Blockchain and Cryptocurrencies Undermine Financial Safeguards of Nonproliferation Regime; Necessitate Taskforce Creation

Emily Turner Tatton
December 2018

Executive Summary

The introduction of blockchain technologies and cryptocurrencies to the international financial system has the potential to circumvent the critical financial underpinnings of the nuclear nonproliferation regime. By allowing for anonymous, secure transactions without an intermediary, cryptocurrencies create the possibility of illicit transactions that are not easily detected by law enforcement or national security organizations. The sobering risks presented to the United States and the entire world by an increase in WMD proliferation mandate immediate and effective measures to mitigate the potential undermining of current proliferation safeguards through emergent technologies.

As it currently stands, the nuclear nonproliferation and verification system rests upon the ability to trace financial transactions that support WMD proliferation and associated supply chains. This ability is severely diminished by the introduction of cryptocurrencies. Blockchain facilitates anonymous transactions without intermediaries and has already been used in significant illegal activity, demonstrating the potential for this technology to be used as a means to finance illegal transfer of nuclear and radioactive material as well as controlled dual-use technologies. Individuals, organized non-state actors, and state actors all have varying degrees of motivation and capability to manipulate cryptocurrencies to bring about their WMD-related proliferation goals. The most pertinent threats are from organized terrorist groups, lone wolf actors, China, and Iran and other countries seeking to acquire WMD.

This emergent threat with the potential to increase nuclear proliferation necessitates the creation of a new interagency taskforce with members from key institutions across the United States Government (USG). Designated as the Blockchain Taskforce for Counterproliferation (BTC), this organization will report directly to the Director of National Intelligence (DNI), who can then disseminate BTC analysis to all relevant actors within the USG and assist in the implementation of their policy recommendations. A technically and analytically diverse taskforce from specified sections within the Department of State, Department of Treasury, and the Intelligence Community will collaborate with the private sector and key international institutions, particularly the International Atomic Energy Association (IAEA) and the Financial Action Task Force (FATF), to examine and counter the critical effects of blockchain on nuclear proliferation.

---

a The acronym BTC is chosen intentionally as a play on the Initial Coin Offering stock ticker symbol for Bitcoin (BTC), the cryptocurrency that brought the concept of blockchain out of the dark web and into daily conversations.
Note on Scope, Methodology, and Sourcing Materials

The primary purpose of this analysis is to identify (a) the extent to which blockchain technologies are beginning to undermine the nuclear nonproliferation regime, (b) the over-the-horizon threat blockchain technologies present to global nuclear security, and (c) the primary steps that the US government can and should take to counter this emergent threat to national security. Methodologically, this research employs open-source intelligence analysis to evaluate the most important aspects of the technology that impact the nonproliferation regime. It is intended that the academic research here be presented in a policy paper format. While the emphasis of the paper is on nuclear proliferation, the principles introduced apply to all forms of weapons of mass destruction (WMD) and conventional arms proliferation.

A number of the sources used in this research come from bloggers’ and investors’ commentary on emergent blockchain and cryptocurrency technologies, many of whom were anonymous. As the global economy is centered on confidence, the choice to implement the opinion of these individuals (using sources that are often considered less than credible) was intentional. The thought leaders on blockchain and cryptocurrency drive the market potential of these technologies and are ultimately going to become key decisionmakers on how they are implemented in the future. To conceptualize the general consensus and specific opinions toward the future of cryptocurrency, the insight provided by these individuals was unparalleled. Especially in researching emerging technologies, it is essential to use all available sources to understand the landscape and especially the security implications involved. As these blogs are the primary sources for those making trades in the market, it necessitates that those crafting security policy recognize the same trends they do. Given this context, the use of opinionated and anonymous sources is justified. Where available, the author pooled the opinions of multiple sources to ensure that a consensus rather than a singular opinion was being explored.

Further, the section that explores Chinese intent to utilize cryptocurrency required translation of primary language materials. Employing the author’s mastery of the Mandarin Chinese language at approximately a 3+/4 level on the Interagency Language Roundtable scale, a broader range of sourcing material was used to access open-source intelligence and perform primary research that drew from both English and Chinese language materials.

