

November 2020

Self-Hosted Wallets and the Future of Free Societies

A Guide for Policymakers

Miller Whitehouse-Levine
Lindsey Kelleher





Acknowledgments

The authors thank Kristin Smith, Jason Somensatto, Jack Gavigan, Josh Swihart, Craig Salm, Flavia Naves, Joanna Marathakis, Jake Chervinsky, and Brian Avello for their feedback and suggestions, which significantly strengthened this paper.

About the Blockchain Association

The crypto industry seeks to revolutionize many of the most important and regulated functions of our society. Naturally, no other industry of comparable size and age has so quickly captured the focus of policy makers and regulators. This attention creates unique challenges and opportunities: policies enacted over the next few years could prove to be existential threats to the industry, or they could lay the foundation for a flourishing and vibrant cryptocurrency and blockchain economy in the United States. We work to prevent the former and advance the latter.

Our mission is to forge consensus around common policy challenges and advance solutions that enable the blockchain industry to thrive in the United States.





Table of Contents

Abbreviations	1
Summary	2
Section 1: Background and Regulation	4
Self-hosted wallets and hosted wallets	5
Peer-to-peer value transfer and cryptocurrencies	7
Self-hosted wallets are the foundation of digital peer-to-peer value transfer	9
Overview of Existing Regulation	10
Current regulatory situation	10
Financial Crimes Enforcement Network (FinCEN)	13
The Financial Action Task Force (FATF)	13
Recent Policy Developments and the FATF's "Tools"	15
June 2020 FATF 12-Month Review	15
FATF "Tool" #1: "Banning or denying licensing of platforms if they allow [self-]hosted wallet transfers"	16
FATF "Tool" #2: "Introducing transaction or volume limits on peer-to-peer transactions"	17
FATF "Tool" #3: "Mandating that transactions occur with the use of a VASP or financial institution"	17
Section 2: Arguments	18
Additional restrictions on self-hosted wallets would represent a disproportionate and ineffective response to the risks posed by the illicit use of digital assets and undermine law enforcement's ability to establish attribution in cases involving digital assets	20
Overview	20
Cryptocurrencies have not been widely adopted by illicit actors	21
Noncompliant VASPs are the greatest money laundering risk in cryptocurrency markets, not peer-to-peer transactions	25
The interaction between the peer-to-peer and regulated VASP ecosystems assists law enforcement	26
Conclusion	27
Additional restrictions on self-hosted wallets would lay the foundation for omniscient surveillance by eliminating a digital cash-like payment option	29
Cash dethroned	30
Peer-to-peer payments and authoritarian governments	32
Hong Kong	33
Venezuela	35
Additional restrictions on self-hosted wallets would eliminate the unique features of cryptocurrencies that make them a catalyst of financial inclusivity	38
Peer-to-peer payments and financial inclusivity in the United States	38
Peer-to-peer payments and global financial inclusivity	41
Additional restrictions on self-hosted wallets would indiscriminately apply payments regulation on a diverse and developing ecosystem with applications beyond the transmission of money	43
The Bottom Line: This is a policy decision that has vast societal implications and therefore should be adjudicated by Congress	46



Abbreviations

AML	Anti-Money Laundering
BSA	Bank Secrecy Act
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism
CVC	Convertible Virtual Currencies
FATF	Financial Action Task Force
FDIC	Federal Deposit Insurance Corporation
FinCEN	Financial Crimes Enforcement Network
G7	Group of Seven
IMF	International Monetary Fund
KYC	Know Your Customer
ML	Money Laundering
MSB	Monney Services Business
OTC	Over-the-Counter
PRC	People's Republic of China
SAR	Suspicious Activity Report
TF	Terrorist Financing
UN	United Nations
VASP	Virtual Asset Service Provider

Summary

This report is divided into two sections that seek to offer policymakers a broad introduction to self-hosted wallets.¹ The first section describes what self-hosted wallets are, their role in the digital asset ecosystem, and the current regulatory framework for managing digital asset transactions involving self-hosted wallets. The second section argues that imposing restrictions on individuals' ability to use self-hosted wallets would be misguided.

Self-hosted wallets allow individuals to engage in transactions over the internet on a peer-to-peer basis, meaning that no other individuals or entities are parties to the transaction. Peer-to-peer transactions over the internet were impossible before the advent of the first cryptocurrency, and—as is explored throughout this paper—this seemingly straightforward innovation has widespread, profound, and exciting implications for policymaking and society. The ability to “cut out the middleman” in digital transactions creates a new paradigm for individuals, policymakers, and law enforcement alike because traditional digital financial transactions necessarily involve regulated intermediaries.

Some domestic and international regulators are concerned that individuals' ability to engage in transactions without the use of middlemen creates unacceptable money laundering and terrorist financing (ML/TF) risks. Their concerns are understandable: illicit actors exploit the digital asset ecosystem, just as they exploit cash and the traditional financial system. This report addresses these concerns head-on, arguing that allowing individuals to transact on a peer-to-peer basis over the internet is a net positive for society and is therefore good policy. The paper presents four core arguments:

- 1.** Cryptocurrencies have long suffered from the (thankfully) fast-fading misperception that they are primarily used for illicit purposes. However, the best available evidence suggests that the percentage of activity (as well as absolute dollar amount) in the traditional financial system that is illicit is higher than the percentage of activity in the digital asset ecosystem that is illicit. Moreover, as evidenced by a string of recent forfeitures, law enforcement has become adept at identifying and seizing ill-gotten digital assets. **Thus, additional restrictions on individuals' ability to use self-hosted wallets would not only represent a disproportionate response to the risks posed by the illicit use of digital assets but would also undermine law enforcement's ability to establish attribution in cases involving digital assets by bifurcating the peer-to-peer and regulated ecosystems.**

¹While this report uses the terms “self-hosted wallet” and “hosted wallet,” both the FATF and FinCEN use the terms “unhosted wallet” and “hosted wallet.” The Blockchain Association believes that using self-hosted versus hosted more appropriately characterizes and delineates wallets controlled by individuals and wallets controlled by financial institutions.



2. As the economy and individuals' lives have become increasingly digital-first, the use of cash transactions has declined precipitously, driving the vast majority of transactions to online platforms. Because traditional digital financial transactions necessarily involve an exploitable intermediary, they are by definition not private. **In the same way, restrictions on self-hosted wallets would lay the foundation for total surveillance of citizens' financial lives by eliminating a digital cash-like payment option, with potentially disastrous consequences for free societies.**
3. **Additional restrictions on self-hosted wallets would eliminate the unique features of digital assets that make them a catalyst of financial inclusivity.** Because anyone with an internet connection can create and use self-hosted wallets to transact with others, they are the critical feature of digital assets that could make basic financial services available to the billions of people currently without access to these services.
4. **Finally, additional restrictions on self-hosted wallets would indiscriminately apply payments regulation to a diverse and developing ecosystem with applications that extend far beyond the transmission of money.** While payments using cryptocurrencies, one type of digital asset, are the use case of distributed ledgers that is currently the focus of regulators and policymakers, self-hosted wallets do not necessarily control digital assets that are used for payments. Just like a home safe, self-hosted wallets could be used to store cash-like assets in addition to other digital assets, including important documents and even immutable digital art. Importantly, with the digital asset and blockchain ecosystem still in its infancy, preemptively applying payments regulation to self-hosted wallets would inappropriately "pigeonhole" an innovative ecosystem that could bring revolutionary products and services to the market.

While readers may not agree with the conclusions drawn in this paper, restricting individuals' ability to use self-hosted wallets, and by extension engage in peer-to-peer transactions, would have broad and long-lasting consequences for our society. With so much at stake, the Blockchain Association firmly believes that the debate surrounding peer-to-peer transactions using self-hosted wallets must be addressed by Congress. In other words, restricting peer-to-peer transactions using self-hosted wallets is a policy decision that has vast societal implications, and it should therefore be adjudicated by our elected representatives.



Section 1

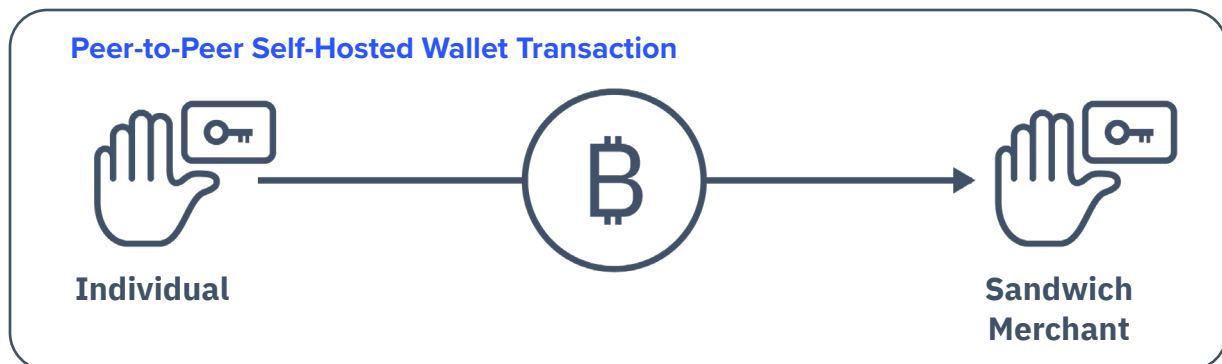
- Background and Regulation
- Overview of Existing Regulation
- Recent Policy Developments and Potential Policies



Background and Regulation

Self-hosted wallets and hosted wallets

In any cryptocurrency transaction, an individual must have a “public address” and “private key” compatible with the relevant cryptocurrency network. These addresses and private keys are simply strings of random numbers and characters. The public address can be thought of as a phone number; an individual user shares his or her public address with other users from whom the original user would like to receive an asset (or a call).² To effectively conceptualize the transaction process that occurs with crypto networks, imagine that a person is at a grocery store purchasing a sandwich. When the sandwich buyer approaches the register, the merchant would present his public address to the sandwich buyer so that the buyer could direct payment to the merchant’s address. To initiate the transaction and transfer cryptocurrency to the merchant’s public address, the buyer uses his “private key,” which is cryptographically tied to the buyer’s public address. If the buyer’s public address and private key do not match, the network ignores the transaction. Importantly, anyone with an internet connection can generate a public address and private key costlessly and without any other prerequisite.



Individuals use cryptocurrency “wallets” to manage their public addresses and associated private keys. Fundamentally, all cryptocurrency wallets do is help individuals manage public addresses and private keys. That being said, wallets vary significantly in their level of sophistication and function. For the purposes of this paper, the most consequential defining characteristic is whether a wallet is (1) “self-hosted,” meaning that the wallet (and associated private keys) is controlled by the owner of the assets, who is responsible for managing,

² While most commonly associated with cryptocurrencies, distributed ledgers have applications well beyond the transmission of assets meant to be used for payments or as stores of value.



custodying, protecting, and using the assets, or (2) “hosted,” meaning that the wallet is controlled by a third-party who manages these responsibilities on behalf of the owner of the assets. Comparing self-hosted and hosted cryptocurrency wallets to everyday tools that individuals use to manage their cash can help clarify the distinction between self-hosted and hosted wallets.

The bi-fold wallet in your pocket, a handbag, a home safe, or a spare change jar is comparable to a “self-hosted” cryptocurrency wallet.

While self-hosted wallets come in a variety of forms³, they all share a critical feature: individuals using a self-hosted wallet rely on themselves to manage, custody, protect, and use the assets associated with their public addresses and private keys. Like cash in a bifold, no third-party is involved. But just as there are limits to the prudence of storing one’s own cash, e.g. under the mattress, there are limits to the prudence of “storing” one’s digital assets with a self-hosted wallet, which ultimately drives some individuals to seek out specialized third-parties to help them manage their cash or assets.

