Policy Brief

Digital Assets

(e) We must support technological advances that promote responsible development and use of digital assets

Executive Summary

The world has seen a rise in popularity of digital assets in the past few years, especially in the financial sector with cryptocurrencies like Bitcoin and Ethereum taking the market by storm and being established as accepted forms of currency exchange on a large scale. The increasing popularity of decentralized blockchain networks being used for money transfer means that the government has no control over the money. This could lead to problems like funding terrorist activities, money laundering, etc. going unnoticed. The U.S. government has therefore decided to implement a CBDC (Central Bank Digital Currency) to counter the disadvantages of an unregulated currency while retaining the benefits like foreign transfers at no additional cost, etc.

My position on the matter is that the government should not be a direct copy of any existing system but should same design for the programmability of money and preserving user privacy. The reason is that the existing systems were designed such that it would be free of any sort of control. Apart from there being a complete and verifiable record of transactions to ensure that all digital data is consistent and accountable for, existing cryptocurrencies are free from any form of monitoring, and are not trackable. It is money free of the government’s control. The need for a CBDC is that the government be able to track it.

Introduction

Digital currencies have been on the rise and have provided a lot of benefits to people as a decentralized system to transfer funds but what does this freedom come at the cost of? In “A rigged economy” [1], Stiglitz mentions how the gap between the rich and the middle class keeps on increasing year over year when it comes to total wealth. Wouldn’t that mean further increase in the difference between the rich and the poor now that the government can do nothing to monitor them? With government money, the rich could only work around the laws, but here, there are no laws, no taxes. With no regulation, will the rich not get richer?

Studies [2] have also pointed to digital currencies being used to fund terrorist activities, which would now be untraceable and lead to greater loss of life. Money laundering has also been on the rise [3] since the introduction on Bitcoin, up to 30% according to findings. This does not help the US economy which has been facing counterfeiting and laundering of the 100$ bills for years, especially in small towns where people are unaware and unsuspecting. The question that then arises is whether the CBDC being introduced by the US government will be more secure if it is a copy of existing systems like Bitcoin?

Technological advances are made by the day, and they don’t wait for anyone. People are upgrading their lives yearly by the purchase of newer smart electronic devices and are transitioning to the digital age. Digital currencies are here and are here to stay. They will not be taken down, and will keep advancing, so what should the government do about it?

Research Overview

The research team from the National Security Research Division conducted the following research on the use of digital currencies by terrorist organizations. They [2] conducted an extensive literature review of scholarly works and news reports on terrorist organizations, terrorism finance and economics, and cryptocurrencies. In addition, the team inter- viewed current and former members of the intelligence community and law enforcement engaged in CTF. The team used these data to identify several major areas in which terrorist groups require financing, whether for supporting major attacks or providing for day-to-day operations. These data also were analyzed to identify similarities and differences among major terrorist groups with respect to their uses of finance for their activities. Finally, the properties (i.e., strengths and weaknesses) of major and emerging cryptocurrencies were identified and compared with terrorist finance requirements.

Given the key role of funding in supporting terrorist operations, counterterrorism efforts—in particular, the subfield of counterterrorism finance (CTF)—often focus on tracking the flow of money through bank accounts and preventing financial transactions that might be used to support attacks and other terrorist activities. However, the success of CTF strategies in reducing terrorist access to fiat (i.e., government-issued) currencies has raised concerns that terrorist organizations might increase their use of such digital cryptocurrencies as Bitcoin to support their activities.

Bitcoin is both a protocol for securely storing and transmitting tokens (virtual coins) and the name of the unit of value in the system. Bitcoin revolves around a public ledger called the blockchain, which is maintained by an online peer-to-peer network that tracks transactions and maintains a complete history of verified transactions. Media reports have outlined the notion that some, or even many, terrorist organizations have unlimited, untraceable sources of digital money, such as Bitcoin, which will be used to undermine the successes of CTF. Policymakers also have raised concerns about terrorist use of digital currencies.

This report focuses on two key questions. First, whether terrorist groups are currently using cryptocurrencies to support their activities and, if not, why they are not using such currencies. Second, to understand what properties of new and future cryptocurrencies, such as the potential for improved anonymity and high-volume transactions, would make them more viable for terrorist use—that is, more difficult for law enforcement to identify and track. To answer these questions, the research team conducted an extensive literature review of scholarly works and news reports on terrorist organizations, terrorism finance and economics, and cryptocurrencies. In addition, the team interviewed current and former members of the intelligence community and law enforcement engaged in CTF. The team used these data to identify several major areas in which terrorist groups require financing, whether for supporting major attacks or providing for day-to-day operations. These data also were analyzed to identify similarities and differences among major terrorist groups with respect to their uses of finance for their activities. Finally, the properties (i.e., strengths and weaknesses) of major and emerging cryptocurrencies were identified and compared with terrorist finance requirements.

Whether and how terrorist organizations would use a cryptocurrency system depends on the available technology and its properties, as well as on the organization’s needs and capabilities. Newer cryptocurrencies might emerge with properties that terrorist organizations find more attractive than those of currently available cryptocurrencies. For instance, if a future cryptocurrency provides better anonymity than Bitcoin for large-sum transactions and is more widely adopted than Zcash, another form of digital currencies, then terrorist organizations might be willing to employ that currency for specific activities. Thus, it is important to look at individual terrorist groups to analyze what they would need from cryptocurrencies and compare those needs with the properties of available cryptocurrencies.

