumer verification procedures.[190] Fourth, it also distinguished itself from PayPal by being irreversible: once transactions were made, there were no chargebacks.[191] A libertarian philosophy supported both its use of gold as backing and its refusal to request identification from its users.[192] Its founder, Douglas Jackson, argued that e-gold was not subject to regulation as a payment system distinct from a money transmitter and a bank, though it had qualities of both.[193]

E-gold's anonymity, ease of use, and inexpensiveness made it appealing to illicit actors.

E-gold became quite successful—in its prime, it had more than 8 million accounts open and $85 million in cash assets.[194] But a few years after it began to build a following, the criminal activity taking place on e-gold drew scrutiny. Experts noted the similarities of systems such as e-gold to hawala services, and argued that it was only a matter of time before terrorists started using e-gold to finance their activities. They pointed to one case where the U.S. and Russian governments requested information about a potential terrorist using the system; the user had threatened an attack if a ransom was not paid into his or her e-gold account.[195] In December 2005—after a year in which transactions worth $1.5 billion were conducted through e-gold, generating $2 million in revenue—the FBI and Secret Service raided the offices of e-gold's parent company.[196] A year later, in 2006, Douglas Jackson made a public show of helping law enforcement find violations in his service, searching user records and transaction history, compromising his libertarian beliefs in an effort to save himself and his company.[197]

Although Jackson worked with the government, providing information that led to arrests, and was working on making e-gold a "clean" service, such efforts were too little too late.[198] In April 2007, e-gold was charged by the U.S. Department of Justice and U.S. Attorney for the District of Columbia with violating money transmission laws and knowingly providing fund transfers to criminals.[199] The indictment identified concerns about VCs continuing to be used by criminals and becoming appealing to terrorists as well.[200] Prosecutors asserted that more than 70 percent of the 65 most valuable e-gold accounts were associated with criminal activity.[201] As a result, the assets of e-gold were seized, including what the defendants claimed were all of their assets in related bank accounts.[202] At the time, though, government officials admitted that e-gold fell into a regulatory blind spot where it was not required to self-report suspicious activity.[203] The three defendants were spared jail time after pleading guilty to money laundering and running an unlicensed money transmitting business. Although the company initially attempted to reform its customer verification processes and register appropriately with regulators, the service did not survive these legal proceedings.[204]

Considering the lessons from e-gold's growth and demise for the development of future systems that might finance terrorism, e-gold's anonymity, ease of use, and inexpensiveness were the attributes that made it appealing to illicit actors. In particular, e-gold's commitment to anonymity was correctly perceived as a clear advantage for criminal and terrorist financiers. Other aspects, including its backing by gold, would be less necessary and more incidental for terrorist groups seeking to finance their operations. Finally, its operations in the United States gave U.S. law enforcement the reach and power needed to deal a serious blow to the business. Terrorists seeking to avoid exposure to U.S. law enforcement may have learned from this example, among others, to avoid financial avenues and technology in U.S. jurisdiction.

LIBERTY RESERVE

Liberty Reserve, created in 2006, promptly and deliberately filled the gap that e-gold left in the illicit finance space; two of its founders had run a company that was an exchanger for e-gold.[205] It served as a bank, money transmitter, and virtual currency to the criminal underground until it was shut down in 2013.[206] To put money into a Liberty Reserve account, any money transfer service, including postal money orders, credit cards, and bank wires, could be used to convert funds into one of

Liberty Reserve's two currencies, which were pegged to the euro and dollar, respectively.[207] An LR, as the unit of currency was called, could be sent to anyone else with a Liberty Reserve account, who could then withdraw it in exchange for fiat currency.[208]

Liberty Reserve emphasized anonymity, which was a large part of why it grew. Although it nominally required a name, address, and birthday, investigators were able to create accounts with obviously fake information.[209] As investigators noted, Liberty Reserve did not validate the information, and the same user could open multiple accounts; a valid email address was the only technical requirement to establish a Liberty Reserve account.[210] Its structure facilitated money laundering in a fashion similar to the e-gold system, and it drew on many of the same techniques. To deposit or withdraw currency into or from an account on the site, one had to pass the money through exchangers, who bought LRs in large quantities and charged a transaction fee. This way, an account on Liberty Reserve would have no identifying information about its customer.[211] For an additional small fee (75 cents per transaction), Liberty Reserve hid users' account numbers when they sent money to others, thereby making their transactions untraceable.[212] In addition, the company offered a private messaging system that it advertised as "much more private and secure than email or instant messenger."[213] Finally, although it was slightly more expensive than e-gold, it still had a nominal transaction fee. The company charged a 1 percent commission on every transaction within its system up to $2.99,[214] though there were additional fees to convert currency in and out of the system. These fees could become substantial for larger transaction amounts.[215]

Liberty Reserve, like e-gold, became a hugely important part of the VC ecosystem during its seven-year lifespan, because it made communications and transactions with criminals easy and inexpensive. From 2009 to 2013, it processed $300 million per month in transactions and about 78 million separate financial transactions.[216] When it was shut down in 2013, it had 5.1 million users, 600,000 of whom claimed to be based in the United States.[217] The website's founder, Arthur Budovsky, maintained that he originally created it for people without bank accounts to buy and sell goods on the Internet, playing an equivalent role to PayPal for people without bank accounts.[218] Indeed, there is reason to believe that not all of the transactions conducted on Liberty Reserve were illegal.[219] But at its heart, Liberty Reserve was driven by criminal activity; the 500 biggest accounts on its service created 44 percent of its business, and of those, 32 belonged to credit card thieves and 117 to Ponzi scheme operators.[220]

This criminal activity drew law enforcement to Liberty Reserve. In 2010, the U.S. Secret Service began investigating the company; by 2011, the Global Illicit Financial Team took over the investigation.[221] Although Liberty Reserve's main operation in Costa Rica was shut down between November 2011 and May 2013, the company continued to run through Budovsky's other businesses.[222] Finally, in May 2013, Liberty Reserve was permanently shut down as the United States brought charges against several key persons in the operation. Budovsky was sentenced to 20 years in prison and was extradited from Spain to serve his sentence; his co-founder, Vladimir Kats, was sentenced to 10 years.[223]

After Liberty Reserve was taken down, much of its customer base went to a centralized virtual currency platform called WebMoney.[224] Europol's 2016 "Internet Organised Crime Threat Assessment" cited WebMoney as a common centralized service for criminals, especially for payments between criminals, although its popularity has decreased compared to currencies like Bitcoin.[225] WebMoney does not allow U.S. citizens to open accounts, thus attempting to seal itself off from U.S. jurisdiction.[226]

Liberty Reserve demonstrated that a niche market exists for a trusted illicit finance network on the dark web.

The example of Liberty Reserve is relevant to the threat of terrorist financing in a few ways. Like e-gold, this system innovated through using exchangers, creating another layer of anonymity and obfuscation between the system and potential criminals, in addition to offering further privacy-enhancing services for a fee. Arguably, any system used by terrorists in the future would entail this as well as potentially additional anonymity innovations. Liberty Reserve also demonstrated that a niche market exists for a trusted illicit finance network on the dark web. Finally, like e-gold, Liberty Reserve was shut down by the U.S. government, a lesson from which future systems for terrorist financing might learn by developing systems with limited or protected access to the U.S. financial system.

BITCOIN

Bitcoin's characteristics—including its irreversibility, use of the blockchain, pseudonymity, and decentralization—make it "more flexible, more private, and less amenable to regulatory oversight," as experts have explained.[227] As has been noted, although no more than anecdotal evidence exists indicating that Bitcoin is being directly used to finance terrorism, it has proven to be a useful tool for illicit financial activity more broadly. Early users bought narcotics on Silk Road, an illegal online marketplace, and gambled.[228] These types of crimes are increasing in sophistication and complexity. More recently, in January 2016, 10 people were arrested in the Netherlands on charges related to money laundering through Bitcoin.[229] According to Europol, Bitcoin is becoming more prominent in investigations of payments between criminals, and was estimated to be responsible for more than 40 percent of these payments in the European Union in 2015.[230]

A major obstacle to Bitcoin scaling as a tool for terrorism finance is the blockchain, the publicly accessible ledger that records all transactions that take place through Bitcoin. Thus while Bitcoin wallets are not necessarily linked to real identities (though exchanges in well-regulated jurisdictions do establish these links), it will always be possible to unravel a chain of transactions. Experts including Aaron Brantly have explained that cryptocurrencies are part of the arms race of cryptography: "As one person develops a cryptographic algorithm allowing transactions to be more anonymous, another person immediately begins work on solving it to peel back the anonymity."[231] Once the sequence of transaction is revealed, Bitcoin addresses can be linked to real-life identities through forensic techniques, after which one's entire transaction history becomes visible.

Bitcoin is often used in ransomware attacks, a threatening development that connects cybercrime to financial crime.

Even so, cybercriminals and narcotics traffickers have made and continue to make extensive use of cryptocurrencies such as Bitcoin. Bitcoin is often used in ransomware attacks, a threatening development that connects cybercrime to financial crime. Online criminals conducting ransomware attacks deploy malware to encrypt data and demand a ransom before providing the decryption key. In February 2016, for example, a hacker seized control of Hollywood Presbyterian Medical Center's computer systems, and the hospital had to pay a $17,000 ransom in bitcoins to regain control.[232] Recently, ransomware attacks have spiked in frequency and significance. In April 2016, the FBI told CNN that in the first three months of 2016 alone, ransomware reaped $209 million from affected consumers.[233] From January to September 2016, the rate of ransomware attacks on businesses increased from one every two minutes to one every 40 seconds, with 62 new variants emerging.[234] Experts have also observed that there has been a 3,500 percent increase in criminals' use of the net infrastructure that supports ransomware.[235] Similarly, Symantec estimates that global losses to ransomware are in the hundreds of millions of dollars.[236] Ransomware attackers, mostly from Eastern Europe and China, target businesses and local governments; as a result, companies are stockpiling bitcoins in the event that they should be hit.[237] Hospitals are a particular target for ransomware, because in order to function, they have an absolute and immediate need for their data, including patient records and drug histories.[238]

Ransomware is so closely linked to Bitcoin because of the anonymity required to launch successful ransomware attacks, which Bitcoin readily provides.[239] Suggestions for ways to impede Bitcoin's irreversibility, immediacy, or decentralization have been dismissed because of how it could compromise the essential nature of the virtual currency.[240] Thus far, because Bitcoin has been adopted by this brand of criminal, there is reason to believe terrorists may take advantage of it more fully as well, as examples discussed in Chapter 2 evince. But without securing anonymity and increasing technological sophistication, systematic use of Bitcoin by terrorists remains unlikely.

04 CHAPTER

Virtual Currency Abuse in the Future: Criminals vs. Terrorists

Policymakers studying whether and how virtual currency may become a central pathway for terrorist financing must continuously examine two main characteristics of evolving virtual currency. First, as discussed in the previous chapter, they must examine how financial technologies with the same goals as virtual currencies have successfully prevented illicit financial activity generally and terrorist financing specifically. Second, they must understand the reasons for which criminal groups today are attracted to virtual currencies to determine whether terrorists, by contrast to other criminals, may seek to use them in the same way in the future.

Several of the reasons for which terrorists have not turned to virtual currencies at scale, while criminals have done so, are described in this section. Because Bitcoin is not completely anonymous, potential terrorist financiers, particularly those operating in the United States and Europe, may be reluctant to use this most liquid, convertible cryptocurrency. But as new cryptocurrencies become more anonymous, and if terrorist groups develop more of the characteristics of criminal enterprises, such as broader person-to-person networks of trust, technical sophistication, and the need for a wider funding base, virtual currencies might become more attractive.

In examining the use of virtual currencies, the U.S. government has assessed that criminal groups will adopt them when doing so offers certain perceived advantages. The U.S. Secret Service, which has jurisdiction over significant financial crimes, has identified five advantages in particular that have motivated criminal groups to adopt virtual currencies. Specifically, they are:

1. The greatest degree of anonymity for both users and transactions.
2. The ability to quickly and confidently move illicit proceeds from one country to another.
3. Low volatility, which results in lower exchange risk, increasing the virtual currency's ability to be an efficient means to transmit and store wealth.
4. Widespread adoption in the criminal underground.
5. Trustworthiness.[241]

Conscious of these advantages, criminal groups have embraced virtual currencies in self-contained online marketplaces like AlphaBay, and ecosystems like Liberty Reserve, described above, and Silk Road.[242]

In these circumstances virtual currencies are used in a number of ways, and because of their broad utility—in particular their convertibility—criminals are incentivized to adopt them at scale. This is perhaps the most important point of distinction between terrorist groups and criminals—terrorists mostly need fiat currency to fulfill the funding requirements described above, and so there is no reason to introduce the complications involved in using virtual currencies if they would rapidly need to be reconverted back to fiat currency. One common way, for example, that criminal groups use virtual currencies is to purchase and sell technical tools required to conduct cyberattacks—such as exploits designed to take advantage of particular software vulnerabilities.[243] Another common way virtual currencies are used is to purchase stolen data, monetized on the dark web.[244] Ransomware is another example of how these currencies enable cybercrime. Such uses of Bitcoin and other cryptocurrencies are consistent with the criteria identified above. Most important, they facilitate anonymous transactions or make available, for a fee, extra steps to ensure anonymity. Enterprises such as Liberty Reserve and Silk Road also operated on a global basis. And the fact that they were relatively self-contained ecosystems (albeit criminal ones) meant there was some level of trust among the participants in the marketplace.

