**Speak Out: Verifying and Unmasking Cryptocurrency User Identity**

Hadar Y. Jabotinsky*[[1]](#footnote-1)┼* & Michal Lavi[[2]](#footnote-2)\*

**Abstract**

*Terror attacks pose a serious threat to public safety and national security. New technologies assist these attacks, magnify them and render them deadlier. The more funding terrorist organizations manage to raise, the greater their capacity to recruit members, organize and commit terror attacks. Since the September 11, 2001 terror attacks, law enforcement agencies have increased their efforts to develop more anti-terrorism and anti-money laundering regulations, which are designed to block the flow of financing of terrorism and cut off its oxygen. However, at present most regulatory measures focus on traditional currencies. The more efforts to restrict the financing of terrorism by traditional fiat currencies succeed, the greater the likelihood that cryptocurrencies will be used in order to fund illicit behavior. Cryptocurrencies, electronically generated and stored tokens which can be exchanged via a decentralized payment system, are a game changer, significantly affecting market functions like never before and making it easier to finance terrorism and other types of criminal activity. These decentralized and (usually) anonymous usable currencies facilitate a high volume of transactions, providing terrorists extensive fundraising, management, transfer and spending money for illegal activities. The ability of terror organizations and those who finance them to increase their activities and attacks by using cryptocurrencies poses a major threat to national security.* *As cryptocurrencies gain popularity, the issue of how to regulate them becomes more urgent.*  *The scope and utility of financing of terrorism begs for a coherent legal response.*

*This Article proposes to reform the regulation of cryptocurrencies. It advocates the promotion of mandatory obligations directed at cryptocurrency issuers, wallet providers and exchanges to verify the identity of users on the blockchain. Thus, courts could grant warrants obligating companies issuing cryptocurrencies to unmask the identity of cryptocurrency users when there is probable cause that their activities support terrorism or other money laundering activities. Such reforms would make it possible to suffocate the financing of terrorism and other types of criminal activity financed through cryptocurrencies, and in so doing would make it possible to curb harmful lethal activities and promote national security. As we are aware of the legal challenges our solution poses, this Article also addresses substantial objections that might be raised regarding the proposed reforms, such as jeopardizing innovation, First Amendment freedom of expression objections, Fourth Amendment protection from surveillance and measures for promoting efficiency in the application of the proposed reforms.*

**Table of Contents**

[**Introduction** 3](#_Toc41917000)

**[I. Intermediaries as Gatekeepers– Traditional Regulation of Intermediaries for Combating Violations of Law](#_Toc41917001)** [10](#_Toc41917001)

*[A.The Infrastructure as a Gatekeeper of Illegal Transfer of Money for Terrorist Activity-](#_Toc41917002)* [14](#_Toc41917002)

*[(1) Traditional Financial Intermediaries at the Service of National Security](#_Toc41917003)* [15](#_Toc41917003)

[(a)Anti -Money Laundering Statutes 15](#_Toc41917004)

[(b) Anti -Terror Act- Material Support and the Criminalization of Financing of Terrorism 20](#_Toc41917005)

**[II. What are Cryptocurrencies, How do they Work and What are their Benefits for Terrorism](#_Toc41917006)** [23](#_Toc41917006)

[***A. Cryptocurrencies*** 23](#_Toc41917007)

*[B. Why and How are Cryptocurrencies Used by Terrorist Organizations?](#_Toc41917008)* [26](#_Toc41917008)

([1) The Anonymity of Some Cryptocurrencies and its Importance to Terrorist Activities 27](#_Toc41917009)

[(a)Current Limitations on the Adoption of Cryptocurrencies by Terrorists and the Future 31](#_Toc41917010)

[(b)The Problem of Counter Terrorism Financing (CTF) in Cryptocurrency 32](#_Toc41917011)

**[III. Speak Out: The Case for Ex ante Verification and Validation of Cryptocurrency User Identity](#_Toc41917012)** [34](#_Toc41917012)

[A. Reform Proposal for Verifying, Validating and Unmasking Cryptocurrency User Identity 36](#_Toc41917013)

[*B. Unmasking and the Fourth Amendment after Carpenter- The Need for a Court Warrant* 38](#_Toc41917014)

[(1)The Fourth Amendment: Reasonable Privacy Expectations 39](#_Toc41917015)

[(2)The Third-Party Doctrine – No Reasonable Expectation to Information Held by Third Parties 40](#_Toc41917016)

[(3) Shifting the Approach to the Fourth Amendment:](#_Toc41917017) *[Carpenter v. United States](#_Toc41917017)* [41](#_Toc41917017)

[(4) Extending Carpenter to Unmasking Cryptocurrency Users 43](#_Toc41917018)

[**IV. Speak Out: Addressing the Objections and Limitations** 43](#_Toc41917019)

[*A.* *The First Amendment* 44](#_Toc41917020)

[1 ) Identity Verification, Unmasking and Cryptocurreny - User Freedom of Expression 44](#_Toc41917021)

[2) Identity Verification, Unmasking and Freedom of Expression of Wallet Providers, Exchanges and Issuing Firms 47](#_Toc41917022)

[B. From the Cathedral to the Bazaar and Back to the Cathedral Again? Concerns Regarding Centralized Distribution of Power 48](#_Toc41917023)

[C. Administrative Costs of Identity Verification and Unmasking 50](#_Toc41917024)

[D. Data Breach Concerns 51](#_Toc41917025)

[E. Global Law Enforcement 53](#_Toc41917026)

[Conclusion 54](#_Toc41917027)

# Introduction

On August 28, 2015 Ali Shukri Amin was sentenced to 11 years in prison to be followed by a lifetime of supervised release and monitoring of his internet activities for conspiring to provide material support and resources to the Islamic State of Iraq and Syria[[3]](#footnote-3) (a.k.a. ISIL, also known as ISIS). Amin pleaded guilty on June 11, 2015. He confessed that he used Twitter to provide advice and encouragement to ISIS and its supporters. Amin, who used the Twitter handle @Amreekiwitness, provided instructions on how to use Bitcoin, a virtual currency, to mask the provision of funds to ISIS, as well as to facilitate the efforts of ISIS supporters seeking to travel to Syria to fight with ISIS. Amin used this account to conduct Twitter-based conversations on ways to develop financial support for ISIS using online currencies, such as Bitcoin, and ways to establish a secure donation system or funding for ISIS. For example, Amin tweeted a link to an article he had written entitled "Bitcoin wa' Sadaqat al-Jihad" (Bitcoin and the Charity of Jihad). The article discussed how to use bitcoins and how jihadists could utilize this currency to fund their efforts, including statements on how to set up an anonymous donation system to send money, using Bitcoin, to the mujahedeen.[[4]](#footnote-4)

In January 2015, *Haaretz*, a daily Israeli news outlet, reported on the first instance of an ISIS cell fundraising using Bitcoin on the dark net.[[5]](#footnote-5) The fundraiser was a man identified as Abu-Mustafa, and his Bitcoin account number indicated he had managed to raise five bitcoins (approximately $1,000) before the FBI shut down his account.[[6]](#footnote-6)

The currency used in all of the abovementioned transactions was Bitcoin, the first and perhaps most well-known cryptocurrency.[[7]](#footnote-7) Cryptocurrencies are electronically generated and stored tokens which can be exchanged via a decentralized payment system called a blockchain. The blockchain is a peer-to-peer network, which allows users to trade the tokens without relying on banks or other financial institutions, thus cutting out the financial intermediaries and eliminating their fees. [[8]](#footnote-8) As mentioned, the first and perhaps most well-known cryptocurrency is Bitcoin,[[9]](#footnote-9) yet there are new cryptocurrencies tailored for different audiences.[[10]](#footnote-10) This disruptive technology was dubbed a "trust machine”,[[11]](#footnote-11) because it eliminates the need to rely on the institutions that traditionally served as trusted intermediaries in financial markets and operated within an ecosystem based on self-sovereign identity.[[12]](#footnote-12) As such, cryptocurrencies have the potential to lead a revolution in many sectors of our day-to-day lives.[[13]](#footnote-13) Some even believe that this revolution could revolutionize perceptions of property, expression and identity.[[14]](#footnote-14)

As the coronavirus (a.k.a. Covid – 19) began to spread, the use of cryptocurrencies increased.[[15]](#footnote-15) One plausible explanation is that trust in institutions and traditional financial intermediaries dropped, resulting in an increased need for alternatives. The decentralized anonymous cryptocurrency model is a natural candidate as cryptocurrencies are viewed as storing value and they are borderless – you can purchase them almost anywhere in the world and use them later on in most countries without a need for exchange or transfer. From the consumer’s point of view, being able to use cryptocurrencies has its benefits as the tokens help circumvent the intermediaries, thereby making financial services cheaper and more inclusive. Trust is placed in technology and not in other people or intermediaries, improving markets and businesses.

Yet, there is a downside: with great innovation comes a social cost. These models of governance are especially vulnerable to harmful behaviors due to the anonymity of the coin owners. They can be abused by illicit actors who use them for money laundering schemes, facilitating and conducting cyberattacks and demanding ransom, among other acts. Cryptocurrencies can even be exploited for crowd-funding campaigns and aid terrorists in receiving funding.[[16]](#footnote-16) The anonymity of users on the blockchain makes it more difficult for law enforcement agencies to identify and track illegal transactions.

As counter-terrorism efforts through various regulatory measures imposed on the traditional financial system succeed, the use of cryptocurrencies by terrorists is likely to increase and have long-term effects on the financing of terrorism and related activities.[[17]](#footnote-17) For example, in addition to the previously mentioned usage of Bitcoin by ISIS, in the past several years terrorist groups in Gaza have also solicited support in Bitcoin.[[18]](#footnote-18) The use of cryptocurrencies allows terrorists to fund attacks more easily than they did in the past using fiat currencies,[[19]](#footnote-19) and enables more frequent and extensive attacks, which cost lives.[[20]](#footnote-20) For example, if supporters are not donating as much to terrorist groups as they did before due to an increase in the legal and financial risks of doing so, a sufficiently robust, secure, and anonymous cryptocurrency could re-enable donations as a significant source of financing of terrorism.[[21]](#footnote-21) For that reason, the use of cryptocurrencies by terrorists is a major problem. Curtailing such fundraising is crucial for national security and public safety.[[22]](#footnote-22)

When deciding how to combat money laundering and financing of terrorism in traditional financial markets, a consensus emerged, or rather seemed to exist, that going after the money was a key instrument in the war against terrorism. Such consensus translates into duties and obligations of financial institutions,[[23]](#footnote-23) through anti-money laundering laws and anti-terrorism statutes.[[24]](#footnote-24) Counter Terrorism Financing (CTF) focuses on tracking the flow of money through bank accounts and preventing financial transactions that might be used to support attacks and other terrorist activities.[[25]](#footnote-25)

However, increased use of cryptocurrencies by terrorists could undermine the efficacy of CTF because cryptocurrencies are decentralized. Therefore, regulators cannot rely on a central gatekeeper or intermediary to stop the flow of money for illicit purposes through the blockchain. Moreover, some cryptocurrencies allow anonymous transactions. The only truly public feature of the cryptocurrency ledger is the documentation of ownership and transfers. The names of the individuals performing the transfers are not listed on the ledger. Instead, ownership is represented by a set of letters and numbers representing the public cryptocurrency address of the user. Thus, the use of cryptocurrencies provides terrorists with streams of funding without meaningful tools for detection and prevention. The story of Ali Shukri Amin, who provided instructions over Twitter on how to use Bitcoin to mask the provision of funds to ISIS, is just one striking example of many demonstrating the risks posed by the anonymity surrounding cryptocurrencies.[[26]](#footnote-26)

More and more regulators are concerned about the use of cryptocurrencies for illegitimate activities such as the financing of terrorism. In fact, in an attempt to solve the problem, the European Union has recently amended its Anti-Money Laundering Directive. The new Directive now mandates cryptocurrency exchanges and custodian crypto-wallet providers to follow the same regulatory requirements as banks and other financial institutions.[[27]](#footnote-27) A more extreme approach that emerged due to concerns of fraud, money-laundering and deception of investors has led some countries, such as China and South Korea, to prohibit Initial Coin Offerings (ICOs) altogether, while others strive to reach an understanding of the currencies in order to come up with coherent regulation policies.

This Article proposes to register the identity of token holders on the blockchain with the corporations issuing the token in order to decrease the future viability of cryptocurrencies for terrorists or other illicit users and cut off the oxygen that enables their activities. Furthermore, we recommend that the registry visible to token holders should remain anonymous and a court warrant should be required to unmask the identity of the token holders. The Article is structured as follows:

**Part I** presents an overview of the role of intermediaries as the new gatekeepers of violations of law by users and customers. It addresses conventional regulations of financial intermediaries for combating the transfer of money for illicit purposes. Itexplains that the twenty-first century has created a pluralistic model, a new school of regulation, with many different actors. This model can be condensed into a triangle of actors: the state, the infrastructure that facilitates violations of the law and the violator.[[28]](#footnote-29) Examples of such regulations will be provided. Part I concludes with a description of anti-money laundering and anti-terrorism regulations that apply to traditional financial gatekeepers.

**Part II** explores the features of cryptocurrencies, and even more relevant the features of the blockchains on which they are registered, focusing on the main blockchains: Bitcoin and Ethereum. This Part explains that, due to the decentralized structure of the blockchain and the anonymity of token holders, at present transactions made on the blockchain cannot be regulated. The anonymity of transactions on the blockchain facilitates the use of these anonymized tokens by terrorists. Without meaningful regulation of illicit transactions, terrorism can flourish and pose a threat to national security and public safety.

**Part III** proposes to mitigate the problem by registering and verifying the identities behind token owners. This is also known as permissioned (private) blockchains, such as the one intended for Facebook’s new cryptocurrency, the Libra.[[29]](#footnote-30) On such a blockchain, an access control layer is added in order to govern who has access to the network. Token holder access is then vetted by the network owner. Such regulation would allow unmasking of the token owner only where there is probable cause. A court warrant would be required to unmask token owner identity. Therefore, such a regulatory change would be in line with the Fourth Amendment even after the fundamental changes of the Supreme Court in *Carpenter* narrowed the third-party doctrine.[[30]](#footnote-31) Imposing such obligations on companies issuing cryptocurrencies is just and efficient because these companies benefit commercially from the use of their financial products. The benefits of such an obligation to maintain a registrar of token holders would exceed their costs and have the potential to stifle financing of terrorism at this crucial juncture.

**Part IV** addresses objections to the proposed solution. *Inter alia*, this part addresses First Amendment freedom of expression concerns, as well as considerations such as usability, administrative costs, data security and enforcement methods.

# **I. Intermediaries as Gatekeepers– Traditional Regulation of Intermediaries for Combating Violations of Law**

Traditional, or “old-school”, regulation imposes imprisonment or fines to regulate or control violations of law.[[31]](#footnote-32) This type of regulation can be labelled “*dualist”* or “*dyadic”*.[[32]](#footnote-33) In this model, there are essentially two players: the state and the violator.[[33]](#footnote-34) However, in the twenty-first century there are multiple players, necessitating a pluralist model. Companies at the center of the economy provide infrastructure that facilitates both legal and illegal activities. Policymakers have enlisted players such as online intermediaries, technology firms, financial intermediaries and payment processing intermediaries to regulate the activities they facilitate. Such regulations can be within the context of administrative law,[[34]](#footnote-35) yet in many cases the obligation to regulate that is imposed on companies that provide infrastructure falls within the bounds of civil and criminal law. Professor Balkin has dubbed this type of enforcement "the new-school regulation".[[35]](#footnote-36) Balkin focused on the role this model plays in regulating speech by companies that provide infrastructure such as ISP, websites that host content (content providers) and even search engines.[[36]](#footnote-37) Yet, the same structure is used to deter and enforce other violations of law. This model includes many different players, but it can be condensed into a triangle of actors: the state, the law violator and the infrastructure, which serves as a gatekeeper.

Violations of law are often committed under a cloak of anonymity and from jurisdictions without effective rule of law. Such violations pose a challenge to law enforcement. In order to cope with this challenge and mitigate the harm caused by violators, enforcement relies heavily on intermediaries that provide the infrastructure for such activities.[[37]](#footnote-38) Thus, when an enforcer investigates and executes interventions, legal demands may fall upon third parties, individuals, and businesses that were merely used as conduits by the suspect.[[38]](#footnote-39) Imposing legal obligations and liability on the infrastructure for third-party violations of law is a powerful incentive to mitigate harm, as it ensures the cooperation of companies with law enforcers and incentivizes them to operate safely.

