FINANCING TERRORISM IN THE AGE OF CRYPTOCURRENCY

Dr. Abbas Mustafa Sadik

Sudanese expert in digital media, media analysis, terrorist groups and extremism studies

Cryptocurrency has attracted a significant global attention with its increasing value and widespread use. However, some governments have taken a stance against it, including Arab governments, that they completely banned the possession, purchase, and circulation of cryptocurrency. Meanwhile, a number of public and private institutions in Arab countries are willing to take the risk and employ new technologies, and soon acknowledge such currency without having to wait for regulation laws to be passed.

What is Cryptocurrency?

Cryptocurrency is a digital asset designed to function as a financial-transaction medium that records currency ownership in a Ledger, which is a computerized database, such as the Blockchain. The Blockchain functions as a database for public financial transactions and is able to continuously operate a large records list known as Blocks. Each Block contains a time-stamped chain of information and a link to the previous Block. All operations are strongly encrypted in order to secure the transactions, control the minting of additional regular coins, and verify the transfer of currency ownership.

Back in 1983, American cryptographer David Chaum conceived cryptographic electronic money called eCash. Later in 1995, his conceptions came to life in what was known as DigiCash, which was a form of early electronic crypto payment.

Bitcoin, which was first released in 2009 as an open-source software, is the first decentralized cryptocurrency. Satoshi Nakamoto, who authored the Bitcoin white paper, created and deployed Bitcoin's original reference implementation, and devised the first Blockchain database, is presumably the developer of Bitcoin. During this process, the developer was supposedly the first to solve the issue of digital currency double spending via a peer-to-peer network. However, many have claimed to be Nakamoto since Satoshi Nakamoto is a pseudonym used by the person or persons who developed Bitcoin.

Cryptocurrency and Terrorism

What we are most concerned about here is terrorists using cryptocurrency. On August 13, 2020, the US Ministry of Justice declared that counter-terrorism authorities had dismantled a series of fundraisers online run by three organizations classified as terrorist by the US. This highlights the weaknesses of those terrorist networks and provides valuable lessons for future attempts of countering terrorist financing online.

Two of those fundraisers have received contributions in Bitcoins at least since 2019. The third was started on a fake website set up with the outset of COVID-19 pandemic by an alleged financial intermediary between ISIS and a Turkish hacker. The website claimed to sell self-protection tools during the pandemic, such as N95 face masks.

Terrorist organizations are financed through many traditional and novel sources—from extensive resources based on territorial control to kidnapping for ransom, as well as small donations from supporters all over the world. These organizations have sustained diverse sources of financing over the past few decades.

One of the diversification aspects is fundraising through, for example, traditional online fundraising platforms, social media, and most recently via cryptocurrency and other means. The global outbreak of the COVID-19 pandemic has prompted terrorist groups to increasingly use virtual assets and financial services online. Yet terrorist groups remain resourceful when it comes to online fundraising.

Important Studies

The American RAND Corporation has studied how terrorist groups can potentially rely on cryptocurrency on a wider scale given their needs and the technical pros and cons of digital currency that can be utilized to their advantage. RAND suggests that this study should be relevant to stakeholders, including counter-terrorism policymakers and investors in digital currency.

This study was conducted by RAND's International Security and Defense Policy Center (ISDP), National Security Research Division (NSRD) that conducts research and analysis for the Office of the US Secretary of Defense, the Joint Staff, the Unified Commands, the defense agencies, the Department of the Navy, the Marine Corps, the US Coast Guard, the US Intelligence Community, allied foreign governments, and relevant foundations.

This study argues that, given the financial support meant to facilitate terrorist operations, counter-terrorism efforts in particular are directed towards tracing out

capital flows in bank accounts and preventing financial transactions that can potentially be used to support further terrorist attacks and activities. However, Combating Terrorist-Financing (CTF) strategies having successfully prevented terrorist access to banknotes (i.e., officially minted by the government) has raised concerns over an increasing terrorist use of digital cryptocurrencies, such as Bitcoin, to support their terrorist activities.

RAND suggests that 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 aforementioned Blockchain, which is maintained by an online peer-to-peer network that tracks transactions and maintains a complete history of verified transactions.