Most commonly, individuals entrust banks to manage, custody, protect, and facilitate the use of their assets. In this way, bank accounts are analogous to “hosted” cryptocurrency wallets: while the individuals still own their assets, the “storage” of these assets is provided and controlled by a third-party. For example, when one stores assets in a safety deposit box, the individual still owns the assets, but the method of storage—the box and vault—is provided and controlled by a third-party: the bank. Hosted wallet providers similarly specialize in offering users a safe place to store their cryptographic assets by providing individuals access to wallets controlled by a provider.⁴ A third-party provides the hosted wallet, and users gain access to the hosted wallet provider’s platform through a variety of digital means, similar to online banking services. Critically, just as in the traditional financial system, the use of a hosted wallet provider necessitates reliance on a third-party, meaning that digital asset transactions completed through the use of hosted wallets are not peer-to-peer. To better understand the differences between transacting with hosted wallets versus self-hosted wallets, it is helpful to once again return to the analogy of making a purchase at a grocery store.

³ Some of the simplest self-hosted wallets are “paper wallets,” which are pieces of paper with a public address and corresponding private key written on it, and “brain wallets,” which are a public address and private key that is memorized by an individual and therefore “stored” or “saved” in his or her brain. Other self-hosted wallets can offer users more convenient experiences, such as software programs that not only store the user’s public address and private key but also interface with the relevant cryptocurrency network to more simply initiate transactions. Hardware wallets are another type of self-hosted wallet; they are physical devices that store public addresses and private keys offline, offering a more secure storage tool.

⁴ In the cryptocurrency ecosystem, hosted wallet providers include custodial exchanges, which allow their customers to exchange cryptocurrency for fiat currency or other cryptocurrencies.



Peer-to-peer value transfer and cryptocurrencies

Going to a grocery store and buying a sandwich with cash is akin to buying a sandwich with a self-hosted wallet. Going to a grocery store and buying a sandwich with a credit card, on the other hand, is akin to buying a sandwich using a hosted wallet provider. It is in this comparison that the fundamental role of self-hosted wallets and, by extension, the innovation of cryptocurrencies is revealed: they allow individuals to transfer value on a peer-to-peer basis over the internet, meaning that only the two individuals seeking to exchange value are party to the transaction. In other words, without self-hosted wallets, digital peer-to-peer transactions would not be possible.

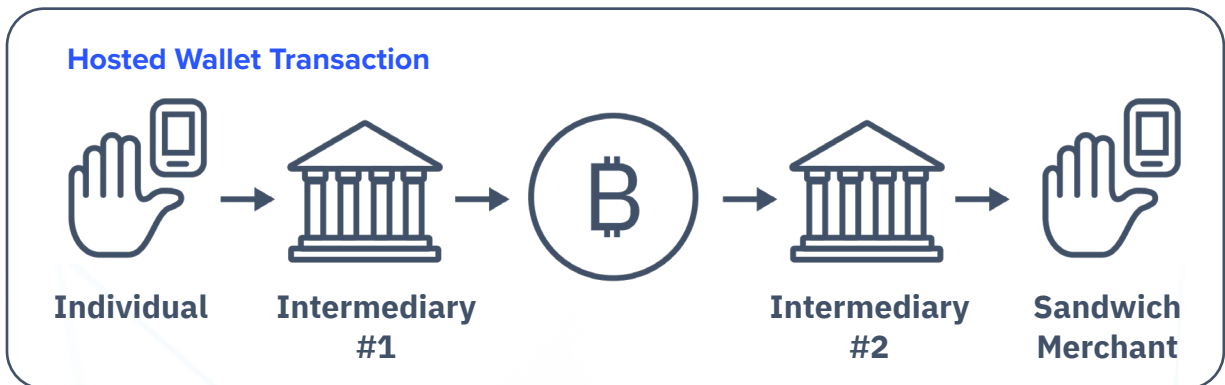
Buying one's lunch with cash has several unique features that digital peer-to-peer transactions using self-hosted wallets replicate. First, when an individual buys lunch with cash, they have the exclusive right to initiate the transaction, and they and the sandwich merchant do not need to rely upon or receive permission from anyone to complete the transaction. Second, the transaction is settled instantly; as soon as the cash exits the buyer's wallet and enters the merchant's register, the transaction is complete. The buyer and seller can transact with the confidence provided by "trustlessness:" both parties are already familiar with the asset being transferred and its value, which means there is no need to trust one another or have any pre-existing relationship to transact with confidence. Finally, the transaction is known only to the two individuals party to the transaction, and neither the buyer nor the seller need to know anything about one another to transact. The fact that the buyer holds enough cash in hand to purchase the sandwich and that the seller has the sandwich is sufficient information to complete the transaction with confidence.

Unlike cash and digital peer-to-peer transactions using self-hosted wallets, digital transactions through the traditional financial system and digital asset transactions involving hosted wallets require transacting parties to rely upon, trust, and receive permission from intermediating third-parties.

For example, when an individual purchases a sandwich with a credit card, at least five parties are involved in the transaction. To begin, the buyer (party one) hands the credit card to the merchant (party two) who initiates the transaction



with a point of sale terminal. The buyer's credit card details are sent to the sandwich merchant's bank or payment processor (party three), after which the merchant's bank or payment processor forwards the buyer's credit card details to the relevant credit card network (party four). Next, the card network preliminarily clears the payment and requests payment authorization from the financial institution that issued the buyer's credit card (party five). Next, the issuing financial institution validates the authenticity of the transaction and checks whether the buyer has sufficient funds to make the purchase. The issuing financial institution either approves or declines the transaction and sends these details back to the merchant through the various intermediaries already listed. Once the merchant receives this confirmation, the transaction is complete as far as the customer is concerned, but the process of clearing and settling the transferred funds can take several days.⁵



⁵ Worldpay Editorial Team. "How Credit Card Processing Works." Fidelity National Information Services, July 10, 2019. <https://www.fisglobal.com/en/insights/merchant-solutions-worldpay/article/how-credit-card-processing-works>.



The layers of trust, reliance, and permission necessary to complete traditional digital payments and hosted wallet digital asset transactions reveal the unique simplicity of a cash and self-hosted wallet transactions, i.e. peer-to-peer transactions. With credit cards and hosted wallets, both the buyer and the merchant must trust their respective financial institutions to manage their assets responsibly. All of the intermediating parties must not only be functional but also “bless” or grant their permission for the transaction to be successful. Additionally, any of the intermediating parties could disrupt the transaction for any reason—whether legitimate or not. The transacting parties must also share personally identifiable information (PII) with the intermediating third-parties, such as social security or employee identification numbers, billing addresses, and sensitive financial information, which is stored by intermediaries, and there is often a fee imposed on the transacting parties by the third party intermediaries. Finally, the participating intermediaries survey the transaction, which means that details about the transaction, like the amount of funds being transferred, when and where the transaction takes place, and details of the item purchased, are collected and stored.

Self-hosted wallets are the foundation of digital peer-to-peer value transfer

While the methods by which cryptocurrency networks leverage distributed ledgers and decentralized computing to operate can be burdensome to understand and are beyond the scope of this paper,⁶ the fundamental innovation that these tools facilitate is relatively straightforward:

cryptocurrency networks allow individuals to transfer value over the internet on a peer-to-peer basis, in other words without involving any intermediating third-party.

Considering that the use of a hosted wallet by definition necessitates the use of an intermediating third-party, the unique role of self-hosted wallets in the cryptocurrency ecosystem is evident. In fact, transactions employing self-hosted wallets can be equated to the fundamental innovation of cryptocurrencies. Without self-hosted wallets, digital value transfers on a peer-to-peer basis, i.e. cash-like transactions over the internet, would not be possible. The remainder of this paper will explore some of the myriad policy implications, ranging from financial inclusivity to individual liberty, that are associated with the ability to conduct cash-like transactions over the internet. As the use of physical cash continues to decline not only abroad but also in the United States, the implications of potentially restricting individuals’ ability to use self-hosted wallets to manage, custody, and use the public addresses and private keys associated with their digital assets without relying on intermediating third-parties will become more and more enormous.

⁶ For an explanation of decentralized networks for a policymaking audience, please see: Peter Van Valkenburgh, “Open Matters: Why Permissionless Blockchains Are Essential to the Future of the Internet,” Coin Center Report (Washington D.C.: Coin Center, December 14, 2016), <https://www.coincenter.org/open-matters-why-permissionless-blockchains-are-essential-to-the-future-of-the-internet/>.

Overview of Existing Regulation

Current regulatory situation

Individual nations are responsible for anti-money laundering, combatting the financing of terrorism (AML/CFT), and financial surveillance legislation and enforcement. In the United States, implementation of these policies usually falls to the Financial Crimes Enforcement Network (FinCEN), a “subsidiary” of the Department of the Treasury.⁷ In 1989, the G7 formed the Financial Action Task Force (FATF), which now has 39 member nations, to coordinate national AML/CFT regimes and financial surveillance policy.⁸ The FATF’s policy recommendations influence financial surveillance regulation in the United States,⁹ and the United States maintains a delegation to the FATF. While the FATF and FinCEN work in conjunction with one another, they are independent organizations whose approach to financial surveillance, especially in the case of digital assets, must be analyzed discretely to understand the current regulatory framework managing peer-to-peer transactions using self-hosted wallets.

In the United States, cryptocurrency businesses like hosted wallet providers, custodial exchanges, fiat “on-ramps,”¹⁰ and over-the-counter (OTC) brokers¹¹ are regulated as money services businesses (MSBs) and are therefore responsible for compliance with the Bank Secrecy Act (BSA), sanctions, financial surveillance, and AML/CFT requirements.¹² On the other hand, peer-to-peer transactions, non-custodial digital asset platforms, and self-hosted wallets are not regulated under the BSA.¹³

A few notes on terms: in the United States, there are several types of MSBs, but for the most part, digital asset businesses are defined as “money transmitters.” The FATF, however, uses a different term to describe digital asset businesses subject to international AML/CFT requirements: “virtual asset service providers” (VASPs). For the purposes of this paper, mentally equating VASPs, MSBs, and money transmitters may help clarify existing regulations and potential policies.

⁷ FinCEN, “What We Do,” Financial Crimes Enforcement Network, January 2020. <https://www.fincen.gov/what-we-do>.

⁸ FATF, “What Do We Do,” Financial Action Task Force, January 2020. <https://www.fatf-gafi.org/about/whatwedo/>.

⁹ U.S. compliance with the 40 FATF recommendations, as of February 2020: Compliant, 22.5%; Largely Compliant, 55.0%; Partially Compliant, 12.5%; and Non-Compliant, 10.0%. <https://www.fatf-gafi.org/media/fatf/documents/reports/fur/Follow-Up-Report-United-States-March-2020.pdf>.

¹⁰ FinCEN, “Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies (CVC),” (Washington D.C.: Financial Crimes Enforcement Network, May 9, 2019), 8, <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf>.

¹¹ FinCEN, “Application of FinCEN’s Regulations,” 15.

¹² FinCEN, “Application of FinCEN’s Regulations,” 16.

¹³ Ibid.



Like the vast majority of cash transactions,¹⁴ digital peer-to-peer transactions themselves are not subject to BSA and financial surveillance requirements. When our sandwich buyer hands his cash to the merchant, neither party is obligated to verifiably determine the identity of the other party or ascertain the source of the cash being transferred. Moreover, neither the manufacturer of the bifold wallet in which the buyer stores his cash nor the manufacturer of the sandwich merchant's cash register is subject to AML/CFT requirements. The same is true for home safe and handbag manufacturers, etc., even though these companies provide “devices” in which individuals store and manage their assets.

Peer-to-Peer Cash Transaction



Currently, this same logic and regulation applies to digital peer-to-peer transactions. When an individual sends cryptocurrency to another individual on a peer-to-peer basis, neither party is required to comply with AML/CFT requirements. Moreover, the entities that “create” self-hosted wallets are not subject to these requirements either. For example, just like a home safe manufacturer, companies that provide self-hosted wallet software do not manage or otherwise have access to the self-hosted wallet users’ private keys, meaning that the self-hosted software wallet provider has no control whatsoever over the users’ assets or activities. Taken to an informative extreme: the manufacturer of the paper on which a public address and private key is written is not subject to the AML/CFT regime, nor is the paper manufacturer responsible for whatever the self-hosted paper wallet user does with the assets associated with the public address and private key “stored in” the paper wallet.

¹⁴ Cash transactions over \$10,000 involving financial institutions are subject to BSA requirements. (Transfer and Reorganization of Bank Secrecy Act Regulations, 31 C.F.R. § 1010 (2010) <https://ecfr.federalregister.gov/current/title-31/subtitle-B/chapter-X/part-1010>).