THREATSCAPE

Background: Current Financial Safeguards to Counter WMD Proliferation

The nuclear nonproliferation regime includes a broad international framework of treaties, agreements, and organizations which work to prevent the spread of nuclear weapons and contribute to the progress of arms control and disarmament. The regime has several major components which serve to create legally binding nonproliferation obligations, strengthen international norms to counter the spread of nuclear weapons, control access to materials and technologies related to WMD, and enforce existing treaties, all while building trust between states. The nonproliferation and verification regime has been largely successful in meeting its goals to date: only nine countries possess nuclear weapons, global nuclear weapons inventories
have been reduced from 64,449 at the height of the Cold War to approximately 17,300 warheads today, and no nuclear weapon has been used by any actor since the initial uses by the United States against Japan in 1945.³

The nonproliferation regime is in many ways contingent upon financial systems and controls that detect and prevent the spread of nuclear and radioactive materials.⁴ Proliferation finance is defined by the Financial Action Task Force as “the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical, or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in a contravention of national laws or, where applicable, international obligations.”⁵ Proliferation financing facilitates the movement and development of goods related to the production of weapons of mass destruction and contributes to global instability.⁶ Prior to the introduction of cryptocurrency into the realm of proliferation finance, detection of the sale of components, the transfer of dual-use goods, and the consistency of networks through which these goods were exchanged was already difficult and posed a real challenge to US and international institutions.⁷ Emerging blockchain technology only makes this challenge greater.

The international community put the nonproliferation regime into place because of its consensus that the deliberate use of biological, chemical, radiological, and nuclear weapons is uniquely abhorrent and the spread of these materials must be controlled.⁸ This includes strong and established financial mechanisms in place to track proliferation finance by wire transfer, trade finance products, cash, checks, and credit cards.⁹ Notably, no nuclear nonproliferation research has been published to date involving virtual currencies, and the nonproliferation regime is now faced with a new and largely unexplored vulnerability.¹⁰

**Blockchain and Cryptocurrencies Open New Vulnerabilities in Nonproliferation Regime**

The rise of digitized financial assets, including both programmable and artificial intelligence (AI)-driven cryptocurrencies, have begun to transform the international financial system in ways that render sanctions and export control laws weak, creating obstacles in detecting the financing of WMD proliferation and technology transfer by nation-states, individuals, and non-state actors. Cryptocurrencies allow for rapid, borderless transaction settlements between participants, circumventing the need for a financial institution to act as an intermediary and disrupting current techniques to identify and counter dangerous proliferation.¹¹ The recent shift towards integration of AI within cryptocurrency is increasing transaction efficiency and decreasing transaction detectability.¹² The high levels of pseudonymity and anonymity unique to cryptocurrencies further exacerbate the vulnerability.

Blockchain technologies serve as the foundation for cryptocurrency.¹³ Blockchain can be defined as a system that allows a network of computers to maintain a single updated and secure ledger.¹⁴ When applied to the financial system, blockchain removes the need for an intermediary (such as a bank or third party) by creating a decentralized ledger system that stores and verifies information through a system of cryptographic codes.¹⁵ This has three major consequences: peer-to-peer transfer is possible, transactions can be anonymous but are recorded and
transparent to all those with access to the entire blockchain, and cryptographic protocols ensure that recorded transactions in the ledger cannot be altered. Cryptocurrencies, then, are digital assets that employ the encryption techniques of blockchain to regulate the generation of units of currency and to verify the transfer of funds. Simply put, blockchain serves as a ledger and cryptocurrencies serve as a medium of exchange.

This chart from the Bulletin of Atomic Scientists illustrates the fundamentals of the technology behind blockchain and cryptocurrency.