Terrorists mostly need fiat currency to fulfill their funding requirements, so there is no reason to introduce the complications involved in using virtual currencies.

Liberty Reserve, Silk Road, and similar entities achieved scale because they filled a particular niche in the criminal ecosystem: they enabled criminals to buy and sell services *from one another* in a self-contained network. Until they were infiltrated and taken down, two of the most successful adoptions of virtual currencies facilitated global transactions among criminal groups that were able to scale because marketplaces facilitated trusted interactions. Because the groups that took advantage of virtual currencies were already engaged in sophisticated cybercrime, one of the biggest obstacles to adoption—broad comfort with sophisticated technology—had already been surmounted.

In contrast to criminal groups, terrorists have not yet adopted virtual currencies at scale.[245] One basic problem is limited adoption of the technical systems and sophistication needed for a virtual currency ecosystem to

Terrorists have been slow to adopt virtual currencies in part because of a lack of the needed technological and telecommunications infrastructure—including basic Internet service—in the areas where they operate. (avlxyz/Flickr)

flourish. As noted, terrorist groups such as Boko Haram, AQIM, AQAP, ISIS, and others often operate in inhospitable environments where telecommunications networks and other Internet services are not reliable, and where broad adoption of technology is limited.[246] If the areas in which these groups operate lack the basic technical and telecommunications infrastructure for their ecosystems to support the use of Bitcoin, then there is no reason for terrorist groups to accept value from outside donors in that form. After all, if the group cannot easily exchange Bitcoin for large quantities of hard currency or cannot use it easily to purchase weapons, other materiel, food, and housing in the areas where they operate, it does not do them much good.

This dynamic stands in stark contrast with that of criminal groups which, at present, make the most extensive use of virtual currencies. These tend to be either cybercriminal groups or others, for example narcotraffickers engaged in large (often cross-border) enterprises that invest in technically sophisticated tools. Since the people with whom cybercriminals and narcotraffickers exchange goods and services also use Bitcoin, the barriers to adoption for their use are low. Terrorist groups, therefore, face significant challenges of technological adoption in comparison with these criminal networks.

But there are also significant differences in the types of trust that characterize the networks of organized criminal groups using cryptocurrencies and the terrorist ecosystems that might have a desire to use them. The significant factor that unites members of ecosystems like Liberty Reserve, Silk Road, and other online marketplaces where tools of cybercrime are bought and sold is their common engagement in criminal activity. This generates a form of trust in the system, derived from a shared interest in preserving the illicit marketplace. Even though participants in these marketplaces may not personally know each other, they use cryptocurrencies to transfer value because they trust that, as repeat players with a shared interest in not getting caught, everyone will play by the same basic rules. As Lillian Ablon, Martin Libicki, and Andrea Golay explain, "The harder-to-access tiers [of dark web markets] where participants are highly vetted . . . are often well structured and policed, with their own constitution-like rules and guidelines to follow."[247] Reputation is paramount—"The black market has several tiers of access, with the higher tiers requiring lots of vetting before they can be entered, or even revealed."[248] Publicly accessible, low-tier channels have more fraudulent goods than the upper echelons, which are, in turn, continually getting more difficult to access without establishing mutual confidence with other criminals, including by "reputation, personal relationships, middlemen, or intermediaries," or, for example, by giving samples of goods (including stolen data or cyber exploits).[249]

Fundamentally, by contrast, terrorist financing for groups such as Hamas, Hezbollah, and al Qaeda has entailed the movement of funds from an external source to the areas where the terrorist groups operate. The role of trust is therefore very different, because terrorist financing networks operate over extended geographies with the involvement of many parties. This means there might be several steps between the sender of the funds and the ultimate recipients, attenuating the trust needed for cryptocurrency networks to scale. Al Qaeda received funds from Gulf-based donors;[250] Hamas received support from charities and state sponsors including Iran;[251] and Hezbollah received funds from Iran,[252] but also from complicated global money laundering schemes.[253] At some point in the transaction chain, the ultimate recipients of funds must know and trust the

Common engagement in criminal activity generates a form of trust in the system, derived from a shared interest in preserving the illicit marketplace.

facilitators who bundle money for transmission to terrorist groups,[254] but the initial donors might not even be witting (for example in the case of redirected charitable gifts), and often do not know the identities of the recipients. For now, because of the incomplete anonymity of many cryptocurrencies, coupled with the fact that terrorist groups are often interacting with people outside their community, it is difficult to achieve the kind of trust necessary for cryptocurrency networks to scale in the terrorism context.

Perhaps the most important reason for which terrorist groups have not adopted virtual currencies at scale is that they have not needed to do so. Other means of transferring value—cash, prepaid cards, or unlicensed money transmitters and hawalas—have served their needs reliably.[255] And those methods of transferring value can achieve scale in a way that Bitcoin cannot, at present. In 2009 alone, there were 6 billion prepaid card transactions with an aggregate value of more than $140 billion.[256] Prepaid cards are regulated in the United States and in the EU,[257] but criminals are finding enterprising ways to circumvent those rules and use repositories such as gift cards to launder funds.[258] As those other forms of transferring value come under regulatory and law enforcement pressure, terrorist groups may try to diversify their mechanisms of moving money.

> **Other means of transferring value—cash, prepaid cards, or unlicensed money transmitters and hawalas—have served the needs of terrorist groups reliably.**

In this chapter, the discussion of illicit use of virtual currencies indicates that terrorist use of the financial technology is not an imminent or systemic threat. But this could change. Given the gravity of the terrorism threat to U.S. national interests more broadly, staying ahead of evolving trends in terrorist financing is a worthy goal. Therefore, the project for financial policy officials and regulators is insulating the system from terrorist abuse and adapting an approach to regulatory oversight that keeps it closely focused on innovation, adaptation, and contemporary vulnerabilities.

05 CHAPTER

Updating the Policy and Regulatory Framework to Address Terrorist Use of Virtual Currencies

The risk that terrorists will increasingly use virtual currencies to move and store money in the future indicates a need to consider whether our current financial regulatory architecture is up to the task of preventing this eventuality. Observers and policymakers have highlighted a need for vigilance to prevent this from occurring, which in practice translates into adaptations to financial regulation and compliance. Additionally, it means a policy posture on financial technology oversight that is designed to both protect the benefits that can be afforded by virtual currencies and prevent their abuse.

In the United States, the core policy framework for monitoring and halting criminal financial activity and bulk cash movement, including for terrorist financing, is the Bank Secrecy Act (BSA), first adopted in 1970 and amended several times thereafter. The BSA reflected the fundamental insight that law enforcement needed an established mechanism to obtain information from banks about the illicit funds transfers that underlie criminal activity. It focuses on banks and MSBs as the core regulatory targets, because these institutions are the gateways through which all money, including the proceeds of crime and terrorist financing, pass. Trying to track illicit dollars in any currency occurs most effectively at these nodes in the financial system. Additional authorities enacted in the USA Patriot Act offer policymakers more legal mechanisms to compel financial information from banks about illicit activity, and they require financial institutions to stay away from the jurisdictions, institutions, and types of activity that criminals and money launderers use to avoid detection.

These statutes require financial institutions, the gateways, to be the first line of defense against illicit activity moving around the financial system. They are charged with blocking the movement of dirty money that transits their systems and keeping out bad actors, and with adopting broader risk management approaches that will make it harder for abuse to take place in the first place.

Fundamental Challenges to Countering Terrorist Financing in the Era of Virtual Currencies

A few basic challenges in the current policy and regulatory framework impede law enforcement and intelligence officials, as well as the private sector, from collaborating more nimbly to weed out illicit actors. The first general challenge is that, in a dynamic technology environment with a large number of new entrants, companies are sometimes unaware of the regulatory requirements to which they are subject, and they are often unable to afford sophisticated legal counsel to help them navigate the compliance process. Thus, even when some financial technology startup companies that deal with virtual currencies do realize that they are, in fact, MSBs for purposes of financial regulation, they may lack the institutional resources to build the requisite compliance systems and sustain viable businesses. One particular challenge in this area is the requirement for a virtual currency firm to obtain licenses in all states in which it operates and maintain compliance consistent with both federal and applicable state standards where they are licensed to operate. With only a single federal registration for virtual currency firms, compliance costs would be more manageable for smaller firms, and regulators would be better able to oversee firms. In the case of Ripple Labs Inc., the company was assessed a $700,000 penalty by FinCEN for willfully violating requirements of the BSA by failing to implement an anti–money laundering program.[259] Ripple acted as an MSB and sold virtual currencies without registering with FinCEN, and failed to implement and maintain an adequate AML program to guard against use of its products by terrorist financiers.[260]

> **Financial regulatory officials have not devoted the same or, arguably, adequate resources to regulating and examining non-bank financial institutions, by comparison with banks.**

Financial regulatory officials have not devoted the same or, arguably, adequate resources to regulating and examining non-bank financial institutions, by comparison with banks.[261] This has been the case even while non-bank institutions present a demonstrated illicit-finance risk. This problem, along with the ignorance of many virtual currency firms about their exposure to financial regulation, likely will diminish over time, as the broader financial technology industry, specifically including exchanges dealing with virtual currencies, matures. This will occur as firms undergo more audits and gain greater familiarity with financial regulators and regulatory frameworks, and as financial regulators simultaneously learn more about the functioning of virtual currencies. Such activities will ideally include, for example, collaboratively exploring some of the enhanced customer verification and due diligence practices that may be available to virtual currencies.[262]

The second and related challenge is that regulators in different jurisdictions (and even in the same jurisdiction) are taking a variety of approaches to the oversight of new payment technologies and virtual currencies. For example, some of the regulators in some jurisdictions have moved faster than others to clarify that certain financial payment technologies, such as virtual currency exchanges, are a new kind of MSB, subject to exams, and must have AML programs. In 2013, FinCEN issued guidance indicating that Bitcoin exchanges were MSBs and subject to regulation as such.[263] Other regulators in other jurisdictions have not offered similar guidance—or have gone so as far as imposing limits on the use of virtual currencies.[264] This uneven outreach to virtual currency companies has sometimes resulted in conflicting regulatory approaches.[265] Even when regulators clarify that certain new payment technologies are "covered entities" subject to regulation, the ability of banking regulators to supervise and of law enforcement officials to take action is nascent.

Finally, the regulation of virtual currencies is highly dynamic, shifting both within and across jurisdictions at a rapid pace. This makes achieving a stable compliance architecture exceedingly difficult.

The Culture of Compliance and Virtual Currencies

In addition to the regulatory challenges in countering terrorist financing that may occur via virtual currency, as discussed above, a further impediment is linked particularly to the culture of compliance. The current rules-based bank supervisory structure entails a fundamental tension between regulatory and compliance approaches to illicit financial activity. Specifically, supervision focuses strictly on the failure of banks to prevent illicit activity, rather than being more oriented toward detecting and monitoring it. The latter approach is often favored by law enforcement officials.

The current structure and requirements for U.S. supervision of major banks in its jurisdiction (which in practice includes the preponderance of all global banks) places overwhelming emphasis on prevention rather than detection. While it is indeed important for financial institutions not to facilitate illicit financial activity, the work of shutting it out has become an elaborate, expensive compliance exercise.[266] This has involved an emphasis on shedding, rather than managing, risky clients. The result has been that risky activity is often pushed to less well-regulated institutions.[267] Compliance activity has become relatively rote, if expensive, and the fact that banks get no "credit" with regulators for adopting innovative approaches to detecting illicit activity does not incentivize the development of novel strategies to track the evolving terrorist financing threat. But the problem may actually be even more significant. When banks do create novel strategies to counter terrorist financing, they are expected by their examiners to maintain both the novel and the conventional strategies, thereby creating a disincentive for banks to innovate and bear the financial burden of parallel counterterrorist financing programs.[268]

It is easier, less expensive, and less problematic for banks to completely avoid any risk and limit scrutiny for terrorist financing to basic compliance with the rules, while avoiding risky clients.

Moreover, the recent record of expensive civil and criminal penalties for sanctions and AML violations has raised the stakes for banks, making them more willing to refrain from engaging entire geographic areas or lines of business because of perceptions of excessive risk.[269] Banking officials report that when they have disclosed evidence of terrorist financing found at their banks, they have been criticized or penalized by federal supervisors for failing to report similar transactions previously, subsequently, or with regularity.[270] Additionally, they say that, perversely, the compliance incentives in this environment do not encourage them to try to detect terrorist financing or other criminal activity. It is simply technically easier, less expensive, and less problematic for their relationship with bank supervisors to completely avoid any risk and limit their scrutiny for terrorist financing to basic compliance with the rules, while avoiding risky clients.

