# Anti-Money Laundering Regulation of Privacy-Enabling Cryptocurrencies


**DANA V. SYRACUSE** | PARTNER
+1.212.261.6892
DSyracuse@perkinscoie.com

**JOSHUA L. BOEHM** | COUNSEL
+1.602.351.8161
JBoehm@perkinscoie.com

**NICK LUNDGREN** | ASSOCIATE
+1.206.359.8094
NLundgren@perkinscoie.com


PerkinsCoie.com/Blockchain


Perkins Coie LLP

PERKINSCOIE

# Introduction

Privacy-enabling cryptocurrencies, commonly known as privacy coins, are enhanced versions of early cryptocurrencies that were developed to protect the financial privacy of individuals and businesses alike. Each privacy coin leverages innovative mechanisms that provide privacy, encryption, and security to its users. Alongside their positive effects, however, these mechanisms have raised an important compliance question:

Is it possible for regulated entities to comply with anti-money laundering ("AML") obligations when supporting privacy coins?

*The answer, in our view, is yes.*

Not only do privacy coins provide public benefits that substantially outweigh their risks, existing AML regulations properly and sufficiently cover those risks, providing a proven framework for combatting money laundering and related crimes.

In reaching that conclusion, we profile several privacy coins, detail key AML regulations and intergovernmental recommendations affecting privacy coins, and explain the measures that have allowed financial institutions, intermediaries, and virtual asset service providers (collectively, "VASPs") to comply with AML obligations when facilitating privacy coin transactions. We also dispel the misconception that privacy coins are fundamentally incompatible with AML compliance, focusing on measures that have allowed VASPs to comply with AML obligations when conducting or facilitating privacy coin transactions.

This white paper proceeds in four parts, as follows:

In Part 1, we discuss the importance and benefits of financial privacy for individuals and businesses, as well as how privacy coins address identified deficiencies.

In Part 2, we survey several different privacy coins and the mechanisms that each uses for privacy, encryption, and security.

In Part 3, we survey the approaches taken in the United States (at the federal and state level), Japan, and the United Kingdom with respect to AML regulation of privacy coins in addition to the recommendations set forth by the Financial Action Task Force, an intergovernmental body.

Finally, in Part 4, we explore the effectiveness of targeted AML regulation on VASPs and how unique features of certain privacy coins assist VASPs with compliance. We conclude that privacy coins protect legitimate individual and commercial privacy interests and that existing financial regulations sufficiently address the AML issues that privacy coins present.

*Important Note: Perkins Coie LLP represents clients with interests in privacy coins. Certain of those clients have engaged Perkins Coie LLP to provide advice regarding the topics addressed in this white paper. Although the authors have obtained knowledge from those paid engagements and received comments from clients with interests in privacy coins, among other commenters, this white paper reflects the opinions of the authors alone, and not the opinions of Perkins Coie LLP or any of its clients. Furthermore, the content in this white paper is for informational purposes only and may not be relied upon by any party as legal advice. VASPs, and others engaged in privacy coin-related activities, should contact qualified counsel for advice regarding the laws and regulations that may apply to their activities.*

# Table of Contents

*Authors: Dana V. Syracuse, Joshua L. Boehm, & Nick Lundgren*[*]

Page



[*] Dana V. Syracuse is a partner, Joshua L. Boehm is a counsel, and Nick Lundgren is an associate in the Blockchain Technology & Digital Currency industry group at Perkins Coie LLP. The views set forth in this white paper are the authors' sole responsibility. The authors thank Glenn Austin, Caitlin Barnett, Jayson Benner, Jerry Brito, David Chaum, Joseph Cutler, Robby Dermody, Justin Ehrenhofer, Jack Gavigan, Naveen Jain, John Jefferies, DJ Mills, Sarah Shtylman, Riccardo Spagni, Ryan Taylor, Peter Van Valkenburgh, Stephanie Vaughan, and Louis Willacy for insightful comments and generous contributions.

# Part 1

## Financial Privacy: The Utility of Privacy Coins

Individual financial privacy and commercial financial privacy are critical to financial transactions in today's data-driven world. Recognizing the importance of financial privacy, VASPs adopted and implemented strategies, controls, and other protections to safeguard their customers' information, data, and funds. Additionally, VASPs developed various methods to safely facilitate financial transactions and cross-border remittances. As a result, individuals and businesses became reliant on these centralized parties (i.e., financial intermediaries, institutions, and other virtual asset service providers) and incurred costly fees for the convenience of making safe transactions.

The first generation of decentralized cryptocurrencies, namely Bitcoin, sought to remediate society's reliance on centralized financial parties and their high fees by providing a decentralized, low-cost way to transact and remit funds. However, initial cryptocurrency protocols, including the Bitcoin protocol, sacrificed a substantial degree of financial privacy to effectuate the transition toward decentralization. This sacrifice ultimately led to the emergence of privacy coins, which offer individuals and businesses a similar degree of financial privacy, while also providing the benefits of decentralization and low-cost transaction processing.[1]

> …initial cryptocurrency protocols, including the Bitcoin protocol, sacrificed a substantial degree of financial privacy…

### INDIVIDUAL FINANCIAL PRIVACY

While privacy rights are not absolute, governments generally recognize individual privacy as an important right and provide substantial privacy-related legal protections to individuals.[2] Governments have also shown that they are enforcing those individual statutory protections.

In September 2017, the United States Federal Trade Commission ("FTC"), the Consumer Financial Protection Bureau ("CFPB"), and all 50 states and U.S. territories settled data breach claims with Equifax that affected 147 million people for up to $425 million to help those affected, $175 million to 48 of the states, the District of Columbia, and Puerto Rico, and $100 million to the CFPB in civil penalties.[3] Among other things, the complaint alleged that Equifax failed to secure personal information stored on its network in violation of the Gramm-Leach-Bliley Act ("GLBA") Safeguard Rule[4] and the FTC Act.[5]

---

[1] The terms "coin" and "token" generally have the same meaning for purposes of this white paper. Use of "coin" and "token" interchangeably reflects the colloquial use by the network upon which the coin resides or the governing body that regulates such coin or token and is not meant to draw a distinction.

[2] *See, e.g.,* The Right to Financial Privacy Act, 12 U.S.C.A. §§ 3401 - 3423 (2018); *see also* the Gramm-Leach-Bliley Act, 15 U.S.C.A. § 6801 (2011); the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 (2020); General Data Protection Regulations, Regulation (EU) 2016/679.

[3] *See* FTC, *Equifax Data Breach Settlement* (Sept. 2019), https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement; *see also* FTC, *Equifax to Pay $575 million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach*, FTC (July 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related.

[4] *See* 16 C.F.R. Part 314 (2019).

[5] *See* 15 U.S.C.A. § 45 (2006).