There are an estimated 5.8 million unique active users of cryptocurrency wallets, and less than 35% of large exchanges are done with a formal government license, leaving a significant portion of financial activity undetected. The threat of hacking and identity theft continues to grow, increasing the demand for anonymous transactions. Increases in the types of cryptocurrencies available also create a broader audience base, but also make it more difficult to track all of the possible digital exchanges taking place from the security perspective.

This chart from the Visual Capitalist illustrates the exponential growth of cryptocurrencies over the last five years.
Forensic analysis is in place that can detect some cryptographically secured transactions, but these methods are unpredictable and limited to well-established cryptocurrencies including Bitcoin (BTC), Ripple (XRP), and Ethereum (ETH). For newer cryptocurrencies, such as Monero (XMR) and Zcash (ZEC), US and international authorities have yet to find ways to track these transactions. Newer cryptocurrencies have increased anonymity and privacy protection. While this appears to be good for the consumer, it also adds a considerable challenge to those in the US government tasked with tracing illegal transactions on the blockchain. Each new digital currency introduces its own new cryptographic approach and a new set of challenges for the analyst.

Despite uncertain beginnings, the rallying cry across the public and private sectors, and especially among investors, is that cryptocurrency is here to stay. A recent report from the World Economic Forum found that 80 percent of global banks had initiated blockchain-related projects by the end of 2017 and predicted that at least 10 percent of global gross domestic product will be held in blockchain technology by 2027. There is a real and growing prospect that the next great shift in the international financial system could be from fiat money to cryptocurrency, with some top investors and experts suggesting that such a shift could happen in as little as five years. The impact of blockchain and cryptocurrency in the international financial system cannot be fully predicted, but based on current trends and its growing normalcy and acceptance, its impact will likely continue to come at a high velocity and magnitude.

**Cryptocurrency Use in Financing Criminal Activity Indicates Potential for Use in WMD Realm**

Cryptocurrencies constitute the largest unregulated markets in the world. Their increased opacity makes them ideal for illegal transactions and the financing of criminal activity. Some estimates suggest around $76 billion of illegal activity involved bitcoin transactions in 2017, amounting to approximately 46% of all bitcoin transactions for that year. Cryptocurrencies have been used most rampantly among cybercriminals as the payment method of choice in developing ransomware because the decentralized system makes perpetrators harder to trace. Cryptocurrency transactions have been used to fund terrorism, launder money, avoid capital controls, facilitate illegal drug and sex trafficking, and even to pay for murder-for-hire. The large-scale application of cryptocurrencies shows that the use of cryptocurrency transactions to facilitate the trade of other illegal and controlled substances, even those relating to WMD, is possible.

There are three major financial elements in WMD proliferation finance. The first involves raising the funds or obtaining them through illegal means, the second involves disguising the funds, and the third using the funds to pay for the procurement of materials, technology, or logistics. Using cryptocurrency makes each of these stages simpler and allows the actor to complete them without initial detection, and possibly without detection at all. This ease of action and the already prolific network of individuals using cryptocurrency for illegal activities provides a framework for individuals, terrorist organizations, and nations to employ blockchain technology to complete transactions that involve WMD proliferation.
Potential Crypto-financed WMD Proliferation Threat from Non-State and Lone Wolf Actors

Cryptocurrencies increase the feasibility for non-state actors to deploy virtual currency as a means to accomplish otherwise very difficult and illegal transactions, especially when used to acquire or sell restricted nuclear materials. The most likely non-state actors to engage in WMD proliferation or acquisition with the use of cryptocurrencies are formalized terrorist groups such as ISIS and individual, domestic actors. In 2016, President Barack Obama said that the risk of ISIS or other organized extremist groups acquiring nuclear weapons remains “one of the greatest threats to global security.”33 ISIS is actively seeking weapons of mass destruction and personnel with the technical experience to meet its nuclear ambitions.34 Although ISIS’ nuclear ambitions have thus far remained only ambitions, any easily accessible tool that assists their efforts should be a concern.35 Blockchain fits that bill. ISIS has established a reputation for operating much of its financial operations using Zcash, a cryptocurrency that the United States government is still unable to track with any real accuracy.36 Radical supporters of ISIS across the globe have also been caught sending large sums of money to ISIS through laundered cryptocurrency.37 Additionally, there is anecdotal evidence that ISIS has used cryptocurrencies in conventional weapons acquisition.38 ISIS’ early implementation of cryptocurrencies into their normal transactions suggest that they would not hesitate to use cryptocurrency in proliferation finance should the opportunity occur.