By extension, this also discourages banks from taking on new payment technology firms, or virtual currency platforms, given the risks of assimilating such new and unknown customers. Banks therefore do not have as much insight as they could into illicit financial flows in virtual currencies. Thus it is harder for law enforcement and intelligence officials to track and halt such activity. A more holistic and effective approach to countering terrorist financing would encourage and incentivize banks to take on new payment technologies and virtual currency firms while managing the potential risks of abuse.

From a public policy standpoint, it is concerning that banks do not appear to be incentivized to be as proactive as possible in detecting terrorist financing and adopting innovative strategies for information sharing and coordination with law enforcement and intelligence officials. They should be working in coordination with both to sustain and manage certain risky clients. In the present environment of extensive social media connectivity and ease of moving funds electronically, including through relatively anonymous platforms or currencies, there are growing new aspects to terrorist threats. Moreover, the growing trends of Internet-based radicalization, lone wolf terrorist plotters, and anonymous virtual currencies make it significantly more important that there be much more active multi-sectoral collaboration to identify and halt terrorist activities. In order to arrest such activities, virtual currency exchanges, along with banks, technology providers, merchants, and national security and law enforcement officials, must have powerful incentives and easier pathways to collect and share terrorist threat information.

Regulatory Treatment of Virtual Currencies

It may be tempting to assume that new financial regulation is needed to address these various challenges, particularly given how novel virtual currencies are compared with conventional fiat currency and banks. However, this should not necessarily be the operating assumption of stakeholders. An appropriate approach to regulating virtual currencies should include an emphasis on understanding the applicability of the existing financial regulatory architecture to payment systems that service virtual currencies. While conducting this analysis, policymakers should appropriately balance the burden of compliance for virtual currencies with the need to support the innovative value of new, efficient financial technology. Policymakers may, in this framework, consider only moderate adaptations. This should be the case notwithstanding the fact that new financial technology may, in fact, present an enhanced risk of abuse by terrorists and other financial criminals.[271]

The need for new regulation is also diminished because many financial industry watchers believe that traditional, highly regulated global banks will remain the pillars of the global financial system for the foreseeable future, given the essential security, liquidity, longevity, efficiency, and creditworthiness that they provide. The vast majority of commercial and retail financial activity is legitimate.[272] Those conducting this activity seek reliability and stability, as do those who conduct some illicit financial activity. Both types of actors generally only select new financial technologies that guarantee payment and provide an assured counterparty, credit, and credibility. This may in practice limit their exposure to virtual currencies. But to the extent that banks offer services to virtual currencies, financial regulators generally will continue the practice of applying traditional financial regulatory categorizations and requirements to new payment systems. By extension, this means that banks will pioneer and model customer due diligence and anti–money laundering programs for new financial technology and virtual currencies. There are likely many creative new opportunities to synthesize large amounts of financial and other data to identify the financing of terrorism.

Regulators must constantly evaluate what new payment platforms and virtual currencies should fall under their regulation, and develop innovative new skills and methods to supervise them. It is possible that new regulation to apply to virtual currencies and new payment technologies will eventually be necessary. If at some point the ecosystem of anonymous and distributed financial technology is so expansive, and the virtual currencies exchanged in this ecosystem so stable, that it provides a true alternative at scale to the conventional financial system, new regulatory techniques may be needed to supervise these technological platforms. In this instance, the traditional framework of the BSA may need significant reevaluation.

Any virtual currency regulatory regime should aim to have each entity satisfy the fundamental requirements of a rigorous counterterrorist financing and AML compliance program. This includes following KYC procedures, wherever possible extending to users of virtual currency; maintaining certain transactional records; and reporting suspicious transactions of various types. Regulators and regulated entities could consider including new types of electronic data in suspicious activity and "cash" transaction filings. Among the obvious challenges involved with this innovation would be the need for them to understand where relatively anonymous transactions originate, where they are going, and with whom beneficial ownership resides, as well as how much anonymity is feasible while still adequately managing risk, and at what point in the transaction process anonymity is possible.[273]

There are likely many creative new opportunities to synthesize large amounts of financial and other data to identify the financing of terrorism.

Principles for Improving Financial Supervision and Enforcement to Counter Terrorist Use of Virtual Currencies

It is possible to adopt new strategies to better identify and halt terrorist financing through virtual currencies in the current digital financial era. Not all of these strategies are directly linked to the technical specifications of emerging virtual currencies; rather, they are somewhat more methodological from a regulatory oversight and compliance perspective. Nevertheless, they can all help to capture illicit conduct using new kinds of decentralized and anonymous virtual currencies. First and foremost, however, policy leaders must consider several basic principles that will, if embraced, undergird an ability to successfully adopt policy change to promote a greater ability to counter terrorist use of virtual currency.

National security leaders must embrace three basic principles at the highest levels and clarify them to the private sector. These will serve as the front line to identifying terrorist financing using virtual currencies. Concomitantly, supervisory agencies must recognize and embrace these priorities and regulatory agencies must enforce them. They are:

1. Policy leader prioritization of countering terrorist financing and other financial crimes, including through new virtual currencies
2. A policy and regulatory posture that encourages innovation
3. New strategies and legal means for coordination, particularly between the public and private sectors.

These priorities are beneficial for the task of countering terrorist use of virtual currencies; they are also essential to ensure that the current policy and regulatory framework to counter terrorist financing does not become truly antiquated. Financial connectivity, along with new payment technologies and virtual currencies, is already reorganizing ways in which all financial actors raise, store, and move money.

In line with the first principle, to more effectively counter terrorist use of virtual currencies, and indeed to counter terrorist financing more broadly, banks and MSBs must place much greater emphasis on tracking and reporting suspected terrorist financing. Currently, banks, MSBs, and other actors are asked to report on a wide array of suspicious and threatening activities, including money laundering, narcotics, weapons, human trafficking, securities fraud, and cybersecurity. Policymakers and law enforcement officials do not effectively communicate their priorities to private sector entities with limited resources; they must do so and must coordinate to the extent possible with independent regulators to align supervision and enforcement priorities. As a result, banks have no official policy guidance on how to prioritize risks. Therefore, they place no special emphasis on areas of greatest concern to policymakers, law enforcement, and the intelligence community. For the same reasons, they do not necessarily prioritize creative investigative tactics or information sharing.

Intelligence and law enforcement officials are the ultimate beneficiaries of banks' suspicious activity reporting, so it is particularly incongruous that they are not involved in establishing criteria for threat reporting. Nor do they provide feedback on what banks report as being of value for law enforcement activities. This stands in contrast to the fact that the law enforcement and national security communities do establish investigative and enforcement priorities for themselves regularly. The financial sector's perception of threats may be different from those identified by national leaders, as well as being different from those identified by bank supervisors. Additionally, each individual financial institution's perception may differ depending on its geographic footprint and specific array of business activities. These varying perceptions add to the problematic nature of the lack of policymaker and law enforcement priority-setting for private financial reporting on threats. The policy community must establish a hierarchy of financial crime threats on which they expect the financial sector to focus its activities. Terrorist financing, specifically including its occurrence via virtual currency, should be first among such crimes.

> **The policy community must establish a hierarchy of financial crime threats. Terrorist financing, specifically including its occurrence via virtual currency, should be first.**

The second principle, aggressively encouraging innovation in strategies to identify and counter terrorist financing, may involve what some financial sector experts have called a "sandbox" approach. Used in the United Kingdom, this approach urges regulators to give financial sector participants and technology entrepreneurs the regulatory running room to experiment with their technology and see how it interacts with customers

and their data without having the relevant—potentially onerous—regulations applied immediately.[274] Necessarily, this running room involves regulators' tolerance of potential failures. In practice, and for compliance professionals and legal officials, this tolerance takes the form of liability shields.

The final principle calls for more extensive cooperation, specifically among private sector entities and between the public and private sectors. Current U.S. statutes allow for financial information sharing among and between public and private sector actors. In some instances this can be a fruitful means of establishing information flow, including during active investigations to track suspected terrorists. The FBI Terrorist Financing Operations Section has publicly expressed the view that financial institutions have been rapidly and extremely responsive to requests for information to all terrorist incidents.[275] But many private sector representatives embrace a legal interpretation of national financial information sharing laws, data privacy rules, and other regulations. In practice, this has enshrined powerful limitations on data sharing and cooperation—acutely, when it comes to sharing information and cooperating across national boundaries, even among branches or subsidiaries of the same bank.[276] When coupled with a libertarian ethos among technology firms, especially those pioneering new ways to send money around the world outside the reach of traditional financial institutions, information flow regarding illicit finance may be particularly poor.

It is more important than ever for law enforcement and intelligence officials to coordinate closely and with the private sector to map threat networks and plots, including terrorist activity.

In a financial ecosystem where payment anonymity is easier to achieve and social media provides for more anonymous communication, it is more important than ever for law enforcement and intelligence officials to coordinate closely and with the private sector to map threat networks and plots, including terrorist activity. It is crucial that policy authorities signal to stakeholders working to counter terrorism that they must radically broaden their coordination, including through expanded legal pathways and liability protection for information sharing and regulatory or enforcement benefits for cooperation. This approach will help to better address terrorist use of virtual currencies, and terrorist financing in general. It is also fundamental to the development of creative strategies to unite private sector entities and government intelligence and regulatory officials in better understanding the identities and patterns of virtual currency users. Moreover, and of significance to the entire financial regulatory and national security establishment, this approach will meaningfully contribute to a more robust ability to fight all manner of criminal financial activity. Applied together, these three principles are the foundation to better fighting the broad array of threat finance.

06 CHAPTER

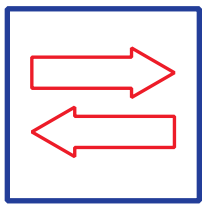
Recommendations and Conclusions

As discussed, anecdotal evidence indicates that terrorists have used virtual currency to move and store money. Policymakers and regulators have the ability, and would be well served, to adapt their approach to supervision and enforcement to better track this illicit finance and work to prevent the threat from achieving scale. Such changes would likely have the beneficial effect of countering terrorist financing more broadly. Additionally, they may also help to address the pernicious and more widespread use of virtual currencies by various types of criminals, including traffickers of drugs, child or other illegal pornography, counterfeit goods, and others. Counterterrorism, national security, and law enforcement officials would all be better off with an invigorated policy focus on preventing terrorist use of virtual currencies.

For now, the most effective strategy for accomplishing this goal is to focus legal and regulatory adaptations on the gateway financial institutions, whether banks, MSBs, or virtual currency exchanges that process virtual currency transactions. As noted, these nodes in the financial system can be effective for identifying suspicious customers or activity. They are relatively centralized and regulated, and therefore require at least a basic degree of transparency and lawfulness. To the extent that such institutions can be encouraged and offered incentives to host virtual currency money movements and exchanges, they can increase their transparency and lawfulness. The more this happens, the more it will benefit the financial system's security and integrity. If virtual currencies scale to a point where they are more broadly used and exchanges themselves become less relevant, this approach might need to change. But for the moment, the most effective governance technique is to focus on exchanges.

The following series of recommendations offers steps to various stakeholders in the counterterrorism and financial technology realm designed to help them better understand terrorist use of virtual currencies, prioritize the issue along with a broader focus on terrorist financing, and refine strategies for preventing such activity from scaling. The recommendations seek to assist regulatory and financial supervisors in protecting valuable financial sector innovation in the virtual currency domain. They also suggest strategies to protect and encourage an innovative approach by financial institutions in detecting illicit financial activity via virtual currencies. Finally, they offer suggestions for more forward-leaning financial information sharing and disclosure, in the service of an improved intelligence, law enforcement, and industry ability to hold terrorist threats at bay. These recommendations, if implemented, will help to mitigate the degree to which terrorists can use virtual currencies, as well as more conventional methods of terrorist financing.

Policy Recommendations



1. Better understand the evolving threat of virtual currencies financing terrorism

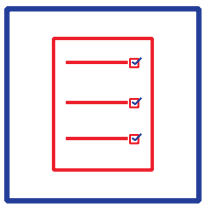
Perhaps the most significant change that policy leaders can implement to more ably counter terrorist use of virtual currency is improving the ability of intelligence and oversight officials to understand the phenomenon. This demands an ongoing investigation of terrorist financing and a novel approach to gaining insight into new financial technologies that terrorists can use. It also demands an ongoing analysis into when, and in what fashion, new regulation is needed to govern evolving and expanding technology.

Expand regulation and guidance to foster greater financial information disclosure and sharing. Congress should move forward with proposals for enhancing requirements for the collection and disclosure of beneficial ownership information in the corporate formation process.[277] Additionally, FinCEN should consider offering new guidance or regulations on sections 314(a) and 314(b) of the USA Patriot Act, to facilitate greater information flow within and among global banks. Federal officials could also consider a rule on cross-border financial flows for exchanges regulated in the United States, contemplating the documentation of virtual currency transactions with FinCEN or another appropriate agency. Given the decentralization of certain virtual currencies, it might be difficult to do this directly after they have achieved a certain scale, but for the moment, virtual currency exchanges remain the subject of regulation. In well-supervised jurisdictions, this remains a viable approach. Information from more traditional banks, when disclosed and exchanged pursuant to these various changes, will help intelligence officials and the law enforcement community to better track terrorist use of virtual currencies, as well as the illicit financial activity of a host of other financial criminals.