As companies that provide infrastructure are also located at a highly visible choke point for regulatory intervention, it seems natural to obligate them to supervise and regulate their platform users. One prominent example is regulation and enforcement of harmful speech by utilizing online intermediaries. Although in the US intermediaries benefit from overall immunity for content published by other content providers,[[39]](#footnote-40) in many states outside the US, intermediaries can be held responsible failing to remove speech that incites terrorism,[[40]](#footnote-41) hate speech,[[41]](#footnote-42) defamation,[[42]](#footnote-43) and even fake news.[[43]](#footnote-44)

In a related context, copyright owners turn to online intermediaries to mitigate copyright infringements and in fact to enforce their intellectual property rights.[[44]](#footnote-45) In such cases, intermediaries may benefit from a legal safe haven if certain steps are taken and they respond to takedown requests by intellectual property (IP) right holders.[[45]](#footnote-47) However, failing to comply may end in vicarious liability for copyright infringements.

A third example is payment systems and networks for banks and merchants, such as Visa or Mastercard, which receive money in order to process consumer purchases. Such payment processing intermediaries attempt to enforce intellectual property rights and mitigate violations of law by “following the money” that flows to online merchants who profit from illegal activities such as piracy and counterfeiting.[[46]](#footnote-48) Creating a payment blockade seriously threatens the website's continued existence and thus is also effective in preventing the unwanted behavior.[[47]](#footnote-49) Blocking payment by payment processing systems is voluntary. Yet, although such practices are not in the shadow of the law, they are in the shadow of potential future laws, such as legislative bills aimed at payment processors.[[48]](#footnote-50) Moreover, litigation costs and potential liability in courts can also motivate payment processors to block payment from reaching entities that profit from illegal activities.[[49]](#footnote-51)

Another function of payment intermediaries is monitoring suspicious merchants and linking their activities across different banks. For example, Visa can search for potential infringements in its payment systems, respond to complaints, investigate or instruct the payment company to investigate the merchant, and report within five business days. After reviewing the report, Visa has the payment company send a “comply or terminate” notice to the suspected infringer.[[50]](#footnote-52) As a checkpoint of the marketplace, payment systems can place the flow of revenues and funding of illicit actors under siege and disrupt their activities to avoid potential regulation.

Beyond the context of online speech and intellectual property infringements, intermediaries can also cut the flow of money which helps operate the chain of crimes and activities that infringe on national security. Traditional financial institutions have been used to aid the enforcement of anti-money laundering and anti-terrorism statues exists for many years. The Financial Action Task Force (FATF), the global organization for combating money laundering and terrorist financing, was formed in 1989 by the G-7 – a group of seven developed countries.[[51]](#footnote-53) The FATF sets international standards aiming to prevent money laundering and financing of terrorism and works to generate the political will which leads countries to adopt legislative and regulatory reforms in this area.

## *The Infrastructure as a Gatekeeper of Illegal Transfer of Money for Terrorist Activity-*

Terrorists need funding for their activities. The greater the funding, the more frequent and lethal attacks they can organize and execute.[[52]](#footnote-54) As money is usually transferred via a financial intermediary, financial institutions are infrastructures that, unwittingly, facilitate the transfer of money for terrorism. Due to this property of financial intermediaries, it is financial institutions such as banks and wire services that can make it difficult for terrorists to receive and transfer money by denying them service. If terrorists are prevented from easily receiving donations and funding, the oxygen for their activities is cut off. Thus, financial transfer chokepoint presents an opportunity to slow down money transfers for terrorist operations, disrupt their activities and block them from perpetrating these illicit activities.[[53]](#footnote-55)

In light of the abovementioned characteristics of financial intermediaries, law enforcement agencies have developed and implemented several successful approaches for preventing the flow of funding to terrorist organizations and other criminals through financial intermediaries. Counter Terrorism Financing (CTF) focuses on tracking the flow of money through bank accounts and preventing financial transactions that might be used to support terror attacks and other terrorist activities.[[54]](#footnote-56) Federal law shifts the weight of preventing donation and payment for terrorism to the financial institutions. Thus, when an enforcer investigates and conducts interventions, legal demands may fall upon financial intermediaries and businesses that were merely used as conduits by the suspect.[[55]](#footnote-57) Assigning responsibility to the financial institutions incentivizes such financial intermediaries to take measures and combat money laundering activities on their platforms (whether the money is transferred through bank accounts or other tools). In addition to impacting terrorist fundraising, this increased enforcement has significantly reduced the ability of terrorist groups to rely on formal banking, especially money management and transfer services, an expansive category that can include digital transfers, prepaid instruments, and mobile payment systems.[[56]](#footnote-58) The anti–money laundering and anti-terrorism statues serve as the main examples of such gatekeeping obligations and financial institution liability. The following subsections focus on these existing regulatory solutions for CTF.

## *(1) Traditional Financial Intermediaries at the Service of National Security*

### (a)Anti-Money Laundering Statutes

Money laundering is a process in which individuals who obtain money through criminal activity (including terrorism) try to conceal the illegal source of this income and make it appear legitimate. Money laundering is a systemic problem which has a great impact on the world’s economy.[[57]](#footnote-59) Money laundering activities are typically comprised of three stages: (1) placement, where the money is introduced into the financial system; (2) layering, masking the origin through multiple, separate transactions and (3) integration, integrating the illegal proceeds of crime into the legitimate financial system. Anti-money laundering regulations try to catch and prevent the latter two steps.

Although anti-money laundering regulation has existed in most developed countries since the 1970s,[[58]](#footnote-60) Western governments have significantly increased the enforcement of these regulations since the September 11, 2001, terror attacks (hereinafter - 9/11). After 9/11, aconsensus immediately emerged, or rather seemed to be present, that going after terrorist money is a key weapon in the war against terrorism.[[59]](#footnote-61) This consensus translated into more duties and obligations for financial institutions around the world.[[60]](#footnote-62) Thus, anti-money laundering has become a core element in combating terrorist activities and crime control, and a central precept in international banking standards.[[61]](#footnote-63)

The US Executive and Congress naturally took action and the US was quick to adopt further measures against money laundering.[[62]](#footnote-64) The result was the enactment of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT)[[63]](#footnote-65) (hereinafter “The Act”),[[64]](#footnote-67) which calls upon every American patriot to play his or her part in defending against the threat of terrorism. The purpose of the Act is "[t]o deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes."[[65]](#footnote-68) The Act enhances partnership between the public and private sector in policing the channels of international financial transfers[[66]](#footnote-69) and aims to apply to foreign financial institutions and foreigners not residing within jurisdiction of the United States.[[67]](#footnote-70) The Act requires financial institutions, the gateways, to serve as the first line of defense against illicit activity in the financial system. These institutions are charged with blocking any movement of money generated through crime or designated for terrorism that is transmitted through their systems. They are also supposed to Know their Clients (by filling in a Know Your Client (hereinafter - KYC) questionnaire and getting to know the client’s activities in the account),[[68]](#footnote-71) to help keep out criminals and terrorists. All this should be done by adopting broader risk management approaches that make it harder for abuse to occur in the first place.[[69]](#footnote-72)

Title IIIof the Act, "International Money Laundering Abatement and Anti-Terrorist Financing Actof 2001",[[70]](#footnote-73) relates to the global issues of money-laundering. Anti-money laundering statutes focus on specific areas of banking obligations.[[71]](#footnote-74) As mentioned above, the provisions obligate financial intermediaries to know their customers and require that ordinary users provide documentation of their identity. A second area of obligation concerns due diligence on private banking activities. Additional obligations relate to reviewing relationships with non-US correspondent banks and shell banks and monitoring wire transfers for patterns of money laundering activities.[[72]](#footnote-75) Such requirements can create blockades of illegal transfers and thus allow tracking, monitoring and confiscation of such transfers. Banks are supposed to report unusual activities in their customers’ accounts as well as specific transactions dictated by the laws and regulations. Obviously, complying with anti-money laundering requirements places a very heavy regulatory burden on financial institutions. Especially since failure to comply can result in liability.[[73]](#footnote-76)

The United States supplements this regulatory framework with three criminal laws: two money laundering offenses,[[74]](#footnote-77) both relating to the prohibition against financial transfers relating to the proceeds of an unlawful activity; and one law prohibiting structuring a financial transaction to avoid reporting.[[75]](#footnote-78)

#### a.1 Money Laundering and Comingled Bank Accounts in Court Rulings

Another issue relating to bank accounts and illegal activities such as crime and supporting terrorism relates to comingled funds in bank accounts. The Supreme Court has yet to address the issue and lower courts provide a spectrum of opinions on the matter.[[76]](#footnote-79) The Fourth Circuit ruled that as legal funds cannot be distinguished from illegal funds in the same bank account, all funds in the account are held to be proceeds of criminal activity.[[77]](#footnote-80) A similar approach is taken by other circuit courts,[[78]](#footnote-81) but not by all. For example, the Ninth Circuit demands proof that the funds are the proceeds of criminal activity[[79]](#footnote-82) and the Fifth Circuit ruled that there is a presumption that clean money is spent before dirty money.[[80]](#footnote-83)

Usually, due to specific clauses in the deposit insurance contract, banks are able to freeze accounts with comingled funds if they detect suspicious activity in the account.[[81]](#footnote-84) Courts may also freeze property which was obtained as a result of money laundering activity.[[82]](#footnote-85) However, in *Luis v. United States,* the court held that freezing an account which contained comingled funds violated the defendants’ Sixth Amendment right to assistance of counsel.[[83]](#footnote-86) The dissenting judges, Justice Kennedy and Justice Alito, opined that it is not possible to tell if a defendant spent the legal funds in the account first or if the illegal funds are fungible.[[84]](#footnote-87) However, as mentioned above, the issue has not yet been resolved, as the Supreme Court has yet to address it.

### (b) Anti -Terror Act- Material Support and the Criminalization of Financing of Terrorism

Financial institutions play an important role in efforts to cut off financial support for terrorist organizations. Anti-terror statutes prohibit the provision of material support for terrorism and expose financial institutions that facilitate the transfer of money to terrorist organizations to ex-post civil and criminal liability. Section 2339A of the United States Code prohibits providing “material support or resources . . . knowing or intending that they are to be used in preparation for, or in carrying out” a violation of certain offenses, including terror.[[85]](#footnote-88) Section 2339C addresses the collection of funds. It imposes penal sanctions against the provision or collection of funds “with the intention that such funds be used, or with the knowledge that such funds are to be used, in full or in part, in order to carry out” a statutorily enumerated predicate crime.[[86]](#footnote-89)

Unlike § 2339A and 2339C, § 2339B does not include a knowledge or intentional mens rea element,[[87]](#footnote-90) or specific intent, but rather prohibits the willful provision of anything of value to a group designated as a Foreign Terrorist Organization (FTO).[[88]](#footnote-91) Thus, if a provider, such as a bank or other financial institution, knows that an organization has been officially designated as a “terror” organization, or if it knows that an organization engages in terrorism, it may be found guilty.[[89]](#footnote-92)

It is difficult to separate licit operations and expenses, such as salaries and social services, from clearly illicit spending, such as terrorist recruitment and training, because of the lack of information and the close relationship between these activities. It is especially difficult since legitimate activities help terrorists mask illegal activities.[[90]](#footnote-93) For example, operating costs, such as propaganda, recruitment, salaries, and social services, indirectly contribute to an organization’s ability to propagate violence. However, the Anti-Terror Act applies to any support provided to a terrorist organization. In *Holder v. Humanitarian Law Project* (*HLP*),[[91]](#footnote-94) the Supreme Court upheld the constitutionality of 2339B, and determined that the Federal Government has the authority to prohibit groups from working with terrorist organizations even when their violent operations are interlinked with more benign functions, such as charity work.[[92]](#footnote-95) Because of the grave danger posed by terrorist organizations, the Supreme Court interpreted coordination in broad terms, determining that working in coordination with or at the command of FTOs serves to legitimize and further their terrorist means, and therefore these actions are considered material support.[[93]](#footnote-96)

As explained above,[[94]](#footnote-97) Sections 2339A and 2339B do not create a private civil cause of action, but § 2333 “…*allows private parties who are nationals of the United States to sue in federal district court and receive treble damages and attorney’s fees if they were injured in their ‘person, property, or business by reason of international terrorism...*’”[[95]](#footnote-98) This scienter requirement “may be satisfied when an entity recognizes it is supporting a terrorist organization; it needs not be aware that its aid is going to advance a specific terrorist conspiracy.”[[96]](#footnote-99)

In the wake of terrorist attacks, victims and their families are left with a troubling reality: they have little chance of bringing those directly responsible to justice in court.[[97]](#footnote-100) Civil liability for those who provide material support to terrorist groups is therefore thought to serve several purposes: (1) it allows victims and their families to hold anyone in the chain of causation directly accountable, (2) it allows for potentially significant financial recourse, and (3) it encourages banks to “think twice” about their role in the causal chain of terrorism.[[98]](#footnote-101) There is a growing trend to press civil claims against banks. However, even though liability can be imposed on banks for material support,[[99]](#footnote-102) courts are deeply divided over whether the Anti Terror Act allows for secondary liability based on the theory that a bank aided or abetted the acts of terrorism. Courts also disagree on the required level of fault needed to establish civil liability under § 2333(a).[[100]](#footnote-103) Thus, despite the potential benefits of Anti Terror Act claims, the current framework creates inconsistent civil judgments.[[101]](#footnote-104)

In summary, laws impose obligations and liability on intermediaries to improve the efficiency of enforcement of illegal activities, including terrorist activities. However, such enforcement methods are only as effective as the way in which courts impose them. The war against money laundering is ongoing and can only be won if it becomes difficult to circumvent the laws and regulations relating to anti-money laundering and financing of terrorism. Getting around traditional intermediaries makes it possible to circumvent the enforcement of illegal transfers and use of money for terrorist activities. As this Article demonstrates, using cryptocurrencies circumvents traditional intermediaries and enforcement and enables the flow of money to support and manage terrorist activities.

# **II. What are Cryptocurrencies, How do they Work and What Are their Benefits for Terrorism?**

## ***A. Cryptocurrencies***

Cryptocurrencies are electronically generated and stored currencies which enable users to trade objects with one another.[[102]](#footnote-105) In 2008, the first and perhaps most well-known cryptocurrency, Bitcoin, was introduced to the world in a document called a “white paper”. This first white paper, entitled “Bitcoin: A Peer-to-Peer Electronic Cash System” was posted online by an unknown author masking him or herself under the name “Satoshi Nakamoto”.[[103]](#footnote-106) The Bitcoin network, the white paper revealed, is both a protocol for securely storing and transmitting tokens (virtual coins) and the name of the unit of value in the system. The white paper further explains that the Bitcoin is an encrypted digital token which can be transferred from one user to the next without the need for a central entity to register the transactions.[[104]](#footnote-107) Instead, transactions are recorded in distributed ledger technology (DLT) which allows all users to keep track of the registered transactions. As the technology is made out of blocks connecting to each other via an encrypted digital signature, it is called a “blockchain”.[[105]](#footnote-108)

The Bitcoin blockchain is where Bitcoin tokens are traded and stored. The blockchain is maintained by an online peer-to-peer network, a distributed ledger technology that tracks transactions and maintains a complete history of verified transactions.[[106]](#footnote-109) Accordingly, and true to the nature of a public blockchain, any user of the system can participate in all aspects of its operations, including all transactions, and no single participant has control. To support anonymity and transaction ownership, Bitcoin transaction participants are identified by a unique string of random numbers rather than by a name or other personal information.[[107]](#footnote-110) The same is true for Ether, another cryptocurrency which is widely used. Ether is a token which runs on the Etheruem blockchain.[[108]](#footnote-111) The Etheruem blockchain allows users to make use of “smart contracts”,[[109]](#footnote-112) that can replace legal contracts.[[110]](#footnote-113) Smart contracts are basically computer orders which follow the logic of “if x occurs do y”.[[111]](#footnote-114) This blockchain allows other firms to use it in order to develop their own tokens and issue them in a process called Initial Coin Offering (ICO). Full anonymity is also maintained for users on the Etheruem blockchain.