Individual acts of terror not connected to an organized terrorist group or ideology have also been on the rise. In the United States, domestic attacks are far more common a threat. Lone wolf shooters committed 158 shootings that resulted in 68 deaths in 2018, and 31 percent of recent mass shootings globally have occurred within the borders of the United States.39 If cryptocurrencies make the acquisition of more deadly and destructive weapons more easily available, the same people motivated to carry out mass shootings in this way could be interested in WMD as an option in place of firearms. The anonymity and low barriers-to-entry for blockchain transactions make them an ideal option for individuals looking to cause destruction.40

Potential Crypto-financed WMD Proliferation Threat from State Actors

Various state actors have strong motivation based in national status or pure security concerns to acquire or proliferate nuclear weapons. Currently, the state actor most likely to use cryptocurrencies in WMD acquisition or proliferation is Iran. China also presents a challenge in its proclivity for blockchain and its potential to eclipse other states in this realm of proliferation finance monitoring. Other adversarial states have divergent views on the potential of cryptocurrency, with some states showing an indication for future use.

Iran’s long-standing nuclear aspirations, paired with the country’s consistent attempts to circumvent export controls and country-specific sanctions against its nuclear weapons program, make Iran the most probable state actor to use cryptocurrencies to acquire WMD materials.41 In fact, Iran has openly announced its plans to develop its own national blockchain-based financial infrastructure with the express purpose to circumvent US sanctions (and likely to counter growing capital flight among its citizens in an economy that never recovered even when sanctions were lifted under the JCPOA).42 The Iranian commitment to cryptocurrency spiked almost
immediately when the US unilaterally withdrew from the JCPOA and re-imposed previous economic sanctions. Like many other world leaders, the Iranian Parliament, its Central Bank, and its Directorate of Science and Technological Affairs have stated that they see cryptocurrency as the economic tender of the future. US withdrawal from the JCPOA appears to have simultaneously fueled Iran’s inclinations to pursue both cryptocurrencies and nuclear materials, a combination that could have disastrous consequences and rapidly propel the country toward breakout capacity, simultaneously enabling Iranian-supported Hezbollah and Hamas to move toward that threshold.

Given that China is a nuclear power, the Chinese threat is less likely to occur in the form of actual proliferation or acquisition of WMD by use of cryptocurrency. The true threat posed by China is in its potential to rule the cryptocurrency market. China currently leads the world in the number of blockchain projects currently underway in the country—at 263 projects, China holds one-quarter of the total worldwide. China’s ability to create policy that drastically shifts the market became evident in 2018 when a Chinese Communist Party (CCP) ban on Bitcoin exchanges caused a rapid fall in its stock valuation. The CCP has consistently spoken out against cryptocurrency speculation, the use of cryptocurrency for illegal transactions, and its distaste for the way cryptocurrencies have diminished some of its control over all financial operations in the country. To counter these problems, there is a strong indication that the People’s Bank of China, under direction of the CCP, will soon release its own national cryptocurrency—one that can be regulated by the Chinese government. If the CCP does release its own national cryptocurrency, due to the high population and high use of cryptocurrencies in Asia, it is likely that the nation’s cryptocurrency could quickly overpower all others in both valuation and supply, giving China a distinct advantage in detecting any illegal activity that uses its cryptocurrency as tender.