Research shows that, should a single cryptocurrency emerge that provides widespread adoption, better anonymity, improved security, and that is subject to lax or inconsistent regulation, then the potential utility of this cryptocurrency, as well as the potential for its use by terrorist organizations, would increase. Even if no such currency emerges, there will be some use by terrorist groups, but the extent of that use will depend on the currency’s viability. Factors that tend to discourage use include continued instability and infighting in the cryptocurrency community, cooperation between international law enforcement and the intelligence community and developments in regulation and enforcement.

Discussion of research findings

There is little indication that terrorist organizations are using cryptocurrency in any sort of extensive or systematic way. There are, however, lone-wolf actors and loosely associated groups that are likely to attempt, or are already attempting, to use these systems. This is likely true regardless of the wisdom of doing so, as shown by the ill-informed (and ill-fated) claims of Ali Shukri Amin. On the other hand, despite claims to the contrary, there are “still only a small number of publicly documented and confirmed cases of TF [terrorist finance] involving VCs [virtual currencies].”

However, neither the technology nor the groups are static, and this might change the dynamics in the future. The incentives for finding alternatives discussed in this chapter are important, but the technical properties of cryptocurrency systems, as described in Chapter Three which argue against the use of these systems by terrorist organizations are likely to change in more-varied ways. This could make successful use of these technologies easier or harder.

The utility of cryptocurrencies in the future, as both terrorist methods and cryptocurrencies develop, is unclear. Nonetheless, several recent advances in cryptocurrencies will facilitate their use by the most sophisticated groups that threaten terrorism against Western countries, and the use of cryptocurrencies will be especially enabling for actors that already engage in transnational fundraising and criminal activities. Research shows that, should a single cryptocurrency emerge that provides widespread adoption, better anonymity, improved security, and that is subject to lax or inconsistent regulation, then the potential utility of this cryptocurrency, as well as the potential for its use by terrorist organizations, would increase. Even if no such currency emerges, there will be some use by terrorist groups, but the extent of that use will depend on the currency’s viability. Factors that tend to discourage use include continued instability and infighting in the cryptocurrency community, cooperation between international law enforcement and the intelligence community, and developments in regulation and enforcement.

The indications here provide only a rough guide to how cryptocurrency is most likely to be used, which methods are important to investigate, and which sources of funds are most important to monitor or intercept. As time passes, it will become more obvious how crypto- currency will and will not be used. As these uncertainties are resolved, terrorist groups will evolve in ways that are unlikely to be fully predict- able but will be partially observable over time. The operational challenge of CTF will need to change as well.

Similar studies for money laundering and counterfeiting have shown that since the introduction of digital currencies, these crimes have been on a rise and even if currently a connection between the two cannot be proved at the time, the capabilities of these systems certainly leave scope for scaling of these crimes due to lack of accountability.

Conclusion and Recommendation

Current concerns about cryptocurrency as a significant enabler of terrorist groups are almost certainly overblown, but coming improvements in cryptocurrency technologies will likely have a significant long-term effect on CTF. The speed at which these technologies are adopted, and the details of which technologies are used and how they are deployed, are critical uncertainties that have important operational impacts. These operational challenges are partly extending current methods of CTF and partly adapting methods from computer security.

Impending change from traditional financial methods to more sophisticated “fintech” (i.e., financial technology) will pose challenges, starting with the addition of new sources to monitor and investigate. This does not necessarily require intentional use by terrorist organizations but simply can be a byproduct of banks changing their practices. For example, the U.S. Treasury “has access to unique financial data about flows of funds within the international financial and commercial system,” which is invaluable for tracking illicit flows of money. These sources are potentially imperiled by the trend toward de-banking finance via cryptocurrencies because the adoption of cryptocurrencies might enable secure international fund transfers without needing the current centralized system—perhaps using such cryptocurrency systems as Ripple that exist outside the traditional financial system.

The financial community is historically very conservative, and this has made the tracking of funds a well-understood specialized discipline of forensic accounting. Modern cryptocurrencies are potentially much more flexible, and this may create challenges in financial accounting that look like those involved in attributing and preventing computer intrusions. The field of cryptocurrencies is much less certain, much more dynamic, and one in which innovations might allow terrorist groups to circumvent monitoring. On the other hand, it is a field where sophistication matters; money laundering may be made harder to detect when conducted by sophisticated actors, but many terrorist groups’ technical abilities are not currently suited to this type of activity.

This is just one crime discussed in detail. Each crime studied in depth will show that Digital currencies are a big influence for these crimes and once a standard system like the CBDC is established, these organizations indulging in financial crimes can take their operations and expand them to a global scale, as this would be a government provided standard that is exchangeable for the world’s most stable currency, that is the United States Dollar. This gives the wrong people a lot of unnecessary power and will lead to untraceable crimes, as this currency is unregulated.

I recommend creating a new system and set of rules for the CBDC should not be a direct copy of any existing system but should same design for the programmability of money and preserving user privacy.

References

[1] <https://www.scientificamerican.com/article/the-american-economy-is-rigged/>

[2] <https://www.rand.org/pubs/research_reports/RR3026.html>

[3] <https://www.bbc.com/news/technology-60072195>

[4] <https://triblive.com/local/westmoreland/state-police-warning-of-counterfeit-100-bills-circulating-in-area/>

Rutwik Rajendra Ghag.

868143200