The most recent and talked about cryptocurrency is Facebook’s initiative – the Libra. Using Libra, a global coin which is designed to replace some of the fiat currencies, will allow you to send money to others or buy things with almost zero fees.[[112]](#footnote-115) In order to use Libra, users will have to download a wallet application such as Novi, the app Facebook designed for its new currency. This app will be built into WhatsApp and Facebook Messenger[[113]](#footnote-116) and users of these apps will form its user base.[[114]](#footnote-117) This intended token will allow users to exchange fiat currencies, such as USD, EUR etc., in return for Libra, and exchange back to fiat currencies when they please. The Libra token will be pegged to a basket of short-term government securities and bank deposits in order to mitigate the fluctuation usually associated with cryptocurrencies.[[115]](#footnote-118)

Unlike other cryptocurrencies, such as Bitcoin, Ether and most tokens which are built on the Ethereum blockchain, Libra will run on what is known as a “private blockchain” which is not truly decentralized. The blockchain intended for Libra will be run by the Libra Association members. This means that the ledger of transactions will be accessible only to them, and that they can also control who enters the system.[[116]](#footnote-119)

ICOs are attractive to entrepreneurs for different reasons, some more legitimate than others. Legitimate reasons might include the fact that issuing tokens, as opposed to issuing stocks, enables entrepreneurs to maintain all of their rights in the corporation without dilution while still raising money, reaching more investors worldwide and avoiding costly regulatory demands.[[117]](#footnote-120) For all these reasons, the market for ICOs bloomed in the years 2016 – 2019, raising over USD 300 Billion from investors worldwide.[[118]](#footnote-121) During this time, exchanges designated solely for cryptocurrencies, and supplying the market with liquidity, began to pop-up. These exchanges form the marketplace where buyers and sellers of tokens can conduct exchanges.[[119]](#footnote-122)

However, alongside the legitimate reasons for issuing tokens there are illegitimate reasons, including using the anonymity of the token for money-laundering,[[120]](#footnote-123) fraud, tax evasion,[[121]](#footnote-124) ponzi schemes and support for terrorist organizations.[[122]](#footnote-125)

## *B. Why and How are Cryptocurrencies Used by Terrorist Organizations?*

Terrorists require significant funding for their operations, propaganda, recruitment, training, salaries and management.[[123]](#footnote-126) For example, ISIS approved a USD 2 billion budget for 2015. Costs of specific attacks can range from an estimated USD 10,000 for the 2015 Paris attacks to USD 400,000–500,000 for the 9/11 attacks.[[124]](#footnote-127) Money is the fuel and oxygen of terrorist activities. The more funding organizations have, the more they can recruit members, organize and commit terror attacks.Terrorist groups' sources of revenue and fundraising activities combine traditional and non-traditional methods. These organizations depend on numerous sources of income derived from both criminal activities and the abuse of legitimate activities to generate funds. Examples of criminal activities include arms and drug trafficking, kidnapping for ransom, extortion, and racketeering. In addition, terrorist organizations and their associates also divert funds from charities, donations, sponsorships and legal sources such as businesses and personal credit loans.[[125]](#footnote-128)

After generating funds, terrorist organizations must manage their money. If the money received is not yet under the direct control of the terrorist organization, or if it cannot be transferred because of operational security concerns, terrorists may use money laundering and other transfer mechanisms to support the cash needs of their members and associates. Terrorist groups and organizations *spend* the money they generate on salaries and services as well as on illicit operations, terrorist recruitment, training, propaganda and attacks, including weapon purchases or other related expenses.[[126]](#footnote-129)

### 1.The Anonymity of Some Cryptocurrencies and its Importance to Terrorist Activities

Cryptocurrencies are attractive to terrorists, as using anonymous tokens can promote their activities, aid organizational transactions, and allow them to accept funds as well as manage and spend them. Such tokens make it possible to transfer money instantly around the world without making use of intermediaries, such as banks, which require more transparency and are obligated to report suspicious activity in the accounts of their depositors. Anonymous cryptocurrencies make it possible to hide and protect the identity of the user. While the original purchase of the currency may be visible (e.g., through the banking system), all following transfers of the virtual currency are difficult to detect.[[127]](#footnote-130) Indeed, the anonymity on the blockchain is incomplete[[128]](#footnote-131) and might be insufficient for some users,[[129]](#footnote-132) as the degree of anonymity depends on operational and technical factors, and therefore transactions can be deanonymized through a variety of methods.[[130]](#footnote-133) However, such methods of deanonymization have their costs and uncovering identities can take time. Moreover, dark wallets,[[131]](#footnote-134) which seek to render deanonymizing cryptocurrency transactions impossible, disrupt potentially identifying characteristics on the blockchain, enabling illicit financial transactions.[[132]](#footnote-135)

Anonymity in financial transactions is an important aspect of each and every one of a terrorist’s financial activities. First, anonymity is important for *fundraising*.[[133]](#footnote-136) Since it is illegal to provide material support to known terrorist organizations, lack of anonymity serves as a deterrent to donors.[[134]](#footnote-137) Likewise, recipients of funds meant for terrorist operations require anonymity, as being actively involved with raising funds for terrorist organizations and/or operations is illegal and would, if unmasked, be blocked by the authorities.[[135]](#footnote-138) Thus, if cryptocurrencies remain anonymous, the anonymity they allow will make it possible to circumvent the Western banking system, which limits donations for jihad through restrictions on the financial system.[[136]](#footnote-139) Second, anonymity of financial transactions is of critical importance for *illegal drug and arm trafficking.* Terrorist organizations require anonymity to avoid detection by the authorities during and after the transaction.[[137]](#footnote-140) Finally, anonymity is highly important for *funding terrorist attacks.* In particular,it is crucial for terrorist organizations that the attacker who receives the money is not detected prior to the operation.[[138]](#footnote-141)

Terrorists can conceal their identity and reduce the risk that their communications and financial activities will be detected. While terrorists have been active on various online platforms for more than two decades, the surface web has turned out to be too risky for anonymity-seeking terrorists as they can be monitored, traced and found.[[139]](#footnote-142) However, the majority of the internet lies below the metaphorical waterline, unsearchable and inaccessible to the general public.[[140]](#footnote-143) The deepest layers of the deep web, a segment known as the dark net, contain content that has been intentionally concealed, including illegal and anti-social information.[[141]](#footnote-144) It also allows hidden transfer of funds, using cryptocurrencies that fulfill terrorists’ need for anonymous and secure streams of funding. This recent trend is one of the most alarming combinations of organized terrorism and dark net capabilities.[[142]](#footnote-145) Because some cryptocurrencies provide the same form of anonymity in the financial setting as the dark net does for communication systems, cryptocurrencies are susceptible to abuse by terrorists who can utilize them and generate great benefit.[[143]](#footnote-146)

Unlike regular bank transfers and accounts, government law enforcement agencies and counterterrorist professionals find it difficult to stop transactions, track cryptocurrency assets and freeze such assets to disrupt illicit funding.[[144]](#footnote-147) Individuals can store infinite amounts of value in their heads simply by memorizing a private key that gives access to funds on the blockchain. This makes it difficult to enforce capital controls over cryptocurrencies. Terrorists can raise funds by accepting cryptocurrency donations from anyone and anywhere in the world by publishing their public cryptocurrency key on a website, thereby avoiding relying on third party intermediaries.[[145]](#footnote-148) For example, this makes it possible to exploit the Bitcoin system for crowdfunding campaigns for terrorist activities.[[146]](#footnote-149) Such illicit funding networks are hard to disrupt.[[147]](#footnote-150) As technology makes it easier to use and access cryptocurrencies and the dark web, they become a more routine aspect of our lives and terrorists have more opportunities to fundraise, operate, and commit illicit operations, evading detection by authorities.[[148]](#footnote-151) Consequently, the threat posed to national security grows.[[149]](#footnote-152)

### Current Limitations on the Adoption of Cryptocurrencies by Terrorists and the Future

As this Article has demonstrated above, anonymous cryptocurrencies can be attractive to terrorists; yet it should be noted that terrorists have not yet adopted cryptocurrencies on a large scale. Because the value of cryptocurrencies is unstable, using them causes terrorist organizations unwanted uncertainty. Another reason for the limited scale of use is that use of such tokens reduces the ability of terrorist leaders to exercise control over funds entrusted to agents. In addition, the problems and difficulties associated with exchanging cryptocurrencies into fiat currencies remain.[[150]](#footnote-153) Finally, the low level of penetration of modern technical communicational tools (such as internet reception) in some geographical areas where terrorist organizations operate also affects the scale of adoption.[[151]](#footnote-154)After all, if a group of terrorists, or a terrorist organization, cannot easily exchange cryptocurrencies for large quantities of fiat currency or cannot use them easily to purchase weapons, other materiel, food, and housing in the areas where it operates, these currencies do not contribute to its operations.[[152]](#footnote-155)

In the future, however, the utility of cryptocurrencies is expected to grow as both terrorist methods and cryptocurrencies develop. Cryptocurrencies are expected to become sufficiently liquid and convertible. Such expected advances could facilitate the use of cryptocurrencies for all users and allow terrorist groups and organizations to engage in transnational fundraising and plan vast terror operations and attacks. Thus, one should not underestimate the future risk terrorist use of cryptocurrencies poses to national security.

### The Problem of Counter Terrorism Financing (CTF) in Cryptocurrencies

Public blockchains use peer-to-peer networks that are managed autonomously. The information on the blockchain is secured and decentralized, without encountering the compliance regulations of the established financial system. As a result, it is very difficult for law enforcement and security organizations to identify the users on the blockchain.[[153]](#footnote-156) Various regulators and legislators have identified the tremendous risk of cryptocurrencies and their potential to undermine the successes of Counter Terrorism Financing (CTF). Thus, since May 2017, a US congressional subcommittee has been developing a bill to study the use of digital currencies by terrorists.[[154]](#footnote-157) In January 2018, a bill was introduced in Congress to ask the US Treasury Department to “prioritize the investigation of terrorist and illicit use of new financial technology, including digital currencies,” among other provisions.[[155]](#footnote-158) In addition, the Financial Crimes Enforcement Network (FinCEN) declared that it “regards developers as well as exchanges of [virtual currency] as ‘money transmitters’ for the purposes of the US Bank Secrecy Act”.[[156]](#footnote-159) FinCen is the authority in charge of combating money-laundering and financing of terrorism through the financial system. It does so through laws such as the Bank Secrecy Act, which it supplements with instructions regarding registration with FinCen and the management of accounts. Among others, it requires money transmitters to have a risk-based KYC and anti-money laundering program and to report suspicious transactions.[[157]](#footnote-160) In a letter from 2018, FinCEN made it clear that virtual currency exchanges and administrators are considered money services businesses and are therefore subject to these requirements.[[158]](#footnote-161) The European Banking Authority has also classified terrorist use of cryptocurrencies as a high priority risk.[[159]](#footnote-162)

During 2018 – 2019, more and more regulators around the world began to impose regulations on ICOs in an attempt to protect investors and prevent the illegal use of tokens. Some states, such as South Korea and China, banned ICOs altogether.[[160]](#footnote-163) South Korea banned all forms of cryptocurrency-based fundraising activities and announced steps to marginalize cryptocurrency trading.[[161]](#footnote-164) China deemed ICOs illegal. In September 2017, the most important cryptocurrency exchanges in China announced that they would voluntarily halt trading until further reports of government interventions are publicly announced.[[162]](#footnote-165)

Shortly after the announcement in China, the Swiss Financial Markets Supervisory Authority (a.k.a. FINMA) announced that it was investigating a number of ICOs for breaching anti-money laundering and financing of terrorism provisions and other regulations.[[163]](#footnote-166) Yet, regulatory uncertainty still dominates this market and regulators and courts around the world have yet to come up with a coherent solution which can prevent money laundering and financing of terrorism through cryptocurrencies.[[164]](#footnote-167)

Indeed, a key task of the policy enforcement, intelligence and financial regulatory communities must be to prevent terrorist groups from using cryptocurrencies on a large scale.[[165]](#footnote-168) However, in our opinion, regulation should not ban initial coin offerings altogether, throwing the baby out with the bathwater and relinquishing the tremendous benefits of cryptocurrencies. Instead, this Article proposes to focus on the illicit activities and design identification and verification mechanisms that could be embedded into technology to enable unmasking of illicit actors that abuse cryptocurrencies for illegal operations. Considering whether anonymity is too wide to prevent use by terrorists and criminals and outlining ways to narrow it is the key issue that needs to be addressed in the fight against money laundering and financing of terrorism via cryptocurrencies.[[166]](#footnote-169)

# **III. Speak Out: The Case For Ex ante Verification and Validation of Cryptocurrency User Identity**

The growing trend of using anonymous cryptocurrencies for terrorist purposes makes it significantly more important to identify the users behind the tokens.[[167]](#footnote-170) The anonymity offered by some cryptocurrencies is one of the biggest problems in combating money laundering and financing of terrorism, as it prevents cryptocurrency transactions from being adequately monitored. This lack of monitoring leaves room for shady transactions to occur outside of the regulatory perimeter, and enables terrorist organizations to use cryptocurrencies and obtain easy access to "clean cash".[[168]](#footnote-171)

Researchers have recommended considering a system of mandatory user registration.[[169]](#footnote-172) However, financial regulatory officials have not devoted adequate resources for regulating and examining non-bank financial institutions.[[170]](#footnote-173) With respect to uncovering the anonymity of users, no immediate action has been taken and in the US there is no mandatory obligation to register and validate the identity of cryptocurrency users.[[171]](#footnote-174) At the time of writing this Article, regulatory oversight in the US is limited to KYC measures, which only partially reduce the anonymity built into cryptocurrency system.[[172]](#footnote-175)

As mentioned earlier, KYC measures place an obligation on financial intermediaries to become familiar with their clients. The main reason behind this requirement is that the financial intermediary needs to be able to identify unusual transactions in the client’s account and report them to the anti-money laundering authorities or the police. Requiring a KYC from people receiving cryptocurrencies on an exchange is a first measure, but it is not at all satisfactory with regard to the ability to completely block illicit transactions.[[173]](#footnote-176) People trading cryptocurrencies on exchanges sometimes only make a single transaction on an exchange. This means that the exchange is not familiar with their usual trade patterns in virtual assets and so cannot detect what seems to be irregular cryptocurrency activity .

In addition, as cryptocurrencies are not restricted to a geographical setting, if exchanges operating in the US or the EU become too nosy about the identity of the client, terrorists and other criminals might simply use an exchange operating in a different jurisdiction which does not require a KYC.[[174]](#footnote-177) Lastly, KYC requirements on exchanges will not prevent funding at the ICO stage, as during the ICO people purchasing the token usually do not purchase it through an exchange but rather pay the issuing firm directly using their credit card. Thus, funds can be collected by terrorists or criminals directly from the public, purchasing the token in an ICO, and then be used on the dark net in order to purchase weapons and other equipment needed to commit the crime or attack. This means that the regulatory oversight, however, is limited: in the US, oversight does not cover non-exchange transactions, such as those brokered by local bitcoins.com, and does not cover fully on-blockchain transactions that occur outside of a regulated entity, such as trading one cryptocurrency for another.[[175]](#footnote-178)

## A. Reform Proposal for Verifying, Validating and Unmasking Cryptocurrency User Identity

This juncture, when terrorists are beginning to discover the benefits they can derive from cryptocurrencies in order to commit terror attacks, is exactly the time to consider whether anonymous tokens are truly necessary. Does allowing anonymity of users not veer too far in favor of terrorists?[[176]](#footnote-179) This is the key issue that needs to be addressed in the fight against money laundering and financing of terrorism via cryptocurrencies.[[177]](#footnote-180) This Part proposes a mandatory obligation on wallet providers, exchanges and firms issuing new tokens to identify the cryptocurrency users on the blockchain. This identification would be anonymized and not available for all to see. However, law enforcement agencies could request wallet providers, exchanges and issuing firms to "speak out" and unmask the identities of cryptocurrencies when there is probable cause to suspect illegality in their activities. To be clear, our suggestion is not that blockchain transactions be exposed by name to everyone, but rather that the firms issuing cryptocurrencies be required to sell them only to clients they have screened via a KYC.

In addition, all new users of the coin will have to identify themselves to the firm who issued the token. This way, if a money-laundering activity is detected on the token, the identity of the people behind the wallets can be revealed to the authorities. An example of this idea is the Libra token and the token issued by Saga.[[178]](#footnote-181) Both these tokens are designed to create an international token which would replace fiat currencies in part, and enable global transactions. Ideally, everyone entering the blockchain to purchase one of these tokens would be required to identify themselves to the corporation issuing the token.[[179]](#footnote-182) This means that at any given time, the issuing firm/institution would have a registrar of all blockchain users and could assist authorities in combating money laundering and financing of terrorism.

In fact, this suggestion is currently mirrored in part by the 5th European Anti-Money Laundering Directive (hereinafter - 5AMLD), which was legislated on July 9, 2018 and entered into force in January 2020.[[180]](#footnote-183) This Directive is designed to achieve greater transparency in financial transactions in order to prevent money laundering and financing of terrorism. For the first time, this Directive also covers cryptocurrency transactions, since it applies to crypto service providers such as virtual-fiat exchanges and crypto wallet providers.[[181]](#footnote-184) According to the 5AMLD fact sheet: “*The rules will now apply to entities which provide services that are in charge of holding, storing and transferring virtual currencies*.”[[182]](#footnote-185) The fact sheet further specifies that the law will increase transparency with regards to the real ownership of legal entities and provide the EU authorities with valuable information which will help them tackle terrorist financing risks linked to the use of anonymous tokens. Our suggestion takes the idea of lifting the vail of anonymity one step further: we believe that the firms issuing the tokens should also be obligated to unmask the identity of their clients by requiring a KYC from anyone entering their blockchain and using their token.