Illicit Financial Flows

In recent years, the mass media have often published in-depth reports and investigations confirming that some or even many terrorist organizations have unlimited, untraceable flows of digital currencies used to undermine the successes of CTF efforts. Policymakers have also raised concerns over terrorist use of digital cryptocurrencies; the global cryptocurrency market cap hit over $2 trillion on April 5, 2021.

As per the research study by RAND, in order to understand the potential terrorist use of cryptocurrencies, it is useful first to consider how terrorist organizations use money, and then to identify needs and opportunities for such use. The study examines terrorist organizations' use of money in three parts: receipt, management, and spending.

According to RAND's report, Financing Terrorism through Cryptocurrencies – A Danger for Europe? that was published in the Journal of Money Laundering Control, transfers of Bitcoins and other cryptocurrencies are not always completely anonymous as it may seem. Such transfers potentially leave electronic traces that may reveal the identity of cryptocurrency users involved. Although some platforms like Telegram offer a safe space for terrorists, online fundraisers often go beyond such platforms that they reach channels breached by officials.

Mainstreaming Bitcoin URI schemes on these channels as well as official or well-known websites potentially allows third parties to find them and run advanced analytics of the Blockchain, particularly suspicious patterns of transactions. This helps to reveal the user's IP address and owners of other relevant accounts.

Furthermore, many virtual stock markets that deal with and store cryptocurrencies are subject to AML and CTF regulations, such as Know Your Customer (KYC), or require registration in the Financial Crimes Enforcement Network (FinCEN) as Money Services Businesses (MSBs). Such regulations affect all listed stock exchanges, including those of clients headquartered in the US, and include gathering personal information on account holders.

ISIS Deadliest Parasite

A research study, themed DOES THE BITCOIN HYPE MAKE THE WORLD LESS SAFE? published by Emerald concludes that ISIS is the deadliest parasite of cryptocurrencies. One ISIS supporter states that this digital system is capable of increasing ISIS' fundraisers, and that it is such an easy process that they are rushing to use as soon as possible.

The Ghost Security Group, a hacktivist and anti-terrorism group, claimed to have found a chain of transactions to Bitcoin wallets believed to be owned by ISIS. The total amount of funds held in the wallets were reported to be between $4.7 million and $15.7 million, representing between 1–3% of the group's total annual income. The Group confirmed to News BTC that ISIS is extensively using Bitcoin for funding their operations. Similar claims were reported by Deutsche Welle in 2015, when they reported that one Bitcoin wallet believed to belong to ISIS received around $23 million within one month.

One major concern is the ability to purchase and transfer Bitcoins via cash-to-Bitcoin ATMs. Angela Irwin and George Milad, Researchers at the Centre of Policing, Intelligence and Counter Terrorism, Macquarie University, Sydney, Australia, observed that using such ATMs is a weakness given how easily and quickly transfers are made around the world. These ATMs allow Bitcoin purchases via credit/debit cards. They date back to October 29, 2013, in Vancouver, Canada, when Robocoin announced the very first Bitcoin ATM machine accessible to the public.

Bitcoin has had its share of funding criminal activities. With the increased anonymity it offers, it has been popular on the Dark Web, and has been used in drugs and contraband trades.

Cryptocurrency Regulation

Irwin and Milad demonstrated how, for a number of years, financial institutions have successfully used red flag indicators and suspicious behavior models to detect money

laundering and terrorism financing activity. They said that it is unlikely that similar red flag indicators exist for detecting illicit transactions travelling through the Bitcoin Blockchain, referring to insufficient or ineffective levels of verification being carried out in many cases to determine their money laundering or terrorism financing risk.

Irwin added that even though tracking the Bitcoin users' public keys can provide access to transaction dates, users remain anonymous unless the transactions are associated with other data verification requirements, such as e-mail. This restricts the opportunity to verify the user's information.

Therefore, with the continued growth of Bitcoin and other cryptocurrencies, cryptocurrency regulation has become more urgent. Accordingly, Irwin and Milad concluded that it is essential that steps are taken now to understand potential weaknesses in this technology before it, and similar ones, become mainstream methods of transferring illicit funds around the world. Failing to respond now may result in unforeseen dire consequence.