Formalize the congressional focus on terrorist financing and financial technology. Relevant congressional committees, including the House Financial Services Committee and Senate Banking Committee, should formally add terrorist financing and financial technology, including virtual currency, into their oversight mandate. The committees can fold this into existing work to investigate terrorist financing, and they should draw upon the Congressional Research Service to gather information on the threat. Congressional staff may also consider establishing a congressional study group to further advance oversight and the consideration of updated financial oversight statutes, as appropriate.

Call for an independent task force to advise federal officials. The Treasury Department, Department of Justice (DOJ), intelligence community, and other agencies should work with financial services trade associations, such as the American Bankers Association and the Association of Certified Anti-Money Laundering Specialists, as well as think tanks with a special focus on illicit finance and counterterrorism, to conduct independent research on terrorist use of new financial technology, including virtual currencies.

Expand regulator outreach to financial technology firms and developers. Given the new entry of technology firms into the business of moving and storing value, as well as the rapid pace of innovation and change in this area, financial regulators and policy officials should focus unique attention on outreach to the technology sector, including the developers of virtual currency and new payment technologies. Regulators and officials should seek to foster encounters that are constructive and oriented toward mutual information flow and collaboration. This will help all parties to understand new developments in financial technology and terrorist financing threats.



2. Prioritize terrorist financing as a matter of public policy and law enforcement significance

Policy and law enforcement leaders must jointly signal to the public and private sectors the importance of countering terrorist financing, including through virtual currencies and other new technologies. This will be meaningful if the prioritization is clearly linked to incentives and the likelihood of enforcement and regulatory examinations in certain high priority areas, with a clearly diminished emphasis in other areas. That is, regulators should reward innovative and effective efforts to counter terrorist financing, while increasing their focus on these areas. Similarly, they should decrease attention and examination or enforcement in other lower priority areas such as structured payments for relatively small-scale money laundering. At present, there is no process by which policy and law enforcement officials can prioritize areas of illicit financial activity for private sector scrutiny and reporting, while the private sector receives regulatory assent for reallocating assets in accordance with these priorities. The effect of all this is that everything becomes a priority, but in fact nothing is a priority. This is surely not the case from a national threat-assessment perspective. A real prioritization will appropriately signal to stakeholders a more enhanced level of significance and resources that they should devote to the challenge. In turn, this will contribute to the effectiveness of counterterrorist financing efforts, in the interest of national security.

Initiate an intelligence prioritization process to highlight counterterrorism finance information. FinCEN or the DOJ should initiate a process, modeled on the National Intelligence Priorities Framework, to rank the counter–illicit finance priorities of the U.S. government. This methodology can elevate terrorism as a priority, signaling to policymakers, law enforcement officials, and financial institution supervisors the need to focus on the topic in enforcement and targeting activities. Financial officials will need to contemplate a strategy for how to grade banks on how well they direct resources to these priority areas.

Prioritize terrorist financing. Recognizing that many bank supervisory agencies are statutorily independent, Congress and the executive branch should emphasize the importance of TF. These priorities should translate into supervision and enforcement approaches.

Expand outreach to the private sector on countering terrorist financing. The Treasury Secretary, or an appropriate deputy in the Treasury Department from the Office of Terrorism and Financial Intelligence, should conduct outreach to the private sector to communicate a priority focus on countering TF. This will signal to banks and MSBs the need to devote appropriate resources to this area.

3. Prioritize terrorist financing as a compliance matter within private institutions

Banks should expand their focus on terrorist financing, including via the use of virtual currencies, as an area of illicit finance in response to the articulated government prioritization of this issue. This work must be undergirded by enhanced efforts to share information on terrorist threats with appropriate law enforcement agencies, including the FBI, and peer institutions. Additionally, in practice the prioritization should be demonstrated by a desire to lead regulators in the establishment of innovative models to counter terrorist financing.

Invest further resources in financial intelligence units (FIUs). Banks should expand their investigative capacity to conduct proactive and targeted monitoring initiatives to identify terrorist threats, as well as to conduct reactive work when an incident occurs. They can usefully model such efforts after federal FIUs, and are well placed to

gather enterprise-wide information about illicit finance threats. Additionally, these initiatives should be coordinated with federal counterparts.

Propose specific legal changes to improve counterterrorist financing efforts. Banks and private sector leaders should identify and propose specific changes to statute, regulations, and policy that would allow them to overcome some of the impediments to tracking terrorist financing activity, including via virtual currencies. As discussed throughout this paper and in some of the remaining recommendations, these changes should include ideas for improved information sharing and legal liability protection. Banks are uniquely placed to play a leadership role in articulating the current challenges and in undertaking the intellectual and technical work involved in adopting new rules and culture. Again, all of this should be coordinated with policymakers.

4. Offer protection and incentives for private initiatives to halt terrorist financing, including through virtual currency

Federal policymakers, including at the FBI, DOJ, Secret Service, and IRS; as well as banking regulatory authorities such as the Federal Reserve, the OCC, and FinCEN, should contemplate and craft guidance for banks and other regulated financial entities to spur them to collaborate more closely with governmental authorities to track and halt terrorist financing. State level bank supervisors, particularly New York's Department of Financial Services, should participate in this process as well. It could ultimately include adaptation of regulation and enforcement guidance, as well as liability protection to protect financial institutions' innovative strategies. Moving toward this approach would mean the creation of a regulatory "sandbox," an environment that fosters collaborative approaches to compliance in order to best advance the ultimate policy goals.

Consider a "laboratory" approach for pioneering new counterterrorist financing strategies. Regulators should contemplate strategies for stimulating specific private sector initiatives and mechanisms whereby banks and other MSBs can pilot or work to institutionalize new ways to identify and halt TF, including via virtual currencies. This will require limited liability protection, possibly including a safe harbor, comfort letters or regulatory guidance from banking supervisors, and close, ongoing coordination with law enforcement officials. It might also include special licensing for unique industry collaborative investigatory efforts to address TF and share information with law enforcement.

Recognize successful models and best practices, including with incentives. Regulators should consider publicly sharing examples of successful strategies to track terrorist financing, including financing via new technological means. Such sharing could include accolades for the quality over quantity of Suspicious Activity Reports (SARs) filed, or a strong record of sharing SARs with high value to the law enforcement community. Such forms of recognition could offer a reputational benefit to the firm that implemented the strategy and signal to financial overseers the value and prioritization placed on innovative, successful strategies to address TF. Additionally, financial policy officials could offer positive inducements such as investment incentives to firms and foreign official counterparts that make a special effort to share information and coordinate in addressing TF. These measures would not, strictly speaking, constitute rewarding activity that is expected of all financial institutions, but rather highlight extraordinary and aspirational behavior.

5. Make financial technology innovation more sustainable

Financial regulators should consider strategies to limit the regulatory "tax" on development of financial technology, including virtual currency technology. Financial technology companies must shoulder the compliance burden of financial system operators, and policies to limit this strain for virtual currency companies—which may not necessarily be inherently risky—would appropriately underscore a risk-based approach to financial regulation. It would also have the effect of stimulating financial technology innovation. Financial policymakers should consider how to actively support beneficial financial technology development, particularly when it can bring virtual currency and new payment technology platforms successfully into the regulated financial sphere.

Explore a risk-based approach to anti-money laundering program requirements. Policymakers should adapt the current oversight regime for new financial technology firms. Oversight would be moved to a more risk-based approach toward countering TF. This could entail a greater focus on some elements of the programs (for example, a risk-based prioritization of firms engaging in cross-border payments or more tailored SAR filing requirements based on services offered), and on liquidity providers and exchanges in particular, in line with guidance offered by policymakers on national security and law enforcement priorities. Ultimately, if virtual

currencies scale in a significant way, then exchanges will become less relevant, and regulators will need to engage in significant adaptation in how they supervise for AML and CTF compliance in the virtual currency space. Promotion of this kind of innovation will help to prepare the groundwork for a future regulatory architecture.

Explore the idea of a common compliance architecture. In coordination with financial industry representatives, policymakers should consider establishing industry-wide mechanisms to aid regulated firms with compliance activities, including with explicit regulatory permission. This could be particularly useful for new financial technology firms that may be both small and relatively unfamiliar with financial sector regulation. One promising idea is the development of a global KYC registry established through blockchain technology. This would dramatically reduce the cost of establishing an effective AML compliance architecture for new firms with limited resources. Other possibilities would be to offer alternative safe channels for permitting financial flows, or alternative ways to validate the transparency of financial platforms or certain ecosystems that conform with international best practices.

Consider adopting unique regulations for financial technology startups. Financial regulators should consider alternative regulatory schemes for small market capitalization or startup financial technology firms with a path to more conventional regulation after they achieve scale and sustainability. This could include enhanced beneficial disclosure requirements in the initial regulatory stage, to avoid the incentive that such a model would create for evading regulation altogether, along with the subsequent formation of shell companies.

Expand the geographic range of financial technology licensing. At present, certain kinds of financial technology companies must seek separate licenses in each state in which they operate. State and federal banking regulators should think about ways to harmonize the financial supervision landscape.

Conclusion

Terrorists' use of virtual currencies has thus far been episodic and relatively uneven, given the greater accessibility to virtual currencies by groups with relatively more technical sophistication. However, even if terrorist use of virtual currency has not yet achieved scale or become a more systemic security threat, it has the potential to grow. For the policymaking community, the true concern when it comes to terrorist use of virtual currencies and other new payment technologies is what may happen in the future, and their ability to track developments.

As this paper has pointed out, regulatory and legal adaptations can improve the ability of regulators, intelligence and law enforcement officials, and the banks and MSBs abused by terrorists to better detect and halt terrorist use of virtual currencies. However, it will be extremely difficult to make such adaptations, in particular due to the confluence of dynamic financial technology innovation and an AML compliance culture that is significantly focused on completely avoiding risk. In order to get ahead of terrorists' ability to manipulate the features of decentralization and anonymity offered by virtual currency, policymakers will have to, in the first instance, encourage financial institutions to manage—not shun—the risks of this and other new financial technologies. To arrive at this point, the government will have to take on enormous dual challenges: assume greater risk and set a tone of collaboration.

The rewards of achieving a more constructive and collaborative industry-government partnership around countering terrorist use of virtual currencies, and indeed all terrorist financing activity, are tremendous. A true partnership in this domain will help policy leaders to better fight terrorism and encourage valuable financial innovation. It will also better protect financial institutions from abuse and preserve their reputation, while contributing to shareholder value. Particularly given the potential for lone wolf terrorist activity, along with the challenge of detecting, through financial data, terrorist attacks before they occur, it will be impossible to keep terrorists out of the financial system entirely and away from electronic currency, whether virtual or fiat. Additionally, the highly dynamic nature of financial innovation means that regulators and policymakers may not be able to avoid some tension as they strive to keep regulations and compliance benchmarks up to speed with technology, and as they conduct proper outreach to the technology sector.

Notwithstanding these risks and regulatory tensions, the strongest defense against terrorist use of virtual currency is an approach to financial policy and regulatory oversight that seeks to embrace and manage, not avoid, risk. This also corresponds with an effective strategy for stimulating financial technology innovation, and the many benefits that new payment systems and new currencies or financial ecosystems can offer. Ultimately, then, the greatest challenge for policymakers is an acculturation to the reality of significant risk and the difficult work of truly prioritizing. For banks, the greatest challenge is to make detection and insight more important than the avoidance of risk. Successfully addressing these challenges will have a direct and meaningful benefit for U.S. national security, as well as for our economic competitiveness and leadership in innovation.

Endnotes

1. For a similar definition of hawala, see: "Letter dated 4 September 2012 from the Chair of the Security Council Committee pursuant to resolution 1988 (2011) addressed to the President of the Security Council," (United Nations Security Council, September 5, 2012), http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2012_683.pdf, 15.

2. The terms used in this paper to describe types of emerging financial technology have contested definitions. There is no single commonly agreed-upon definition of a "virtual currency." But the definition used by the Financial Action Task Force (FATF) has perhaps the broadest adherence. The FATF describes a virtual currency as "a digital representation of value that can be digitally traded and functions as (1) a medium of exchange and/or (2) a unit of account and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction." A virtual currency, according to the FATF, fulfills its functions "by agreement within the community of users of the virtual currency." FATF does not use the term "digital currency," in order to avoid confusion with virtual currencies and with "e-money," which refers to fiat currency being transferred through electronic means. See "Virtual Currencies: Key Definitions and Potential AML/CFT Risks" (FATF/OECD, June 2014), 4, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf. Domestically, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) defines virtual currency as having many characteristics of real currency but as lacking legal tender status in any jurisdiction. See FinCEN's memo "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," March 18, 2013, https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering. The IRS, which has a tax policy for virtual currency, defines it as "a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value." In some instances, it functions like real currency, but it does not have legal tender status in any jurisdiction. See Internal Revenue Service, "IRS Virtual Currency Guidance," April 14, 2014, https://www.irs.gov/irb/2014-16_IRB/ar12.html. The Commodity Futures Trading Commission, which also regulates virtual currencies, uses but does not quote the FATF's definition. Both the FATF and FinCEN definitions differ from that of the European Central Bank in 2012, which was limited to centralized virtual currencies (issued and controlled by a group of developers). See "Virtual Currency Schemes" (European Central Bank, October 2012), 6, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf. This paper will apply the specific parameters that the FATF lays out to define a virtual currency and avoid using the term "digital currency" for the sake of clarity. Furthermore, this paper also analyzes "cryptocurrencies," a subset of virtual currencies that uses cryptographic techniques for security, including to verify currency ownership and transactions made using the currency. A new payment technology, by contrast to virtual currencies and the systems that enable them, leverages technology to facilitate banking or financial transactions between people using currency.