## *B. Unmasking and the Fourth Amendment after Carpenter- The Need for a Court Warrant*

As mentioned in the previous section, this Article proposes that cryptocurrency wallet providers, issuers of new cryptocurrencies and exchanges should "speak out" and unmask the identity of their users when law enforcement and intelligence agencies require this information for their investigations. The following subsection will explain that in light of the recent Supreme Court decision in *Carpenter v. United States*,[[183]](#footnote-186) governmental agencies cannot compel wallet providers, issuers of new cryptocurrencies and exchanges to turn over an internet user’s identifying records and unmask them without a warrant. Such a warrant requirement is desirable, as it safeguards the legitimate privacy interests of users, while allowing law enforcement and intelligence agencies to conduct investigations and enforce the law. Without a warrant, courts are likely to conclude that regulation for unmasking cryptocurrency user identities is unconstitutional, standing in contrast with the Fourth Amendment[[184]](#footnote-187) and therefore strike it down.

### The Fourth Amendment: Reasonable Privacy Expectations

The Fourth Amendment is at the heart of American democracy.[[185]](#footnote-188) It is key in protecting US citizens against government power,[[186]](#footnote-189) and ensuring that the government cannot gather information about citizens without proper oversight and limitations. It requires the government to justify to a court why it has a compelling reason to be interested in personal information.[[187]](#footnote-190) Government officials are required to obtain a warrant supported by probable cause before they can place a person under surveillance or search. In other words, the government needs to demonstrate reasonably trustworthy information that the government's search will uncover evidence of illegality. If the government fails to follow these procedures, the information will be excluded from trial.[[188]](#footnote-191)

The Fourth Amendment uses the terms “searches and seizures” to cover rummaging into people's papers and trespassing. However, technology has challenged this approach.[[189]](#footnote-192) At first, in *Olmstead v. United States*,[[190]](#footnote-193) the Supreme Court held that wiretaps do not violate the Fourth Amendment, since they do not involve entry upon premises. Yet, in 1967 the Supreme Court in *Katz v. United States**[[191]](#footnote-194)* narrowed the permissible scope of surveillance under the Fourth Amendment and declared Olmstead was a mistake. Whereas the Court previously applied the Fourth Amendment only to physical trespass, it now declared that it protects people, not places.[[192]](#footnote-195) The current approach to application of the Fourth Amendment thus emerges from the concurring opinion of Justice John Harlan in *Katz*. Accordingly, the Fourth Amendment should regulate whenever a person exhibits an "actual (subjective) expectation of privacy that society is prepared to recognize as 'reasonable'".[[193]](#footnote-196) This approach is the "reasonable expectation to privacy test".[[194]](#footnote-197) The goal of this test was to permit the Fourth Amendment to respond to changing technology.[[195]](#footnote-198)

### (2) The Third-Party Doctrine – No Reasonable Expectation to Information Held by Third Parties

A prominent exception to the test of reasonable expectation to privacy that was outlined in *Katz v. United States[[196]](#footnote-199)* is the third-party doctrine: a constitutional rule that permits the state to access business records and transactional data about a company’s consumers without constituting a Fourth Amendment “search.”[[197]](#footnote-200) If information is possessed or known by third parties, then, for the purposes of the Fourth Amendment, an individual lacks reasonable expectation of privacy regarding the information.[[198]](#footnote-201)

This doctrine was crafted by the Supreme Court in the 1970's.[[199]](#footnote-202) In *United States v. Miller*,[[200]](#footnote-203) law enforcement officials sought the financial records of a bank customer named Mitch Miller, issuing subpoenas to his bank to obtain “all records of [his] accounts.” Without advising Miller, the bank turned over his incriminating records to the government.[[201]](#footnote-204) Miller argued that under the Fourth Amendment the government was required to obtain a warrant before receiving the record. Holding that Miller had no reasonable expectation of privacy regarding the bank records, the Court explained that Miller had “voluntarily conveyed” the records to the bank and that the information was “exposed to their employees in the ordinary course of business.” The Court thus extended the third-party doctrine beyond conversations to encompass business records.[[202]](#footnote-205)

Three years later, the third-party doctrine was further expanded in *Smith v. Maryland*.[[203]](#footnote-206) The Supreme Court held that the Fourth Amendment didn't apply to pen registers, devices that record the phone number a person dials,[[204]](#footnote-208) denying that there is a subjective, or reasonable objective expectation, to privacy in such cases. The Court concluded that since people expose their phone number to the phone company, which has the capacity to record the information, they undertake a risk that the numbers dialed will be turned over to the police. Thus, the information is not protected by the Fourth Amendment.[[205]](#footnote-209) Therefore, the Fourth Amendment does not protect bank transactions, phone contacts and other records maintained by third parties.[[206]](#footnote-210) Scholars have criticized the third-party doctrine for failing to comprehend the concept of confidentiality – a well-known concept of promise.[[207]](#footnote-211) As the following section explains, recently the Supreme Court called the third-party doctrine into question and in fact, narrowed it substantially.

### (3) Shifting the Approach to the Fourth Amendment: *Carpenter v. United States*

The role of courts is to protect the balance of power between the state and the people, refusing to let technological change eviscerate individual privacy and security from individuals.[[208]](#footnote-212) The Supreme Court’s decision in *Carpenter v. United States*[[209]](#footnote-213) presents a new way forward that safeguards legitimate privacy interests while still allowing law enforcement to police bad actors.[[210]](#footnote-214)

In *Carpenter*, the Court held that law enforcement officials may not collect historical cell site location information (CSLI) from a cell phone service provider without a warrant showing probable cause.[[211]](#footnote-215) The majority opinion declined to extend the third-party doctrine to the FBI’s collection of seven days of CSLI from cell phone service providers.[[212]](#footnote-216) Thus, it reinvented the "reasonable expectation of privacy"[[213]](#footnote-217) and narrowed what is known as the third-party doctrine.[[214]](#footnote-219) The majority reasoning extends beyond location information, this opinion addresses information the law enforcement authorities can use to locate people generally, not CSLI specifically.[[215]](#footnote-220) Although the *Carpenter* Court expressly declined to overrule *United States v. Miller*, and *Smith v. Maryland*,[[216]](#footnote-221) hints throughout the *Carpenter* opinions suggest that in the future, these two opinions will be narrowed to the specific facts of those 1970s cases, since bank and phone records can be as deeply revealing as CSLI.[[217]](#footnote-222)

### (4) Extending *Carpenter* to Unmasking Cryptocurrency Users

*Carpenter* called into question the third-party doctrine, and signaled a departure from precedent. This departure can justify further extensions beyond the explicit holdings in the case.[[218]](#footnote-223) This Article argues that unmasking cryptocurrency user identities should also be subject to a warrant and require the government to show probable cause of illegality. Cryptocurrency users have a reasonable expectation of privacy similar to the reasonable expectation with regard to bank records. Unmasking the identities of cryptocurrencies users can reveal information regarding the user’s financial activities. Thus, such unmasking should be covered under *Carpenter* and be exempt from the third-party doctrine. Failing to extend *Carpenter* to the unmasking of cryptocurrency user identities would allow them insufficient protection against government intrusion. Consequently, they would be disincentivized from using such tokens for legitimate purposes. Without a warrant requirement for unmasking, such tokens would be grinded to a halt,[[219]](#footnote-224) resulting in losses for the economy and society. Therefore, we conclude that subjecting the unmasking procedure of cryptocurrency users' identities to a warrant achieves the proper balance between legitimate privacy interests and national security considerations of allowing law enforcement to police terrorists and other bad actors in the age of advanced technology.

# **IV. Speak Out: Addressing the Objections and Limitations**

Verifying and unmasking cryptocurrency identities is not a “silver bullet” and it may have some limitations and shortcomings. Several objections to the proposed framework can be anticipated—thus, some wrinkles must be ironed out. This final Part of the Article addresses them.

## *The First Amendment*

In the US, freedom of speech enjoys stronger protection than in other Western democracies.[[220]](#footnote-225) The First Amendment protects freedom of speech against government censorship. [[221]](#footnote-226) The “right to record” can protect data collection.[[222]](#footnote-228) Raw data may also enjoy First Amendment protections[[223]](#footnote-229) and even a source code can be considered protected speech.[[224]](#footnote-230) The following subsections address freedom of expression objections to the proposed verification, validation and unmasking of cryptocurrency user identity.

### 1 ) Identity Verification, Unmasking and Cryptocurrency - User Freedom of Expression

One can argue that imposing an obligation to verify the identity of cryptocurrency users and allow unmasking thereof infringes on the freedom of expression of these cryptocurrency users, as it limits their anonymity and can in turn censor their speech as reflected in their use of cryptocurrencies. As such, it can be argued that courts could strike down this regulation.

Identifying speakers can often provide information about what they are up to, even without knowing the content of communication.[[225]](#footnote-231) Therefore, the right to communicate anonymously is protected by USlaw.[[226]](#footnote-232) A line of cases has made it clear that there is a constitutional right to anonymous religious and political speech.[[227]](#footnote-233)

At first glance, it can be argued that the use of cryptocurrencies is not speech and restrictions on anonymity of cryptocurrency users do not constitute restrictions on the marketplace of ideas, but rather on the marketplace of commerce.[[228]](#footnote-234) Yet, one might still argue that cryptocurrencies are not just a form of digital payment, they have non-financial applications. Such tokens enable their users to engage in expressive activity with one another.[[229]](#footnote-235) Cryptocurrencies enable users to include non-financial data (called "arbitrary data") that, once the associated (often nominal) transaction is validated, is immutably published onto the cryptocurrency's blockchain.[[230]](#footnote-236) In addition, cryptocurrencies have communication value as they allow their users to communicate in ways previously unimaginable and to express their lack of trust in central economies.[[231]](#footnote-237) Verifying the identity of cryptocurrency users and subjecting them to the possibility of unmasking could result in censorship of expressive activities.

However, although the use of cryptocurrencies can be considered speech, the proposed regulation focuses on illegal aspects of *financial activities* *and applications* enabled by the use of cryptocurrencies, and not on expressive values. Focusing on financial conduct can be perceived *at most,* as commercial speech.[[232]](#footnote-238) Even if recognized as speech, regulation of such speech can be subject only to intermediate scrutiny standards.

Identity verification and validation of cryptocurrency users' identities applies to all users with neutrality to content. Unmasking reveals the identity of users and does not restrict the choice to use cryptocurrencies. Moreover, there are safeguards that prevent the authorities from unmasking identities of cryptocurrency users regularly, posing a high standard of probable cause for illegality. Such safeguards are likely to prevent infringement of legitimate free choice to use cryptocurrency. A substantial chill on legitimate use of cryptocurrencies is not expected, because users would know that unmasking can only occur when a warrant has been issued and when there is probable cause for misuse of the cryptocurrency for illegal financial transfers of money or illegal transactions. The obligations of identity verification and unmasking cryptocurrency user identity are thus likely to pass the intermediary scrutiny test from the perspective of preserving users' free speech. Such regulation is constitutionally justified, as there are substantial national security interests in such regulation and it is narrowly tailored to serve such interests.[[233]](#footnote-239)

### 2) Identity Verification, Unmasking and Freedom of Expression of Wallet Providers, Exchanges and Issuing Firms

Another freedom of expression objection concerns the expression rights of wallet providers and the corporations issuing the tokens (hereinafter - issuing firms). It can be argued that the proposed obligations regarding identity verification and unmasking limit their freedom to shape the software codes of their systems, as code is information, and information is speech.[[234]](#footnote-240) Because computer language and code are speech, an obligation to program a system that allows verification of user identities ex ante and user unmasking ex post, infringes the right to freedom of expression of wallet providers, exchanges and issuing firms.[[235]](#footnote-241)

It should be noted that the rush to claim First Amendment protections for non-expressive but code-dependent technologies has been criticized by scholars as diluting core First Amendment principles and threatening the Amendment’s strength.[[236]](#footnote-242) However, currently courts recognize such freedom of expression interests in code.[[237]](#footnote-243) Thus, one might argue that courts could strike down the proposed regulations for violating the First Amendment rights of wallet providers.

However, although such technological tools can be considered as speech, the value of such speech is not absolute. Programing a tool that instructs technology that shapes financial systems is not a way of participating in the marketplace of ideas and public opinion, but rather a form of market behavior that uses "speech".[[238]](#footnote-244) Due to the commercial nature of the speech that constructs the code as part of a product, or a tool in the marketplace, the obligation to embed identity verification and unmasking capabilities in the code should not be subject to strict scrutiny standards, but rather to intermediary scrutiny standards only. Due to the importance of such regulation in stifling terror operations and attacks, the interest in such regulation is substantial. This regulation is content neutral: it avoids dictating exactly how to program the code. Furthermore, it does not interfere with the general operation of the system. Rather, it sets enabling verification of identity and unmasking as goals. As such, it is narrowly tailored to serve national security interests.

## B. From the Cathedral to the Bazaar and Back to the Cathedral Again? Concerns Regarding Centralized Distribution of Power

In the traditional "cathedral" model, the medium of currency exchange requires the involvement of large centralized government institutions. In contrast, cryptocurrencies operate in an autonomous and distributed manner, independently of any trusted authority or centralized operator. They lack sovereign backing and many features of national currency systems. Cryptocurrency systems can be likened to a "bazaar",[[239]](#footnote-245) as a libertarian ethos animates many of the individuals and entities that are involved in the creation and growth of the cryptocurrency movement.[[240]](#footnote-246)

However, placing legal obligations on wallet providers, exchanges and issuing firms can lead to centrality and in fact signal a shift back to the "cathedral" model, where central intermediaries regulate the market. Similarly, the internet was once thought to be a harbinger of disintermediation - a sovereign medium controlled from the bottom up by users - but now the internet has shifted and created new gatekeepers (the online intermediaries).[[241]](#footnote-247) A similar development could occur to the cryptocurrency system, which is already becoming less decentralized.[[242]](#footnote-248) One might argue that imposing identity verification and unmasking obligations on wallet providers, exchanges and issuing firms would increase their involvement in regulation, distort the distribution of power in the infrastructure and undermine the model of a decentralized system that avoids the shortcomings of traditional financial institution and state control. Such obligations might impair user trust in the system and hinder innovation. Therefore, one might argue that it is unwise to discourage a successful innovative model just because illicit actors, such as terrorists, use it.[[243]](#footnote-249)

Indeed, imposing obligations on wallet providers, exchanges and issuing firms is no panacea. However, identity verification and unmasking obligations that are subject to a court warrant are not directed at transactions or at the technology. Thus, they are different from traditional gatekeeping such as payment blockades.[[244]](#footnote-250) Because the identity of users is encrypted and can only be unmasked subject to a warrant where there is probable cause to illegality, such regulation would primarily target illicit actors that use the system.[[245]](#footnote-251) It would have little impact on legitimate financial transactions by innocent users and general transfers of money. Therefore, it is not expected to have far-reaching influence on the system's special structure or on the trust of innocent users therein.

Indeed, the proposed regulation allocates increased power to wallet providers, exchanges and issuing firms. Despite targeting illicit actors, it might disrupt the decentralized structure of the system. However, when balancing the possible social costs of such disruption against the national security benefits, the proposed intervention is worthwhile.

## C. Administrative Costs of Identity Verification and Unmasking

The third objection concerns the administrative costs of the verification of identity of cryptocurrency users, the costs of storing and securing such information, and the costs of responding to unmasking procedures. Any heavy new regulatory regime would make all transactions costlier and less convenient.[[246]](#footnote-252) One might argue that imposing such costs on wallet providers, exchanges and issuing firms is far-reaching. Such regulation might even cause some wallet providers, exchanges and issuing firms to exit the market.[[247]](#footnote-253) Moreover, new investors might refrain from investing in such systems and decline to develop new types of innovative cryptocurrencies. Thus, such regulation could lead to market inefficiency.

Indeed, the proposed regulation has its costs, yet it can be argued that the benefits of such a solution in stifling terrorist activities and enhancing national security exceed the costs of implementing such an identity verification framework. Overall, the proposed regulation promotes welfare maximization.[[248]](#footnote-254) In the US, similar obligations to storing information on users, such as IP addresses and unmasking procedures are common, despite the burden they impose. For example, there are John Doe subpoenas to unmask the identity of anonymous speakers from their ISP, or from the website on which they posted defamatory comments.[[249]](#footnote-255) Imposing obligations on traditional intermediaries to provide information in John Doe procedures can be justified from an economic perspective because they are in the best position to collect, store and provide such information in legal procedures. The proposed regulation can be justified based on similar arguments.