While neither cash nor digital peer-to-peer transactions are regulated, comprehensive regulation of third-party intermediaries in both the traditional financial system and digital asset ecosystem allows law enforcement to prevent and disrupt illicit activity like money laundering and terrorist financing. For example, AML/CFT regulations require that traditional financial institutions like banks and stock exchanges identify their customers (commonly known as know your customer (KYC) requirements) and comply with financial surveillance requirements like the submission of suspicious activity reports (SARs). In effect, as soon as the asset, e.g. cash, is handed over to a third-party financial institution, comprehensive financial regulation and surveillance enters force. The financial institution is legally obligated to collect comprehensive information about the individual and the assets. The same is true in the digital asset ecosystem. The moment an individual's digital asset "touches" a third-party VASP, like a hosted wallet provider or a custodial exchange, that third-party—being a "regulated entity" subject to AML/CFT requirements—is responsible for collecting the same information and compliance with the same rules and regulations as traditional money transmitters.

As in the traditional financial sector, the interaction between the peer-to-peer ecosystem and regulated cryptocurrency ecosystem "balances" the competing policy priorities of protecting individuals' financial privacy and autonomy while preemptively surveilling the majority of financial activity to prevent unwanted activity. Indeed, the interaction between the two ecosystems ensures that the risks posed by peer-to-peer transactions are limited while the societal utility they provide is maintained.



Financial Crimes Enforcement Network (FinCEN)

In May 2019, FinCEN released guidance addressing how its regulations apply to cryptocurrency businesses (hereafter, “May 2019 FinCEN Guidance”). The document first distinguishes between hosted and self-hosted wallets: “hosted wallet providers are account-based money transmitters that receive, store, and transmit CVC [convertible virtual currencies] on behalf of their account holders,”¹⁵ while self-hosted “wallets are software hosted on a person’s computer, phone, or other device that allow the person to store and conduct transactions in CVC.”¹⁶ The use of a self-hosted wallet inherently means that the self-hosted wallet “...owner interacts with the payment system [crypto network] directly and has total independent control over the value”¹⁷ associated with the self-hosted wallet’s public address and private key. In other words, there is no intermediating third-party involved in the transaction. Thus, “in for far as the person conducting a transaction through the [self-]hosted wallet is doing so to purchase goods or services on the user’s own behalf, they are not a money transmitter.”¹⁸

In practice, this guidance means that transactions involving hosted wallet providers (money transmitters) are subject to the United States’ AML/CFT regime while peer-to-peer transactions involving self-hosted wallets are not. Just like traditional financial institutions that provide individuals accounts, hosted wallet providers are subject to AML/CFT requirements like KYC, customer due diligence (CDD), and SAR filing obligations. On the other hand, transactions involving self-hosted wallets are not subject to these requirements, similar to how the vast majority of cash transactions are not either.

¹⁵ FinCEN, “Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies (CVC).” (Washington D.C.: Financial Crimes Enforcement Network, May 9, 2019), 15, <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf>.

¹⁶ The Blockchain Association does not necessarily endorse FinCEN’s definitions. FinCEN, “Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies (CVC).” (Washington D.C.: Financial Crimes Enforcement Network, May 9, 2019), 16, <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf>.

¹⁷ Ibid.

¹⁸ Ibid.



The Financial Action Task Force (FATF)

In June 2019, the FATF released “Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers” (hereafter, the “June 2019 FATF Guidance”).¹⁹ FinCEN’s regulation of transactions involving hosted versus self-hosted wallets closely mirrors the FATF’s guidance, but the FATF includes an important nuance. The relevant sentences are reproduced below:

“[The June 2019 FATF Guidance] recognizes that unlike traditional fiat wire transfers, not every VA [virtual asset] transfer may involve (or be bookended by) two obliged entities [i.e., MSBs in the United States]... The FATF does not expect that VASPs and financial institutions, when originating a VA transfer, would submit [KYC information] to individual [self-hosted wallet] users who are not [VASPs]. VASPs receiving a VA transfer from an entity that is not a VASP or other obliged entity (e.g., from an individual VA user using his/her own DLT [distributed ledger technology] software, such as a self-hosted wallet), should obtain the required originator information from their customer.”²⁰

As already discussed, every traditional digital value transfer is inherently intermediated by a third-party, meaning that on each “end” of traditional digital value transfers is a financial institution subject to AML/CFT requirements (“obliged entities”). Digital transactions in which “obliged entities” directly transact with the peer-to-peer sector are therefore unique to the cryptocurrency ecosystem. In these situations, the FATF recommends that a VASP (or hosted wallet provider) “should obtain the required originator information from their customer,” meaning that the recipient (using the hosted wallet regulated ecosystem) of a digital asset from the peer-to-peer ecosystem is required to disclose the transaction originator’s information to the hosted wallet provider.

¹⁹ FATF, “Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,” Paris, 2020, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html.

²⁰ FATF, “Guidance for a Risk-Based Approach to Virtual Assets,” 30.

Recent Policy Developments and the FATF's "Tools"

In response to the May 2019 FinCEN Guidance and the June 2019 FATF Guidance, domestic and international regulators have expressed concern that the ability to digitally transfer value on a peer-to-peer basis creates unacceptable risks associated with money laundering, terrorist financing, tax evasion, and other illicit activities. To address these concerns, domestic and international regulators are considering the implementation of policies that would restrict the use of self-hosted wallets and ipso facto restrict digital peer-to-peer transactions generally.²¹ In its first 12 month review of the revised 2019 FATF standards, published in June 2020, the FATF identified a "range of tools that are available" to national regulators "if" they deem the risks associated with digital peer-to-peer transactions to be unacceptable.²² Moreover, in response to the June 2019 FATF Guidance, Switzerland implemented a stricter regime than recommended by the FATF, which could be replicated elsewhere.²³

June 2020 FATF 12-Month Review

In June 2020, the FATF released its first 12 month review of the June 2019 FATF Guidance (hereafter, "the 12-Month Review"). The 12-Month Review addresses some FATF member jurisdictions' concern regarding digital peer-to-peer transactions and subsequently presents three "tools" that national regulators could implement should they consider the risks associated with the "peer-to-peer sector" to be too great. The relevant passage reads:

"The launch of new virtual assets however could materially change the ML/TF risks, particularly if there is mass-adoption of a virtual asset that enables anonymous peer-to-peer transactions. There are a range of

²¹In August 2020, Scott Rembrandt, Deputy Assistant Secretary for Strategic Policy, Office of Terrorist Financing and Financial Crimes at U.S. Department of the Treasury and Head of the U.S. Delegation to the FATF, said that navigating the potential risks associated with unhosted wallets "is something that the FATF is going to take up in its next 12 Month Review. I think it's fair to say that a number of FATF members have some concerns about unhosted wallets, the scale of their use, [and] this open question of the scale of funds flowing through unhosted wallets, that I think a number of FATF members will want greater clarity on. I don't want to prejudge the outcome of the 12 Month Review; we'll see what happens... [but] unhosted wallets is something people are paying a lot of attention to at the FATF." At the same event, Tom Neylan, a policy analyst at the FATF, said that "One of the things that we are monitoring in our second 12 Month Review is really the extent to which people are moving away from VASPs and into [self-hosted wallets and decentralized networks] because this is a big concern. We don't want to see an unregulated alternative emerge that's vulnerable to criminal exploitation. It wouldn't be fair to the regulated and compliant VASP sector, but it would also be a huge loophole in the anti-money laundering framework. So one of the things our review is looking at is is that happening? Are we seeing a large scale towards those markets? And if we are, that's going to be a problem that we will have to deal with." Chainalysis. The FATF Regulatory Roundtable. LINKS Virtual Session: Chainalysis, 2020. <https://go.chainalysis.com/FATF-regulatory-roundtable.html>.

²²FATF, "12-month Review Virtual Assets and VASPs," Paris, 2020, 15 www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html.

²³FINMA, "FINMA Guidance: Payments on the Blockchain," Bern, Switzerland, August 26, 2019, <https://www.unlock-bc.com/news/2019-08-30/swiss-finma-issues-new-guidance-for-payments-on-blockchain>.



tools that are available at a national level to mitigate, to some extent, the risks posed by anonymous peer-to-peer transactions if national authorities consider the ML/TF risk to be unacceptably high. This includes banning or denying licensing of platforms if they allow unhosted wallet transfers, introducing transactional or volume limits on peer-to-peer transactions or mandating that transactions occur with the use of a VASP or financial institutions. As of yet, no common practises or consistent international approach have emerged regarding the use of these different tools.”²⁴

This passage deserves close analysis. Note that the language includes several hedges: new virtual assets “could materially change the ML/TF risks;” the tools listed could mitigate risks “if national authorities consider the ML/TF risk to be unacceptably high;” and no consensus has “emerged regarding the use of these different tools.”²⁵ Additionally, the FATF’s 12 Month Review questions whether “the number and value” of peer-to-peer transactions is large enough to even be considered a material ML/TF risk. While these statements may give readers the impression that the FATF will not adopt new restrictions on peer-to-peer transactions in their next review, which is due out in June 2021, regulators’ public comments suggest that new restrictions are being considered. Exploring the practical effects of the FATF’s proposed “tools” in plain language evidences the major implications of them.

FATF “Tool” #1

“Banning or denying licensing of platforms if they allow [self-] hosted wallet transfers”

In plain language, this “tool” would prohibit individuals using a hosted wallet from transacting with any self-hosted wallet. In the traditional financial system, this policy would equate to banning ATMs and in-branch cash transactions, in other words banning the withdrawal and deposit of peer-to-peer assets.

²⁴ FATF, “12-month Review,” 15.

²⁵ FATF, “12-month Review,” 7.



FATF “Tool” #2:

“Introducing transaction or volume limits on peer-to-peer transactions”

In plain language, this “tool” would place restrictions on how individuals transact with a peer-to-peer bearer asset. In familiar terms, this policy would equate to “capping” the number or value of transactions one could make using cash. It is unclear to the Blockchain Association how this policy would be consistently applied and enforced in practice, given that doing so in the peer-to-peer cryptocurrency ecosystem would present many of the same challenges as implementing such a policy for cash transactions would.

FATF “Tool” #3

“Mandating that transactions occur with the use of a VASP or financial institution”

In plain language, this “tool” would ban digital peer-to-peer transactions and cryptocurrencies. In traditional terms, this would be a ban on cash transactions.

Unpacking these tools reveals the potentially widespread effects of these policies. Placing restrictions on peer-to-peer transactions—the FATF’s proposed “tools” or others—would have profound implications not only for the cryptocurrency ecosystem but also for society that must be carefully considered by U.S. policymakers. The remainder of this paper will examine the potential and wide ranging consequences of implementing policies that undermine the use of self-hosted wallets, and by extension, digital peer-to-peer transactions.



Section 2

■ Arguments



Arguments

The implementation of additional restrictions on self-hosted wallets would (1) represent a disproportionate response to the actual risks posed by the illicit use of digital assets and undermine law enforcement's ability to establish attribution in cases involving digital assets by "bifurcating" the peer-to-peer and intermediated (regulated) ecosystems, (2) lay the foundation for omniscient surveillance systems by preemptively undermining a cash-like option as the economy becomes "digital-only," (3) eliminate the unique features of cryptocurrencies that make them a catalyst of financial inclusivity, and (4) apply payments regulation to a diverse and developing ecosystem with applications well beyond payments. Given the vast potential consequences of additional restrictions on digital peer-to-peer transactions, any potential policy change related to self-hosted wallets should be debated publicly and decided on by Congress as opposed to by regulatory action.

Additional restrictions on self-hosted wallets would represent a disproportionate and ineffective response to the risks posed by the illicit use of digital assets and undermine law enforcement’s ability to establish attribution in cases involving digital assets

Overview

Although digital assets’ novelty and pseudonymity may make them attractive for criminal use, they have not been widely adopted by criminals, terrorists, and other nefarious actors. While there might be many reasons why criminals have not adopted the use of digital assets in volume, this paper will argue that both the relatively limited size of the digital asset ecosystem today and the effectiveness with which illicit actors exploit the existing financial system disincentivize criminals from adopting digital assets or any other new method of hiding, laundering, and raising assets. In addition, because non-compliant entities that are already subject to the global AML/CFT regime—namely non-compliant OTC brokerages and exchanges—represent the greatest “hole” in the AML/CFT regime in the digital asset ecosystem, additional restrictions on self-hosted wallets would not address the substantially greater risk posed by non-compliant VASPs. As such, applying additional restrictions to self-hosted wallets and peer-to-peer transactions would represent a disproportionate and preemptive policy response that would not address the actual methods through which criminals exploit digital assets.