Chinese impact on the blockchain and cryptocurrency market is meaningful in any context, but it becomes especially important in light of future proliferation finance. The debate regarding full implementation of cryptocurrencies into the international financial system is ongoing. Nations are each still working out their individual approach to cryptocurrency. Similar to the Iranian situation, Russia and Venezuela are sanctioned states which have taken an interest in creating their own national cryptocurrency to circumvent sanctions. But in Pakistan, historically the most prolific and consistent perpetrator of WMD proliferation, cryptocurrencies are banned in entirety. In January 2018, a US cybersecurity firm uncovered a North Korean scheme that sponsored the hacking of foreign computers to mine Monero and state-led efforts to steal cryptocurrencies. However, the increasing adoption of cryptocurrency by banks and other influential, long-standing financial institutions throughout the US, Europe, Asia, and the Middle East (including in both emerging and established markets) indicates that states may soon need to institutionalize cryptocurrencies to stay relevant in the global marketplace. As cryptocurrencies continue to rise, the possibility for their use by a broader range state actors for nuclear proliferation and other illicit activities does as well.
RECOMMENDATIONS

I. Build Resilience With BTC Taskforce Led by NCPC, OFAC, ISN, and CT Finance

The first step toward countering this new proliferation threat introduced by blockchain and cryptocurrency is to create a taskforce for coordination across the national security agencies involved to ensure that the project is centralized and well-managed. Without interagency collaboration and the specific assignment to hone in on this issue, individual agencies lack the jurisdiction and capabilities to successfully assess the risk and implement broad changes to counter it. This taskforce will assume the name Blockchain Taskforce for Counterproliferation (BTC). Its primary responsibilities will be to analyze the potential of cryptocurrencies to exploit and undermine the nonproliferation regime, determine what adjustments need to be made across the US government, and work with these organizations to implement changes as needed. This group will report directly to the Office of the Director of National Intelligence (ODNI). This will ensure a clear, direct line to someone of the cabinet level to assist in both disseminating relevant intelligence to all relevant organizations in the US government vertically and implementing needed changes across organizations horizontally, with the authority level necessary to create change in these hierarchical organizational structures.

BTC should consist of members from the National Counterproliferation Center (NCPC) housed within the Office of the Director of National Intelligence (ODNI), the Office of Foreign Assets Control (OFAC) housed within the US Department of Treasury, and the Bureau of International Security and Nonproliferation (ISN) and the Counterterrorism Finance Unit (CT Finance) housed within the US Department of State.57 NCPC is the primary organization within the US Intelligence Community charged with combating the spread of WMD and associated delivery systems.58 OFAC administers and enforces economic and trade sanctions against foreign countries and regimes, terrorists, international narcotics traffickers, and those involved in WMD proliferation with targets based on US foreign policy and national security goals.59 OFAC has been at the forefront of US government efforts to counter digital currency-based threats to the financial system and export controls.60 From the US Department of State, ISN and CT Finance include top experts in nonproliferation and counterterrorism finance, with particular understanding of the diplomatic aspects of these issues.61 These combined areas of expertise, paired with broad institutional connections and organizational cultural awareness, will allow for successful assessment of the threats being faced and the best ways to implement lasting change within institutions with disparate organizational cultures and goals.

To improve the exchange of diversity of thought from each of these agencies, selection should include at least four personnel of varying regional and topical expertise from each.62 There should also be consistent and open collaboration with the International Atomic Energy Agency (IAEA), the nuclear weapons verification force of the United Nations, and the Financial Action Task Force (FATF), the intergovernmental body charged with combatting money laundering, terrorist financing, and other threats to the international financial system.63 Nuclear proliferation will never be solely a US problem, and any recommendations put together by the BTC should be passed forward to the IAEA for multilateral consideration and potential implementation. Furthermore, as is possible within the bounds of high-level classified issues, private sector
experts in blockchain technologies should also be brought in to elevate the level of subject matter knowledge among the BTC team and identify key trends in the public sector and global marketplace with regard to blockchain.

II. Prevent Proliferation through Interagency Awareness and Collaboration

In order to allow the BTC to employ every resource the US government has to offer to mitigate this growing threat that could undermine nonproliferation efforts, every institution with a role in upholding the nonproliferation regime will need to (a) inform their decision-making in this arena with an understanding of blockchain and the vulnerabilities it introduces and (b) augment their current capabilities to more fully avert the spread of nuclear weapons. Systematic changes and collaboration across the US national security community, the private sector, and international organizations will be necessary to prevent the widespread use of cryptocurrencies for illegal proliferation financing.