In addition, identity verification of cryptocurrency users is not revolutionary. Such verification is conducted voluntarily by Libra and Saga, which verify the credentials of all coin users.[[250]](#footnote-256) It can therefore be argued that the costs of identity verification are not unreasonable. Therefore, in light of the importance of verification and unmasking for national security and crime prevention, such verification should be obligatory for all cryptocurrency wallet providers, exchanges and issuing firms.

## D. Data Breach Concerns

The fourth objection focuses on data breach concerns. The proposed regulation obligates wallet providers to verify the identity of their users, including biometric information. Such dossiers of personal information can be hacked and misused by illicit actors, raising security and privacy risks, [[251]](#footnote-257)such as identity theft and fraud.[[252]](#footnote-258) Privacy law focuses on the obligations of data collectors and processors to obtain informed and explicit consent for the collection of personal data and does not protect personal information from hacks.[[253]](#footnote-259) Such data breaches can result in tremendous harm, including identity theft, economic harm and anxiety.[[254]](#footnote-260)

Indeed, data storage of personal information on the identity of cryptocurrency users can be hacked and misused by illicit actors. Data breach is a major problem in the information age in general. However, the risk of data breach should not prevent the collection and storage of personal information. Rather, regulators should focus on effective data security and restrict insecure designs that create unwarranted privacy risks.[[255]](#footnote-261) Two design features can mitigate the risk of data breach harm. First, the personal data should be encrypted. Encryption of personal data will enable a high level of confidentiality.[[256]](#footnote-262) Encryption is an effective tool for citizens and businesses to defend themselves against abuse of technologies, such as hacking, identity and personal data theft, fraud and the improper disclosure of confidential information. By enhancing privacy, it promotes the security of technology users.[[257]](#footnote-263)

Second, the encryption can be combined with anonymization techniques.[[258]](#footnote-264) The personal identifies can be de-anonymized and identified only when required by a court warrant to unmask the users. Such a design is not absolute because the hacker can also de-anonymize the information, yet it increases the price hackers pay for data misuse and reduces the risk of identity theft.[[259]](#footnote-265)

## E. Global Law Enforcement

The fifth limitation, or difficulty, concerning imposing the proposed obligations on wallet providers, exchanges and issuing firms is a pragmatic one. Enforcement of identity verification and unmasking obligations raises jurisdictional enforcement difficulties. Indeed, as terrorists use cryptocurrencies globally and do not limit their financial activities to a single territory, cross-border enforcement of the proposed regulation on wallet providers in different jurisdictions presents challenges.

Yet, as in other domains, there are multiple tools for coordination among regulators and law enforcement agencies.[[260]](#footnote-266) For example, in the context of child pornography and other criminal activities, states can rely on the assistance of other states in accordance with the Convention on Cybercrime, which requires states to cooperate to promote criminal investigations and procedures.[[261]](#footnote-267)

In the context of finance, a global policy framework grounded in U.N. Security Council resolutions, national legislation, and global standards had been established to block terrorist access to the formal financial system.[[262]](#footnote-268) Yet, agencies, financial intelligence units, and law enforcement officials should work to stay ahead of the evolving threat of financing of terrorism, which is influenced by changes in the global financial market and the emergence of new financial technologies. Thus, they should also work together to develop a framework for cooperation in the enforcement of obligations of cryptocurrency wallet providers, exchanges and issuing firms.[[263]](#footnote-269) International collaboration is crucial in order to successfully impose and enforce rules for combating the financing of terrorism and strengthening the global fight against terrorism as a whole.[[264]](#footnote-270) The need to develop a global framework to address the challenge of terrorist cryptocurrency use does not undermine the proposed regulation. Quite the contrary, a global framework of international enforcement and collaboration would enable complete global application of the proposed regulation, rendering it more efficient.

# Conclusion

Terrorism is not new, its roots of terrorism were planted at least 2,000 years ago.[[265]](#footnote-271) Yet the speed in which technologies emerge is new, expanding the extensive global reach of terrorism, and rendering it more widespread, dangerous and deadly.[[266]](#footnote-272) New technologies raise new questions and problems that legislators, policy makers and law enforcement and intelligence agencies must address in order to mitigate national security risks. This Article focused on the problem of cryptocurrencies as an enabler for the flow of terrorist funding. It argued that the law should respond to changes in the ecosystem of financing of terrorism and address the challenges arising from terrorist use of cryptocurrencies and the threat it poses to national security. Because cryptocurrencies are built on peer-to-peer networks which allow users to trade the tokens without relying on financial institutions as intermediaries, traditional solutions to financing of terrorism, which target the flow of finance, are infeasible. Therefore, policy makers should outline a new framework for addressing the problem of cryptocurrency use for illicit funding.

This Article proposed to impose new user identity verification obligations on wallet providers, cryptocurrency exchanges and the firms issuing the tokens. It proposed that the identity of users should not be available to all, rather it could only be unmasked by a court warrant where there is probable cause that a user was involved in illicit transactions or money transfer. Thus, the proposed framework endeavors to reach a balance between national security concerns and the fundamental Fourth Amendment rights of legitimate users.

Finally, the Article addressed the objections and shortcomings of the proposed framework and responded to them. The Article concludes that the proposed framework has vast potential to meet the challenges posed by illicit cryptocurrency use for financing of terrorism, and to mitigate the growing national security and public safety risks. Such a framework is of course preferable to turning a blind eye to the growing use of cryptocurrency for illicit funding, or banning the use of cryptocurrencies altogether. We therefore conclude with a call for policy makers and legislators to adopt the proposed framework.

1. ┼ Cegla visiting research fellow, Tel Aviv University. [↑](#footnote-ref-1)
2. \* Ph.D.(Law). Postdoctoral Fellow, University of Haifa, Faculty of Law; Federmann Cyber Center Hebrew University, Cyberlaw Fellow; Cheshin Fellow, Hebrew University, Faculty of Law, 2018. [↑](#footnote-ref-2)
3. See <https://en.wikipedia.org/wiki/Islamic_State_of_Iraq_and_the_Levant> [↑](#footnote-ref-3)
4. FATF REPORT Emerging Terrorist Financing Risks (manuscript at 36) [www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf](http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf) [↑](#footnote-ref-4)
5. Also referred to as the dark web. It is an encrypted network of websites connected to one another. The dark net is part of the greater deep web. The deep web includes all unindexed websites that don't pop up when you do an internet search. See Gabriel Weiman, Going Darker? The Challenge of Dark Net Terrorism. [www.wilsoncenter.org/sites/default/files/media/documents/publication/](http://www.wilsoncenter.org/sites/default/files/media/documents/publication/). [↑](#footnote-ref-5)
6. Danna Harman, *US-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.; for expansion and more examples of the use of cryptocurrencies for terrorism, see Zachary K. Goldman, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss, *Terrorists Use of Virtual Currencies, Center for a New American Security* (May, 2017)(manuscript at 12-13). [↑](#footnote-ref-6)
7. It should be noted that Bitcoin is not the only cryptocurrency. There are over 5000 cryptocurrencies in the world right now and this number is rapidly growing. [↑](#footnote-ref-7)
8. Primavera, De Filippi, *Blockchain Technology and Decentralized Governance:* *The Pitfalls of a Trustless Dream. Decentralized Thriving: Governance and Community on the Web 3.0.* (January 23, 2019), <https://ssrn.com/abstract=3524352>  Are these two separate articles? It looks like two titles but it’s confusing. [↑](#footnote-ref-8)
9. Cynthia Dion-Schwarz, David Manheim, Patrick B. Johnston, Terrorists Use of Cryptocurrencies, Technical and Organizational Barriers and Future Threats, RAND National Security Research Division (NSRD)(2019) at 57("Bitcoin, which was launched by the pseudonymous Satoshi Nakamoto in early 2009, is both a protocol for securely storing and transmitting tokens (virtual coins) and the name of the unit of value in the system."). [↑](#footnote-ref-9)
10. *See id.* at 2 e.g Omni Layer (MasterCoin), BlackCoin, Zcash, Ether, Libra and many more. [↑](#footnote-ref-10)
11. "The Trust Machine” The Economist (Oct. 31, 2015). [↑](#footnote-ref-11)
12. De Filippi supra note 7 id. [↑](#footnote-ref-12)
13. Don Tapscott & Alex Tapscott, *How the Tech Behind Bitcoin Will Change Your Life,* Time (May 6, 2016) [time.com/4320254/blockchain-tech-behind-bitcoin/](https://time.com/4320254/blockchain-tech-behind-bitcoin/). [↑](#footnote-ref-13)
14. Timothy C. May, ‘*The Crypto Anarchist Manifesto’*, [groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html](http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html). [↑](#footnote-ref-14)
15. Hadar Jabotinsky & Roee Sarel, *How Crisis Affects Crypto: Coronavirus as a Test Case*, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3557929>. [↑](#footnote-ref-15)
16. Brenna Smith, *The Evolution of Bitcoin in Terrorist Financing*, Bellingcat (Aug. 9, 2019) [www.bellingcat.com/news/2019/08/09/the-evolution-of-bitcoin-in-terrorist-financing/](https://www.bellingcat.com/news/2019/08/09/the-evolution-of-bitcoin-in-terrorist-financing/). [↑](#footnote-ref-16)
17. Dion-Schwarz, Manheim, Johnston, *supra* note 8, at 29 (explaining that cryptocurrencies are likely to increase in acceptance, yet right now there are not enough ATM (Automated Teller Machine) kiosks that allow users to purchase crypto currencies by using cash or debit card. [↑](#footnote-ref-17)
18. Goldman, et al., *Terrorists Use of Virtual Currencies, supra* note 5 (manuscript at 4). [↑](#footnote-ref-18)
19. Dion-Schwarz, Manheim, Johnston, *supra* note 8, at 7. [↑](#footnote-ref-19)
20. On recent incitement to terrorism on social media and the attacks that followed, see Michal Lavi*, Do Platforms Kill?* 43 Harv. J.L Pub. Poly 477(2020). [↑](#footnote-ref-20)
21. Dion-Schwarz, Manheim, Johnston, *supra* note 8, at 9. [↑](#footnote-ref-21)
22. Dion-Schwarz, Manheim, Johnston, *id.* ("We see little current evidence of the adoption of cryptocurrencies by terrorist organizations …but that very well might change as countermeasures shut off funding and as the cryptocurrency technology changes"). [↑](#footnote-ref-22)
23. Joseph J. Norton, Hera Shams, *Money Laundering Law and Terrorist Financing: Post-September 11 Responses - Let Us Step Back and Take a Deep Breath*? 36International Lawyer(ABA)103,104 (2002). [↑](#footnote-ref-23)
24. Olivia G. Chalos, *Bank Liability Under the Antiterrorism Act: The Mental State Requirement Under § 2333(a)*, 85 Fordham L. Rev. 303,326 (2016) (addressing § 2333 donor liability cases and the requirement for knowledge that the consequences were “substantially certain” to result from the donor’s risky conduct, and the donor deliberately disregarded this fact.). [↑](#footnote-ref-24)
25. Dion-Schwarz, Manheim, Johnston, *supra* note 8, id. [↑](#footnote-ref-25)
26. *See* FATF Report, *supra* note 2. [↑](#footnote-ref-26)
27. The [5th Anti-Money Laundering Directive (Directive (EU) 2018/843)](https://ec.europa.eu/info/law/anti-money-laundering-aml-directive-eu-2018-843_en) (June 19, 2018). [↑](#footnote-ref-27)
28. See in a related context of regulation of speech, Jack M. Balkin, *Free Speech is a Triangle*, 118 COLUM. L. REV. 2011 (2018). [↑](#footnote-ref-29)
29. *See* [libra.org/en-US/](https://libra.org/en-US/); The Libra White Paper[: libra.org/en-US/white-paper/#cover-letter](https://libra.org/en-US/white-paper/" \l "cover-letter). [↑](#footnote-ref-30)
30. Carpenter v. United States 138 S. Ct. 2206 (2018); Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH 357,385(2019)(explaining how Carpenter alone presents a fundamental change to Fourth Amendment doctrine. It requires a warrant in many situations where none was required before). [↑](#footnote-ref-31)
31. Lavi*, Do Platforms Kill?*, *supra* note 19, at 505. [↑](#footnote-ref-32)
32. Balkin, *Free Speech is a Triangle*, supra note 27, at 2015 (referring to a related context of speech regulation). [↑](#footnote-ref-33)
33. Balkin, id. at 2013. [↑](#footnote-ref-34)
34. Van Loo, Rory, *The New Gatekeepers: Private Firms as Public Enforcers*, Va. L Rev. (forthcoming). (Referring to the rise of the enforcer-firm regulation that gives a prominent role to the administrative state’s newest gatekeepers). [↑](#footnote-ref-35)
35. See Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2297–99 (2014) (focusing on this model’s role in regulating speech, Balkin explains that states attempt to regulate, coerce or co-opt key players that shape the internet in order to get their infrastructure to surveil, police, and control speakers.) [↑](#footnote-ref-36)
36. *See e.g.* the right to be forgotten in the European Union Case *C-131/12, Google Spain SL v. Agencia Española de Protección de Datos* (May 13, 2014), Michal Lavi, *The Good, The Bad and the Ugly Behavior*, 40 Cardozo L. Rev. 2597,2630(2019). [↑](#footnote-ref-37)
37. Aniket Kesari, Chris Hoofnagle & Damon McCoy, *Deterring Cyber Crime Focus on Intermediaries* 32 Berkeley Tech L J 1093,1131(2017). [↑](#footnote-ref-38)
38. *Id.* at 1096. [↑](#footnote-ref-39)
39. Section 230(c)(1) of the Communications Decency Act (CDA)(47 U.S.C. § 230 (2018)); Jeff Kosseff, The Twenty-Six Words that Created the Internet 246(2019); Eric Goldman, *Why Section 230 Is Better than the First Amendment*, 95 Notre Dame L. Rev. Reflection 33 (2019); Michal Lavi, *Content Providers’ Secondary Liability: Asocial Network Perspective*, 26 Fordham Intell. Prop. Media & Ent. L. J 855, 889 (2016). [↑](#footnote-ref-40)
40. Lavi*, Do Platforms Kill?*, *supra* note 19 at 507; M.R. Leiser & Edina Harbinja, *Content Not Available,* (2019). For criticism, see Danielle Keats Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, 93 NOTRE DAME L. REV. 1035, 1043–45 (2018). [↑](#footnote-ref-41)
41. In fall 2017, the German government drafted the Network Enforcement Act (NetzDG) for accommodating hate speech and fake news. The Act applies to criminally offensive speech as defined in the German Penal Code, including defamation. It stipulates a differential timeframe for intermediaries to remove harmful content. Intermediaries have to make sure that they delete content that appears evidently unlawful within 24 hours of filing of a complaint. See Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken [NetzDG] [Act to Improve Enforcement of the Law in Social Networks], Oct. 1, 2017, NETZWERKDURCHSETZUNGSGESETS VOM 1 at § 3(2)(4) (Ger.), Wolfgang Schulz, *Regulating Intermediaries to Protect Privacy Online – the Case of the German NetzDG*, in Personality And Data Protection Rights on The Internet (forthcoming); *See also* Meg Leta Jones, *Silencing Bad Bots: Global, Legal and Political Questions for Mean Machine Communication*, 23 COMM. L. & POL’Y 159,177 (2018); Evelyn Mary Aswad, *The Future of Freedom of Expression Online*, 17 DUKE L. & TECH. REV. 26,43 (2019) (discussing the adoption of codes of conduct against hate speech by major online corporations to meet the standards proposed by the UN). [↑](#footnote-ref-42)
42. Delfi AS v. Estonia, Eur. Ct. H.R. App. No. 64569/09 ¶ 43 (Grand Chamber 2015) (The European Court of Human Rights held the popular Delfi news website accountable for defamatory statements about a famous Estonian business executive. Following an article about the executive’s business ventures, anonymous users posted in the comments section, including personal threats and offensive language. The court held Delfi responsible even though it removed the comments upon knowledge.). *See also* ECJ Judgment in Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* (Oct. 3, 2019)(the Court of Justice of the European Union held that law does not preclude intermediaries such as Facebook from being ordered to remove identical and, in certain circumstances, equivalent comments previously declared unlawful). [↑](#footnote-ref-43)
43. For example, Singapore allows the government to order intermediaries to remove false statements. Bill No. 10/2019 Protection from Online Falsehoods and Manipulation Bill bit.ly/30hacIC. Part four of the law refers to directions to internet intermediaries and providers of mass media services. See Jason Luger, *Planetary Illiberalism and the Cybercity-state: in and Beyond Territory*, TERRITORY, POLITICS, GOVERNANCE is this part of the title? 1(2019); See recently, Niharika Mandhana, Phred Dvorak, *Ordered by Singapore, Facebook Posts a Correction,* The Wall Street Journal (Nov. 30 ,2019) on.wsj.com/2L9FU4P. For further information on anti-fake news laws, see *The Rise of "Fake News" Laws Across South East Asia,* Public Media Alliance (Dec, 6, 2019) bit.ly/2Xbl3TO (overviewing fake news laws across South East Asia, particularly on media freedom). [↑](#footnote-ref-44)
44. Jacqueline Lipton, Rethinking Cyberlaw - A New Vision for Internet Law 66(2015). [↑](#footnote-ref-45)
45. See e.g. Digital Millennium Copyright Act (DMCA); 17 U.S.C. § 512 (2012), Kesari, Hoofnagle & McCoy, *supra* note 36, at 1095. See also the European Union Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce) 2000 O.J. (L 178) 1. (July 17, 2000). *See* Article 14(1). It should be noted that the EU imposes obligations on intermediaries regarding copyright infringement beyond a notice and takedown regime. See Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (June 7, 2019) (The “Copyright Digital Single Market Directive”) Art 17 of the Copyright Single Market Directive. [↑](#footnote-ref-47)
46. Anne Marie Bridy*, Internet Payment Blockades*, 67 Fla. L. Rev. 1523 (2016). [↑](#footnote-ref-48)
47. Id. at 1525. [↑](#footnote-ref-49)
48. Bridy*, Internet Payment Blockades*, at 1540 (intermediaries tend to coalesce around voluntary enforcement agreements “not inthe shadow of existing law, but in the shadow of potential law").