Similarly, in July 2019, the United Kingdom's Information Commissioner's Office ("UK ICO") issued a £183.39 million ($230 million) fine to British Airways in connection with a data breach whereby the payment data of British Airways customers was skimmed by a malicious third party via a formjacking attack.[6] Not only did British Airways' violation of the General Data Protection Regulation ("GDPR")[7] result in a large fine, it also opened the door to a class action involving up to 500,000 affected consumers.[8]

These statutory protections,[9] among others, are critical guardrails for an individual's financial privacy. Without these protections and related enforcement efforts, the billions of noncash payments occurring each day would be at risk of unwanted exposure and exploitation.[10]

Notwithstanding statutory protections, when individuals transact using cash, or to a lesser extent, debit or credit cards, those individuals maintain a level of privacy whereby third parties that are not a party to the transaction do not have insight into the transaction's details or even knowledge that the parties effectuated the transaction.

For example, individuals expect that they can donate to charitable causes without revealing to neighbors, their employers, or the general public which charities they supported and how much they donated. If this information cannot be kept private from public view, as it is for the most part when using a credit card, then social deterrence may prevent individuals from donating to charities they would otherwise support, or worse, subject such individuals to discrimination or harassment if the charities are associated with a controversial position.

Additionally, nonprivate transactions are susceptible to aggressive data-mining and harvesting techniques that certain marketing and advertising firms use to target nonconsenting individuals while abusing their personal privacy. Furthermore, nonprivate transactions expose individuals to bad actors that can use public information to identify specific targets for illicit purposes such as identify theft, mugging, kidnapping, and blackmailing.

## COMMERCIAL FINANCIAL PRIVACY

Businesses rely on and expect financial privacy. Without maintaining confidentiality, commercial transactions would be visible for competitors and nefarious actors to analyze, predict, front-run, and exploit. This radically transparent type of environment would likely result in market manipulation by participants, a hindrance to innovation, and an unfair advantage for competitors and counterparties alike.

Today, the majority of commercial transactions (as measured in value) are facilitated through wire or ACH transfers. If this transactional information was not kept confidential, the general public would be able to calculate the revenues, expenses, and other payments that all businesses made or incurred. Additionally, competitors would be able to readily identify each other's supply chain partners, investment strategies, and primary sources of profit, thereby empowering

---

[6] *See* UK ICO Statement (July, 8, 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-ico-announces-intention-to-fine-british-airways/; *see also* Neil Ford, *British Airways data breach: class action lawsuit approved*, IT Governance UK Blog (Oct. 11, 2019), https://www.itgovernance.co.uk/blog/british-airways-data-breach-class-action-lawsuit-approved.

[7] *See generally* General Data Protection Regulation (EU) 2016/679.

[8] *See* Neil Ford, *British Airways data breach: class action lawsuit approved*, IT Governance UK Blog (Oct. 11, 2019), https://www.itgovernance.co.uk/blog/british-airways-data-breach-class-action-lawsuit-approved (referencing the approval of the class action lawsuit); *see also* TechCentral.ie, *The biggest data breach fines, penalties and settlements to date* (Dec. 20, 2019), https://www.techcentral.ie/the-biggest-data-breach-fines-penalties-and-settlements-to-date/ (noting that 500,000 customers were affected).

[9] This refers to the GLBA Safeguard Rule, FTC Act, and GDPR.

[10] The Federal Reserve determined that 174.2 billion noncash payments were made in the United States alone in 2018. *See* U.S. Federal Reserve, *The 2019 Federal Reserve Payments Study* (Dec. 2019), https://www.federalreserve.gov/newsevents/pressreleases/files/2019-payments-study-20191219.pdf; *see also* Capgemini Financial Services Analysis, *Non-Cash Payments Volume*, (2019), https://worldpaymentsreport.com/non-cash-payments-volume-2/#non-cash-transactions-2017-2022f.

them with valuable, proprietary information. Ultimately, this would have a negative impact on the overall economy and would consequently affect businesses and individuals alike.

To illustrate, most grocery store chains source their inventory from third-party producers. While the existence of the relationship can be easily deduced based on the good being made available at the grocery store, the details of each specific transaction are not generally known. If the details were known, competitors and customers would know the cost the grocery store paid for each product, the gross margin that the grocery store makes per sale, and the quantity and sell-through time of each order. This information would provide valuable insight to other grocery businesses because they would be able to see what products are most profitable in specific areas, in addition to knowing exactly how much other businesses have paid for the same product. Moreover, the suppliers of these goods would be forced to further compete on price to the detriment of their margins, which in turn would likely have negative repercussions for investors and for smaller industry players since they would not be able to scale as easily.

… maintaining commercial privacy is critical for protecting the status quo of domestic and international business operations.

Financial markets present another compelling example of the need for commercial privacy, insofar as trading firms often rely on such privacy to prevent front-running of their trades or inadvertent disclosure of their positions.

In sum, maintaining commercial privacy is critical for protecting the status quo of domestic and international business operations. The adoption of cryptocurrencies will continue to expand, and businesses must have a way to utilize this innovative and still-evolving technology without having to sacrifice traditional privacy protections.

## CRYPTOCURRENCIES—A DECENTRALIZED WAY TO CONDUCT TRANSACTIONS, BUT OFTEN LESS PRIVATE

Forms of cryptocurrency originated in 1994 when DigiCash demonstrated the first peer-to-peer cryptographic payment over the Internet using cyberbucks.[11] A defining aspect of DigiCash technology was consumer privacy, which used "blind signatures" to decouple the account of withdrawal from the eventual deposit of the same funds.[12]

Roughly 15 years later, Bitcoin was created,[13] which introduced the first decentralized cryptocurrency. Bitcoin also enabled a low-cost way to transact. For example, a Bitcoin transaction for remitting the equivalent of $200 internationally would cost as little as $0.04[14] to effectuate and validate on the network.[15] This is substantially lower than the global average cost of $14.00 to remit $200 through the traditional financial system.[16]

---

[11] *See* Press Release, DigiCash bv., *World's first electronic cash payment over computer networks* (May 27, 1994), https://chaum.com/ecash/articles/1994/05-27-94%20-%20World_s%20first%20electronic%20cash%20payment%20over%20computer%20networks.pdf.

[12] *See* Press Release, DigiCash bv., *First Bank to Launch Electronic Cash* (Oct. 23, 1995), https://chaum.com/ecash/articles/1995/10-23-95%20-%20First%20Bank%20to%20Launch%20Electronic%20Cash.pdf

[13] The "Genesis Block" (block 0) of Bitcoin, the first cryptocurrency, was mined on January 3, 2009.

[14] An estimate in October 2019 of the fee to have a transaction mined (i.e., posted) within six blocks, which takes roughly one hour. *See* Bitcoin, *Bitcoin Transaction Fees* (last visited July 17, 2020), https://bitcoinfees.info/.

[15] This uses a presumed average Bitcoin transaction size of 250 bytes. *See* Bitcoin, *Bitcoin Transaction Fees* (last visited July 17, 2020), https://bitcoinfees.info/.