The US government will require significant and broad coordination to enhance the nonproliferation regime with blockchain as a growing variable in the equation. The Intelligence Community, specifically the CIA, NSA, and DIA, will need to be involved in constructing and monitoring frameworks by which these sorts of financial transactions can be identified. The Department of Homeland Security (DHS) Intelligence and Analysis Unit (I&A) and the Federal Bureau of Investigation (FBI) will need to be called upon to assist in monitoring illicit financial activities using blockchain, with the specific task to monitor domestic threats coming from the US internally. The United States Secret Service (USSS), with its role to counter financial fraud, will also need to be trained on the possibility of fraud and diversion through blockchain technologies. Although not a direct influencer of the nonproliferation regime, the President and the US military should be made aware of the threat and advance possible options to support it. Finally, more specific legislation from the US Congress outlining the exact legal and illegal elements of blockchain and cryptocurrency use will eventually be necessary, but it will need to be informed by the analysis of the BTC and all other organizations involved.

Outside of the US government, private sector collaboration will be vital in restructuring the nonproliferation regime. One of the best networks already in place that can be leveraged to assist in BTC initiatives is the connection between the Intelligence Community and the venture capital and tech innovation communities through In-Q-Tel. Within that established network, BTC can likely find subject matter experts who can contribute to the restructuring of financial safeguards within the nonproliferation regime. If it becomes necessary to draw on individuals outside of the In-Q-Tel network, academics in finance and stock market analysts could serve as viable second options for the role of non-governmental subject matter expert.

After all relevant US public and private sector institutions are made aware of this threat, it will become important to collaborate with multilateral international institutions. Along with the IAEA and FATF, the Global Initiative to Combat Nuclear Terrorism (GICNT) is an international organization that works to coordinate international efforts to detect, investigate, and respond to proliferation by nonstate actors, with special attention to working with nations to develop comprehensive detection mechanisms to monitor proliferation of nuclear materials and the related financial transactions. With these three institutions as the primary points of contact,
BTC collaboration with international institutions will provide the highest order of restraint on actors who would seek to use cryptocurrencies for proliferation finance.

**III. Improve Detection and Attribution through Enhanced Technological Asset Acquisition**

Countering proliferation finance through technical expertise has always been an important aspect of ensuring that the nonproliferation regime remains intact. The United States has been uniquely situated to make this issue a global priority because of the global dominance of the US dollar, superior intelligence and financial investigation processes, and its global role in counterproliferation. In order to continue to serve that role, the United States needs to ensure that it continues to hold the technical expertise and reputational superiority to do so.

In current nonproliferation efforts, one of the greatest difficulties is the ability of terrorist and criminal networks to recognize government activity and detection. Criminal financing mutates and the danger of detection allows terrorists to change their game and stay a step ahead of the authorities. Especially in international criminal networks, authorities often fall behind because of a lack of information- and intelligence-sharing between countries. The decentralized networks on which cryptocurrencies operate create even more fault-lines for authorities attempting to track down those who engage in illegal transactions due to increased anonymity.

To sustain its technical edge in counterproliferation leadership, the US will need to once again work with the private sector. Blockchain and cryptocurrencies are just one small aspect of the growing fintech (innovations of finance and technology) sector. Other areas of this sector of technology can be implemented in tracking illicit financial activity. Additionally, there are several applications of blockchain itself that could actually be used to improve the nonproliferation regime and the financial verification processes included in it. Acquisition and early implementation of these types of innovative technologies into the national security organizations is becoming increasingly necessary. Because of financial constraints and differing goals, the public sector is rarely focused on emergent technologies. However, in this century technological advances can erode national security safeguards with unprecedented pace, forcing the national security enterprise to seek innovative and collaborative relationships with the private sector to stay on top of new changes in tech. Beyond these collaborative relationships, substantive progress needs to be made in restructuring the bureaucratic institutions of the US government so that innovation is incentivized and not discouraged.