The illicit use of cryptocurrencies presents challenges to law enforcement that will develop over time. For example, today, 95% of criminal activity in the cryptocurrency ecosystem involves bitcoin, which has a blockchain that is accessible and searchable by anyone with an internet connection.²⁶ Blockchains that reveal transaction information (“transparent blockchains”) can be leveraged to associate transactions with criminal enterprises and establish attribution for criminal activity involving cryptocurrencies. In the future, individuals and businesses may seek to use cryptocurrencies without transparent blockchains that more closely replicate the privacy features of physical cash. While evidence suggests that illicit actors have not adopted cryptocurrencies that offer enhanced privacy features, should criminal enterprises begin to adopt cryptocurrencies without transparent blockchains, the interaction between the peer-to-peer and regulated VASP ecosystems will nonetheless create “choke points” that can provide law enforcement information in the course of investigations. Indeed, criminal actors must “cash out” their cryptocurrency into fiat currency,²⁷ which means that, in instances of criminal activity involving cryptocurrencies without transparent blockchains, law enforcement has access and insight into the illicit activity at these “choke points,” i.e. regulated VASPs. This is doubly true when the predicate crime produces fiat-based gains: launderers seeking to use cryptocurrency would also have to purchase it at regulated “choke points.” This situation almost identically mirrors the familiar interaction between the anonymous peer-to-peer cash ecosystem and the regulated financial ecosystem. That being said, today, when they are used for illicit purposes, the cryptocurrencies most commonly used to facilitate illegal activities feature transparent blockchains.²⁸

Cryptocurrencies have not been widely adopted by illicit actors

The unique characteristics of cryptocurrencies, namely their pseudonymity, novelty, and accessibility, make them potential mediums for bad actors to conduct business. Cryptocurrencies’ decentralized governance and operation, which allows for anyone with an internet connection to use them, means that criminals also have access to them. Additionally, criminals may perceive cryptocurrencies to be attractive mediums through which they can move assets without being subject to money laundering and terrorist financing controls. Like cash transactions and unlike transactions through intermediating financial entities, peer-to-peer transactions using self-hosted wallets are not subject to the financial surveillance requirements meant to identify and disrupt criminal activity. As such, criminals may assume that cryptocurrency transactions are anonymous. All of these assumptions are mistaken, however.²⁹

²⁶ Simms, Thomas. “At Least 95 Percent of Crypto Crimes Involve Bitcoin, Chainalysis Executive Says.” *Cointelegraph*, April 25, 2019. <https://cointelegraph.com/news/at-least-95-percent-of-crypto-crimes-involve-bitcoin-chainalysis-executive-says>.

²⁷ Chainalysis, “The 2020 State of Crypto Crime,” Chainalysis Inc., January 2020, 12, <https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf>.

²⁸ Chainalysis, “The 2020 State of Crypto Crime,” 5.

²⁹ Neal B. Christiansen and Julia E. Jarrett, “Forfeiting Cryptocurrency: Decrypting the Challenges of a Modern Asset,” *Department of Justice Journal of Federal Law and Practice* 67, no. 3 (September 2019): 166.



While some of the foundational features of cryptocurrency networks may appear to make them easily exploitable by criminals, evidence suggests that illicit actors, notably terrorist organizations and money launderers, have not adopted cryptocurrency use en masse.

Indeed, a report published by the RAND Corporation in 2019 states that “there is little indication that terrorist organizations are using cryptocurrency in any sort of extensive or systematic way,”³⁰ and the Department of Justice’s *Journal of Federal Law and Practice* maintains that

“in the case of terrorist organizations, cryptocurrency is still not the preferred method to transfer value.”³¹

According to a report published by the European Commission, terrorists have not adopted cryptocurrencies because they “do not provide substantial benefits for a wide range of terrorist and extremist actors over other established [terrorist financing] methods.”³² A preference for fiat currencies and law enforcement’s growing ability to disrupt terrorist activity facilitated by cryptocurrencies have discouraged their use among terrorists. Instead, according to the Department of Justice, more “established” methods, such as the “long tradition of using hawalas... along with the use of commercial money transfer businesses,” remain terrorists’ financing methods of choice. It is important to note that traditional “commercial money transfer businesses,”³³ entities already subject to ML/TF controls, remain one of the “favored” methods of financing for terrorists. Terrorist financing is not the only illicit financial activity that law enforcement faces, however.

Money laundering is a substantially larger problem by volume than terrorist financing. Interestingly, as with terrorist financing, cryptocurrencies do not offer a more attractive medium to facilitate money laundering than other established means. Recent reporting surrounding the “FinCEN Files” tangibly illustrates the effectiveness with which criminals move their assets through the established financial system despite financial surveillance requirements meant to disrupt their activity.³⁴ Yet the fact that illicit and criminal actors adeptly exploit the traditional financial system to facilitate their activities is old news.

³⁰ Cynthia Dion-Schwarz, David Manheim, and Patrick B. Johnston, “Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats” (Santa Monica, CA: RAND Corporation, 2019), 21, https://www.rand.org/pubs/research_reports/RR3026.html.

³¹ Michele R. Korver, C. Alden Pelker, and Elisabeth Poteat, “Attribution in Cryptocurrency Cases,” Department of Justice *Journal of Federal Law and Practice* 67, no. 1 (February 2019): 255.

³² Tom Keatinge, David Carlisle, and Florence Keen, “Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses,” Counter-Terrorism (European Union: Policy Department for Citizens’ Rights and Constitutional Affairs, May 2018), 29, [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU\(2018\)604970_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf).

³³ Michele R. Korver, C. Alden Pelker, and Elisabeth Poteat, “Attribution in Cryptocurrency Cases,” Department of Justice *Journal of Federal Law and Practice* 67, no. 1 (February 2019): 255.

³⁴ Jason Leopold et al., “FinCen Files” (New York, N.Y.: BuzzFeed News, September 20, 2020), <https://www.buzzfeednews.com/fincen-files>.



According to the United Nations, “globally, it appears that much less than 1% (probably around 0.2%) of the proceeds of crime laundered via the financial system are seized and frozen.”³⁵

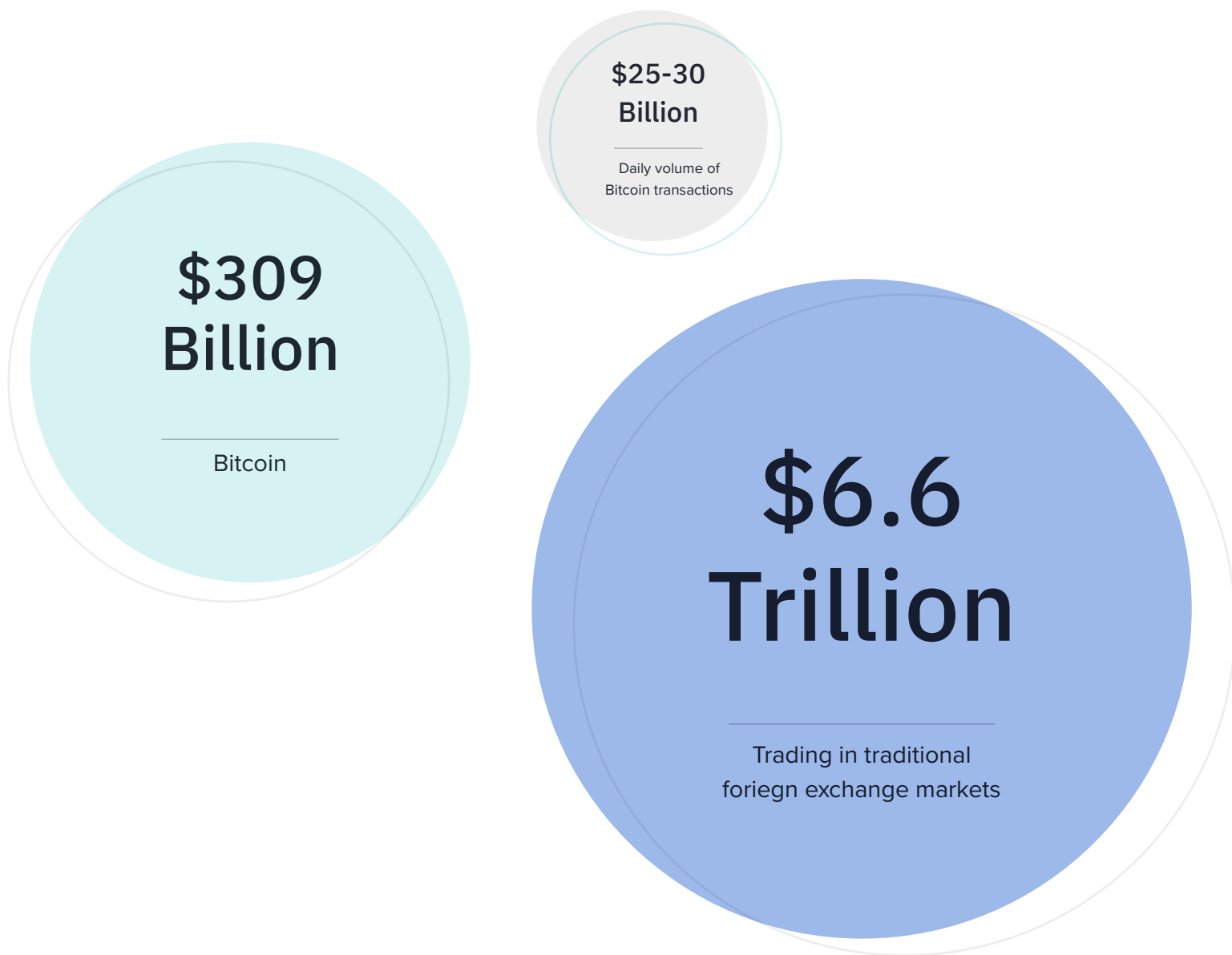
In other words, of the estimated \$1.6 trillion laundered in 2009, law enforcement froze and seized an estimated \$3.2 billion ($\$1.6 \text{ trillion} \times 0.002 = \3.2 billion).³⁶ In addition to the traditional financial system being largely accessible to illicit actors, the limited liquidity and depth of the digital asset ecosystem makes it an unlikely choice for large scale illegal activity.

³⁵ Thomas Pietschmann and John Walker, “Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes,” Research Report (Vienna, Austria: United Nations Office on Drugs and Crime, October 2011), 7, https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf.

³⁶ United Nations Office on Drugs and Crime. “UNODC Estimates That Criminals May Have Laundered US\$ 1.6 Trillion in 2009.” Press Release, October 25, 2011.



Currently, relative to traditional financial markets, cryptocurrency markets are miniscule and are therefore not liquid or deep enough to facilitate large scale money laundering. The largest cryptocurrency by market capitalization is bitcoin, which has a capitalization of about \$309 billion,³⁷ and the combined market capitalization of stablecoins that reference the US dollar is about \$23 billion.³⁸ Actual average daily volume of all transactions involving bitcoin is uncertain, but even the highest average estimates range around \$25-30 billion.³⁹ Comparing this activity to trading in traditional foreign exchange markets, which according to the Bank of International Settlements' *Triennial Central Bank Survey* reached \$6.6 trillion *per day* in April 2019,⁴⁰ and it becomes clear that traditional foreign exchange markets are significantly larger than cryptocurrency markets. In fact, the amount of money laundered through the traditional financial system is almost certainly larger than the market capitalization of all cryptocurrencies combined.



³⁷ Bitcoin's market capitalization on 11/16/2020. "Today's Cryptocurrency Prices by Market Cap," CoinMarketCap, 2020, <https://coinmarketcap.com/>.

³⁸ As of 11/16/2020. "Today's Cryptocurrency Prices by Market Cap," CoinMarketCap, 2020, <https://coinmarketcap.com/>.