[16] The assumed remittance amount of $200 represents a common benchmark used by authorities. *See* Cecchetti Stephen & Kim Schoenholtz, *The stubbornly high cost of remittances*, VOX CEPR Policy Portal (Mar. 27, 2018), https://voxeu.org/article/stubbornly-high-cost-remittances; *see also Remittance Prices Worldwide*, published by the World Bank for Q2 2019, Issue 30 (June 2019) (noting the global average cross-border remittance cost of 6.84% for all remittance amounts).

However, the Bitcoin protocol, due to its decentralized and transparent nature, lacks the financial privacy protections that traditional financial intermediaries and institutions offer their customers.[17] When individuals transact with certain cryptocurrencies like Bitcoin, the transaction information becomes public, traceable, and permanently stored in the Bitcoin network.[18] Moreover, anyone can view any Bitcoin address, the value that a given Bitcoin address controls, and all past, proposed, and pending transactions in which a Bitcoin address has engaged.[19]

For example, several websites track and list the public addresses, including Bitcoin amounts and certain transaction information, of the top Bitcoin holders worldwide.[20] This information, however, is not restricted to a few insiders, given that anyone with access to the Bitcoin blockchain can deduce this type of information.[21] While linking a natural person or entity with these seemingly random public addresses appears impossible, it is not. To illustrate, if an individual sends Bitcoin to a friend, that individual now knows the friend's Bitcoin address and can view all transactions related to it, as well as the Bitcoin balance that remains. Likewise, when someone registers for an account with a cryptocurrency exchange, the exchange typically requires the registrant to provide identifying information that the exchange now associates with the registrant and cryptocurrency addresses. In both cases, the financial privacy of the address owner is jeopardized whereby unwanted third parties can review the account history linked or suspected to be linked to an individual.

Privacy coins essentially combine the benefits that the traditional financial system and initial cryptocurrencies like Bitcoin offered.

The creation and value proposition of privacy coins, as discussed below, stems from the difference between Bitcoin transactions and traditional financial transactions, in addition to the desire to limit unnecessary disclosure of certain information to traditional financial intermediaries and the world at large.[22]

## PRIVACY COINS—ALLOWING DECENTRALIZED TRANSACTIONS WITH PRIVACY PROTECTIONS

Privacy coins are cryptocurrencies specifically designed to allow individuals and businesses to keep certain details about themselves and their transactions out of the public eye. This enables individuals and businesses to reveal information in a selective or predetermined manner that is not much different from how cash operates today.

Likewise, privacy coins have enabled users to transact in a low-cost, decentralized manner, while maintaining the added benefit of financial privacy that was only previously available through financial intermediaries and institutions in the traditional financial system. While privacy coins take different approaches in how they obfuscate transaction information, each offers users a unique way to protect financial information without sacrificing utility or convenience. Privacy coins essentially combine the benefits that the traditional financial system and initial cryptocurrencies like Bitcoin offered.

---

[17] *See* Bitcoin, *Protect Your Privacy* (last visited July 17, 2020), https://bitcoin.org/en/protect-your-privacy.
[18] *Id.*
[19] *Id.*
[20] *See, e.g.*, BitinfoCharts, *Bitcoin Rich List* (last visited July 17, 2020), https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html.
[21] *See, e.g.*, Yahoo Finance, *Number of bitcoin addresses with at least 10 bitcoins reaches all-time high* (Sept. 9, 2019), https://finance.yahoo.com/news/number-bitcoin-addresses-least-10-174357984.html (showing that the number of addresses with at least 10 Bitcoins has reached an all-time high as of September 1, 2019).
[22] *See* Cryptoassets Taskforce: Final Report, Chart 3.A (Oct. 2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf (noting that full distribution of data raises concerns about privacy in financial services).

A useful analogy in understanding the value proposition of privacy coins, as compared to cryptocurrencies like Bitcoin, comes from the internet's foundational protocols.

Early websites used the Hypertext Transfer Protocol ("HTTP") to transfer data from a web server to a browser to enable users to view webpages.[23] The key issue with HTTP is that the information sent from the server to the browser is not encrypted, thereby allowing malicious actors to view, steal, and exploit transmitted data.

In response, the Hypertext Transfer Protocol Secure ("HTTPS") was developed in the early 1990s as an extension of HTTP to remediate these issues. HTTPS uses Transport Layer Security ("TLS")[24] to authenticate the accessed website and protect the privacy and integrity of the exchanged data while in transit,[25] resulting in protection from a man-in-the-middle ("MITM") attack.[26] Refer to Figure 1-C-1 and Figure 1-C-2 below for visual illustrations of HTTP versus HTTPS.[27]

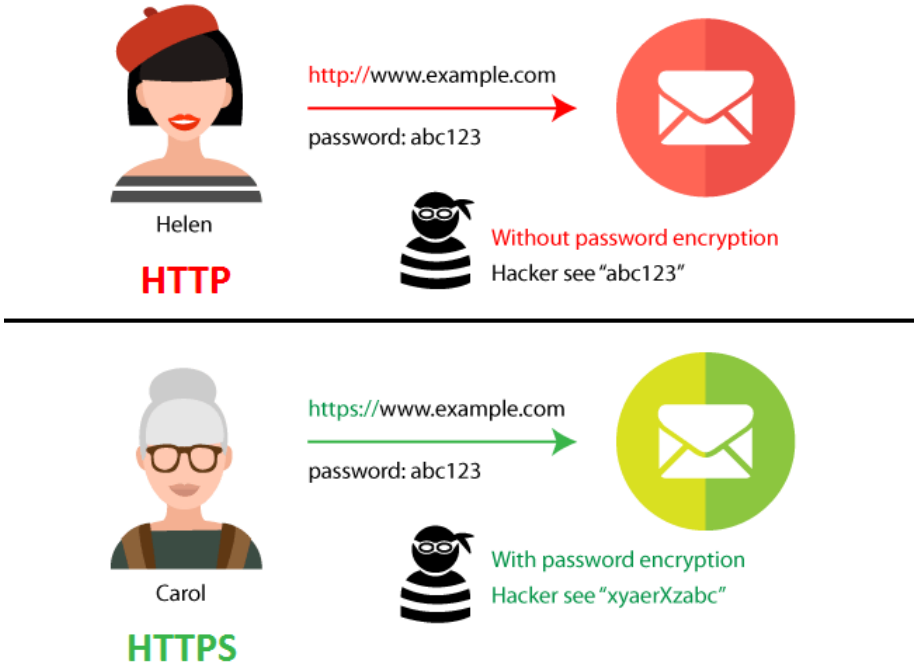



Figure 1-C-1
Source: https://seopressor.com/blog/http-vs-https/

[23] *See* SEOPressor, *HTTP vs HTTPS: The Difference And Everything You Need To Know* (Nov. 11, 2019), https://seopressor.com/blog/http-vs-https/.
[24] TLS was formerly known as Secure Sockets Layer ("SSL"). *See* Wikipedia, *HTTPS* (last updated July 15, 2020), https://en.wikipedia.org/wiki/HTTPS.
[25] *See Secure your site with HTTPS*, Google, https://support.google.com/webmasters/answer/6073543?hl=en.
[26] An MITM attack occurs where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other. *See* Wikipedia, *Man-in-the-middle attack* (last updated July 15, 2020), https://en.wikipedia.org/wiki/Man-in-the-middle_attack.
[27] Source for Figure 1-C-1 and Figure 1-C-2: SEOPressor, *HTTP vs HTTPS: The Difference And Everything You Need To Know* (Nov. 11, 2019), https://seopressor.com/blog/http-vs-https/.