    For example,the bills Combating Online Infringements and Counterfeits Act (COICA)(Combating Online Infringements and Counterfeits Act (COICA), S. 3804, 111th Cong. (2010), the Stop Online Piracy Act (SOPA)(ne Piracy Act, H.R. 3261, 112th Cong. (1st Sess. 2011), and the Protect Intellectual Property Act (PIPA)(Protect Intellectual Property Act (PIPA)), S. 968, 112th Cong. (2011) all aim to prevent services from completing payment transactions involving customers located within the United States, and target the internet site associated with the [targeted] domain name. Such legislative bills influence intermediaries to block entities that profit from illicit activities. [↑](#footnote-ref-50)
49. See e.g. Perfect 10, Inc. v. Visa Int’l Serv. Ass’n, 494 F.3d 788, 793 (9th Cir. 2007)(Perfect 10 sued Visa, MasterCard, and other payment intermediaries (collectively: “Visa”) on the theory that they were contributorily and vicariously liable for infringements occurring on so called Stolen Content Websites to which Visa provided payment processing services. The majority dismissed the case, Judge Kozinsky dissented). [↑](#footnote-ref-51)
50. Kesari, Hoofnagle & McCoy, *supra* note 36, at 1127. [↑](#footnote-ref-52)
51. History of the FATF <https://www.fatf-gafi.org/about/historyofthefatf/>; James T. Gathii, *The Financial Action Task Force and Global Administrative Law*, J. Prof. Law 197 (2010). [↑](#footnote-ref-53)
52. Dion-Schwarz, Manheim, & Johnston, *supra* note 8 (referring to Arabinda Acharya, Targeting Terrorist Financing: International Cooperation and New Regimes, New York: Routledge, 2009). [↑](#footnote-ref-54)
53. Kesari, Hoofnagle & McCoy, at 1106. [↑](#footnote-ref-55)
54. Dion-Schwarz, Manheim, Johnston, *supra* note 8. [↑](#footnote-ref-56)
55. Kesari, Hoofnagle & McCoy, *supra* note 36, at 1096. [↑](#footnote-ref-57)
56. Dion-Schwarz, Manheim, & Johnston, at 10 referring to Code of Federal Regulations, Title 31, Money and Finance: Treasury; Subtitle B, Regulations Relating to Money and Finance; Subchapter X, Financial Crimes Enforcement Network, Department of the Treasury; Parts 1010, 1021, and 1022, Bank Secrecy Act Regulations;

    Definitions and Other Regulations Relating to Money Services Businesses. [↑](#footnote-ref-58)
57. “The International Monetary Fund estimates that money laundering amounts to between 2 to 5 percent of the global gross domestic product, or roughly $1.45 and $3.6 trillion per year.” Norman Abrams, Sara Sun Beale, Susan Riva Klein, Federal Criminal Law and its Enforcement 603 (6th ed. 2015). [↑](#footnote-ref-59)
58. In 1970, Congress passed the Bank Secrecy Act requiring financial institutions to report to the government on cash transactions exceeding USD 10,000 (31 U.S.C. § 5311 (2018), see especially 31 U.S.C. § 5313; 31 CFR § 1010.311). In 1996, federal regulations began requiring banks to report suspicious activities (12 CFR §§ 21.11, 163.180). [↑](#footnote-ref-60)
59. Goldman, et al., *Terrorists Use of Virtual Currencies, supra* note 5 ( “following the money” has been a particularly effective component of an overall strategy to degrade the capabilities of terrorist groups)(manuscript at 4). [↑](#footnote-ref-61)
60. Norton & Shams, *supra* note 22, at 104. [↑](#footnote-ref-62)
61. Id. at 105. [↑](#footnote-ref-63)
62. See Olivia G. Chalos, *Bank Liability Under the Antiterrorism Act: The Mental State Requirement Under § 2333(a)*, 85 Fordham L. Rev. 303,317 (2016) (referring to 18 U.S.C. § 1956(a)(2) which prohibits the transportation, transmission, or transfer of funds from a place inside the United States to a place outside the United States “with the intent to promote the carrying on of specified unlawful activity. The statue criminalizes “reverse”

    money laundering, or the movement of “clean” money overseas for an illicit purpose). [↑](#footnote-ref-64)
63. Uniting and Strengthening America by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism Act of 200, precedes a seven-letter acronym (PATRIOT). [↑](#footnote-ref-65)
64. USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001); 18 U.S.C. § 1, Norton &Shams, *supra* note 22, at 104. [↑](#footnote-ref-67)
65. Norton & Shams *id*. At 107. [↑](#footnote-ref-68)
66. *Id.* At 116. [↑](#footnote-ref-69)
67. I*d.* At 108. [↑](#footnote-ref-70)
68. *See* 12 U.S.C. § 635(i) (2012); 31 C.F.R. § 1020.200 et. seq. (2016); Kesari, Hoofnagle & McCoy, *supra* note 36, at 1096; Bridy*, Internet Payment Blockades* *,supra* note 45, at 1565; Norton & Shams, *supra* note 22, at 106, 121 ("financial institutions are required to consult the list of suspected terrorists and terrorist organizations provided **by** *"any* government agency" (emphasis added) to determine whether a potential customer appears on the list. This could result in an enormous regulatory burden that is too soon to assess. The financial institutions are already aware of problems imposed **by** the variations in spelling of Arabic names."). [↑](#footnote-ref-71)
69. Goldman, et al., *Terrorists Use of Virtual Currencies, supra* note 5 (manuscript at 30). [↑](#footnote-ref-72)
70. USA PATRIOT Act, tit. III, 115 Stat**.** at 296-342. Norton & Shams *id.* [↑](#footnote-ref-73)
71. Norton & Shams, *supra* note 22, at 106. [↑](#footnote-ref-74)
72. Norton & Shams, *supra* note 22, at 106. [↑](#footnote-ref-75)
73. Id. at 118. [↑](#footnote-ref-76)
74. 18 U.S.C. §§ 1956, 1957 (2018). [↑](#footnote-ref-77)
75. 31 U.S.C. § 5324 (2018). [↑](#footnote-ref-78)
76. *See, e.g.*, *United States v. Silver*, 864 F.3d 102, 115 (2d Cir. 2017), *cert. denied*, 138 S. Ct. 738(2018); *United States v. Haddad*, 463 F.3d 783, 792 (7th Cir. 2006); *United States v. Pizano*, 421 F.3d 707, 723 (8th Cir. 2005); *United States v. Loe*, 248 F.3d 449, 467 (5th Cir. 2001); *United States v. Davis*, 226 F.3d 346, 357 (5th Cir. 2000); *United States v. Rutgard*, 116 F.3d 1270, 1292 (9th Cir. 1997); *United States v. Sokolow,* 91 F.3d 396, 409 (3d Cir. 1996); *United States v. Moore*, 27 F.3d 969, 976–77 (4th Cir. 1994); *United States v. Johnson*, 971 F.2d 562, 570 (10th Cir. 1992); *United States v. Jackson*, 935 F.2d 832, 840 (7th Cir. 1991)). See also Sarah Scharf, *The Question of Commingled Funds in the Criminal Prosecution of Individuals for Money Laundering*, working paper (manuscript with authors). [↑](#footnote-ref-79)
77. *Moore*, 27 F.3d at 976-977. [↑](#footnote-ref-80)
78. Such an approach has been adopted by the Second, Third, Seventh, Eighth, and Tenth Circuits. See *Silver*, 864 F.3d at 115; *Pizano*, 421 F.3d at 723; *Sokolow,* 91 F.3d at 409; *Johnson*, 971 F.2d 562 at 570; *Jackson*, 935 F.2d at 840; Scharf *supra* note 75 at 2. [↑](#footnote-ref-81)
79. *Rutgard*, 116 F.3d at 1292. [↑](#footnote-ref-82)
80. *United States v. Davis*, 226 F.3d 346, 357 (5th Cir. 2000) (“[W]hen the aggregate amount withdrawn from an account containing commingled funds exceeds the clean funds, individual withdrawals may be said to be of tainted money, even if a particular withdrawal was less than the amount of clean money in the account.”). *See also* *United States v. Loe*, 248 F.3d 449, 467 (5th Cir. 2001); Scharf *supra* note 75 at 2. [↑](#footnote-ref-83)
81. See e.g., *Deposit Agreement and Disclosures*, Commerce Bank, J., <https://www.commercebank.com/personal/bank/deposit-agreement> (Last visited May 20, 2020); Scharf *supra* note 75 at 2. [↑](#footnote-ref-84)
82. 18 U.S.C. §1345 (2018). [↑](#footnote-ref-85)
83. *Luis v. United States*, 136 S. Ct. 1083, 1103 (2016). [↑](#footnote-ref-86)
84. *Id.* at 1109; Scharf *supra* note 75 at 3. [↑](#footnote-ref-87)
85. 18 U.S.C. § 2339A (2018); Ronbert H. Schwartz, *Laying the Foundation for Social Media Prosecutions Under 18 U.S.C. § 2339B*,48 Loyola Chi L. J. 1181, 1186 (2017); Lavi*, Do Platforms Kill?*, *supra* note 19, at 510. [↑](#footnote-ref-88)
86. 18 U.S.C. § 2339C(a). [↑](#footnote-ref-89)
87. Mens rea is the criminal intent or state of mind of the person committing the crime. [↑](#footnote-ref-90)
88. 18 U.S.C. § 2339B (2018); Lavi, *Do Platforms Kill? id*. an organization that the Secretary of State has designated as foreign terrorists*.* The list of FTOs maintained by the State Department encompasses sixty-one such groups (Bureau of Counterterrorism, US Dep’t of State, *Foreign Terrorist Organizations).*  [↑](#footnote-ref-91)
89. *See* Rachel E. VanLandingham, *Jailing the Twitter Bird: Social Media, Material Support to Terrorism and Muzzling the Modern Press*, 39 CARDOZO L. REV. 1, 48 (2017). [↑](#footnote-ref-92)
90. Dion-Schwarz, Manheim, & Johnston *supra* note 8 referring to Eli Berman, *Radical, Religious, and Violent: The New Economics of Terrorism*, Cambridge, Mass.: MIT Press, 2009. [↑](#footnote-ref-93)
91. *Holder v. Humanitarian Law Project* (*HLP*)561 U.S. 1 (2010); Chalos, *Bank Liability Under the Antiterrorism Act* at 32 ("§ 2339B only requires knowledge of the terrorist group’s *status* as a foreign terrorist organization or participation in terrorist-related activities—not specific intent for violent acts"). [↑](#footnote-ref-94)
92. *Holder Id.* at 7–8; Lavi*, Do Platforms Kill?*, *supra* note 19, at 510. [↑](#footnote-ref-95)
93. *Id.* at 30–31; Lavi*, Do Platforms Kill?*, *supra* note 19, at 511. [↑](#footnote-ref-96)
94. Lavi*, Do Platforms Kill?*, *id,* Olivia G. Chalos, *Bank Liability Under the Antiterrorism Act: The Mental State Requirement Under § 2333(a)*, 85 Fordham L. Rev. 303,315 (2016) ("The provision is designed to criminalize all financial supporters of terrorists, including those who fund terrorism in the guise of philanthropic and charitable activities. It is the most frequently charged of the terrorist financing statutes"). [↑](#footnote-ref-97)
95. Lavi *id.* at 511; Alexander Tsesis, *Social Media Accountability for Terrorist Propaganda*, 86 FORDHAM

    L. REV. 605, 620 (2017); Susan Klein & Crystal Flinn, *Social Media Compliance Programs and the War Against Terrorism*, 8 HARV. NAT’L SECURITY J. 53, 85(2017). [↑](#footnote-ref-98)
96. Lavi *id.* [↑](#footnote-ref-99)
97. Chalos, *Bank Liability Under the Antiterrorism Act*, *id.* At 307. [↑](#footnote-ref-100)
98. Chalos, *id. at* 306 (2016). [↑](#footnote-ref-101)
99. See the case of *Linde v. Arab Bank PLC*, No. 04-CV-02799 (E.D.N.Y. Sept. 22, 2014) (the court imposed liability on a bank for material support. The bank provided funding to Hamas, which used the money for terror attacks between 2000 and 2004. The bank funded several other FTOs in addition to Hamas. *Linde v. Arab Bank PLC*, No. 04-CV-02799 (E.D.N.Y. Sept. 22, 2014); See also *Linde v. Arab Bank, PLC* 384 F. Supp. 2d 571 (E.D.N.Y. 2005). (It should be noted that in Linde, the bank was more than a financial institution and actually cooperated with the FTO.) [↑](#footnote-ref-102)
100. For expansion on the divide in the interpretation of “mental element”, *See* Chalos id. at 307; Schwartz, *Laying the Foundation for Social Media, supra* note 84, at 1088. [↑](#footnote-ref-103)
101. Chalos id. At 308. [↑](#footnote-ref-104)
102. Hadar Y. Jabotinsky, *The Regulation of Cryptocurrencies: Between a Currency and a Financial Product*, Fordham Inte'll Prop. Media & Ent. (forthcoming). [↑](#footnote-ref-105)
103. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008), [git.dhimmel.com/bitcoin-whitepaper/](https://git.dhimmel.com/bitcoin-whitepaper/). [↑](#footnote-ref-106)
104. *Roee Sarel, “Your Bitcoin is Mine: What Does Law and Economics Have to Say on Protecting Rights in Crypto-currencies?* (2020)(manuscript at 5) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3542545>. [↑](#footnote-ref-107)
105. For overviews and further details on the blockchain technology, and for a detailed explanation of how it works, see generally Dylan Yaga et al., *Blockchain Technology Overview* (2019), <https://arxiv.org/ftp/arxiv/papers/1906/1906.11078.pdf>; Lin William Cong & Zhiguo He, *Blockchain Disruption and Smart Contracts*. 32(5) Rev. Financ. Stud. 1754 (2019). For an overview of Bitcoin in particular, see Christian Rueckert, *Cryptocurrencies and Fundamental Rights,* 5(1) J. Cybersecurity 1 (2019). [↑](#footnote-ref-108)
106. Dion-Schwarz, Manheim, Johnston, *supra* note 8; Robby Houben, Alexander Snyers, Cryptocurrencies and Blockchain, Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion, July 2018 (manuscript at 15). [↑](#footnote-ref-109)
107. *Id.*at 2. [↑](#footnote-ref-110)
108. Shaanan Cohney & David A. Hoffman, *Transactional Scripts in Contract Stacks*, [U. of Penn, Inst. for Law & Econ. Research Paper No. 20-08](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3523515" \l "#)(2020)(manuscript at 16) ("a programmer named Vitalik Buterin proposed and developed Ethereum, a blockchain based computing platform, with an associated cryptocurrency, *ether*…The protocol’s explicit goal was to permit enhanced scripting—more complicated logical operations than recording ownership—on a blockchain" *See generally,* Gavin Wood et al., *Ethereum: A Secure Decentralised Generalised Transaction Ledger,* 151(2014) Ethereum Project Yellow Paper 1-32 (2014). [↑](#footnote-ref-111)
109. *Smart Contracts: 10 Use Cases for Business*, AMBISAFE, https://ambisafe.com/blog/smartcontracts-