3. Stuart Levey, Under Secretary, Terrorism and Financial Intelligence, Department of the Treasury, testimony to the Subcommittee on Oversight and Investigations, Financial Services Committee, U.S. House of Representatives, July 11, 2006, 1–2. http://financialservices.house.gov/media/pdf/071106sl.pdf.

4. "Who We Are," FATF, http://www.fatf-gafi.org/about/.

5. "Consolidated FATF Strategy on Combatting Terrorist Financing" (FATF, February 19, 2016), 1, http://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Terrorist-Financing-Strategy.pdf.

6. James Freis, Tom Keatinge, Troels Oerting, and Karen Walter, "Trends in Counter Terrorist Financing: Panel Summary," *SIBOS 2016 in Review* (SWIFT: October 2016), 4.

7. "2015 National Terrorist Financing Risk Assessment"(Department of the Treasury, June 2015), 3, https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf.

8. Ibid., 47.

9. Ibid., 56, 57.

10. Ibid., 58.

11. "EBA Opinion on 'Virtual Currencies,'" EBA/Op/2014/08 (European Banking Authority, July 4, 2014), 33, https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.

12. Liana Rosen (specialist in international crime and narcotics, foreign affairs, Defense and Trade Division of the Congressional Research Service), "Task Force on Anti-Terrorism and Proliferation Financing Briefing" (United States Congress, March 3, 2017). Discussion with author.

13. Brendan I. Koerner, "#jihad: Why ISIS Is Winning the Social Media War," *Wired,* April 2016, https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/.

14. Nicholas Blanford, "How Off-the-Shelf Drones Are Changing War in Syria and Lebanon," *Christian Science Monitor,* August 16, 2016, http://www.csmonitor.com/World/Middle-East/2016/0816/How-off-the-shelf-drones-are-changing-war-in-Syria-and-Lebanon.

15. Andy Greenberg, "New Dark-Web Market Is Selling Zero-Day Exploits to Hackers," *Wired*, April 17, 2015, https://www.wired.com/2015/04/therealdeal-zero-day-exploits/; Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar" (RAND, 2014), 11–12, http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

16. "Combining an anonymous interface with traceless payments in the digital currency bitcoin, the site allowed thousands of drug dealers and nearly 1 million eager worldwide customers to find each other—and their drugs of choice—in the familiar realm of ecommerce," quoted from Joshuah Bearman and Tomer Hanuka, "The Untold Story of Silk Road, Part 1," *Wired*, May 2015, https://www.wired.com/2015/04/silk-road-1/. See also "Part 2: The Fall," *Wired*, June 2015, https://www.wired.com/2015/05/silk-road-2/; Thomas Fox-Brewster, "Life after Evolution: Meet the Dark Web Drug and Gun Entrepreneurs Succeeding Solo," *Forbes*, April 9, 2015, https://www.forbes.com/sites/thomasbrewster/2015/04/09/drug-and-gun-vendors-thriving-on-their-own/#6574c57535f6.

17. Ransomware, in which cybercriminals encrypt a victim's files and decrypt those files only after receipt of a ransom, generally paid in Bitcoin, is a notable exception.

18. Ablon, Libicki, and Golay, "Markets for Cybercrime Tools and Stolen Data," 15.

19. "Bitcoin," CryptoCurrency Market Capitalizations , https://coinmarketcap.com/currencies/bitcoin/; "Monero," CryptoCurrency Market Capitalizations, https://coinmarketcap.com/currencies/monero/.

20. See "FinCEN Awards Recognize Partnership between Law Enforcement and Financial Institutions to Fight Financial Crime," Financial Crimes Enforcement Network, May 10, 2016, https://www.fincen.gov/news/news-releases/fincen-awards-recognize-partnership-between-law-enforcement-and-financial.

21. Government Accountability Office, *Financial Institutions: Fines, Penalties, and Forfeitures for Violations of Financial Crimes and Sanctions Requirements*, GAO-16-297, March 22, 2016, 11, http://www.gao.gov/assets/680/675987.pdf.

22. Paul Taylor, "How Banks Can Avoid the De-Risking Trap," *American Banker,* July 19, 2016, https://www.americanbanker.com/opinion/how-banks-can-avoid-the-de-risking-trap.

23. For examples of this trend, see Rob Barry and Rachel Louise Ensign, "Cautious Banks Hinder Charity Financing," *The Wall Street Journal,* March 30, 2016, https://www.wsj.com/articles/cautious-banks-hinder-charity-financing-1459349551; Rob Barry and Rachel Louise Ensign, "Losing Count: U.S. Terror Rules Drive Money Underground," *The Wall Street Journal,* March 30, 2016, https://www.wsj.com/articles/losing-count-u-s-terror-rules-drive-money-underground-1459349211; Lanier Saperstein and Geoffrey Sant, "Account Closed: How Bank 'De-Risking' Hurts Legitimate Customers," *The Wall Street Journal,* August 12, 2015, https://www.wsj.com/articles/account-closed-how-bank-de-risking-hurts-legitimate-customers-1439419093. Federal financial supervisors recently released a paper that attempted to assuage the concerns of banks about this trend. See Office of the Comptroller of the Currency, Department of the Treasury, "Risk Management Guidance on Periodic Reevaluation of Foreign Correspondent Banking," October 5, 2016, https://www.occ.gov/news-issuances/bulletins/2016/bulletin-2016-32.html.

24. Virtual currency professional conversation with author, 2016; Pratin Vallabhaneni, David Fauvre, and Andrew Shipe, "Overcoming Obstacles to Banking Virtual Currency Businesses," Coin Center, May 2016, 4–6, https://coincenter.org/wp-content/uploads/2016/05/banking-obstacles.pdf; Paul Vigna and Michael J. Casey, *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order* (New York: St Martin's Press, 2015), 117.

25. Luis Buenaventura, "There's a $500 Billion Remittance Market, and Bitcoin Startups Want In on It," Quartz, September 11, 2016, https://qz.com/775159/theres-a-500-billion-remittance-market-and-bitcoin-startups-want-in-on-it/; Swati Pandey, "Australian Bank Exit from Remittances Sends Money Transfers Underground," Reuters, February 25, 2016, http://www.reuters.com/article/australia-remittances-banks-idUSL3N1632JD; Jamila Trindle, "Bank Crackdown Threatens Remittances to Somalia," *Foreign Policy,* January 30, 2015, http://foreignpolicy.com/2015/01/30/bank-crackdown-threatens-remittances-to-somalia/.

26. Vigna and Casey, *The Age of Cryptocurrency,* 160.

27. Mark Garrison, "Regulation May Be Coming for Bitcoin," Marketplace, September 18, 2015, https://www.marketplace.org/2015/09/18/tech/regulation-may-be-coming-bitcoin.

28. Paul Vigna, "Bitcoin Price Plunges on Fears of a Currency Split," *The Wall Street Journal,* March 19, 2017, https://www.wsj.com/articles/bitcoin-price-plunges-on-fears-of-a-currency-split-1489949541.

29. "Terrorist Financing" (FATF/OECD, February 29, 2008), 7, http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf.

30. Thomas H. Kean, and Lee Hamilton, "The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States Executive Summary," (Washington, D.C.: National Commission on Terrorist Attacks upon the United States, 2004), 14, http://govinfo.library.unt.edu/911/report/911Report_Exec.pdf.

31. Carla E. Humud, Robert Pirog, and Liana Rosen, "Islamic State Financing and U.S. Policy Approaches," Report No. 43980 (Congressional Research Service, April 10, 2015), 13.

32. "Terrorist Financing," 7–10; "Emerging Terrorist Financing Risks" (FATF/OECD, October 2015), 9–10, http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

33. Robert Windrem, "Terror on a Shoestring: Paris Attacks Likely Cost $10,000 or Less," NBC News, November 18, 2015, http://www.nbcnews.com/storyline/paris-terror-attacks/terror-shoestring-paris-attacks-likely-cost-10-000-or-less-n465711; National Commission on Terrorist Attacks upon the United States et al., "The 9/11 Commission Report," 14.

34. "Terrorist Financing," 21.

35. "Emerging Terrorist Financing Risks," 13.

36. "Terrorist Financing," 15.

37. Ibid., 11.

38. Kristina Wong, "Senators: ISIS Is 'Best Funded' Terror Group Ever," *The Hill*, August 26, 2014, http://thehill.com/policy/defense/216023-senators-isis-is-best-funded-terrorist-group-in-history.

39. Humud, Pirog, and Rosen, "Islamic State Financing," 1.

40. "Testimony of A/S for Terrorist Financing Daniel L. Glaser before the House Committee on Foreign Affairs Subcommittee on Terrorism, Nonproliferation, and Trade, and House Committee on Armed Services' Subcommittee on Emerging Threats and Capabilities," Department of the Treasury, press release, June 9, 2016, https://www.treasury.gov/press-center/press-releases/Pages/jl0486.aspx; "Statement of Deputy Assistant Secretary Andrew Keller, U.S. Department of State, Bureau for Economic and Business Affairs before the United States House of Representatives Committee on Foreign Affairs Subcommittee on Terrorism, Nonproliferation, and Trade, June 9, 2016," Committee on Foreign Affairs, U.S. House of Representatives, statement to the Subcommittee on Terrorism, Nonproliferation, and Trade, 2–3.

41. "Financing of the Terrorist Organization Islamic State in Iraq and the Levant (ISIL)" (FATF/OECD, February 2015), 10, http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf.

42. Ibid., 12.

43. Ibid.

44. "Statement of Deputy Assistant Secretary Andrew Keller," 3.

45. "Testimony of A/S for Terrorist Financing Daniel L. Glaser."

46. "Financing of the Terrorist Organization ISIL," 18, 20.

47. Ibid., 12.

48. Benoit Faucon and Ahmed Al Omran, "Islamic State Steps Up Oil and Gas Sales to Assad Regime," *The Wall Street Journal*, January 19, 2017, https://www.wsj.com/articles/islamic-state-steps-up-oil-and-gas-sales-to-assad-regime-1484835563.

49. Ibid.

50. "Emerging Terrorist Financing Risks," 31.

51. Ibid.

52. Ibid., 34.

53. "Financing of the Terrorist Organization ISIL,", 25–26.

54. Joby Warrick, "Private Donations Give Edge to Islamists in Syria, Officials Say," *The Washington Post*, September 21, 2013, https://www.washingtonpost.com/world/national-security/private-donations-give-edge-to-islamists-in-syria-officials-say/2013/09/21/a6c783d2-2207-11e3-a358-1144dee636dd_story.html.

55. "Emerging Terrorist Financing Risks," 31.

56. Juan C. Zarate, chairman and co-founder, Financial Integrity Network, "The Next Terrorist Financiers: Stopping Them Before They Start," Statement to the Financial Services Committee, Task Force to Investigate Terrorism Financing, U.S. House of Representatives, June 23, 2016, 2.

57. Ibid., 7–8.

58. "Emerging Terrorist Financing Risks," 20–21.

59. National Commission on Terrorist Attacks upon the United States et al."The 9/11 Commission Report," 14.

60. Ibid.

61. "Combating the Abuse of Alternative Remittance Systems: International Best Practices" (FATF, June 20, 2003), 5, http://www.fatf-gafi.org/media/fatf/BPP%20SRVI%20June%202003%202012.pdf.

62. "Two Indicted in Missouri on Charges of Providing Material Support to a Terrorist Organization; A Third Defendant Is Charged with Structuring Violations," FBI, November 3, 2010, https://archives.fbi.gov/archives/stlouis/press-releases/2010/sl110310.htm.

63. Ibid.

64. "Money Laundering Through the Physical Transportation of Cash" (FATF, October 2015), 3, http://www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-through-transportation-cash.pdf.

65. "Terrorist Financing," 23.

66. "Terrorist Financing in West and Central Africa" (FATF/GIABA/GABAC, October 2016), 27.

67. Jacob Shapiro, "Bureaucratic Terrorists: al-Qaida in Iraq's Management and Finances," in Brian Fishman, ed., "Bomber, Bank Accounts, and Bleedout," Harmony Project report (Combating Terrorism Center at West Point, July 22, 2008), 8, 73, https://www.ctc.usma.edu/posts/bombers-bank-accounts-and-bleedout-al-qaidas-road-in-and-out-of-iraq.