³⁹ Galen Moore, "We Still Don't Know Bitcoin's Real Volume," CoinDesk, January 6, 2020, sec. Markets.

⁴⁰ Monetary and Economic Department, "Triennial Central Bank Survey: Foreign Exchange Turnover in April 2019" (Basel, Switzerland: Bank for International Settlements, September 16, 2019), 3, https://www.bis.org/statistics/rpfx19_fx.pdf.



The FATF cautions that “due to the illegal nature of the transactions, precise statistics are not available and it is therefore impossible to produce a definitive estimate of the amount of money that is globally laundered every year. The FATF therefore does not publish any figures in this regard.”⁴¹ Indeed, estimating the amount of money laundered through the traditional financial system is challenging because illicit actors are adept at obfuscating their criminal activity from law enforcement and national governments. According to the United Nations, however, “the most widely quoted figure for the extent of money laundered has been the [International Monetary Fund] ‘consensus range’ of 2% to 5% of global GDP, made public by the IMF in 1998... The best estimate for the amount available for laundering through the financial system, emerging from a meta-analysis of existing estimates, would be equivalent to 2.7% of global GDP (2.5%-4%) or US\$1.6 trillion in 2009.”⁴² From this statistic, it becomes clear that the value of illicit funds laundered each year through the traditional financial system is almost certainly greater than the value of all cryptocurrencies combined.

While the best available evidence suggests that the entire cryptocurrency ecosystem is substantially smaller than the amount of assets laundered through the traditional financial system each year, estimates of the level of illicit activity in cryptocurrency markets further prove that cryptocurrencies have not been widely adopted by illicit actors. Unlike the traditional financial system, the transparency of cryptocurrency networks allows for a clearer view into criminal financial activity involving cryptocurrencies. According to blockchain analysis firm Chainalysis, the percent of all cryptocurrency transaction volume that was illicit in 2017, 2018, and 2019 was 0.7%, 0.4%, and 1.1%, respectively.⁴³ These estimates are all well below the IMF’s “consensus range” of 2% - 5% in the traditional financial system.

Noncompliant VASPs are the greatest money laundering risk in cryptocurrency markets, not peer-to-peer transactions

In order for criminals and terrorists to successfully launder funds through the cryptocurrency ecosystem, they must eventually exchange their cryptocurrency for cash.⁴⁴ To successfully “off-ramp” their illicit cryptocurrency into fiat currency, criminals must exploit VASPs (often using sophisticated “synthetic identities” to fool KYC and CDD processes) or leverage non-compliant VASPs that do not conduct required CDD. As such,

the core vulnerability in the global AML/CFT regime appears to be illicit OTC brokers, which facilitate off-exchange cryptocurrency trades and are already subject to AML/CFT requirements.

According to Chainalysis’s “2020 Crypto Crime Report,” “while exchanges have always been a popular off-ramp for illicit cryptocurrency, they’ve taken in a steadily

⁴¹ “Money Laundering,” Financial Action Task Force, 2020, <https://www.fatf-gafi.org/faq/moneylaundering/>.

⁴² Pietschmann and Walker, “Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes,” 5.

⁴³ Chainalysis, “The 2020 State of Crypto Crime,” 5.

⁴⁴ Chainalysis, “The 2020 State of Crypto Crime,” 9.



growing share [of bitcoin from criminal sources] since the beginning of 2019,” reaching over 50% by the end of 2019.”⁴⁵ Chainalysis has determined that at exchanges, a few accounts received the vast majority of illicitly obtained bitcoin⁴⁶ by value in 2019. For example, at the two exchanges that received the most illicit bitcoin throughout 2019, about 0.2% of accounts that were sent illicit bitcoin received 75% of the total illicit funds sent to exchanges.⁴⁷ In other words, a few illicit “whales” are responsible for the lion’s share of illicit activity at exchanges (which, again, received nearly half of illicit bitcoin by the end of 2019). Additionally, Chainalysis, in its report, “suggests that many [of these whales] are OTC brokers” that specialize in facilitating illicit activity.⁴⁸ As a reminder, under the FATF’s 2019 Guidance and FinCEN’s May 2019 Guidance, both exchanges and OTC brokers are obliged entities, i.e. VASPs and MSBs, and are therefore subject to AML/CFT requirements. While the vast majority of OTC brokers are legitimate, “some of them specialize in providing money laundering services to criminals. OTC brokers often

have much lower KYC requirements than the exchanges they operate on. Many of them take advantage of this laxity and help criminals launder and cash out funds.”⁴⁹ The report concludes that “the money laundering infrastructure driven by OTC brokers enables nearly every other type of crime” involving cryptocurrencies.⁵⁰

Relevant to this paper is the fact that none of this illicit activity is in any way facilitated by peer-to-peer transactions using self-hosted wallets. At least two “layers” of KYC requirements, the foundation of the global AML/CFT regime, must fail (often due to illicit actors’ ever-more-sophisticated use of synthetic identities) or be willfully disregarded for OTC broker-facilitated laundering to be successful: level 1) OTC brokers’ AML/CFT requirements for their customers, and level 2) exchanges’ AML/CFT requirements for OTC brokers. The implementation of additional restrictions on self-hosted wallets would have no effect on this type of illegal activity, which represents the greatest ML/TF risk in cryptocurrency markets.

The interaction between the peer-to-peer and regulated VASP ecosystems assists law enforcement

When cryptocurrencies are used for illicit purposes, criminals, in order to successfully launder their assets, must exchange their cryptocurrency for fiat currencies at regulated “choke points,” notably VASPs.⁵¹ If the predicate crime produces gains in fiat currency, then launderers must also exchange their ill-gotten fiat for cryptocurrency at regulated financial institutions. The legal obligations and transparency of these regulated cryptocurrency “choke points” can give law enforcement significant insight into the activity of illicit actors, similar to the familiar interaction between the anonymous peer-to-peer cash and regulated financial ecosystems.

⁴⁵ Chainalysis, “The 2020 State of Crypto Crime,” 9.

⁴⁶ Simms, Thomas. “At Least 95 Percent of Crypto Crimes Involve Bitcoin, Chainalysis Executive Says.”

⁴⁷ Chainalysis, “The 2020 State of Crypto Crime,” 12.

⁴⁸ Ibid.

⁴⁹ Ibid.

⁵⁰ Chainalysis, “The 2020 State of Crypto Crime,” 15.

⁵¹ Chainalysis, “The 2020 State of Crypto Crime,” 9.



All cryptocurrencies, whether or not they have transparent blockchains, are subject to these protections. It is important to note that some cryptocurrencies offer enhanced privacy for their users in order to offer digital cash-like transactions, yet, among illicit actors, bitcoin remains the preferred cryptocurrency of choice, which features a transparent blockchain.⁵² Rather than explain how law enforcement leverages the interaction between the peer-to-peer and regulated VASP ecosystems to identify and disrupt illicit behavior, the next section collates articles from the Department of Justice's *Journal of Federal Law and Practice* to let the United States' premiere law enforcement officials explain.

Law enforcement can leverage information on transparent blockchains to “follow the money” and establish attribution in cases involving cryptocurrencies.⁵³ According to the articles, “cryptocurrency, despite the purported anonymity it grants criminals, provides law enforcement with an exceptional tracing tool: the blockchain.”⁵⁴ Indeed, “armed only with the knowledge of a target's cryptocurrency address and this single—but highly valuable—data set, law enforcement can learn a myriad of vital pieces of information about a target.”⁵⁵

“While this information can be highly valuable to a criminal investigation, the value largely depends on the investigators' ability to **put the information into context**. On its own, viewing cryptocurrency transactions on the blockchain shows only the transfer of some quantity of funds from one string of letters and numbers to another at a point in time. Correlating that activity to real world events—for example, the payment of funds by a victim or an undercover agent—provides additional context. **The greatest value, however, may come from the ability to associate certain addresses with known entities, particularly virtual currency exchanges [i.e. “choke points”]**. The known entities may collect records regarding the user's true identity and by tracing a target's funds to the entity, law enforcement can glean valuable insight into a target's true identity.”⁵⁶

In sum, the interaction between the hosted and self-hosted ecosystem is the foundation of law enforcement's ability to “tie” information to real world criminal activity and identities. Without overlap between the self-hosted and hosted ecosystems, law enforcement would have much more difficulty ascertaining the identity of individuals using self-hosted wallets for illicit purposes. In essence, bifurcating or restricting the cross-pollination between the hosted and self-hosted ecosystems would undermine law enforcement's ability to attribute illicit activity involving cryptocurrencies, with or without transparent blockchains, to criminal actors. Indeed,

⁵² Christiansen and Jarrett, “Forfeiting Cryptocurrency: Decrypting the Challenges of a Modern Asset,” 166.

⁵³ Simms, Thomas. “At Least 95 Percent of Crypto Crimes Involve Bitcoin, Chainalysis Executive Says.”

⁵⁴ Christiansen and Jarrett, “Forfeiting Cryptocurrency,” 166.

⁵⁵ Ibid.

⁵⁶ Korver, Pelker, and Poteat, “Attribution in Cryptocurrency Cases,” 246.

⁵⁶ Korver, Pelker, and Poteat, “Attribution in Cryptocurrency Cases,” 246–47.



many of the individuals charged in recent high-profile “busts” involving cryptocurrencies were identified because their illicitly obtained cryptocurrency was eventually sent to a hosted wallet at a regulated intermediary that law enforcement was able to subpoena to establish attribution for the relevant criminal activity.

Criminals have not widely adopted cryptocurrencies. Cryptocurrency markets are currently insufficiently deep and liquid to facilitate large scale illicit financial activity, and due to the effectiveness with which criminals already exploit the traditional financial system, there is little incentive to adopt cryptocurrencies. In addition, the largest “gap” in the AML/CFT regime when it comes to cryptocurrency markets is non-compliant VASPs, not peer-to-peer transactions. As such, applying additional restrictions to peer-to-peer transactions would not only fail to achieve the intended policy goal of addressing ML/TF risks in the cryptocurrency ecosystem but also impede law enforcement’s existing ability to leverage blockchain analysis to hunt down and disrupt the limited illicit activity facilitated by cryptocurrencies.

There is no evidence to suggest that placing additional restrictions on self-hosted wallets in the United States or regulated entities’ ability to facilitate transactions involving self-hosted wallets would discourage the already limited and comparatively miniscule criminal use of cryptocurrencies. Without a doubt, criminals would simply practice their own form of “regulatory arbitrage” to continue using cryptocurrencies, and instead of potentially transacting with regulated entities that could be subpoenaed, simply employ entities out of law enforcement’s reach to launder their funds. At the same time, the freedom and liberty of individuals using cryptocurrencies for legitimate purposes (about 99% of all transaction activity⁵⁷) would be seriously restricted, with potentially disastrous effects.

⁵⁷ Chainalysis, “The 2020 State of Crypto Crime,” 5.

Additional restrictions on self-hosted wallets would lay the foundation for omniscient surveillance by eliminating a digital cash-like payment option

Overview

As the world becomes increasingly digitized, the use of cash is in a steady state of decline. Cash's decline has significant policy implications due to the fact that cash transactions underpin individuals' privacy and autonomy, which are both fundamental civil liberties. **If cash usage continues to be substituted for digital transaction options and peer-to-peer transactions using self-hosted wallets are restricted, only non-private payment options will be available to individuals. This lack of transactional privacy will not only threaten fundamental civil liberties but also hasten the creation of all-knowing surveillance systems.** Alarming, both global and domestic examples, which will be further explored in this section, evidence this danger. Free societies must ensure that there are digital payment methods that replicate the privacy and autonomy of cash transactions. Peer-to-peer transactions using self-hosted wallets represent the only extant option, so it is essential that their use remain largely unrestricted.