     10-use-cases-business/ ("Smart contracts do not require any intermediaries. Hence, you pay **no fees.**As there’s no bureaucracy involved,**transactions become fast and cheap.** Moreover, the transparency guaranteed by the blockchain reduces the possible risks of fraud.")*;* Alexander Savelyev, *Contract Law 2.0: “Smart” Contracts as the Beginning of the End of Classic Contract Law*, 26 INFO. & COMMC’N. TECH. L. 116 (2017). *Ethereum Smart Contract Best Practices*, GitHub: ConsenSys: Ethereum Smart Cont. Best Pracs., https://consensys.github.io/smart-contract-bestpractices. [↑](#footnote-ref-112)
110. Primavera De Filippi & Samer Hassan, *Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code*, First Monday (Dec. 5, 2016), https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657 (“[S]mart contracts are actually meant to replace legal contracts.”). [↑](#footnote-ref-113)
111. Jabotinsky, *supra* note 101, at 17. [↑](#footnote-ref-114)
112. Jabotinsky, supra note 14, manuscript at 24. [↑](#footnote-ref-115)
113. Josh Constine, *Facebook Announces Libra Cryptocurrency: All You Need to Know*, Techcrunch (June 18, 2019), [techcrunch.com/2019/06/18/facebook-libra/](https://techcrunch.com/2019/06/18/facebook-libra/). [↑](#footnote-ref-116)
114. John Taskinsoy, *This Time is Different: Facebook’s Libra Can Improve Both Financial Inclusion and Global Financial Stability as a Viable Alternative Currency to the U.S. Dollar. Journal of Accounting*, 5 Finance & Auditing Studies (forthcoming) available at: [papers.ssrn.com/sol3/papers.cfm?abstract\_id=3434493](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3434493) ("With a user base of close to 3 billion (i.e. Messenger, WhatsApp, Instagram, and Facebook), Facebook’s Libra is forecasted to dominate daily transactions for goods/services and money transfers online"). [↑](#footnote-ref-117)
115. Jabotinsky, *supra* note 14, manuscript at 23. Cryptocurrencies which are pegged to other assets are also known as “stable coins”. [↑](#footnote-ref-118)
116. Jabotinsky, *supra* note 14, manuscript at 24. [↑](#footnote-ref-119)
117. Sarel, *supra* note 103, at 6. [↑](#footnote-ref-120)
118. Id. at 7. [↑](#footnote-ref-121)
119. Id. [↑](#footnote-ref-122)
120. See generally, Van Wegberg et al., *Bitcoin Money Laundering: Mixed Results? An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin*, 25 J. Fin. Crime 17 (2018). [↑](#footnote-ref-123)
121. See generally, Thomas Slattery, *Taking a Bit out of Crime: Bitcoin and Cross-Border Tax Evasion*, 39 Brook. J. Int’l L. 829 (2014). [↑](#footnote-ref-124)
122. Sarel, *supra* note 103, manuscript at 6-7. [↑](#footnote-ref-125)
123. FATF Report, Emerging Terrorist Financing Risks (2015) [www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf](http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf), [↑](#footnote-ref-126)
124. Goldman, et al. *Terrorists Use of Virtual Currencies supra* note 5 (manuscript at 10). [↑](#footnote-ref-127)
125. Goldman, id. [↑](#footnote-ref-128)
126. Dion-Schwarz, Manheim, Johnston, *supra* note 8(at13). [↑](#footnote-ref-129)
127. FATF REPORT, *supra* note 122(at 35). [↑](#footnote-ref-130)
128. Paul Carroll & James Windle, *Cyber as an Enabler of Terrorism Financing, Now and in the Future*.13 J. of Policing, Intelligence and Counter Terrorism, 285-300(2018). [↑](#footnote-ref-131)
129. Stephan Breu & Theodor G. Seitz, *Legislative Regulations to Prevent Terrorism and Organized Crime from Using Cryptocurrencies and Its Effect on Economy and Society*, in Legal Impact on the Economy (Vaypan & Egorova eds., 2018) (manuscript at 4). [↑](#footnote-ref-132)
130. Dion-Schwarz, Manheim, Johnston, *supra* note 8 (manuscript at 25); Brenna Smith, *The Evolution of Bitcoin in Terrorist Financing*, Bellingcat (Aug. 9, 2019) www.bellingcat.com/news/2019/08/09/the-evolution-of-bitcoin-in-terrorist-financing/; Carroll & Windle, *supra* note 127 ("Cryptocurrencies provide increased, rather than complete, anonymity as they are added to blockchains which can be used to trace the originating electronic wallet from which the cryptocurrency was sent".) [↑](#footnote-ref-133)
131. Dark wallet, homepage, undated. As of February 22, 2015:

     <https://www.darkwallet.is> *See also* Dion-Schwarz, Manheim, Johnston, *supra* note 8, at 21 ("In a grossly misinformed article, Ali Shukri Amin, writing under the pen-name Taqi’ulDeen alMunthir, claimed that darkwallet allowed “totally anonymous” use of bitcoin, which would be accomplished if users “simply . . . set up a wallet and post their wallet address online” (Taqi’ulDeen alMunthir, “Bitcoin wa Sadaqat alJihad: Bitcoin and the Charity of Violent Physical Struggle,” blog post, originally on Al Khila Faharidat Wordpress blog, 2014). [↑](#footnote-ref-134)
132. Goldman et. al *supra* note 5 (manuscript at 15). [↑](#footnote-ref-135)
133. Dion-Schwarz, Manheim, Johnston, *supra* note 8 at 32. [↑](#footnote-ref-136)
134. For expansion on the Material Support Statues, see infra part I.A (1)(b). [↑](#footnote-ref-137)
135. Dion-Schwarz, Manheim, Johnston, *supra* note 8 at 32. [↑](#footnote-ref-138)
136. For such limitation, see infra part I.A.(1). [↑](#footnote-ref-139)
137. Dion-Schwarz, Manheim, Johnston at 32. [↑](#footnote-ref-140)
138. Dion-Schwarz, Manheim, Johnston at 33. [↑](#footnote-ref-141)
139. See Gabriel Weiman, Going Darker? The Challenge of Dark Net Terrorism www.wilsoncenter.org/sites/default/files/media/documents/publication/ going\_darker\_challenge\_of\_dark\_net\_terrorism.pdf (at 4). [↑](#footnote-ref-142)
140. The dark web can be accessed by any internet user by using special software such as Tor (short for The Onion Router) or I2P (Invisible internet Project), a tool for anonymously communicating online. Weiman, Going Darker, *supra* note 147(at 8). [↑](#footnote-ref-143)
141. Weiman, id. [↑](#footnote-ref-144)
142. Weiman, id. At 7. [↑](#footnote-ref-145)
143. Goldman et al. *supra,* note 5. [↑](#footnote-ref-146)
144. Krishnan, Armin, *Blockchain Empowers Social Resistance and Terrorism Through Decentralized Autonomous Organizations*,13 J. of Strategic Security 41,44(2020). [↑](#footnote-ref-147)
145. Krishnan, Armin, at 45(giving an example of ISIS, which reportedly solicited donations by posting a Bitcoin address). [↑](#footnote-ref-148)
146. Brenna Smith, *The Evolution of Bitcoin in Terrorist Financing*, Bellingcat (Aug. 9, 2019). [www.bellingcat.com/news/2019/08/09/the-evolution-of-bitcoin-in-terrorist-financing/](https://www.bellingcat.com/news/2019/08/09/the-evolution-of-bitcoin-in-terrorist-financing/) [↑](#footnote-ref-149)
147. Carroll & Windle, *supra* note 127. [↑](#footnote-ref-150)
148. See Weiman, id. (manuscript at 4). [↑](#footnote-ref-151)
149. Carroll & Windle, *supra* note 127. [↑](#footnote-ref-152)
150. Dion-Schwarz, Manheim, Johnston, *supra* note 129 at 27, See also Carroll & Windle, *supra* note 127. [↑](#footnote-ref-153)
151. At this point, terrorists differ from criminals and that is the main reason for the slow adoption of cryptocurrencies by terrorists relative to criminals. [↑](#footnote-ref-154)
152. *See* Goldman et al., *supra* note 5 at 6. ("This is true, for example, of al Qaeda in the Islamic

     Maghreb (AQIM) in the Sahel, in the Arabian Peninsula (AQAP) in Yemen, and, in some measure, ISIS in Iraq and Syria.") See also FATF REPORT Emerging Terrorist Financing Risks (2015) (manuscript at 7)("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."). [↑](#footnote-ref-155)
153. Stephan U. Breu *supra* note 128(manuscript at 2). [↑](#footnote-ref-156)
154. 115th Congress 1st Session Miss Kathleen Rice from New York introduced the following bill to direct the Under Secretary of Homeland Security for Intelligence and Analysis to develop and disseminate a threat assessment regarding terrorist use of virtual currency.