68. "Emerging Terrorist Financing Risks," 37–38.

69. Ralph Ellis, "Maryland Man Charged with Trying to Aid ISIS," CNN, December 14, 2015, http://www.cnn.com/2015/12/14/us/maryland-terror-arrest/.

70. "Emerging Terrorist Financing Risks," 38.

71. J. E. Reich, "Using Internet Slang on Venmo Might Get You Flagged As a Terrorist," Tech Times, March 11, 2016, http://www.techtimes.com/articles/140422/20160311/using-internet-slang-on-venmo-might-get-you-flagged-as-a-terrorist.htm.

72. Alexandra Starr, "In Wake of Attacks, France Moves to Regulate Prepaid Bank Cards," NPR, the Two-Way, November 23, 2015, http://www.npr.org/sections/thetwo-way/2015/11/23/457090827/in-wake-of-attacks-france-moves-to-regulate-prepaid-bank-cards.

73. French Ministry for the Economy and Finance, "France's Contribution: New Efforts to Combat Terrorist Financing at European Level," Paris, November 27, 2015, 7, http://www.economie.gouv.fr/files/files/PDF/20151127_France's_contribution_-_New_efforts_to_combat_terrorist_financing_at_European_level.pdf .

74. Foo Yun Chee, "EU Proposes Stricter Rules on Bitcoin, Prepaid Cards in Terrorism Fight," Reuters, July 5, 2016, http://www.reuters.com/article/us-eu-security-financing-idUSKCN0ZL1RH.

75. "Virtual Currencies: Key Definitions," 9–10.

76. Ibid., 10.

77. Ibid., 9–10.

78. Yaya J. Fanusie, "The New Frontier in Terror Fundraising: Bitcoin," The Cipher Brief, August 24, 2016, https://www.thecipherbrief.com/column/private-sector/new-frontier-terror-fundraising-bitcoin-1089.

79. Resty Woro Yuniar, "Bitcoin, PayPal Used to Finance Terrorism, Indonesian Agency Says," *The Wall Street Journal*, January 10, 2017, http://www.wsj.com/articles/bitcoin-paypal-used-to-finance-terrorism-indonesian-agency-says-1483964198.

80. Tim Johnson, "Computer Hack Helped Feed an Islamic State Death List," *McClatchy DC Bureau*, July 20, 2016, http://www.mcclatchydc.com/news/nation-world/national/article90782637.html.

81. "Virginia Teen Pleads Guilty to Providing Material Support to ISIL," Department of Justice, press release, June 11, 2015, http://www.justice.gov/opa/pr/virginia-teen-pleads-guilty-providing-material-support-isil.

82. Adam Taylor, "The Islamic State (or Someone Pretending to Be It) Is Trying to Raise Funds Using Bitcoin," *The Washington Post*, June 9, 2015, https://www.washingtonpost.com/news/worldviews/wp/2015/06/09/the-islamic-state-or-someone-pretending-to-be-it-is-trying-to-raise-funds-using-bitcoin/?utm_term=.17ae7b7b7221.

83. Danna Harman, "U.S.-based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests," *Haaretz*, January 29, 2015, http://www.haaretz.com/middle-east-news/.premium-1.639542.

84. Aaron Brantly, "Financing Terror Bit by Bit," *CTC Sentinel* 7, no. 10 (October 2014), 4, https://www.ctc.usma.edu/posts/financing-terror-bit-by-bit.

85. Ibid.

86. Harman, "U.S.-Based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests"; Taylor, "The Islamic State (Or Someone Pretending to Be It) Is Trying to Raise Funds Using Bitcoin"; "Virginia Teen Pleads Guilty to Providing Material Support to ISIL"; Johnson, "Computer Hack Helped Feed an Islamic State Death List"; Fanusie, "The New Frontier in Terror Fundraising: Bitcoin"; Yuniar, "Bitcoin, PayPal Used to Finance Terrorism, Indonesian Agency Says."

87. Carter Dougherty and Greg Farrell, "Treasury's Cohen Sees No Widespread Criminal Bitcoin Use," *Bloomberg*, March 18, 2014, https://www.bloomberg.com/news/articles/2014-03-18/treasury-s-cohen-says-regulation-helps-virtual-currencies.

88. Joshua Baron, Angela O'Mahony, David Manheim, and Cynthia Dion-Schwarz, "National Security Implications of Virtual Currency: Examining the Potential for Non-State Actor Deployment" (RAND, 2015), 19.

89. Europol, "Changes in Modus Operandi of Islamic State Terrorist Attacks," January 18, 2016, 7, http://www.wienerzeitung.at/_em_daten/_wzo/2016/01/25/160125_1356_europol_dokument_aenderungen_in_der_verfahrensweise_mit_is_terroranschlaegen_pdf_englisch.pdf.

90. Brantly, "Financing Terror Bit by Bit," 1; Baron et al., "National Security Implications of Virtual Currency," 19.

91. Nathaniel Karp and Boyd W. Nash-Stacey, "Technology, Opportunity and Access: Understanding Financial Inclusion in the U.S.," Working Paper N. 15 (BBVA Research, July 2015), 33, https://www.bbvaresearch.com/wp-content/uploads/2015/07/WP15-25_FinancialInclusion_MSA.pdf .

92. Dayo Olopade, "Africa's Tech Edge," *The Atlantic*, May 2014, http://www.theatlantic.com/magazine/archive/2014/05/africas-tech-edge/359808/.

93. Ibid.; "Mobile Payments Go Viral: M-PESA in Kenya," World Bank, March 2010, http://web.worldbank.org/WBSITE/EXTERNAL/COUNTRIES/AFRICAEXT/0,,contentMDK:22551641~pagePK:146736~piPK:146830~theSitePK:258644,00.html.

94. Department of the Treasury, "2015 National Terrorist Financing Risk Assessment," 47.

95. Josh Meyer, "How Mobile Payments Might Be the Global Money-Laundering Machine Criminals Have Dreamed About," Quartz, June 17, 2013, https://qz.com/94570/how-mobile-payments-might-be-the-global-money-laundering-machine-criminals-have-dreamed-about/.

96. David S. Evans, "Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms" (University of Chicago Coase-Sandor Institute for Law and Economics, April 15, 2014), 10.

97. Bradley Reaves, Nolen Scaife, Adam Bates, Patrick Traynor, and Kevin R.B. Butler, "Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World," (paper included in the proceedings of the 24th USINEX Security Symposium, Washington, D.C., August 2015), 17.

98. Danielle Camner Lindholm and Celina B. Realuyo, "Threat Finance: A Critical Enabler for Illicit Networks," in *Convergence: Illicit Networks and National Security in the Age of Globalization*, Michael Miklaucic and Jacqueline Brewer, eds. (Washington, DC: National Defense University Press, 2013) 119.

99. "PayPal Completes Acquisition of Xoom," Xoom, November 2015, http://blog.xoom.com/2015/11/paypal-completes-acquisition-of-xoom.html.

100. Robin Sidel and Daisuke Wakabayashi, "Apple, Banks in Talks on Mobile Person-to-Person Payment Service," *The Wall Street Journal*, November 11, 2015, http://www.wsj.com/articles/apple-in-talks-with-u-s-banks-to-develop-mobile-person-to-person-payment-service-1447274074.

101. "Virtual Currencies: Key Definitions," 4–5.

102. Ibid., 5.

103. John Bohannon, "Why Criminals Can't Hide Behind Bitcoin," *Science*, March 9, 2016, http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin.

104. For example, bitcoins can be "tumbled" by having their individual transactions mixed with others, obfuscating the trail of ownership. See Jamie Redman, "Tumbling Bitcoins: A Guide Through the Rinse Cycle," Bitcoin News, July 21, 2016, https://news.bitcoin.com/tumbling-bitcoins-guide-rinse-cycle/.

105. Andy Greenberg, "Monero, the Drug Dealer's Cryptocurrency of Choice, Is on Fire," *Wired*, January 25, 2017, https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/.

106. Ibid.

107. Yuji Nakamura, "New Digital Currency Spikes As Drug Dealers Get More Secrecy," *Bloomberg Technology*, August 29, 2016, https://www.bloomberg.com/news/articles/2016-08-29/new-digital-currency-spikes-after-giving-criminals-more-secrecy; Greenberg, "Monero, The Drug Dealer's Cryptocurrency of Choice."

108. Greenberg, "Monero, The Drug Dealer's Cryptocurrency of Choice."

109. Michael del Castillo, "The FBI Is Worried Criminals Might Use the Private Cryptocurrency Monero," CoinDesk, January 31, 2017, http://www.coindesk.com/fbi-concerned-about-criminal-use-of-private-cryptocurrency-monero/.

110. Andy Greenberg, "'Dark Wallet' Is About to Make Bitcoin Money Laundering Easier Than Ever," *Wired*, April 29, 2014, https://www.wired.com/2014/04/dark-wallet/.

111. Ibid.

112. Andy Greenberg, "Waiting for Dark: Inside Two Anarchists' Quest for Untraceable Money," *Wired*, July 11, 2014, https://www.wired.com/2014/07/inside-dark-wallet/.

113. "Virtual Currencies: Key Definitions," 7.

114. Sidney Ember, "Overstock to Allow International Customers to Pay in Bitcoin," *The New York Times*, August 19, 2014, https://dealbook.nytimes.com/2014/08/19/overstock-to-allow-international-customers-to-pay-in-bitcoin/?_r=0.

115. Christopher Langner, "Is Bitcoin Growing Up?" *Bloomberg*, February 12, 2017, https://www.bloomberg.com/gadfly/articles/2017-02-13/bitcoin-might-just-be-growing-up.

116. "Virtual Currencies: Key Definitions," 9. Dong He, Karl Habermeier, Ross Leckow, Vikram Haksar, Yasmin Almeida, Mikari Kashima, Nadim Kyriakos-Saad, Hiroko Oura, Tahsin Saadi Sedik, Natalia Stetsenko, and Concepcion Verdugo-Yepes, "Virtual Currencies and Beyond: Initial Considerations," IMF Staff Discussion Note SDN/16/03 (IMF, January 2016), 6.

117. Nakamoto is a pseudonymous identity. Observers have speculated the name could represent either one individual or a team who invented the technology. See Joshua Davis, "The Crypto-Currency," *The New Yorker*, October 10, 2011, http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency.

118. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," November 1, 2008, https://bitcoin.org/bitcoin.pdf.

119. World Bank Group, "Migration and Remittances Factbook 2016 Third Edition," (Washington, D.C.: World Bank, May 2, 2016), xii.

120. "Top of Mind: All About Bitcoin," Global Macro Research Issue 21 (Goldman Sachs, March 11, 2014), 18, http://www.paymentlawadvisor.com/files/2014/01/GoldmanSachs-BitCoin.pdf.

121. Buenaventura, "There's a $500 Billion Remittance Market."

122. Andreas Adriano and Hunter Monroe, "The Internet of Trust," *Finance and Development* 53, no. 2 (June 2016).

123. Ibid.

124. He et al., "Virtual Currencies and Beyond," 10, 22.

125. Jon Evans, "The Controversy over Satoshi Nakamoto's True Identity Is Jeopardizing Bitcoin's Future," Quartz, May 19, 2016, https://qz.com/687493/the-controversy-over-satoshi-nakamotos-true-identity-is-jeopardizing-bitcoins-future/.

126. Buenaventura, "There's a $500 Billion Remittance Market."

127. As of December 2016, Circle does not, however, permit the input of new Bitcoins into the system allowing the transfer of Bitcoins converted into *fiat* currencies and using Bitcoin as the back-end technology. See Fitz Tepper, "Circle Removes Ability to Buy and Sell Bitcoin As It Doubles Down on Mobile Payments," TechCrunch, December 7, 2016, https://techcrunch.com/2016/12/07/circle-removes-ability-to-buy-and-sell-bitcoin-as-it-doubles-down-on-mobile-payments/. Adriano and Monroe, "The Internet of Trust."

128. Emma Dunkley, "Santander Pilots Blockchain Payments App," *Financial Times*, May 26, 2016, https://www.ft.com/content/2df2f65c-234f-11e6-9d4d-c11776a5124d.

129. Matt Higginson, "How Blockchain Could Disrupt Cross-Border Payments," *Banking Perspectives* 4, no. 4 (4th quarter, 2016), 56–58, https://www.theclearinghouse.org/-/media/tch/documents/research/banking%20perspectives/2016/q4/2016-q4-bp-issue-web.pdf?la=en.

130. Veem Inc.,"Legal Disclosures: Anti-Money Laundering Policy," Veem.com, March 6, 2017, https://www.veem.com/legal/; Corin Faife, "Why Bitcoin's Remittance Disruption Slowed to a Crawl," CoinDesk, December 11, 2016, http://www.coindesk.com/why-bitcoins-remittance-disruption-slowed-to-a-crawl/.

131. "How Bitcoin Mining Works," CoinDesk, December 22, 2014, http://www.coindesk.com/information/how-bitcoin-mining-works/.

132. "What Is Blockchain Technology?" Blockchain, December 20, 2016, https://support.blockchain.com/hc/en-us/articles/211160223-What-is-blockchain-technology.