Cash dethroned

Today, it is reasonable to assume that there is an online corollary to any in-person cash transaction. Twenty years ago, when a person needed more shampoo, he or she would go to the store and, more likely than not, purchase it with cash. Now, all the individual needs to do is click a few buttons on the computer and the shampoo will be on his or her doorstep in one to three business days. It is axiomatic to say that economic activity of every variety is becoming increasingly digitized. As major sectors of the economy have transitioned to digital modes of business, not to mention consumers' desire for convenience, the demand for cash has waned. Indeed, several countries, including Sweden, Norway, Denmark, Iceland, Finland, and South Korea, have begun efforts to completely phase out cash at the national level⁵⁸, and large digital payments corporations have begun global campaigns aimed at reducing the use of cash.⁵⁹

⁵⁸ Jerry Brito, "The Case for Electronic Cash: Why Private Peer-to-Peer Payments Are Essential to an Open Society," Research Report (Washington, D.C.: Coin Center, February 2019), 4–5, <https://www.coincenter.org/the-case-for-electronic-cash/>.

⁵⁹ In 2016, Visa Europe launched its 'Cashfree and Proud' Campaign in an attempt to push consumers away from using cash for daily purchases. One of Visa Europe's radio advertisements for the campaign can be viewed here: <https://www.youtube.com/watch?v=uZm5bYGzVYc>.



The decline in individuals' use of cash transactions, regardless of the cause, has significant implications for individuals and society as a whole. In "The Case for Electronic Cash," Jerry Brito examines the role that cash plays in civil and individual liberties: "eliminating cash means that all transactions are necessarily intermediated, and intermediation undermines privacy and autonomy—two values necessary for the individual liberty and human dignity."⁶⁰ Brito, in the report, goes on to examine how privacy and autonomy are essential to civil liberties, maintaining that "the dignity [privacy] affords is a fundamental part of being human."⁶¹ **Brito explains that "without privacy—without the ability to control what one reveals to others about oneself—it is more difficult to avoid becoming an instrument in someone else's design, to preserve one's dignity."**⁶² Further exploration of privacy's intrinsic connection to individual and civil liberties can be found in Samuel D. Warren and Louis D. Brandeis foundational text, "The Right to Privacy."⁶³ Examined together, the arguments of Brito, Brandeis, and Warren underscore how important private transactions, like cash, are to the maintenance of not only individual liberties but also free and open societies. Brito emphasizes that "an open society works only if individuals are free to engage in critical thinking to develop, communicate, critique, and accept or reject ideas. That, in turn, requires freedom of thought and expression and association."⁶⁴ In other words, privacy and autonomy are essential features of a functioning, free society that values the individual liberty and dignity of each of its citizens. As cash usage declines, it becomes increasingly important to develop and protect transactional options that replicate the autonomy and privacy of purchasing something with cash.

As previously discussed, peer-to-peer transactions using self-hosted wallets represent a legitimate replication of cash-like transactions in the digital world. In other words, peer-to-peer transactions using self-hosted wallets can successfully mirror the privacy and autonomy of cash transactions. If cash usage continues to decrease and peer-to-peer transactions using self-hosted wallets are limited or banned, however, only intermediated, non-private digital payment options will be available to individuals. The policy implications of this fundamental undermining of privacy and autonomy would be far reaching, yet the most disturbing and evident lies in the possibility for ever-more-efficient surveillance and control of individuals. Authoritarian governments already exploit non-private digital financial transactions to control their populations, and the following examples demonstrate the potential consequences of restricting a digital cash-like option in this increasingly digital world.

⁶⁰ Brito, "The Case for Electronic Cash," 15.

⁶¹ Brito, "The Case for Electronic Cash," 17.

⁶² Brito, "The Case for Electronic Cash," 14.

⁶³ Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," Harvard Law Review 4, no. 5 (December 15, 1890): 193–220.

⁶⁴ Brito, "The Case for Electronic Cash," 13.



Peer-to-peer payments and authoritarian governments

Roger Huang's article in *Forbes*, "States Will Censor Money: Cryptocurrency is the Counter," highlights one of the most promising applications of cryptocurrency: a tool for citizens to protect their privacy and autonomy and evade the oppressive reach of authoritarian governments. In the article, Huang claims that "cryptocurrencies and their ideal of censorship-resistant money bring a new hope by being a potential counter to this power."⁶⁵

While cryptocurrencies do represent a powerful tool for citizens to counter oppressive governments, this power is conditional on individuals' ability to use self-hosted wallets to transact.

Cryptocurrency transactions employing hosted wallets—regardless of any particular characteristic or feature of the cryptocurrency itself—allow authoritarian governments the same level of access and control as traditional digital payment options. In other words, the presence of a third-party intermediary inherent to any hosted wallet transaction creates a vulnerability to be exploited by hostile actors, oftentimes nation-states. If transactions using cryptocurrencies are conducted using self-hosted wallets, however, governments would not have such unfettered access to and control over their citizens' financial information and assets. Recent events in Hong Kong and Venezuela provide real world examples of the need for peer-to-peer transactions using self-hosted wallets and the consequences of potentially restricting their use.

⁶⁵ Roger Huang, "States Will Censor Money: Cryptocurrency Is The Counter," *Forbes*, June 17, 2019, sec. Crypto & Blockchain, <https://www.forbes.com/sites/rogerhuang/2019/06/17/states-will-censor-money-cryptocurrency-is-the-counter/?sh=22114b0119b2>.



Hong Kong

Hong Kong is currently embroiled in a period of intense civil unrest due to its relationship with the People's Republic of China (PRC). Hong Kong was a British colony until 1997, when Britain handed over control of the region to the PRC. After the handover, China and Hong Kong were to coexist using the "one country, two systems" policy through which, for 50 years after the handover, Hong Kong Basic Law would trump any laws that existed in the PRC. Recent encroachments on Hong Kong's autonomy and liberties, however, led hundreds of thousands of Hong Kong citizens to take to the streets in protest. Not only have these protests mobilized a large majority of Hong Kong's populace, but they have also continued for over a year. In response, China imposed the "National Security Law" on Hong Kong, an amorphous law that is already being leveraged to crush dissent, arrest political activists, rewrite textbooks, remove books from libraries, unseat pro-democracy legislators, etc.⁶⁶ An important and potent component of the PRC and Hong Kong governments' strategy to crush Hong

Kong citizens' liberties has been the use of technology to surveil, censor, and ultimately control its citizens.

Facial recognition technology and data tracking have become a commonplace tool that Hong Kong authorities employ in their attempt to curb dissent. In one particularly poignant example, the messaging application Telegram was used by Hong Kong authorities to track and arrest "the administrator of a Telegram chat group with 20,000 members, even though he was at his home miles from the protest site."⁶⁷ Additionally, Hong Kong's ubiquitous "centralized form of payment,"⁶⁸ known as Octopus, has been extensively used by law enforcement to track both criminals as well as protestors. With "more than 1.5 daily purchases or journeys for every man, woman and child in the city" occurring through Octopus, Hong Kong authorities have a unique ability to track the movements and purchases of almost all of its citizens.⁶⁹

To avoid the technological reach of Hong Kong's increasingly hostile authorities, Hong Kongers are utilizing less centralized platforms to conduct transactions. In an article for the New York Times, Paul Mozur and Alexandra Stevenson explain that "to go to and from the protests, many [Hong Kongers] stood in lines to buy single-ride subway tickets [using cash] instead of using their digital payment cards [Octopus], which can be tracked."⁷⁰ Additionally, Roger Huang, in Forbes, describes the surge in demand for cryptocurrencies, especially bitcoin:

Initially, as protests broke out around mid-June, Bitcoin traded at about a \$160 USD premium on TideBit, a Hong Kong based exchange. As protests have worn on, that premium still persists, with the latest price of Bitcoin on TideBit at \$11,477.34 USD, about \$80 USD higher than the current rate on Coinmarketcap.⁷¹

⁶⁶ Ramzy, Austin, Tiffany May, and Elaine Yu. "China Targets Hong Kong's Lawmakers as It Squelches Dissent." The New York Times. November 11, 2020, sec. Asia Pacific. <https://www.nytimes.com/2020/11/11/world/asia/hong-kong-protest-democracy.html>.

⁶⁷ Paul Mozur and Alexandra Stevenson, "Chinese Cyberattack Hits Telegram App Used by Hong Kong Protesters," New York Times, June 13, 2019, sec. Asia Pacific, <https://www.nytimes.com/2019/06/13/world/asia/hong-kong-telegram-protests.html>.

⁶⁸ Roger Huang, "As Protests In Hong Kong Surge, So Does Demand For Cryptocurrency," Forbes, August 11, 2019, sec. Crypto & Blockchain, <https://www.forbes.com/sites/rogerhuang/2019/08/11/as-protests-in-hong-kong-surge-so-does-demand-for-cryptocurrency>.

⁶⁹ Parry, Simon. "The Long Tentacles of the Law." China Daily, January 6, 2011, HK Edition edition.

⁷⁰ Paul Mozur and Alexandra Stevenson, "Chinese Cyberattack Hits Telegram App Used by Hong Kong Protesters," New York Times, June 13, 2019, sec. Asia Pacific, <https://www.nytimes.com/2019/06/13/world/asia/hong-kong-telegram-protests.html>.

⁷¹ Roger Huang, "As Protests In Hong Kong Surge, So Does Demand For Cryptocurrency," Forbes, August 11, 2019, sec. Crypto & Blockchain, <https://www.forbes.com/sites/rogerhuang/2019/08/11/as-protests-in-hong-kong-surge-so-does-demand-for-cryptocurrency/?sh=5c61e96a75f6>.



In response to this surge in demand, stores and restaurants around the city have begun to accept bitcoin and other cryptocurrencies as a form of payment.⁷² While the acceptance and use of cryptocurrencies in Hong Kong demonstrates citizens' increased desire for privacy and autonomy within the digital payment ecosystem, an examination of the structure that underpins these cryptocurrencies demonstrates that

without employing self-hosted wallets, Hong Kong citizens' use of cryptocurrencies does not actually provide the privacy and autonomy that they so desperately need.

When cryptocurrency transactions occur using hosted wallets, i.e. wallets controlled by a third-party intermediary, authorities have the ability to conduct the kind of surveillance and control that occurred in both the Telegram and Octopus examples. In essence, the presence of a third-party intermediary in cryptocurrency transactions exposes users to the same risks as the centralized platforms that led to the arrest of protestors due to the fact that authorities can compel these third-party intermediaries to release user information, seize assets, etc. If these transactions occur on a peer-to-peer basis using self-hosted wallets, however, there would be no third-party to hand over customer information or data to government authorities. Instead, individuals would hold all autonomy over their digital wallets and the cryptocurrency managed by them.

⁷² Huang, "As Protests In Hong Kong Surge, So Does Demand For Cryptocurrency."



Venezuela

Since 2014, Venezuela has been experiencing an unprecedented economic recession that has sparked both a humanitarian and political crisis that extends to almost every sector of Venezuelan society. Lawyers, doctors, and day laborers alike are struggling to put food on the table for themselves and their families, and millions of Venezuelans have taken to the streets in protest of the horrendous circumstances plaguing the country.⁷³

In 1998, with the election of Hugo Chavez to the presidency, Venezuela began to pivot toward socialism. Chavez, using the economic advantage gained from Venezuela having the world's largest reserves of crude oil, began to invest massive amounts of capital on social programs aimed at helping the impoverished. While Chavez's strategy was initially not problematic, when the price of oil collapsed, the country fell into turmoil. When Chavez died of cancer in 2013, his hand-picked successor, Nicolás Maduro, assumed the presidency of Venezuela. In addition to failing to improve the dismal economic and social circumstances of Venezuela, Maduro's first presidential term was characterized by significant efforts to consolidate his power and silence political opposition. With Maduro's reelection in 2018 marred with significant controversy and international condemnation, opponents of Maduro unified, and in 2019, the head of the National Assembly, Juan Guaidó, invoked the Venezuelan constitution to declare himself interim president. Maduro ultimately refused to recognize Guaidó, which led to two presidents dueling for control of the country.⁷⁴ Venezuela's political crisis is exacerbated by the concurrent collapse of Venezuela's economy and social fabric.