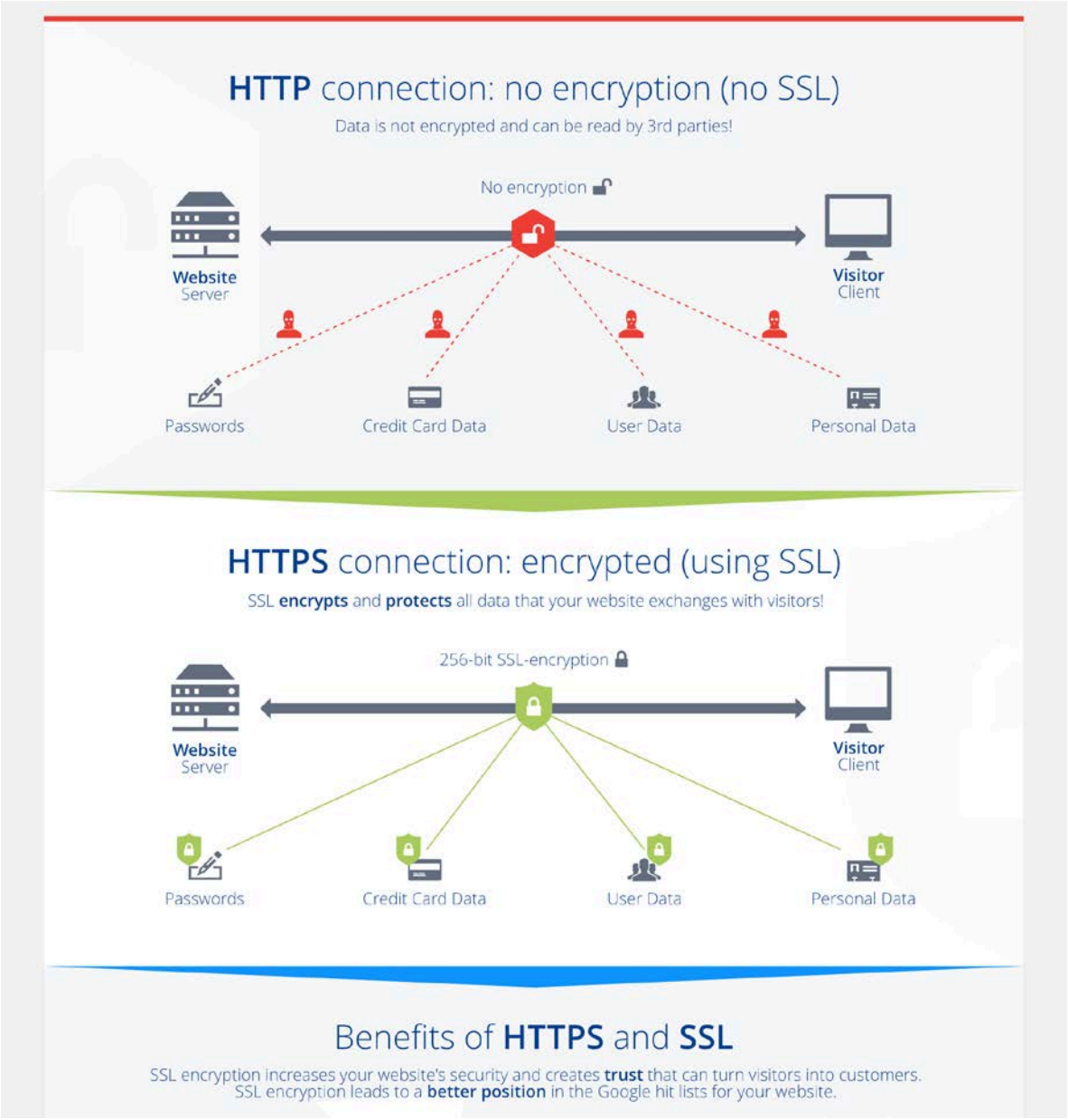



Figure 1-C-2
Source: https://seopressor.com/blog/http-vs-https/

Broad commercial use of encryption software, however, initially faced significant opposition from the U.S. government and law enforcement agencies. Until 1996, encryption software was generally classified in the United States as "munitions," subjecting it to significant export regulations administered by the U.S. Department of State.[28] In the early 1990s, the U.S. government also sought to regulate private use of encryption software through the so-called "Clipper Chip Initiative," which was deployed in 1993 with the goal of subjecting "electronic encryption technology to key escrow in order for the government to hold a key to decode messages" (i.e., a backdoor).[29] These 1990-era battles, dubbed the "Crypto Wars," were largely resolved in favor of public access to encryption software due to "a firestorm of protest on constitutional and economic grounds."[30]

This cleared the way for rapid growth of HTTPS and other encryption software over the following decades, to significant public and commercial benefit. In 2014, Google announced that transitioning from HTTP to HTTPS would grant websites a ranking benefit in an effort to encourage all website owners to switch from HTTP to HTTPS to protect people on the web.[31] In June 2015, the White House Office of Management and Budget issued a memorandum requiring that all publicly accessible federal websites and web services provide service only through a secure connection, and it recommended the use of HTTPS.[32] As of June 2019, over two-thirds of the approximately 150,000 most popular websites surveyed used SSL and TLS enabled websites.[33]

As with earlier generations of encryption software, the privacy-enhancing features of privacy coins have raised concerns among some government and law enforcement agencies. Although those concerns are well-intentioned, the Crypto Wars experience counsels taking a cautious regulatory approach toward promising new technologies so early in their development. Just as HTTPS meaningfully improved on HTTP, privacy coins represent the next generation of the blockchain technology pioneered by the Bitcoin protocol, because privacy coins offer users unique ways to obfuscate certain details to prevent public disclosure when users transact on the privacy coins' respective networks. This desirable characteristic is particularly important for blockchain-recorded transactions because a decentralized blockchain is immutable and can be reviewed at any point in the future. With the rise of big data and machine learning,[34] the need to obfuscate historical transaction and personal data continues to be an important aspect that individuals and businesses alike require. While privacy coins do pose AML risks, effective management of those risks by VASPs as part of a risk-based AML Program (as we explain in the following Parts) should cause the public benefits of privacy coins to outweigh their costs.