133. Mariano Belinky, Emmet Rennick, and Andrew Veitch, "Rebooting Financial Services," *Santander Innoventures,* June 2015, 14–15, http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf.

134. Kevin Maney, "Trust and Verify: The Coming Blockchain Revolution," *Newsweek*, May 23, 2016, http://www.newsweek.com/2016/06/03/blockchain-technology-will-remake-global-financial-system-462537.html?rx=us.

135. Ali Safavi and Kevin Wang, "Blockchain Is Empowering the Future of Insurance," TechCrunch, October 29, 2016, https://techcrunch.com/2016/10/29/blockchain-is-empowering-the-future-of-insurance/.

136. Megan Molteni, "Moving Patient Data Is Messy, But Blockchain Is Here to Help," *Wired,* February 1, 2017, https://www.wired.com/2017/02/moving-patient-data-messy-blockchain-help/.

137. Nathaniel Popper and Steve Lohr, "Blockchain: A Better Way to Track Pork Chops, Bonds, Bad Peanut Butter?" *The New York Times,* March 4, 2017, https://www.nytimes.com/2017/03/04/business/dealbook/blockchain-ibm-bitcoin.html?_r=0.

138. Jackie Burns Koven, "Block the Vote: Could Blockchain Technology Cybersecure Elections?" *Forbes*, August 30, 2016, https://www.forbes.com/sites/realspin/2016/08/30/block-the-vote-could-blockchain-technology-cybersecure-elections/#33cc451d2ab3.

139. Jordan Pearson, "Bitcoin Is Too Libertarian to Save the Developing World, Says UN Paper," Motherboard, February 11, 2016, https://motherboard.vice.com/en_us/article/bitcoin-is-too-libertarian-to-save-the-developing-world-says-un-paper.

140. Joseph Adinolfi, "Bitfinex Hack Shows How Bitcoin's Blockchain Can Be a Liability," MarketWatch, August 4, 2016, http://www.marketwatch.com/story/bitfinex-hack-shows-how-bitcoins-blockchain-can-be-a-liability-2016-08-03.

141. Tanya Andreasyan, "Standard Chartered Explores Blockchain Viability," *Banking Technology*, June 16, 2016, http://www.bankingtech.com/514402/standard-chartered-explores-blockchain-viability/; Brady Porche, "Blockchain Could Spur Credit Card Rewards Revolution," Creditcards.com, November 3, 2016, http://www.creditcards.com/credit-card-news/blockchain-could-spur-credit-card-rewards-revolution.php.

142. "Bitcoin," CryptoCurrency Market Capitalizations, https://coinmarketcap.com/currencies/bitcoin/.

143. "Monero," CryptoCurrency Market Capitalizations, https://coinmarketcap.com/currencies/monero/.

144. "Zcash," Cryptocurrency Market Capitalizations, https://coinmarketcap.com/currencies/zcash/.

145. Jose Pagliery, "Inside the $2 Billion ISIS War Machine," CNN Money, December 11, 2015, http://money.cnn.com/2015/12/06/news/isis-funding/.

146. Department of the Treasury, "2015 National Money Laundering Risk Assessment," 2, https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf

147. Juan C. Zarate and Chip Poncy, "Designing a New AML System," *Banking Perspectives* 4, no. 3 (3rd quarter, 2016), 27, https://www.theclearinghouse.org/-/media/tch/documents/research/banking%20perspectives/2016/q3/2016-q3-bp-issue-web.pdf?la=en.

148. See Aaron Shaw and Benjamin M. Hill, "Laboratories of Oligarchy? How the Iron Law Extends to Peer Production," *Journal of Communication* 64, no. 2 (April 1, 2014), 215–38.

149. Ranier Böhme, Nicolas Christin, Benjamin Edelman, and Tyler Moore, "Bitcoin: Economics, Technology, and Governance," *Journal of Economic Perspectives* 29, no. 2 (spring 2015), 219–20.

150. Ibid., 220–22.

151. Lauren Gensler, "The Idiot's Guide to Laundering $9 Million," *Forbes*, January 11, 2017, http://www.forbes.com/sites/laurengensler/2017/01/11/gift-cards-money-laundering/.

152. Jason Del Rey, "Offshore Gambling Site Laundered $2 Million in Amazon Gift Cards, Feds Say," Recode, March 15, 2016, http://www.recode.net/2016/3/15/11586972/offshore-gambling-site-laundered-2-million-in-amazon-gift-cards-feds.

153. Eric Lichtblau, "How an American Ended Up Accused of Aiding ISIS with Gift Cards," *The New York Times*, January 28, 2017, https://www.nytimes.com/2017/01/28/us/politics/washington-transit-cop-suspected-isis.html.

154. Leslie Walker, "PayPal.com CEO Peter Thiel," *The Washington Post*, August 2, 2001, http://www.washingtonpost.com/wp-srv/liveonline/01/washtech/walker/washtech_walker080201.htm.

155. Ibid.

156. Brian Grow, "Gold Rush," *Bloomberg*, January 9, 2006, http://www.bloomberg.com/news/articles/2006-01-08/gold-rush.

157. Margaret Kane, "eBay Picks Up PayPal for $1.5 Billion," CNET, August 18, 2002, https://www.cnet.com/news/ebay-picks-up-paypal-for-1-5-billion/.

158. Jessica Menton, "PYPL Stock Price Soars 11 Percent on Wall Street Return Following eBay Inc. Spinoff," *International Business Times*, July 20, 2015, http://www.ibtimes.com/paypal-ipo-2015-pypl-stock-price-soars-11-wall-street-return-following-ebay-inc-2016040.

159. "PayPal Reports Fourth Quarter and Full Year 2016 Results," PayPal, January 26, 2017, https://investor.paypal-corp.com/releasedetail.cfm?releaseid=1009339.

160. Sarah Mishkin, "Innovation Key to PayPal's Successful Independence," *Financial Times*, September 30, 2014, http://www.ft.com/cms/s/0/307d8e56-48b7-11e4-9d04-00144feab7de.html#axzz4Hi2zUmBc.

161. Telis Demos, "PayPal Isn't a Bank, But It May Be the New Face of Banking," *The Wall Street Journal*, June 1, 2016, http://www.wsj.com/articles/as-banking-evolves-fintech-emerges-from-the-branch-1464806411.

162. Ibid.

163. Chargebacks occur when a customer contests an order that was received. PayPal opens a dispute resolution process and places a temporary hold on the funds involved. This enables PayPal to potentially reverse the transaction and restore costs to the customer. For more on PayPal's current procedures and policies, see "Resolving disputes, claims and chargebacks," PayPal, https://www.paypal.com/us/webapps/mpp/security/resolve-disputes.

164. Eric M. Jackson and Christopher Grey, "Bitcoin Is The New PayPal," TechCrunch, February 20, 2014, http://social.techcrunch.com/2014/02/20/bitcoin-is-the-new-paypal/.

165. Gregory J. Millman, "How Paypal Manages Fraud Risk," *The Wall Street Journal*, June 18, 2015, http://blogs.wsj.com/riskandcompliance/2015/06/18/how-paypal-manages-fraud-risk/.

166. Jackson and Grey, "Bitcoin Is The New PayPal"; Walker, "PayPal.com CEO Peter Thiel."

167. Mark Berniker and Matt Hunter, "Semi-Secretive CIA-Backed Data Company to Shun IPO, for Now," CNBC, March 12, 2014, http://www.cnbc.com/2014/03/12/whats-behind-silicon-valleys-most-secretive-company.html.

168. Evan I. Schwartz, "Digital Cash Payoff," *MIT Technology Review*, December 1, 2011, https://www.technologyreview.com/s/401297/digital-cash-payoff/.

169. Ibid.

170. Ibid.

171. Ibid.

172. Ibid.

173. "Undertaking to the Chief Executive Officer of AUSTRAC for the Purposes of Section 197 of the AML/CTF Act by PayPal Australia," Australian Transaction Reports and Analysis Center, 3rd Enforceable Undertaking, November 23, 2009, http://www.austrac.gov.au/sites/default/files/documents/eu_paypal.pdf.

174. Rachel Louise Ensign, "PayPal to Pay $7.7 Million to U.S. over Alleged Sanctions Violations," *The Wall Street Journal*, March 25, 2015, http://www.wsj.com/articles/paypal-to-pay-7-7-million-to-u-s-over-alleged-sanctions-violations-1427312161.

175. Office of Foreign Assets Control, Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and Paypal, Inc. (Department of the Treasury, March 25, 2015), 1, https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20150325_paypal_settlement.pdf.

176. Ibid.

177. Brian Krebs, "2016 Reality: Lazy Authentication Still the Norm," Krebs on Security, December 28, 2015, http://krebsonsecurity.com/2015/12/2016-reality-lazy-authentication-still-the-norm/.

178. P. Carl Mullan, *A History of Digital Currency in the United States: New Technology in an Unregulated Market* (New York: Palgrave Macmillan, 2016), 19–20.

179. Kim Zetter, "Bullion and Bandits: The Improbable Rise and Fall of E-Gold," *Wired*, June 9, 2009, https://www.wired.com/2009/06/e-gold/.

180. Grow, "Gold Rush."

181. Tim Jackson, "When Gold Makes Cents," *Financial Times*, July 13, 1999.

182. Jack White and Doug Ramsey, "Making New Money," *Barron's*, April 23, 2001.

183. Julian Dibbell, "In Gold We Trust," *Wired*, January 1, 2002, http://www.wired.com/2002/01/egold/.

184. Grow, "Gold Rush."

185. P. Carl Mullen, *The Digital Currency Challenge: Shaping Online Payment Systems through U.S. Financial Regulations* (New York: Palgrave Macmillan, 2014), 20.

186. Michael Mandel, "Money Ain't What It Used to Be," *Business Week*, January 9, 2006.

187. Grow, "Gold Rush."

188. Jackson, "When Gold Makes Cents."

189. Grow, "Gold Rush."

190. Loretta Napoleoni, *Rogue Economics* (New York: Seven Stories Press, 2011), 148.

191. Jackson, "When Gold Makes Cents."

192. Zetter, "Bullion and Bandits."

193. Ibid.

194. Jennifer L. Hesterman, *The Terrorist-Criminal Nexus: An Alliance of International Drug Cartels, Organized Crime, and Terror Groups* (Boca Raton, Fla.: CRC Press, 2013), 236.

195. Grow, "Gold Rush."

196. Ibid.

197. Zetter, "Bullion and Bandits"; Kim Zetter, "E-Gold Gets Tough on Crime," *Wired*, December 11, 2006, https://www.wired.com/2006/12/e-gold-gets-tough-on-crime/.

198. Ibid.

199. "Digital Currency Business E-Gold Indicted for Money Laundering and Illegal Money Transmitting," United States Department of Justice, press release, April 27, 2007, https://www.justice.gov/archive/opa/pr/2007/April/07_crm_301.html.

200. Ibid.

201. Stephanie Condon, "Judge Spares E-Gold Directors Jail Time," CNET, November 20, 2008, http://www.cnet.com/news/judge-spares-e-gold-directors-jail-time/.

202. Sarah Jane Hughes, Stephen T. Middlebrook, and Broox W. Peterson, "Developments in the Law Concerning Stored-Value Cards and Other Electronic Payments," *Business Lawyer*, 63 No. 237 (November 2007), 259.

203. Grow, "Gold Rush."

204. Condon, "Judge Spares E-Gold Directors Jail Time;" Stephen Foley, "E-Gold Founder Backs New Bitcoin Rival," *Financial Times*, November 28, 2013, https://www.ft.com/content/f7488616-561a-11e3-96f5-00144feabdc0.

205. United States of America v. Liberty Reserve S.A., No. USA-33s-274 (Ed. 9-25-58), United States District Court, Southern District of New York, May 2013, 6, https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/Liberty%20Reserve%2C%20et%20al.%20Indictment%20-%20Redacted.pdf.

206. Jake Halpern, "Bank of the Underworld," *The Atlantic*, May 2015, http://www.theatlantic.com/magazine/archive/2015/05/bank-of-the-underworld/389555/.

207. "Liberty Reserve Digital Money Service Forced Offline," BBC News, May 27, 2013, http://www.bbc.com/news/technology-22680297.

208. Tim Fernholz, "Liberty Reserve: Legit E-Currency, or 'Bank of Choice for the Criminal Underworld'?" *The Atlantic*, May 28, 2013, https://www.theatlantic.com/business/archive/2013/05/liberty-reserve-legit-e-currency-or-bank-of-choice-for-the-criminal-underworld/276312/.

209. Halpern, "Bank of the Underworld."

210. Financial Crimes Enforcement Network, "Notice of Finding That Liberty Reserve S.A. Is a Financial Institution of Primary Money Laundering Concern" (Department of the Treasury, May 28, 2013), 6.

211. Halpern, "Bank of the Underworld."

212. Ibid.

213. "Liberty Reserve Digital Money Service Forced Offline."