One of the primary causes of the crisis is hyperinflation: "[Venezuela's] national currency, the Bolivar, [has] becom[e] practically worthless as hyperinflation rates hit 10,000,000% last year."⁷⁵ With inflation of this magnitude, food prices have skyrocketed, lines to get gas are miles long, and many other sectors of Venezuelan society, including hospitals, are suffering massive resource shortages. Indeed, according to a U.S. Department of State report on Venezuela, "90% of hospitals lack medicine and clean water...[and] one out of five Venezuelans were undernourished in 2019."⁷⁶ Not only has this crisis caused mass suffering among Venezuelan citizens, but it has also caused a mass exodus from the country, with more than 5.2 million Venezuelans fleeing in search of opportunities elsewhere. The lack of stability in all sectors of

Venezuelan society has pushed citizens desperate for any semblance of financial and social normalcy towards external sources of certainty. Cryptocurrency is one such source. According to Chainalysis's "2020 Geography of Cryptocurrency Report," Venezuela "has reached one of the highest rates of cryptocurrency usage in the world...as many Venezuelans rely on cryptocurrency to receive remittances from abroad and preserve their savings against hyperinflation."⁷⁷ As cryptocurrencies have become increasingly popular in Venezuela, several events

⁷³ Patrick J. Kiger, "How Venezuela Fell From the Richest Country in South America into Crisis," History, May 9, 2019.

⁷⁴ Ibid.

⁷⁵ Chainalysis, "Hyperinflation and Sanctions Evasion: What On-Chain Data Tells Us About Venezuelans' Trust in Cryptocurrency," Chainalysis, August 27, 2020, <https://blog.chainalysis.com/reports/venezuela-cryptocurrency-market-2020>.

⁷⁶ Bureau of Conflict and Stabilization Operations, "New Hope for Democracy: In Pursuit of Freedom in Venezuela" (Washington D.C.: U.S. Department of State, September 2020), <https://dos-cso.maps.arcgis.com/apps/Cascade/index.html?appid=7437108347fa49f396e820302420f497>.

⁷⁷ Chainalysis, "Hyperinflation and Sanctions Evasion: What On-Chain Data Tells Us About Venezuelans' Trust in Cryptocurrency."



surrounding the inception of the crypto ecosystem demonstrate the importance of peer-to-peer transactions using self-hosted wallets.

With cryptocurrency gaining traction throughout Venezuela, Maduro responded by creating his own national cryptocurrency project called the PETRO in 2018. Designed to skirt sanctions and combat the devaluation of Venezuela's national currency, the bolívar, the PETRO has not been as well nor as widely received as Maduro and the rest of his administration had hoped. Chainalysis posits that "in Venezuela, the lack of trust in the Maduro regime appears to be pushing citizens away from government-connected cryptocurrency platforms. Instead...they're going to peer-to-peer exchanges that serve the world independent of any government."⁷⁸ Unable to entrust third-party hosted wallet providers subject to the power of Venezuela's corrupt government, Chainalysis' analysis of Venezuelans' response to the PETRO captures why it is important for individuals to have the option to conduct transactions on a peer-to-peer basis using self-hosted wallets. These citizens, wronged time and again by their government, do not want to place any more of their trust or finances in the hands of this government or third-parties subject to its control. They are desperate for a tool that will ensure their financial futures, not perpetuate the present, and peer-to-peer transactions using self-hosted wallets are a viable option. Additionally, as in Hong Kong, peer-to-peer transactions using self-hosted wallets provide users with the assurance that their transactions cannot be disrupted by the government, which is notorious for its blatant affronts to human rights, including censorship, violence, and forced imprisonment.

While Maduro does allow cryptocurrency platforms to operate in Venezuela, the dictator has imposed significant restrictions on the number and type of platforms that are allowed. These restrictions have been especially cumbersome for doctors during the global pandemic. As the pandemic continues and worsens, doctors in Venezuela are struggling both with limited resources and insufficient salaries. The United States, in an attempt to help these doctors, unfroze money that was seized pursuant to U.S. sanctions on Maduro and his government. They released the money to Juan Guiadó, who made the decision to deliver these funds to Venezuelan doctors using a blockchain-based platform. To access the funds, Venezuelan doctors were to make an account on the platform and register to receive the funds. Several problems arose, however, when it came time to actually deliver the funds to the doctors. At the root of these problems was the fact that the transactions were occurring using hosted wallets. Because the doctor's accounts were created using an intermediating platform, the doctors' accounts, as well as the platform itself, were subjected to attacks by the Maduro government:

"Receiving the funds is technically illegal under Venezuelan law. Because of currency controls in Venezuela, the payment is processed on a digital platform widely used on the informal black market. The platform, AirTM, is illegal in Venezuela -- healthcare workers must access it through a virtual private network to bypass digital checkpoints set up by the Maduro government."⁷⁹

⁷⁸ Chainalysis, "Hyperinflation and Sanctions Evasion: What On-Chain Data Tells Us About Venezuelans' Trust in Cryptocurrency."

⁷⁹ Stefano Pozzebon, "Venezuelan Health Workers Are Getting Cash Bonuses from an Unexpected Source," CNN, September 9, 2020, U.S. edition, sec. Americas, <https://www.cnn.com/2020/09/09/americas/venezuela-covid-19-payments-guaid-intl/index.html>.



It is clear from both the doctors' struggles to get their much-deserved bonuses and Venezuelan citizens' reticence to engage with not only a centralized, government-led cryptocurrency but also intermediaries subject to the government's interdictions that peer-to-peer transactions using self-hosted wallets are a fundamental check on the excesses of authoritarian regimes. Self-custody and peer-to-peer transactions offer Venezuelans the opportunity to take their futures into their own hands, a power that must be protected and should be nurtured.

Conclusion

As the global economy edges closer to a cashless, digital first economy, it is crucial that digital, cash-like transactions are preserved. Peer-to-peer transactions using self-hosted wallets represent a legitimate avenue for replicating cash-like transactions due to their lack of dependence on third party intermediaries. If all digital transactions require third party intermediaries that have access to consumer data and information, then the cashless economy of the future will inevitably become a surveillance economy. One need only look to Hong Kong and Venezuela for evidence of this phenomenon. With digital peer-to-peer transactions, however, the privacy and autonomy associated with cash transactions can be replicated, and the civil and individual liberties that underpin democratic societies will be preserved. In other words, the importance of maintaining and preserving the ability to conduct digital peer-to-peer transactions cannot be understated.

Additional restrictions on self-hosted wallets would eliminate the unique features of cryptocurrencies that make them a catalyst of financial inclusivity

Peer-to-peer payments and financial inclusivity in the United States

Not all people enjoy equal access to the financial system. While certain demographics enjoy every benefit that modern financial systems and economies have to offer, other groups are left out in the cold, denied access to even the most basic of financial amenities like a bank account. At the Blockchain Association, it is our belief that digital peer-to-peer payments represent a promising lead in addressing this national inequity.

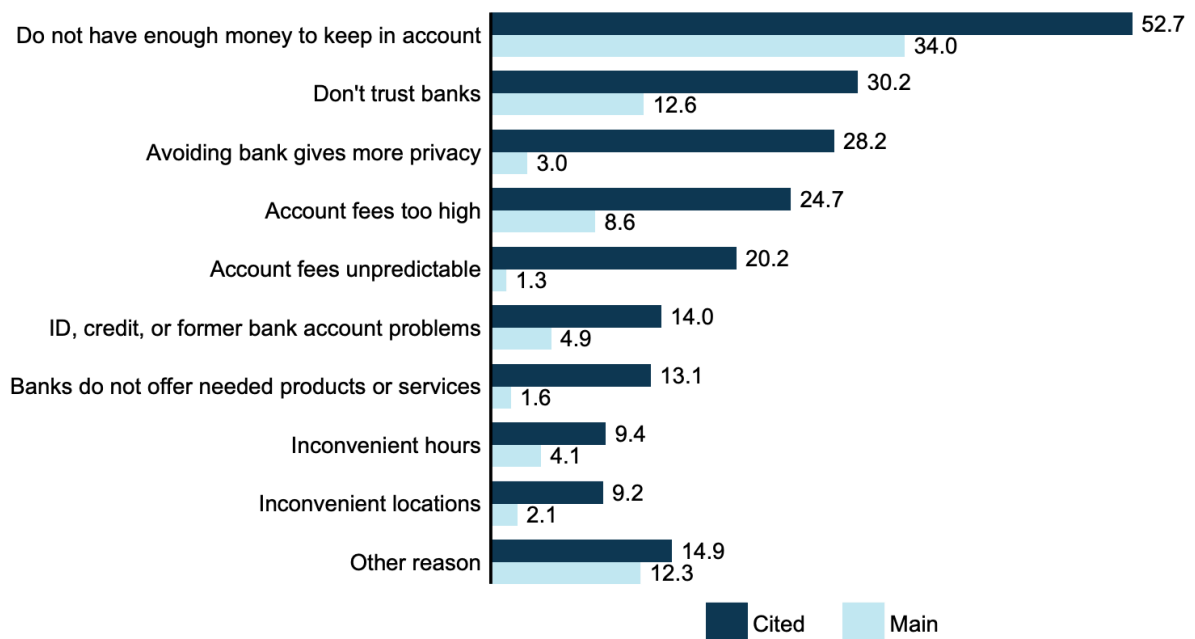
Since 2009, the Federal Deposit Insurance Corporation (FDIC) has conducted a biennial survey, the FDIC National Survey of Unbanked and Underbanked Households, in order to gauge and subsequently address the inclusivity of the United States' financial system. Although the most recent of these surveys occurred in June 2019, the results have not been made public yet, so this section will focus on the findings of the survey that occurred in June 2017. The 2017 survey collected responses from 35,000 households across the United States,⁸⁰ with its primary focus being to provide estimates of the number of unbanked or underbanked households in the U.S.

⁸⁰ Gerald Apaam et al., "FDIC National Survey of Unbanked and Underbanked Households" (Washington D.C.: Federal Deposit Insurance Corporation, 2017), 1.



Before looking at the numbers associated with unbanked and underbanked households in the U.S, it is important to define both concepts. The term unbanked refers to households whose inhabitants have neither a savings nor a checking account. The term underbanked includes households that “had a checking or savings account and used one of the following products or services from an alternative financial services (AFS) provider in the past 12 months: money orders, check cashing, international remittances, payday loans, refund anticipation loans, rent-to-own services, pawn shop loans, or auto title loans.”⁸¹ According to the 2017 survey, 6.5% of U.S. households were unbanked, which amounts to 14.1 million adults and 6.4 million children having zero access to traditional financial institutions. Additionally, 18.7% of U.S. households were underbanked, which suggests that 24.2 million U.S. households, or 48.9 million adults and 15.4 million children, were required to side-step the traditional financial system in order to access necessary funds.⁸²

Figure ES.4 Reasons for Not Having a Bank Account, Unbanked Households, 2017 (Percent)



Source: FDIC National Survey of Unbanked and Underbanked Households" (Washington D.C.: Federal Deposit Insurance Corporation, 2017)

⁸¹ Gerald Apaam et al., "FDIC National Survey of Unbanked and Underbanked Households."

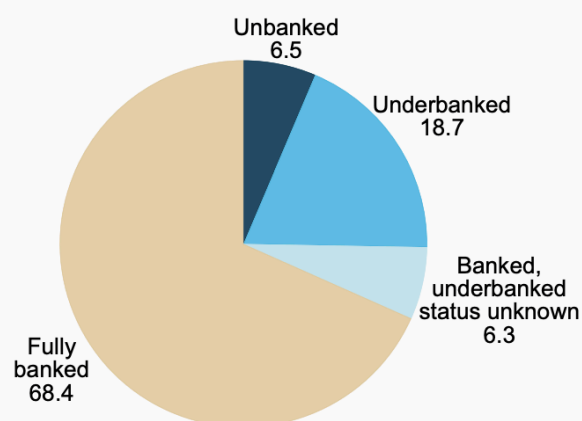
⁸² Ibid.



These numbers are concerning for a variety of reasons. Firstly, the United States is considered a developed nation with a relatively high standard of living, yet a significant percentage of its citizens cannot even access basic financial services. Additionally, the demographics that make up the unbanked and underbanked in the United States are predominantly low-income households of color.

Another important feature of the 2017 FDIC Survey was its attempt to determine why certain households were unbanked. The top four reasons for a household being unbanked were as follows: 1) “Do not have enough money to keep in account,” 2) “Don’t trust banks,” 3) “Avoiding bank gives more privacy,” 4) Account fees too high.”⁸³ In examining these four reasons for U.S. households being unbanked, it becomes clear that digital peer-to-peer transactions represent a viable opportunity to begin to address some of these issues.