---

[28] Paul McLaughlin, *Crypto Wars 2.0: Why Listening to Apple on Encryption Will Make America More Secure*, 30 Temp. Int'l & Comp. L.J. 353 (2016).

[29] *Id.*

[30] *Id.* (quoting Kurt Saunders, *The Regulation of Internet Encryption Technologies: Separating the Wheat from the Chaff*, 17 Marshall J. Computer & Info. L. 945, 952 (1999).

[31] Google, *Google Starts Giving A Ranking Boost To Secure HTTPS/SSL Sites* (Aug. 7, 2014), https://searchengineland.com/google-starts-giving-ranking-boost-secure-httpsssl-sites-199446.

[32] CIO Counsel, *The HTTPS-Only Standard*, https://https.cio.gov/; *see also* White House, *Memorandum for the Heads of Executive Departments and Agencies* (M-15-13) (June 8, 2015), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2015/m-15-13.pdf.

[33] *See* Qualys SSL Laps, *SSL Pulse*, https://www.ssllabs.com/ssl-pulse/.

[34] *See* CIO Applications, *The Rise of Big Data, Analytics of Things* (Nov. 30, 2018), https://www.cioapplications.com/news/the-rise-of-big-data-analytics-of-things-nid-2352.html; *see also* Alastair MacPhail, *The Rise and Fall and Rise of Big Data*, Cerebri (July 23, 2018), https://www.cerebriai.com/the-rise-and-fall-and-rise-of-big-data/.

# Part 2

## Types of Privacy Coins and Mechanisms

While each privacy coin features different anonymizing mechanisms and privacy-enhancing characteristics, privacy coins can be generally categorized into (a) privacy-by-default coins, and (b) privacy-as-an-option coins. In reviewing these two categories, we surveyed five unique privacy coins and the mechanisms and characteristics that each offer.

### PRIVACY-BY-DEFAULT COINS

Privacy-by-default coins offer parties to a transaction anonymity by default through various methods. Monero and Grin are examples of privacy-by-default coins, as detailed below.

MONERO

Originally named BitMonero, the Monero protocol ("Monero") and related XMR coin ("XMR") came into existence in April 2014 as a hard fork of the codebase of Bytecoin.[35] Monero offers both parties to a transaction anonymity by default through the use of one-time addresses for the receiver and ring signatures for the sender.[36] The use of these one-time addresses prevents any third party from being able to identify who controls the receiving address. Likewise, ring signatures enable verification that someone from a fixed set of individuals effectuated the transaction without identifying the specific sender.[37]

Moreover, Monero adopted the cryptographic tool known as confidential transactions, which keeps the amounts transferred visible only to participants in the transaction and those whom they designate.[38] Essentially, the combination of an XMR transaction's three components (one-time addresses, ring signatures, and confidential transactions) enables obfuscation of the parties and amounts involved in a given transaction from public view while still allowing for selective disclosure of certain information.

[35] *See* Kurt M. Alonso, *Zero to Monero: First Edition, A Technical Guide to a Private Digital Currency; for Beginners, Amateurs, and Experts* (v.1.0.0) (June 26, 2018), https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf.
[36] *Id.*
[37] *See* Jon Evans, *Bittercoin: true blockchain believers versus the trough of disillusionment*, TechCrunch (Mar. 12, 2017), https://techcrunch.com/2017/03/12/bittercoin-true-blockchain-believers-vs-the-trough-of-disillusionment/.
[38] *Id.*

THE THREE COMPONENTS

One-time addresses, also known as stealth addresses, protect the privacy of receivers of XMR. Stealth addresses are randomly generated addresses created for each transaction on behalf of the recipient by the sender so that different payments made to the same payee are not linkable.[39]

This enables unforgeable, signer-ambiguous transactions that allow for reasonably untraceable XMR transactions.

Ring signatures, which protect the privacy of senders of XMR, have two characteristics—a ring of public keys ("Ring") and a signature. The Ring is composed of the private key's corresponding public key and a set of unrelated public keys.[40] Each signature is generated with a single private key and a set of unrelated public keys. When verifying a signature, third parties cannot determine which public key in the Ring corresponds to the private key that created it.[41] This enables unforgeable, signer-ambiguous transactions that allow for reasonably untraceable XMR transactions.

The confidential transactions feature is a cryptographic tool that allows for verification that no additional XMR has been created or destroyed as part of a given transaction, without revealing the exact transaction amount.[42]

TWO SETS OF KEYS

Unlike the Bitcoin protocol, Monero users have two sets of private keys and public keys (four keys total). The pair of public keys make up the wallet address of a Monero user, whereas the two private keys (the view key and spend key) allow an individual to determine whether an output is addressed to them (view key) and enables the individual to send XMR and determine whether it has been spent (spend key).[43] To verify transfers of XMR, a third-party observer must know that the XMR is owned by the individual using it. To enable this verification, the individual using the XMR signs the previously received XMR with the one-time address used, thereby proving that the individual knows the private keys and therefore rightfully controls the XMR that the individual is using. The private view key may be given to others to grant transparency into certain details of particular transactions associated with the address or addresses. Monero also contains an optional text field called "tx_extra" that can store arbitrary data in encrypted format. While this text field can be used for a variety of compliance purposes, this use has not been widely recommended by researchers and developers.[44]

---

[39] *See* Hackernoon, *Blockchain Privacy-Enhancing Technology Series — Stealth Address (I)* (Originally published by IoTeX, May 15, 2018), https://hackernoon.com/blockchain-privacy-enhancing-technology-series-stealth-address-i-c8a3eb4e4e43.
[40] *See* Kurt M. Alonso, *Zero to Monero: First Edition, A Technical Guide to a Private Digital Currency; for Beginners, Amateurs, and Experts* (v.1.0.0) (June 26, 2018), https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf.
[41] *Id.*
[42] *See* Bitcoin Wiki, *Confidential Transactions* (last updated Feb. 20, 2019) https://en.bitcoin.it/wiki/Confidential_transactions.
[43] *See* Kurt M. Alonso, *Zero to Monero: First Edition, A Technical Guide to a Private Digital Currency; for Beginners, Amateurs, and Experts* (v.1.0.0) (June 26, 2018), https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf.
[44] *See* Kurt M. Alonso, *The Funds Travel Rule and Monero* (Dec. 5, 2019), https://getmonero.org/2019/12/05/funds-travel-rule.html.