     “Homeland Security Assessment of Terrorists Use of Virtual Currencies Act”. See Breu, *Legislative Regulative Regulation to Prevent Terrorism, supra* note 128. [↑](#footnote-ref-157)
155. Dion-Schwarz, Manheim, Johnston, *supra* note 129 at 3 referring to US House of Representatives, Financial Innovation and Defense Act, H.R. 4752, January 20, 2018. It should be noted that there are other regulatory issues relating to cryptocurrencies such as investor protection and prevention of fraud. These issues have also taken time to be resolved and are still in an ongoing process. For example, In April 2019 the SEC finally issued its long-awaited framework for “investors contract” analysis of digital assets (April 3, 2019), <https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets>. [↑](#footnote-ref-158)
156. Blake Hamil, *EU Cryptocurrency Regulation: Creating a Heaven for Businesses or Criminals?,* 48 GA. J. INT’L & COMP. L 833, 837 - 838 (2020). [↑](#footnote-ref-159)
157. *Id*. at 838. [↑](#footnote-ref-160)
158. BSA Requirements for MSBs, Fin. Crimes Enf’t Network, <https://www.fincen.gov/bsa-requirements-msbs> (last visited June 08, 2020). [↑](#footnote-ref-161)
159. Stephan U. Breu, *supra* note 128 (manuscript at 3) referring to EBA European Banking Authority “EBA Opinion on Virtual Currencies”, published by EBA in July 2014 states on page 33 “Criminals or terrorists use the VC remittance systems and accounts for financing purposes (C03). The risk arises because, as a means of payment, VC schemes are not confined to, and are accepted across, jurisdictional borders. VC transactions require nothing more than internet access, the VC infrastructure is often spread across the globe, making it difficult to intercept transactions, and VC transactions tend not to be reversible. The priority of the risk is high.” www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf [↑](#footnote-ref-162)
160. Jabotinsky, *supra* note 14, manuscript at 3; Saman Adhami et al., *Why do businesses go crypto? An empirical analysis of initial coin offerings,* 100 *Journal of Economics and Business* 64–75 (2018). [↑](#footnote-ref-163)
161. Stephan U. Breu *supra* note 128 id. [↑](#footnote-ref-164)
162. Stephan U. Breu *id. (*manuscript at 5). [↑](#footnote-ref-165)
163. Stephan U. Breu, *id* (manuscript at 5) referring to FINMA Press Release of September 29, 2017: “The Financial Market Supervisory Authority FINMA has observed a marked increase in initial coin offerings (ICOs) conducted in Switzerland. It has today therefore issued FINMA Guidance 04/2017 on this topic. FINMA has also indicated that it is investigating a number of ICO cases to determine whether regulatory provisions have been breached.”www.finma.ch/en/news/2017/09/20170929-mm-ico/ [↑](#footnote-ref-166)
164. The European Union recently issued its 5th Anti-Money Laundering Directive, which now mandates that crypto exchanges and custodial wallet providers adhere to the same regulatory requirements as banks and other financial institutions. All EU member states are required to implement the directive by January 10, 2021 (The [5th anti-money laundering Directive (Directive (EU) 2018/843)](https://ec.europa.eu/info/law/anti-money-laundering-aml-directive-eu-2018-843_en) (June 19, 2018). In Singapore, anyone issuing a cryptocurrency which is considered a security must adhere to Anti-Money Laundering regulation and fill in a KYC on all people buying the token from the issuing firm (The Payment Services Act 2019 (Sing.)). [↑](#footnote-ref-167)
165. Goldman et. al *supra* note 5. [↑](#footnote-ref-168)
166. Robby Houben, Alexander Snyers, Cryptocurrencies and Blockchain, Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion, July 2018 (at 11). [↑](#footnote-ref-169)
167. Goldman et, al *supra* note 5. [↑](#footnote-ref-170)
168. Robby Houben, Alexander Snyers, *Cryptocurrencies and Blockchain, Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion*, July 2018 (manuscript at53). [↑](#footnote-ref-171)
169. Houben, id. (manuscript at 14). [↑](#footnote-ref-172)
170. Goldman et al. *supra* note 5 (manuscript at 30). [↑](#footnote-ref-173)
171. Houben et al*. supra* note 167 (manuscript at 9). [↑](#footnote-ref-174)
172. *Guidance FIN-2013-G001*, U.S. Dept. Of Treasury, Fin. Crimes Enf't Network, (Mar. 18, 2013), <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf> (at 3); Shahla Hazratjee*, Bitcoin: The Trade of Digital Signatures*, 41 T. Marshall L. Rev. 55,75 (2016). [↑](#footnote-ref-175)
173. Scott D. Hughes, *Cryptocurrency Regulations and Enforcement in the U.S* 45 W. St. L. Rev. 1 (2017)("Bitcoin transactions are not facilitated within a consumer protection framework and measures, such as anti-money laundering (AML) or know-your-customer (KYC) policies, are not inherent to the system. Once a transaction is sent, there is no way to perform a chargeback."). [↑](#footnote-ref-176)
174. Olly Jackson, *Cryptocurrency Exchanges Avoiding the US Due to Confusing Regulation*, International Financial L Rev. (Mar 26, 2018). [↑](#footnote-ref-177)
175. Dion-Schwarz, Manheim, Johnston, *supra* note 8 (at 49). [↑](#footnote-ref-178)
176. Robby Houben, *supra* note 167. [↑](#footnote-ref-179)
177. Robby Houben *Id*. At 11("mandatory registration and a pre-set date as of which it applies would be a better approach to unveil the anonymity of cryptocurrency users.") [↑](#footnote-ref-180)
178. Read more about the SAGA initiative here: <https://www.saga.org/> (Last accessed May 24, 2020). [↑](#footnote-ref-181)
179. Identification can be conducted via video conferencing by having a KYC conversation with potential users during which they would also hold up identification documents such as an ID and a passport. Another method, practiced by Saga, is using a selfie taken by the client while also holding a written sentence provided exclusively to him/her by Saga together with an identification document. Saga only identifies clients who buy/sell tokens directly from them, but also makes sure to approve the AML policy of exchanges on which the Saga token is traded. [↑](#footnote-ref-182)
180. [Directive (EU) 2018/843)](https://ec.europa.eu/info/law/anti-money-laundering-aml-directive-eu-2018-843_en) (June 19, 2018). [↑](#footnote-ref-183)
181. [Directive (EU) 2018/843)](https://ec.europa.eu/info/law/anti-money-laundering-aml-directive-eu-2018-843_en) (June 19, 2018) Article 2 (d) (19): ““custodian wallet provider” means an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies...” [↑](#footnote-ref-184)
182. 5th Anti-Money Laundering Directive Fact Sheet 2 (July 9, 2018): [file:///C:/%D7%94%D7%93%D7%A8/My%20Documents/%D7%94%D7%93%D7%A8/articles/AML%20and%20regulation%20of%20crypto/Factsheet\_AMLD\_201807\_2pdf.pdf](file:///C:\\%D7%94%D7%93%D7%A8\\My%20Documents\\%D7%94%D7%93%D7%A8\\articles\\AML%20and%20regulation%20of%20crypto\\Factsheet_AMLD_201807_2pdf.pdf) [↑](#footnote-ref-185)
183. *Carpenter v. United States* 138 S. Ct. 2206 (2018) (accessing historical records containing physical locations of cellphones necessitates a search warrant). [↑](#footnote-ref-186)
184. U.S. CONST. amend. IV. [↑](#footnote-ref-187)
185. *See* Travis Panneck, *Incognito Mode Is in the Constitution*, Minn. L Rev, 511,537 (2019). [↑](#footnote-ref-188)
186. Neil Richards & Woodrow Hartzog, *Privacy’s Constitutional Moment*, 61 B.C. L. REV. (forthcoming 2020)(manuscript at 44)(explaining that the American constitutional system has no explicit constitutional right to privacy, however, it protects individuals against governmental violations of privacy); for expansion see Daniel J. Solove, Nothing to Hide ,The False Tradeoff Between Privacy And Security 93 (2011) Where was this published? [↑](#footnote-ref-189)
187. Solove, Nothing to Hide *id.* [↑](#footnote-ref-190)
188. Solove, Nothing to Hide, *supra* note 185, at 96. [↑](#footnote-ref-191)
189. Solove, id. [↑](#footnote-ref-192)
190. Olmstead v. United States, 277 U.S. 438 (1928), Solove: Nothing to Hide, at 97-98 (explaining that this decision enabled the government to gather a lot of private information). [↑](#footnote-ref-193)
191. *Katz v. United States* 389 U.S. 347 (1967) (ruling that warrantless electronic bugging in a public telephone booth are unconstitutional, thus establishing the doctrine of “legitimate expectation of privacy”). [↑](#footnote-ref-194)
192. *Katz v. United States*, at 351-352. [↑](#footnote-ref-195)
193. *Katz v. United States*, at 361. [↑](#footnote-ref-196)
194. Daniel J. Solove, *Understanding Privacy* 71(2008); Solove: Nothing to Hide, at 94,99. Justice Harlan’s concurrence, later adopted by the Court in full in *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (using Justice Harlan’s two-step formulation to frame the Fourth Amendment analysis that includes subjective expectation of privacy and objective reasonableness of such expectation). For expansion, see Panneck, *Incognito Mode, supra* note 184, at 519; Amitai Etzyoni, *iPhone vs. Trump: How Technology Companies Can Protect Both Customer and National Security,* The National Interest (Jan. 19, 2020). [↑](#footnote-ref-197)
195. Solove, Nothing to Hide, *supra* note 185, at 99. [↑](#footnote-ref-198)
196. *Katz v. United States*, supra note 190, Solove, Nothing to Hide id, at 71. [↑](#footnote-ref-199)
197. For an overview on the background of the doctrine; justifications of it and further expansion, see Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV 561, 567–70 (2009); Jane Bambauer, *Other People's Papers, 94* Tex. L Rev*.*205,206(2015). [↑](#footnote-ref-200)
198. Kerr*, id.*(arguing that the third-party doctrine prevents technology from giving up leg to? criminals and makes it possible to level the playing field.). For criticism of such approach, asserting that it gives too much power surveillance power to the government vis a vis innocent citizens, see Solove, Nothing To Hide, at 109. [↑](#footnote-ref-201)
199. Solove id. at 103. [↑](#footnote-ref-202)
200. United States v. Miller 425 U.S. 435, 437 (1976), for further information see Solove id. at 104, Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH357,385,359(2019); Panneck, *Incognito Mode supra* note 184, at 521. [↑](#footnote-ref-203)
201. *United States v. Miller* id. At 442. [↑](#footnote-ref-204)
202. Panneck, *Incognito Mode, supra* note 199at521-522 [↑](#footnote-ref-205)
203. *Smith v. Maryland* 442 U.S. 735 (1979); Solove: Nothing to Hide, at 104. (a pen register revealing a telephone number dialed from the defendant’s home was not within the Fourth Amendment’s scope). [↑](#footnote-ref-206)
204. *Smith v. Maryland* *Id.* at 746.; *Panneck*, *Incognito Mode is in the Constitution*, at 522. [↑](#footnote-ref-208)
205. *Id.* at 743–44; *Panneck, id.* Solove, Nothing to Hide, at 104. [↑](#footnote-ref-209)
206. Solove, Nothing to Hide, at 105. [↑](#footnote-ref-210)
207. For criticism of the third-party doctrine, see Neil Richards, Intellectual Privacy –Rethinking Digital Liberties in The Digital Age136-139(2015); Solove, Nothing to Hide, at 108 (2011)(explaining that if a bank promises confidentiality, the consumer expects it to keep this promise and there should be a reasonable expectation of privacy). [↑](#footnote-ref-211)
208. Ohm, *supra* note 199 at 386. [↑](#footnote-ref-212)
209. *Carpenter v. United States* 138 S. Ct. 2206 (2018). [↑](#footnote-ref-213)
210. Panneck, *Incognito Mode, supra* note 199 at 513. [↑](#footnote-ref-214)
211. *Carpenter v. United States*, 138 S. Ct. 2206, 2223; Ohm, *supra* note 199 at 361; Olivier Sylvain, *The Market for User Data*, 29 Fordham Intell. Prop. Media & Ent. L.J. 1087,1095 (2019). [↑](#footnote-ref-215)
212. *Carpenter v. United States*, 138 S. Ct. 2206, 2217; Ohm, *supra* note 199 at 363. [↑](#footnote-ref-216)
213. Ohm,id. at 361-362; Panneck, *Incognito Mode, supra* note 199 at 528(explaining that the Court recognized that it was not merely concerned with an individual’s movements, but the private personal information one might discover in knowing about that person’s movements.). [↑](#footnote-ref-217)
214. Ohm, id. at 358. [↑](#footnote-ref-219)
215. Ohm id. at 369("[T]he test that emerges from the majority opinion will also be applied to collections of information maintained by third parties that do not track location, not even by inference, but are of interest to law enforcement."). [↑](#footnote-ref-220)
216. *United States v. Miller* 425 U.S. 435, 437 (1976); *Smith v. Maryland* 442 U.S. 735 (1979); Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (“We do not disturb the ap-plication of *Smith* and *Miller* . . . .”); Ohm id. at 359; Panneck, *Incognito Mode supra* note 184, at 541. [↑](#footnote-ref-221)
217. Ohm *supra* note 199 at 381. *See also* at 385 *id*. (explaining that *Carpenter* turns the third-party doctrine inside out, requiring the government to account for the database design and information-gathering decisions of private parties, decisions made without any state intervention.). [↑](#footnote-ref-222)
218. Panneck, *Incognito Mode, supra* note 199, at 547. [↑](#footnote-ref-223)
219. Solove, Nothing to Hide, *supra* note 185, at 109(expanding on the importance of a warrant). [↑](#footnote-ref-224)
220. Pollicino Bassini, *supra* note 473 *id.* For criticism, see Mary Anne Franks, The Cult of The Constitution (2019) (arguing that legislators, courts and civil rights organizations have interpreted the First Amendment selectively, almost like religious fundamentalists, and in fact shifted even more power from vulnerable populations to powerful ones). [↑](#footnote-ref-225)
221. U.S. CONST. amend. I (“Congress shall make no law . . . abridging the freedom of speech, or of the press.”). [↑](#footnote-ref-226)
222. Margot E. Kaminski, *Privacy and the Right to Record*, 97 B.U. L. Rev. 167 (2017). [↑](#footnote-ref-228)
223. *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 557 (2011); Jane Bambauer, *Is Data Speech*? 66 Stan L Rev. 57(2014) (explaining that the First Amendment can protect raw data as it promotes the creation of knowledge). [↑](#footnote-ref-229)
224. *See* Michael Froomkin, *Lessons Learned Too Well: Anonymity in a Time of Surveillance*, 59 Ariz. L. Rev. 95 (2017); Justin S. Wales, *Bitcoin is Speech: Notes Toward Developing the Conceptual Contours of Its Protection Under the First Amendment,* 74 U. Miami L. Rev. 204, 255 (2019); Kyle Langvardt, *The Doctrinal Toll of "Information as Speech"* 47 Loy. U. Chi. L.J. 761,770(2016)(referring to *Bernstein v. U.S. Dep't of State*, 922 F. Supp. 1426, 1435 (N.D. Cal. 1996) *rehr'g en banc granted,* 192 F.3d 1308 (1999) (the court took the position that source code, whether functional or not, is *always* speech protected by the First Amendment, holding that "the functionality of a language does not make it any less like speech."). [↑](#footnote-ref-230)
225. Froomkin, *id.* at 99. [↑](#footnote-ref-231)
226. Froomkin, *Lessons Learned Too Well*, *supra* note 223, at 149. [↑](#footnote-ref-232)
227. *See* e.g *Talley v. California* 362 U.S. 60 (1960)(the US Supreme Court voided a Los Angeles City ordinance which forbade the distribution of any handbills in any place under any circumstances, if the handbills did not contain the name and address of the person they were prepared for); *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995) (the US Supreme Court voided an Ohio statute prohibiting anonymous campaign literature. The Court held that such a law violates the First Amendment and as such is unconstitutional.). See also *Buckley v. Am. Constitutional Law Found. Inc.*, 525 U.S. 182, 198-200, 204 (1999), *Watchtower Bible & Tract Soc'y v. Vill. of Stratton*, 536 U.S. 150, 160, 166-69 (2002). [↑](#footnote-ref-233)
228. Alexander Tsesis, *Marketplace of Ideas, Privacy, and Digital Audiences,* Notre Dame L Rev. 1585,1588 (2019) (differentiating between marketplace behavior and freedom of expression). [↑](#footnote-ref-234)
229. Wales, *Bitcoin is Speech, supra* note 223. [↑](#footnote-ref-235)
230. Wales, *Bitcoin is Speech, supra* note 223, at 222. [↑](#footnote-ref-236)
231. Wales, *Bitcoin is Speech, at* 242. [↑](#footnote-ref-237)
232. Scholars have criticized the court's treatment of market behavior as speech. However, if courts are to treat the financial aspects of cryptocurrency use as speech, they should be treated as commercial speech at most. For criticism on the lack of differentiation between market behavior and speech in a related context of platform immunity to liability for harmful speech, see Danielle Keats Citron, Mary Anne Franks, *The Internet as a Speech Machine and Other Myths Confounding Section 230 Reform,* U. Chi. Legal F. (forthcoming 2020) (manuscript at 6) (" Section 230’s liability shield has been extended to activity that has little or nothing to do with free speech, such as the sale of dangerous products".). [↑](#footnote-ref-238)
233. Tsesis, *Marketplace of Ideas*, *supra* note 227 at 1614 (explaining the intermediary scrutiny test and the focus of speech restrictions on reasonable time, place, and manner restrictions). [↑](#footnote-ref-239)
234. See Bambauer, *Is Data Speech*?, *supra* note 221 (arguing that data can enjoy First Amendment protection when it promotes the right to create knowledge). [↑](#footnote-ref-240)
235. Langvardt, *The Doctrinal Toll*, *supra* note 223, at 770,798. [↑](#footnote-ref-241)
236. Langvardt, *The Doctrinal Toll*, *supra* note 223. [↑](#footnote-ref-242)
237. See e.g. *Bernstein v. U.S. Dep't of State*, 922 F. Supp. 1426, 1435 (N.D. Cal. 1996). [↑](#footnote-ref-243)
238. See in a related context of algorithmic speech, Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics,* MD. L. Rev. (forthcoming)(at 63). [↑](#footnote-ref-244)
239. This metaphor of cathedral and bazaar was coined by Eric S. Raimond in a related context, comparing centralized licensed computer code and Linux. Eric S. Raymond *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*, O'Reilly Media (1999).  [↑](#footnote-ref-245)
240. See Goldman et al. *supra* note 5. [↑](#footnote-ref-246)
241. *See* Infra Part II (expanding on the role of intermediaries as gatekeepers). *See also* Julie E. Cohen: Between Truth and Power: The Legal Constructions of Information Capitalism 75 (2019) 37 (explaining that some aspects of the conception of "technologies of freedom" have changed beyond recognition and today's networked digital information infrastructure has different and more complicated affordances"). [↑](#footnote-ref-247)
242. Primavera, De Filippi, *Blockchain Technology and Decentralized Governance: The Pitfalls of a Trustless Dream* (January 23, 2019) in Decentralized Thriving: Governance and Community on The Web 3.0. ssrn.com/abstract=3524352 ("Over the years, the governance of the most popular blockchain networks has become highly centralized, and only a few large corporations (such as the main blockchain exchanges and wallet providers) are responsible for making blockchain technology accessible to the wider public."). [↑](#footnote-ref-248)
243. For this argument, see Robby Houben, Alexander Snyers, Cryotocurrencies and Blockchain, Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion (July, 2018)(manuscript at 85). [↑](#footnote-ref-249)
244. On payment blockade, see the discussion in infra part I. *See also* Anne Marie Bridy*, Internet Payment Blockades*, 67 Fla. L. Rev. 1523 (2016). [↑](#footnote-ref-250)
245. *See* Houben & Snyers (manuscript at 56). [↑](#footnote-ref-251)
246. See Breu, *Legislative Regulative Regulation to Prevent Terrorism, supra* note 128*.*. [↑](#footnote-ref-252)
247. This is indeed already happening following the 5th European Anti-Money Laundering Directive. Bottle Pay, a UK-based crypto wallet provider, announced its decision to cease operations at the end of last year. According to a [company blog post](https://bottlepay.helpscoutdocs.com/article/40-official-announcement-on-the-shutdown-of-bottle-pay) published on Dec. 13, 2019: “As we are a UK based custodial Bitcoin wallet provider, we will have to comply with the 5AMLD EU regulation coming into effect on January 10, 2020. The amount and type of extra personal information we would be required to collect from our users would alter the current user experience so radically, and so negatively, that we are not willing to force this onto our community.” (Rachel Wolfson, What the 5th Anti-Money Laundering Directive Means for Crypto Businesses, Cointelegraph (Jan.10, 2020)). [↑](#footnote-ref-253)
248. On the role of legal rules in promotion of welfare maximization, see John R. Hicks, *The Foundations of Welfare Economics*, 49 ECON. J. 696, 708 (1939). [↑](#footnote-ref-254)
249. Nathaniel Gleicher, *John Doe Subpoenas: Toward a Consistent Legal Standard* ,118 YALE L.J 320, 344 (2008)(explaining the consideration and standards that US courts apply when considering whether to order John Doe subpoenas). *See also* Lyrissa Barnett Lidsky, *Anonymity in Cyberspace: What Can We Learn from John, Doe*? B.C L. REV. 1373,1375(2009). [↑](#footnote-ref-255)
250. *See* Libra White Paper, available at: libra.org/en-US/white-paper and Saga’s White Paper, available at: <https://www.saga.org/> See also Mike Orcutt, *The Radical Idea Hiding Inside Facebook's Digital Currency Proposal,* MIT Technology Rev. (June. 25,2019). [↑](#footnote-ref-256)
251. For such a concern in a related context, *see* Fennie Wang, Primavera De Filippi, *Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion*, Frontiers in Blockchain (Jan 2020). Is this all one title? [↑](#footnote-ref-257)
252. Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 U.C. IRVINE L. REV. 107 (2019). [↑](#footnote-ref-258)
253. Dion-Schwarz, Manheim, Johnston, *supra* note 8(at 53) (expanding on increasing security breaches and hacks). *See also,* Wang & De Filippi, id. [↑](#footnote-ref-259)
254. On the tremendous damage caused by data breach, see Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 768 (2018). [↑](#footnote-ref-260)
255. *See* Daniel J. Solove, *The Myth of the Privacy Paradox* (Feb. 11, 2020). GWU Legal Studies Research Paper No. 2020-10; GWU Law School Public Law Research Paper No. 2020-10. [↑](#footnote-ref-261)
256. *See* Rocio de la Cruz, *Privacy Laws in the Blockchain Environment*, Annals of Emerging Technologies in Computing (AETiC) Vol. 3, No. 5, 2019 ("encrypting the data by choosing an encryption option that ensures a high level of confidentiality. The solution I recommend here to minimize risks of breaching the law and/or facing a data breach incident, is anonymising the personal data to the maximum extent that still allows the Blockchain achieve to its purpose."). Check the original….. [↑](#footnote-ref-262)
257. See Houben & Snyers, *supra* note 242 (at 55); *see also* Michael Froomkin & Zak Colangelo, *Privacy as Safety*, 95 Wash. L Rev.101,145-147(2020). [↑](#footnote-ref-263)
258. Rocio de la Cruz, Privacy Laws in the Blockchain Environment, *supra* note 255(proposing to combine encryption with anonymization techniques). [↑](#footnote-ref-264)
259. Ira S. Rubinstein & Woodrow Hartzog*, Anonymization and Risk*, 91 Wash. L. Rev. 703 (2016)(arguing that anonymization should focus on the process of minimizing risk of reidentification and sensitive attribute disclosure, not preventing harm). [↑](#footnote-ref-265)
260. *See* Dion-Schwarz, Manheim, Johnston, *supra* note 8, at 55. [↑](#footnote-ref-266)
261. Convention on Cybercrime art. 14, Nov. 23, 2001, E.T.S. 185. [↑](#footnote-ref-267)
262. Goldman et al., T*errorists Use of Virtual Currencies*, *supra* note 5, at 4. [↑](#footnote-ref-268)
263. Goldman, et. al, *id*. at 10. [↑](#footnote-ref-269)
264. See Houben & Snyers, *supra* note 242 (at 10). [↑](#footnote-ref-270)
265. Mark Burges, *A Brief History of Terrorism*, Pogo (Feb. 13, 2015). [↑](#footnote-ref-271)
266. Michal Lavi*, Do Platforms Kill?* *supra* note 19 at 489. [↑](#footnote-ref-272)