214. Halpern, "Bank of the Underworld"; "Liberty Reserve Digital Money Service Forced Offline."

215. United States of America v. Liberty Reserve S.A., 13.

216. "Liberty Reserve Founder Arthur Budovsky Sentenced in Manhattan Federal Court to 20 Years for Laundering Hundreds of Millions of Dollars Through His Global Digital Currency Business," U.S. Department of Justice, May 6, 2016, https://www.justice.gov/usao-sdny/pr/liberty-reserve-founder-arthur-budovsky-sentenced-manhattan-federal-court-20-years.

217. Halpern, "Bank of the Underworld."

218. Ibid.

219. "Liberty Reserve Digital Money Service Forced Offline."

220. Halpern, "Bank of the Underworld."

221. Ibid.

222. "Liberty Reserve Digital Money Service Forced Offline."

223. Nate Raymond and Brendan Pierson, "Digital Currency Firm Co-Founder Gets 10 Years in Prison in U.S. Case," Reuters, May 13, 2016, http://www.reuters.com/article/us-usa-cyber-libertyreserve-idUSKCN0Y42A2; Joe Palazzolo, "Liberty Reserve Founder Budovsky Extradited to U.S. from Spain," *The Wall Street Journal*, October 10, 2014, https://www.wsj.com/articles/liberty-reserve-founder-budovsky-extradited-to-u-s-from-spain-1412974424.

224. Brian Krebs, "Underweb Payments, Post-Liberty Reserve," Krebs on Security, May 30, 2013, http://krebsonsecurity.com/2013/05/underweb-payments-post-liberty-reserve/.

225. Europol, *The 2016 Internet Organised Crime Threat Assessment* (The Hague: European Policy Office, September 27, 2016) 42, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

226. Krebs, "Underweb Payments, Post-Liberty Reserve."

227. Böhme et al., "Bitcoin: Economics, Technology, and Governance," 213–4.

228. Ibid., 222–4.

229. "Ten Arrested in Netherlands over Bitcoin Money-Laundering Allegations," *The Guardian*, January 20, 2016, https://www.theguardian.com/technology/2016/jan/20/bitcoin-netherlands-arrests-cars-cash-ecstasy.

230. Europol, *The 2015 Internet Organised Crime Threat Assessment* (The Hague: European Policy Office, July 27, 2015) 46, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015.

231. Brantly, "Financing Terror Bit by Bit."

232. Richard Winton, "Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating," *Los Angeles Times*, February 18, 2016, http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html.

233. David Fitzpatrick and Drew Griffin, "Cyber-Extortion Losses Skyrocket, Says FBI," CNN Money, April 15, 2016. http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/index.html?section=money_technology.

234. Lucian Constantin, "Ransomware Attacks Against Businesses Increased Threefold in 2016," *PCWorld,* December 9, 2016, http://www.pcworld.com/article/3149106/security/ransomware-attacks-against-businesses-increased-threefold-in-2016.html.

235. Mark Ward, "'Alarming' Rise in Ransomware Tracked," BBC News, June 7, 2016, http://www.bbc.com/news/technology-36459022.

236. Symantec, "Ransomware and Businesses 2016," July 19, 2016, 3, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf.

237. Matt Zapotosky and Ellen Nakashima, "These Hackers Can Hold a Town Hostage. And They Want Ransom—Paid in Bitcoin," *The Washington Post,* March 21, 2016, https://www.washingtonpost.com/world/national-security/these-hackers-can-hold-a-town-hostage-and-they-want-ransom--paid-in-bitcoin/2016/03/18/1a2e2494-eba9-11e5-bc08-3e03a5b41910_story.html; Tim Simonite, "Companies Are Stockpiling Bitcoin to Pay Off Cybercriminals," *MIT Technology Review,* June 7, 2016, https://www.technologyreview.com/s/601643/companies-are-stockpiling-bitcoin-to-pay-off-cybercriminals/.

238. Kim Zetter, "Why Hospitals Are the Perfect Targets for Ransomware," *Wired*, March 30, 2016, https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/.

239. Josephine Wolff, "The New Economics of Cybercrime," *The Atlantic,* June 7, 2016, http://www.theatlantic.com/business/archive/2016/06/ransomware-new-economics-cybercrime/485888/; Nathaniel Popper, "For Ransom, Bitcoin Replaces the Bag of Bills," *The New York Times,* July 25, 2015, http://www.nytimes.com/2015/07/26/business/dealbook/for-ransom-bitcoin-replaces-the-bag-of-bills.html.

240. Popper, "For Ransom, Bitcoin Replaces the Bag of Bills."

241. "Written testimony of USSS Criminal Investigative Division Special Agent in Charge Edward Lowery III for a Senate Committee on Homeland Security and Governmental Affairs hearing titled 'Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies,'" U.S. Department of Homeland Security, press release, November 18, 2013, https://www.dhs.gov/news/2013/11/18/written-testimony-us-secret-service-senate-committee-homeland-security-and.

242. Bearman and Hanuka, "The Untold Story of Silk Road, Part 1"; Bearman and Hanuka, "The Untold Story of Silk Road, Part 2"; Andy Greenberg, "Prosecutors Trace $13.4M in Bitcoins from the Silk Road to Ulbricht's Laptop," *Wired*, January 29, 2015, https://www.wired.com/2015/01/prosecutors-trace-13-4-million-bitcoins-silk-road-ulbrichts-laptop/.

243. Ablon, Libicki, and Golay, "Markets for Cybercrime Tools and Stolen Data," 25–28; Greenberg, "New Dark-Web Market."

244. See Ablon, Libicki, and Golay, "Markets for Cybercrime Tools and Stolen Data," 8–10; Keith Collins, "Here's What Your Stolen Identity Goes for on the Internet's Black Market," Quartz, July 23, 2015, https://qz.com/460482/heres-what-your-stolen-identity-goes-for-on-the-internets-black-market/.

245. Department of the Treasury, "2015 National Terrorist Financing Risk Assessment," 57–58.

246. Baron et al., "National Security Implications of Virtual Currency," 29.

247. Ablon, Libicki, and Golay, "Markets for Cybercrime Tools and Stolen Data," 4.

248. Ibid., 8.

249. Ibid., x, 8, 15–16.

250. "Remarks of Under Secretary for Terrorism and Financial Intelligence David Cohen before the Center for a New American Security on 'Confronting New Threats in Terrorist Financing,'" Department of the Treasury, press release, March 4, 2014, https://www.treasury.gov/press-center/press-releases/Pages/jl2308.aspx.

251. "Risk of Terrorist Abuse in Non-Profit Organizations" (FATF/OECD, June 2014), 60–64, http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-of-terrorist-abuse-in-non-profit-organisations.pdf ; U.S. Department of State, "State Sponsors of Terrorism Overview," Country Reports on Terrorism 2015, June 2016, https://www.state.gov/j/ct/rls/crt/2015/257520.htm.

252. Donna Abu-Nasr, "In War and Now Finance, Losses Mount for Iranian Ally Hezbollah," *Bloomberg*, June 14, 2016, https://www.bloomberg.com/news/articles/2016-06-14/iran-s-return-isn-t-helping-ally-hezbollah-pay-the-bills.

253. "Treasury Sanctions Maritime Network Tied to Joumaa Criminal Organization," Department of the Treasury, press release, October 1, 2015, https://www.treasury.gov/press-center/press-releases/Pages/jl0196.aspx; "Treasury Identifies Lebanese Canadian Bank SAL as a 'Primary Money Laundering Concern,'" Department of the Treasury, press release, February 10, 2011, https://www.treasury.gov/press-center/press-releases/Pages/tg1057.aspx.

254. Conversely, the destruction of the trusted relationships between terrorist groups and their fundraisers/facilitators can have a deleterious effect on their financial stability. See Stuart A. Levey, "Loss of Moneyman a Big Blow for al-Qaeda," *The Washington Post*, June 6, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/06/04/AR2010060404271.html.

255. Lichtblau, "How an American Ended Up Accused of Aiding ISIS"; Jack Moore, "Hawala: The Ancient Banking Practice Used to Finance Terror Groups," *Newsweek*, February 24, 2015, http://www.newsweek.com/underground-european-hawala-network-financing-middle-eastern-terror-groups-307984; Dominic Casciani, "Syria Aid Convoys: Two Guilty Over Terror Funding," BBC News, December 23, 2016, http://www.bbc.com/news/uk-38419488.

256. Stephanie Wilshusen, Robert M. Hunt, James van Opstal, and Rachel Schneider, "Consumers' Use of Prepaid Cards," Federal Reserve Bank of Philadelphia, August 2012, 3.

257. "Final Rule—Definitions and Other Regulations Relating to Prepaid Access," Financial Crimes Enforcement Network, November 2, 2011, https://www.fincen.gov/resources/statutes-regulations/guidance/final-rule-definitions-and-other-regulations-relating; "Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing and Amending Directive 2009/101/EC" (Strasbourg: European Commission, July 5, 2016), http://ec.europa.eu/justice/criminal/document/files/aml-directive_en.pdf.

258. Claire Groden, "Feds Say This Offshore Gambling Site Used Amazon Gift Cards to Launder Cash," *Fortune*, March 15, 2016, http://fortune.com/2016/03/15/5dimes-amazon-laundering/; Gensler, "The Idiot's Guide To Laundering $9 Million."

259. "FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action against a Virtual Currency Exchanger," FinCEN, press release, May 5, 2015, https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual.

260. Ibid.

261. Author phone interview with AML attorney, 2016.

262. Marion Keyes, "Challenges Faced When Auditing a Digital-Currency Financial Institution" ACAMS, February 2015, 5–7.

263. FinCEN, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," memo, FIN-2013-G001 (March 18, 2013), 1, https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

264. "China Bitcoin Exchanges Halt Withdrawals after PBOC Talks," *Bloomberg*, February 9, 2017 https://www.bloomberg.com/news/articles/2017-02-10/china-bitcoin-exchanges-halt-withdrawals-after-central-.

265. Compare IRS, Notice 2014–21 (March 25, 2014), 2, https://www.irs.gov/pub/irs-drop/n-14-21.pdf; and FinCEN, "Application of FinCEN's Regulations," 1.

266. For example, Western Union spends $200 million a year looking for suspicious activity; this is roughly the annual budget of FinCEN. Barry and Ensign, "Losing Count." Another major bank reported spending three times this much last year. Additionally, author interviews with banking executives, 2016.

267. "A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement" (The Clearing House, February 2017), 8, 22, https://www.theclearinghouse.org/~/media/TCH/Documents/TCH%20WEEKLY/2017/20170216_TCH_Report_AML_CFT_Framework_Redesign.pdf.

268. Author phone interview with bank AML lawyer, 2016.

269. Tracey Durner and Liat Shetret, "Understanding Bank De-Risking and Its Effects on Financial Inclusion: An Exploratory Study," research report (Global Center on Cooperative Security/Oxfam, November 2015), 11; Michaela Erbenova, Yan Liu, Nadim Kyriakos-Saad, Alejandro Lopez-Mejia, Giancarlo Gasha, Emmanuel Mathias, Mohamed Norat, Francisca Fernando, and Yasmin Almeida, "The Withdrawal of Correspondent Banking Relationships: A Case for Policy Action," SDN/16/06 (International Monetary Fund, June 2016), 23–26.

270. Author phone interview with banking industry compliance official, 2016.

271. This enhanced risk stems from substantial use of digital financial technology by relatively high-risk clients, including foreign financial institutions, nonbank financial institutions, third-party payment processors, cash-intensive businesses, nonresident aliens and accounts of foreign individuals, foreign corporations, and entities located in higher-risk geographic locations. See Federal Financial Institutions Examination Council, *Bank Secrecy Act Anti-Money Laundering Examination Manual* , Version 2 (2/27/2015), 19–22.

272. "Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes: Research Report" (UNODC, October 2011), 7, http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf.

273. Keyes, "Challenges Faced When Auditing a Digital-currency Financial Institution," 7–9.

274. Juan C. Zarate and Chip Poncy, "Designing a New Anti-Money Laundering (AML) System," research memo (Center on Sanctions and Illicit Finance, September 2016), 11, http://www.defenddemocracy.org/content/uploads/documents/AML_System_memo.pdf .

275. Dennis M. Lormel, "How Terrorist Trends Evolve and How Financial Institutions Should Respond," *ACAMSToday*, March 7, 2016, http://www.acamstoday.org/how-terrorist-trends-evolve/.

276. Clare Ellis and Ines Sofie de Oliveira, "Tackling Money Laundering: Toward a New Model for Information Sharing," occasional paper (Royal United Services Institute for Defence and Security Studies, September 2015), 6, https://rusi.org/sites/default/files/201509_op_tackling_money_laundering.pdf.

277. "Stopping Terror Finance: Securing the U.S. Financial Sector," report prepared by the Staff of the Task Force to Investigate Terrorism Financing, Committee on Financial Services, U.S. House of Representatives, December 20, 2016, 36–39.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy.

CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan. CNAS does not take institutional positions on policy issues. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

1152 15th Street, NW Suite 950 Washington, DC 20005

t. **202.457.9400** | f. **202.457.9401** | **info@cnas.org** | **cnas.org**

Bold. Innovative. Bipartisan.