Launched on January 15, 2019, Grin is a native privacy coin on the MimbleWimble blockchain protocol.[45] Originating from a document posted by an individual under the pseudonym "Tom Elvis Jedusor," Grin was created because Jedusor found fault with the Bitcoin blockchain's transaction structure and lack of privacy in transactions.[46]

The stated objective of Grin is to empower anyone to transact or save modern money without the fear of external control or oppression through the creation of a virtual currency that is private, scalable, and open.[47]

The Grin network consensus model[48] is an iteration of the proof-of-work consensus algorithm whereby solution time is primarily bound by a computer's memory bandwidth, as opposed to its processing power.[49] This algorithm is specifically designed to be resistant to hardware arms races found in other cryptocurrencies and is designed to solve a complex problem relating to the detection of cycles in a graph that becomes increasingly more difficult to solve as more nodes join.[50]

## CONFIDENTIAL TRANSACTIONS

Several aspects increase the privacy of Grin transactions, but the confidential transactions characteristic is the most important. Like the confidential transactions concept in Monero-based transactions, the confidential transaction feature for Grin transactions shields certain details from the larger public.[51] The confidential transaction feature is used for all Grin transactions.[52] Different than an XMR transaction, Grin transactions have three components: inputs (which reference past outputs), outputs (which detail transaction amounts, ownership, and proof that the amount is not negative), and a proof, which confirms that the sum of the inputs corresponds to the sum of the outputs plus a fee (the "Transaction Kernel").[53]

Several aspects increase the privacy of Grin transactions, but the confidential transactions characteristic is the most important.

The confidential transactions method, as used in Grin, creates opaque transactions that are verifiable but protected.

Grin transactions originate from the sending party, who must know two pieces of information: (1) the amount of Grin available for spending, and (2) the private key, known as the blinding factor, that the party used when receiving this amount.[54] Blinding factors allow users to shield sensitive information while granting other parties the ability to verify

[45] "Beam" is another example of a native privacy coin on the MimbleWimble blockchain protocol.
[46] *See generally* GitHub, *MimbleWimble* (last visited July 17, 2020), https://github.com/mimblewimble/docs.
[47] *See* Grin-Tech, *The Best Automated Trading Robots* (2020), https://grin-tech.org/.
[48] This is also known as the Cuckoo Cycle.
[49] *See* GitHub, *Grin's Proof-of-Work* (last visited July 17, 2020), https://github.com/mimblewimble/grin/blob/master/doc/pow/pow.md.
[50] *Id.*
[51] *See* GitHub, *Introduction to Mimblewimble and Grin* (last visited July 17, 2020), https://github.com/mimblewimble/grin/blob/master/doc/intro.md.
[52] *See* GitHub, *Grin Privacy Primer* (last visited July 17, 2020), https://github.com/mimblewimble/docs/wiki/Grin-Privacy-Primer (highlighting that because all transactions are confidential, there are no nonconfidential transactions that can reveal information about the confidential transactions).
[53] *Id.*
[54] *See* GitHub, *Introduction to Mimblewimble and Grin* (last visited July 17, 2020), https://github.com/mimblewimble/grin/blob/master/doc/intro.md.

that information. With Grin, unlike other privacy coins that use private keys, proof that an individual owns the blinding factor is not achieved by directly signing the transaction.[55]

When effectuating a Grin transaction, the sending party unlocks the amount to be spent using the original blinding factor, and the receiving party uses a separate, new blinding factor to create a destination for the received virtual currency. This process adds a layer of protection between the parties so that the transaction is given effect and also adds a layer of protection to the transaction to obfuscate its details from outside parties.[56]

The blinding factors used also create the basis for the Grin network to validate the transaction. Additionally, each transaction includes a signature[57] and certain additional data (e.g., mining fees)[58] created from the blinding factors.[59] The network uses the Transaction Kernels to ensure that no new Grin was created or double-spent.[60] Essentially, the Grin network verifies that the total of all inputs minus all outputs (including fees) equals zero.[61]

## OTHER PRIVACY-ENHANCING MECHANISMS

The Grin coin leverages two other privacy-enhancing components, the Dandelion relay and the cut-through technique.[62]

Grin transactions use a protocol, known as the Dandelion relay or Dandelion++ protocol, to obfuscate the IP address of the user that sent a given transaction.[63] The Dandelion relay is a technique whereby the originating user delegates another peer (randomly chosen in the network) to broadcast the transaction,[64] thereby making it more difficult to track and ascertain the originating user.[65]

Another component that increases privacy (and scalability) is the cut-through technique. The cut-through technique is a process whereby transactions are merged so that the inputs, outputs, and parties are obfuscated and parts of the data that normally need to be stored by other blockchains are removed when the data is no longer necessary.[66] This technique enables the block to appear as one large transaction, rather than a combination of smaller transactions, thereby increasing the scalability of the network and the privacy of its users over time.[67] Use of the cut-through technique makes it difficult to tell which output matched with each input, while maintaining the ability to validate the block,[68] though archival nodes storing full transaction data belie the cut-through technique's effectiveness at preserving privacy.

---

[55] Unlike Bitcoin and other cryptocurrencies, addresses are not written to the MimbleWimble blockchain.
[56] *See* GitHub, *Introduction to Mimblewimble and Grin* (last visited July 17, 2020), https://github.com/mimblewimble/grin/blob/master/doc/intro.md.
[57] For Grin transactions, the signature uses the kernel excess as the public key.
[58] This additional data constitutes part of the Transaction Kernel.
[59] *See* GitHub, *Introduction to Mimblewimble and Grin* (last visited July 17, 2020), https://github.com/mimblewimble/grin/blob/master/doc/intro.md.
[60] *Id.*
[61] *Id.*
[62] *See* GitHub, *Grin Privacy Primer* (last visited July 17, 2020), https://github.com/mimblewimble/docs/wiki/Grin-Privacy-Primer.
[63] *Id.*
[64] Such action is also known as "fluffing" a transaction.
[65] This delegation may also be aggregated with other transactions that use the same method, further obscuring details. *See* GitHub, *Dandelion++ in Grin: Privacy-Preserving Transaction Aggregation and Propagation* (last visited July 17, 2020), https://github.com/mimblewimble/grin/blob/master/doc/dandelion/dandelion.md*; see also* GitHub, *Grin Privacy Primer* (last visited July 17, 2020), https://github.com/mimblewimble/docs/wiki/Grin-Privacy-Primer.
[66] *Id.*
[67] With automatic removal of unnecessary data from the network, historical data will, over time, no longer be viewable. This is colloquially referred to as the "right to be forgotten" feature. *Id.*
[68] *See* GitHub, *Introduction to Mimblewimble and Grin* (last visited July 17, 2020), https://github.com/mimblewimble/grin/blob/master/doc/intro.md.

## PRIVACY-AS-AN-OPTION COINS

Privacy-as-an-option coins are, by default, transacted in a manner that is visible on a public ledger (unlike Monero and Grin). Yet they allow users the ability to conduct privacy-enhanced transactions by activating optional privacy-enhancing features. Zcash, Dash, and Bitcoin are examples of privacy-as-an-option coins, as we discuss below.

### Zcash (ZEC)

Launched in October 2016, the Zcash protocol ("Zcash") reuses large portions of the Bitcoin codebase to offer users functionality that is similar to the Bitcoin network but that includes the added option of enhancing privacy through the use of zero-knowledge proofs.[69] This optionality enables four different types of transactions on the Zcash network.