Banking Status of U.S. Households, 2017 (Percentage)



Source: FDIC National Survey of Unbanked and Underbanked Households” (Washington D.C.: Federal Deposit Insurance Corporation, 2017)

Digital peer-to-peer transactions remove many of the barriers to entry that restrict unbanked households from accessing financial services. Traditional financial institutions are profit driven, meaning they will oftentimes not conduct business with “unprofitable” individuals, i.e. poor people, people with no credit history, etc. Due to traditional financial institution’s unwillingness to conduct business with “unprofitable” individuals, like the unbanked, it makes sense that the top reason that unbanked households cited for not having a bank account was that they “do not have enough money to keep in account.” With permissionless peer-to-peer transactions, however, no third parties, like traditional financial institutions, are involved, meaning that no company or person has the power to refuse individuals and households access to the system. Everyone has the ability to participate as long as they have internet access.

The second most frequently cited reason by unbanked households for not having a savings or checking account was a lack of trust in banks, which can also be ameliorated by digital peer-to-peer transactions. Because cryptocurrency networks are decentralized, i.e. thousands of different nodes collectively run the software/protocols, there is no need to put one’s trust in a centralized third-party like a bank. This decentralized structure also creates a certain level of pseudonymity, which ultimately resolves the third most cited reason for being unbanked, the desire for privacy. Banks must gather a large amount of personal information about their

⁸³ Apaam et al., “FDIC National Survey of Unbanked and Underbanked Households,” 4.



customers, and data breaches that expose individuals' financial information or history can be severely disruptive. In cryptocurrency networks, however, there is no central authority gathering this type of data, so users have greater discretion to control the amount of personal information that is shared with others.

Finally, digital peer-to-peer payments reduce the costs and fees associated with transacting through an intermediary like a bank. According to a magazine article published by Inside Magazine, "Blockchain can enable near-real time and accurate payments, thus reducing transaction processing cost."⁸⁴ Additionally, many of the fees associated with opening and managing an account with a third party institution will become obsolete with the advent of decentralized networks that eliminate the need for these costly intermediaries.

In conclusion, a portion of the United States' population is either unbanked or underbanked. This lack of access to traditional financial institutions must be addressed. Digital peer-to-peer transactions that are run on blockchain platforms have the potential to make great strides in reducing the number of unbanked, U.S. households by eliminating the need for self-interested intermediaries like banks. Additionally, peer-to-peer transactions are carried out on a trust-minimizing, decentralized platform that is devoid of high fees. In short, these transactions are a credible solution for the millions of people who do not have access to the traditional financial system in the United States.

Peer-to-peer payments and global financial inclusivity

While peer-to-peer transactions represent a legitimate solution for millions of unbanked or underbanked individuals in the United States, these transactions have the potential to help billions of people around the globe gain access to critical financial services. According to the World Bank's report entitled *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution*, "Globally, about 1.7 billion remain unbanked-without an account at a financial institution or through a mobile money provider."⁸⁵ Just like the 2017 FDIC Survey, the 2017 World Bank report attempted to identify the reasons why so many people, almost one fourth of the global population, are unbanked. A summary of these reasons are reproduced below:

"The most common [reason] was having too little money to use an account. Two-thirds cited this as a reason for not having a financial institution account, and roughly a fifth cited it as the sole reason. Cost and distance were each cited by about a quarter of those responding to the question...Lack of documentation and distrust in the financial system were both cited by roughly a fifth of adults without a financial institution account, and religious concerns by 6 percent."⁸⁶

⁸⁴ Marco Lichtfous, Vivek Yadav, and Valentina Fratino, "Can Blockchain Accelerate Financial Inclusion Globally?," Inside Magazine, October 2018, 5.

⁸⁵ Asli Demirgüç-Kunt et al., "The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution" (Washington D.C.: World Bank Group, 2017), 4, file:///Users/LindseyKelleher/Downloads/9781464812590%20(1).pdf.

⁸⁶ Demirgüç-Kunt et al., "The Global Findex Database 2017," 5.



A common denominator among the above reasons is financial institutions. Whether the bank is too far, too expensive, or too corrupt, it is clear that billions of people are not obtaining the financial services that they need due to issues associated with financial intermediaries. CoinDesk's Edan Yago corroborates this claim with his assertion that "entire countries have fallen victim to prejudice and a lazy risk aversion on the part of the banks. Many small countries in the Caribbean, the Pacific and Africa are almost entirely locked out of the global payments system."⁸⁷ Peer-to-peer transactions using self-hosted wallets eliminate the need for these intermediaries and thus are a legitimate solution to the global inequity that is lack of access to basic financial services. In other words, peer-to-peer transactions using self-hosted wallets will give billions the ability to invest in themselves and their futures without the need for or reliance on unpredictable, expensive, censorable, and potentially corrupt intermediaries.

The potential that peer-to-peer transactions using self-hosted wallets have to bolster global financial inclusion is best exemplified by an examination of how these transactions might revolutionize global remittances. Remittances are defined by the World Bank as "the cost of sending and receiving small amounts of money from one country to another."⁸⁸ Generally speaking, migrant workers who have left their home countries in search of greater economic opportunity are the initiators of remittances. In 2016, the World Bank estimated that 232 million migrants were sending money, in the form of remittances, to developing countries, and in 2019, \$714 billion in remittances were sent around the world.⁸⁹ In other words, the livelihoods of some of the world's most vulnerable people are dependent on remittances. While remittances are a lifeline for the least privileged, a notable chunk of this money ultimately does not reach its intended recipient due to the high fees that remittance service providers charge their customers:

"Indeed, if the cost of sending remittances could be reduced by 5 percentage points relative to the value sent, remittance recipients in developing countries would receive over \$16 billion dollars more each year than they do now."⁹⁰

It is clear from this quotation that the costs associated with sending remittances are alarmingly high, and it is the belief of the Blockchain Association that peer-to-peer transactions using self-hosted wallets will more than address this unfair burden. If migrants were able to send remittances using self-hosted wallets, the exorbitant fees charged by the intermediaries facilitating these transfers will be greatly reduced. More money will go to the people who actually need it, and thus greater financial inclusivity around the globe will be engendered through the implementation of peer-to-peer transactions using self-hosted wallets.

⁸⁷ Edan Yago, "There's a Bigger Scam Than Anything in Crypto, It's Called KYC/AML," CoinDesk, July 27, 2018, sec. Business, <https://www.coindesk.com/theres-a-bigger-scam-than-anything-in-crypto-its-called-kyc-aml>.

⁸⁸ Remittance Prices Worldwide, "Remittance Prices Worldwide," The World Bank, 2018, <https://remittanceprices.worldbank.org/en/about-remittance-prices-worldwide>.

⁸⁹ Ibid.

⁹⁰ Ibid.

Additional restrictions on self-hosted wallets would indiscriminately apply payments regulation on a diverse and developing ecosystem with applications beyond the transmission of money

While cryptocurrencies represent the primary application of blockchains, the potential applications of blockchains are limitless. Since the creation of the first cryptocurrency eleven years ago, innovators have explored a range of potential applications of blockchains—including but not limited to payments-like tools—and the permissionless nature of distributed ledgers allows anyone around the world with an internet connection to experiment with them. Importantly, since the ecosystem is still in its infancy, use cases for distributed ledgers will likely emerge that have not yet been imagined. The blanket application of payments regulation to self-hosted wallets would not only fail to recognize the diverse applications (existing and potential) of distributed ledgers but also stymie ongoing experimentation with distributed ledgers that could bring to fruition revolutionary products and services.



To begin with, it is important to understand that distributed ledgers can store unique data sets, including but not limited to a record of transactions in a given cryptocurrency. For example, one's public address and private key may be used to access "a peer-to-peer network that stores files on the internet," in other words a decentralized "cloud storage" network.⁹¹ The types of data one could store via the use of decentralized networks are theoretically limitless, but an everyday example could be family photos. An individual could use a private key managed with a self-hosted wallet to access these photographic digital "assets."

In this regard, self-hosted wallets again resemble traditional "tools" with which individuals safely store assets, which evidences why the blanket application of payments regulation to self-hosted wallets would be fundamentally misguided. While individuals often store financial assets in safes and bi-folds, many individuals choose to store important documents in safes and a family photo in their wallet. A blanket policy mandating that any "asset" moving into or out of these storage tools be subject to payments regulation makes little intuitive sense, and the same logic applies to self-hosted wallets. They can be used hypothetically to "store" any digital information, and applying payments regulation to them fails to recognize this fact.

While applying payments regulation to self-hosted wallets would fail to recognize the diverse existing applications of distributed ledgers, it would also stifle ongoing experimentation with distributed ledgers that could bring to fruition revolutionary products and services. For example, because participation in open blockchain networks is permissionless, computer programs themselves can engage in transactions with other computer programs or individuals. In this manner, self-hosted wallets uniquely allow for machines or computer programs to custody assets and engage in transactions without the intervention of humans. This ability allows for innovations previously impossible, such as "self-owning cars."⁹² Existing payments regulations are ill-suited to addressing inanimate counterparties, and this example evidences why payments regulation should not be applied arbitrarily to an ecosystem with extensive and unknown potential use cases. While ideas like "self-owning cars" may seem outlandish, many innovations that now play pivotal roles in individuals' daily lives likely seemed just as far-fetched when they were initially introduced. One need only look to the many breakthroughs facilitated by the internet for a real-world example of the importance of allowing fledgling technologies the ability to develop to their fullest potential.

⁹¹ Protocol Labs. "Introducing Filecoin, a Decentralized Storage Network," San Francisco, CA, 2017. <https://www.youtube.com/watch?v=ECIPAFPeXIQ>.

⁹² Kelion, Leo. "Could Driverless Cars Own Themselves?" BBC News. February 16, 2015, sec. Tech. <https://www.bbc.com/news/technology-30998361>.



Like with distributed ledgers and self-hosted wallets, no permission is necessary for anyone to use or develop applications on the internet, and therefore innovation is decentralized and placed in the hands of creative individuals anywhere in the world. The internet was first created to allow government researchers to communicate,⁹³ but it has, of course, developed into a diverse ecosystem that underlies myriad economic and individual activities throughout every facet of society.

Preemptively restricting the blockchain and crypto ecosystem by applying payments regulation to self-hosted wallets would be akin to mandating that the internet be used solely for research. It would stifle the ongoing innovation that may eventually bring to market revolutionary products and services that are totally unrelated to payments or financial services, such as a decentralized network for data storage. Distributed ledgers are a new technology, and it remains to be seen whether they can, in practice, achieve the many transformational innovations that proponents claim they will. Yet the past is prologue. “Throwing the baby out with the bathwater” in instances of permissionless innovation could be especially costly. The permissionless protocols that underlie the internet were first created in 1972.⁹⁴ Seventeen years later the World Wide Web was invented,⁹⁵ and thirty-three years later media streaming over the internet was introduced. Imagine what would have been lost had regulation been introduced that pigeon-holed the internet into a single use case. The first distributed ledger began operating just over eleven years ago, so it is vital that this technology be given the same opportunity to blossom.

⁹³ Iansiti, Marco, and Karim R. Lakhani. “The Truth About Blockchain.” Harvard Business Review, February 2017. <https://hbr.org/2017/01/the-truth-about-blockchain>.

⁹⁴ Ibid.

⁹⁵ CERN: Accelerating Science. “Where the Web Was Born,” January 2020. <https://home.cern/science/computing/where-web-was-born>.

The Bottom Line:

This is a policy decision that has vast societal implications, and therefore it should be addressed by Congress

As explored throughout this paper, self-hosted wallets serve as the foundation of peer-to-peer value transfer over the internet and play a central role in a developing ecosystem that has applications well beyond payments and financial services. It is clear that restricting individuals' ability to use self-hosted wallets would have significant consequences for our society.

The issue at hand is nuanced, the potential implications are far-reaching, and numerous valid but sometimes competing interests, such as empowering law enforcement while protecting citizens' fundamental rights, must be considered and balanced. While restricting individuals' use of self-hosted wallets is unnecessary and would be misguided, Congress is entrusted with policymaking in instances of competing interests and wide societal effect. The potential regulation of self-hosted wallets should be no different.