**IV. Response and Risk Mitigation Efforts Continue Unchanged**

Although blockchain and cryptocurrencies are beginning to severely alter the mechanisms of proliferation financing, they do not impact the aspects of the United States’ response to an event of nuclear proliferation or use. The ultimate hope of the policies and practices put into place by the BTC would be to strengthen the nonproliferation regime and prevent such an event. However, because cryptocurrencies have the potential to increase the ease of proliferation finance, decrease the possibility of its detection, and increase the number of actors able to complete such transactions, the BTC should also plan to work with other national security institutions to enhance the US response plans to events of nuclear proliferation and use.
V. Integrate Blockchain Safeguards into International Nuclear Nonproliferation Regime

Despite the threats presented by blockchain technology to undermine the nuclear nonproliferation regime, there is a correlative opportunity to utilize blockchain to strengthen the nonproliferation regime. The nonproliferation regime currently hinges on supply-side controls that limit the spread of nuclear materials and technology through financial agreements, export licensing, targeted sanctions, and various types of international agreements. These controls can be enhanced through the introduction of blockchain technology into national and international nonproliferation and arms control verification mechanisms.

Blockchain technologies have the capability to ensure authentication of supply chains, and if integrated into current financial safeguards, will diminish the possibility for illicit actors to transfer nuclear materials across borders without detection. This can be done because blockchain networks can be limited to approved parties and prevent the export fraud and falsification that is often utilized by illicit actors to obfuscate illegal transactions. In a global supply chain, this means that each party (buyers, sellers, shippers, and insurers) would be required to authenticate and verify the information on a distributed ledger that all parties use.

The leading barriers to implementing blockchain into the nonproliferation regime are policymaker interest, expertise, and scalability. Because blockchain is a new and difficult-to-understand technology, it is unlikely that policymakers will instantly take to the idea of using funds to undergird global supply-side nuclear control system. That beings said, policymakers can be persuaded if prominent think-tanks, academics, lobbyists, and constituents in the nonproliferation arena rise up to press the issue. The lack of expertise needed to logistically implement the technology is also a challenge, and to attract top talent from the fintech world significant salary incentives will be needed. Finally, the scalability of these technologies is limited by the large network and computational capacity needed to record these transactions in a ledger. None of these issues is insurmountable, but must be addressed by BTC as it works to create actionable steps toward implementing blockchain into nonproliferation mechanisms.

Conclusion

In sum, the rise of digitized financial assets, through blockchain and cryptocurrencies, has begun to transform the international financial system in ways that render sanctions and export control laws weak, creating difficult new hurdles in detecting the financing of WMD proliferation. Cryptocurrencies allow for rapid, borderless transaction settlements between participants, circumventing the need for intermediary financial institutions, and disrupting current techniques to identify and counter dangerous proliferation. As adversaries work to utilize emergent technologies such as blockchain to circumvent nuclear nonproliferation controls, it is paramount that the US work to stay ahead as an expert and leader in these technologies moving forward.

To minimize the proliferation threat posed by cryptocurrencies, a multi-faceted approach will be necessary and will be most successful if done under the direction of a targeted interagency taskforce within US government. The new Blockchain Taskforce for Counterproliferation will allow for enhanced, focused, and accelerated implementation of the policy and institutional changes needed to restructure the nonproliferation regime in light of this emergent technology.
Bibliography


Alrawi, Mustafa. “Bitcoin isn’t quite the gold rush it once was, but cryptocurrencies are here to stay.” The National. Dec. 12, 2018. Accessed Dec. 12, 2018 from https://www.thenational.ae/opinion/comment/bitcoin-isn-t-quite-the-gold-rush-it-once-was-but-cryptocurrencies-are-here-to-stay-1.801952.


Endnotes


2 Ibid.


9 Ibid.

10 Ibid.


54 Ibid.


56 Ibid.


68 Ibid.

69 Ibid.


71 Ibid.


75 Ibid.