#### ZCASH TRANSACTION TYPES

The Zcash network supports transparent and shielded transactions by using "t-addresses" (transparent addresses) and "z-addresses" (private addresses). These transactions are categorized into four types: (a) public transactions, (b) shielding transactions, (c) deshielding transactions, and (d) private transactions.[70] Refer to Figure 2-C-1 below for a visualization of each of these transactions.

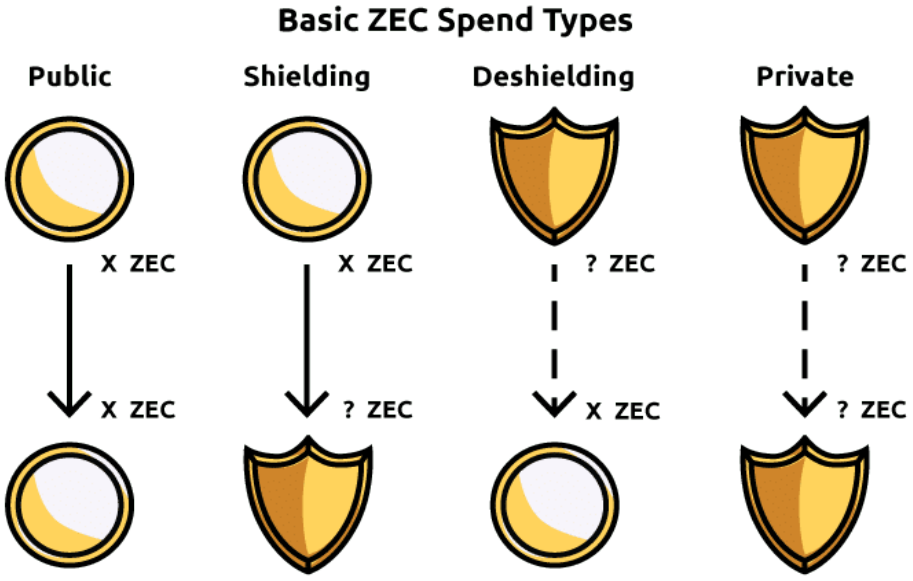



Figure 2-C-1
Source: https://electriccoin.co/blog/anatomy-of-zcash/

[69] *See* Hackernoon, 2019 Privacy Token Review (Original published by Kevin Liu Feb. 15, 2019), https://hackernoon.com/2019-privacy-token-review-c28b6ceef637; *see also* Zooko Wilcox, *What is Zcash?* Coin Center (Dec. 6, 2016), https://coincenter.org/entry/what-is-zcash.

[70] *See* Paige Peterson, *Anatomy of A Zcash Transaction*, Electric Coin Co. (Nov. 23, 2016), https://electriccoin.co/blog/anatomy-of-zcash/.

Public transactions occur when one or more users send Zcash coins ("ZEC") from their t-addresses to one or more other users' t-addresses. These transactions are publicly visible; any third party on the Zcash network can see the sending and receiving addresses and the transaction value—just like users on the Bitcoin network can.[71]

Shielding transactions occur when one or more users send ZEC from their t-addresses to one or more other users' z-addresses. These transactions are semi-private. Specifically, a third party on the Zcash network can identify which address sent ZEC and the amount the transaction involves.[72] However, the recipient addresses, including the number of recipient addresses, remain private.[73]

Deshielding transactions occur when a user sends ZEC from the user's z-addresses to one or more t-addresses. Like shielding transactions, deshielding transactions are semi-private. A deshielding transaction allows others to see which addresses received ZEC and the amount that each of those addresses received but obfuscates the sender's address.[74]

Private transactions occur when a user sends ZEC from the user's z-addresses to one or more z-addresses. These transactions are private and indistinguishable from other private transactions on the Zcash network.[75] Private transactions keep the sending address, receiving address or addresses, and amount involved private.[76]

An encrypted memo field allows the sender of a shielding or private transaction to attach up to 512 bytes of data that is visible only to the recipient. One potential use for this feature is to attach information required by the Travel Rule (as defined and described in Part 3 below) to transactions.[77]

Zero-knowledge proofs are a cryptographic technique that makes it possible to prove certain facts about otherwise encrypted data…

## ZERO-KNOWLEDGE PROOFS EXPLAINED

Zero-knowledge proofs are a cryptographic technique that makes it possible to prove certain facts about otherwise encrypted data and prove that certain facts are true about that data without revealing additional information.[78] For example, a private or semi-private Zcash transaction includes a zero-knowledge proof that no new ZEC were created, proving that the inputs to the transaction equal its outputs. These proofs can be verified by other users of the Zcash network without any need to disclose the number of coins being spent by the transaction.

Additionally, with regard to those private and semi-private transactions, a user using a z-address (private address) has the ability to reveal the transaction details specific to the user's account through the use of a viewing key.[79] The holder of a Zcash z-address can generate a viewing key, which such holder can choose to share with anyone else.[80] This viewing key grants transparency into certain details of particular transactions sent to or from the associated z-address.[81]

---

[71] *See* Zcash, *How It Works* (last visited July 17, 2020), https://z.cash/technology/.
[72] *See* Paige Peterson, *Anatomy of A Zcash Transaction*, Electric Coin Co. (Nov. 23, 2016), https://electriccoin.co/blog/anatomy-of-zcash/.
[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] *See* Zooko Wilcox & Paige Peterson, *The Encrypted Memo Field,* Electric Coin Co. (Dec. 5, 2016), https://electriccoin.co/blog/encrypted-memo-field/.
[78] *See* Zooko Wilcox, *What is Zcash?*, Coin Center (Dec. 6, 2016), https://coincenter.org/entry/what-is-zcash.
[79] *Id.*
[80] *Id.*
[81] *Id.*

Derived from a fork to the Bitcoin codebase in 2014 and initially called Xcoin (and later Darkcoin), the Dash protocol ("Dash") has an efficient governance structure and enables quick transactions with the DASH token ("DASH token").[82] Masternodes running Dash support its governance structure and make decisions regarding funding proposals, which any entity can submit to the network. Masternodes also facilitate what are known as PrivateSend and InstantSend transactions for the network. To act as a masternode for Dash, an operator must control at least 1,000 DASH tokens and maintain minimum computer specifications.[83] In addition to servicing the Dash blockchain network, masternodes receive a payment, like DASH token miners, when a block reward is given.[84] As a result of the 1,000 DASH token minimum ownership requirement, the masternodes create a secondary network whereby no single entity can control the recorded outcome of a given transaction.[85] A select number of random masternodes are automatically chosen to validate any given transaction, whereby the chosen masternodes form a trustless quorum and essentially serve as an oracle.[86] This eliminates the need for the whole network of masternodes to validate the transaction.

## PRIVATESEND AND INSTANTSEND TRANSACTIONS

As mentioned, Dash allows two types of DASH token transactions—PrivateSend and InstantSend. PrivateSend transactions are a branded and standardized implementation of CoinJoin, which is a method for combining multiple transactions from multiple parties into a single transaction to complicate the flow of funds, thus making it harder to associate specific addresses with each participant. CoinJoin can be applied to any transparent blockchain and therefore does not require modification to the Bitcoin protocol.[87]

Indeed, since CoinJoin can be used in connection with Bitcoin transactions just as readily as Dash allows, Dash is technically no more of a "privacy coin" than Bitcoin, which we discuss in more detail below. As the Dash website notes, the widespread perception that Dash is "privacy-centric" is likely a legacy of its former "Darkcoin" moniker and does not accurately reflect its actual functionality.[88] While acknowledging those misconceptions (and with no intention of reinforcing them), we nonetheless address Dash as an illustrative privacy-preserving cryptocurrency here, since a key goal of this white paper is to highlight the wide range of privacy-preserving features across cryptocurrencies and dispel misconceptions about them more broadly.

When used, PrivateSend makes the origin of the DASH tokens reasonably untraceable by aggregating[89] an individual's DASH tokens with other participants' DASH tokens into a common transaction before executing and returning funds to newly created addresses in each participant's wallet.[90] This process protects the fungibility of DASH tokens by

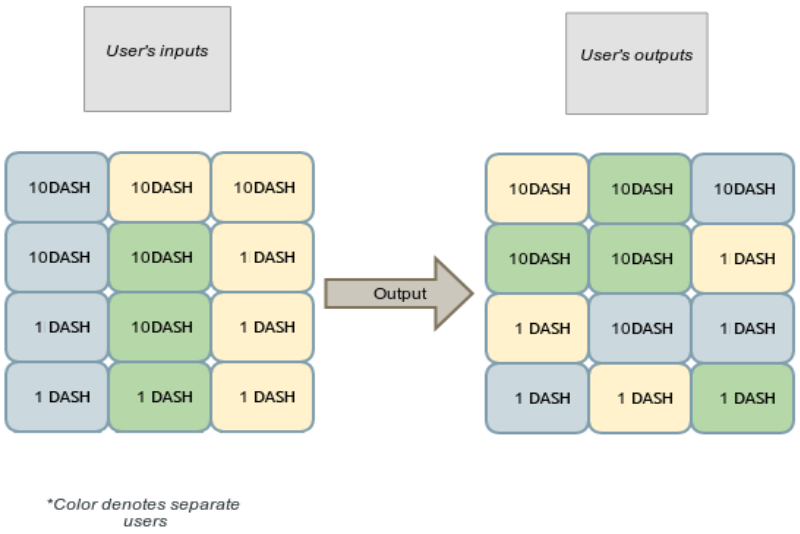
---

[82] *See* Brian Patrick Eha, *Can Bitcoin's First Felon Help Make Cryptocurrency a Trillion-Dollar Market?*, Fortune (June 26, 2017), https://fortune.com/2017/06/26/bitcoin-blockchain-cryptocurrency-market/.
[83] *See* Evan Duffield & Danial Diaz, *Whitepaper*, GitHub (Edited by Nathan Marley Aug. 22, 2018), https://github.com/dashpay/dash/wiki/Whitepaper.
[84] *Id.*; *see also* https://docs.dash.org/en/stable/governance/.
[85] *See* Evan Duffield & Danial Diaz, *Whitepaper*, GitHub (Edited by Nathan Marley Aug. 22, 2018), https://github.com/dashpay/dash/wiki/Whitepaper.
[86] *Id.*
[87] *See* Bitcoin Wiki, *CoinJoin* (last updated June 30, 2019), https://en.bitcoin.it/wiki/CoinJoin.
[88] *See* Dash, *Private-Send Legal Position* (last visited July 17, 2020), https://media.dash.org/wp-content/uploads/Dash-PrivateSend-Position.pdf.
[89] Aggregating is also known as "mixing."
[90] *See* Brian Patrick Eha, *Can Bitcoin's First Felon Help Make Cryptocurrency a Trillion-Dollar Market?*, Fortune (June 26, 2017), https://fortune.com/2017/06/26/bitcoin-blockchain-cryptocurrency-market/; *see also* Wikipedia, *Dash (cryptocurrency)* (last updated June 9, 2020), https://en.wikipedia.org/wiki/Dash_(cryptocurrency); *see also* Dash, *Features* (last visited July 17, 2020), https://docs.dash.org/en/stable/introduction/features.html.

dissociating receivers of DASH tokens from the tokens' specific, unique history, while simultaneously allowing all users to audit the financial integrity of the public ledger without compromising other users' privacy.[91]

To illustrate, PrivateSend first breaks down an individual's inputs into smaller, standardized denominations.[92] PrivateSend then combines individual denominations into one transaction whereby multiple parties[93] form the sending party and the same parties form the receiving party, thus "mixing" the participants' denominated units of DASH tokens.[94] The transactions are coordinated by individual masternodes, which have visibility into the sending and receiving addresses used by each party involved. Thus, each transaction is not completely private, so users must "mix" their funds multiple times using randomly selected masternodes to further increase the anonymity of each user's funds,[95] further breaking down each individual's inputs into smaller, standard denominations.[96] While it is theoretically possible for an individual masternode operator to view certain user data as the transaction components pass through its masternode, the probability of a single masternode operator observing all data through multiple mixing sessions is extremely remote.[97] After an individual has mixed his or her funds using PrivateSend, the individual can use the resulting balances to transact. The recipient and transaction amounts are always transparent in Dash transactions, even when the sender uses mixed PrivateSend inputs. Refer to Figure 2-C-2 below for an illustration of a DASH token transaction.

Figure 2-C-2
Source: https://github.com/dashpay/dash/wiki/whitepaper




[91] *See* Evan Duffield & Danial Diaz, *Whitepaper*, GitHub (Edited by Nathan Marley Aug. 22, 2018), https://github.com/dashpay/dash/wiki/Whitepaper.
[92] *See* Dash, *Features* (last visited July 17, 2020), https://docs.dash.org/en/stable/introduction/features.html.
[93] There must be a minimum of three parties. *See* Dash, *Features* (last visited July 17, 2020), https://docs.dash.org/en/stable/introduction/features.html.
[94] *See* Evan Duffield & Danial Diaz, *Whitepaper*, GitHub (Aug. 22, 2018), https://github.com/dashpay/dash/wiki/Whitepaper.
[95] *Id.*
[96] E.g., (0.001, 0.1, 10); *see* Dash, *Features* (last visited July 17, 2020), https://docs.dash.org/en/stable/introduction/features.html.
[97] *See* Evan Duffield & Danial Diaz, *Whitepaper*, GitHub (Aug. 22, 2018), https://github.com/dashpay/dash/wiki/Whitepaper.

InstantSend is another feature of DASH Tokens and is applied by default to all Dash transactions. InstantSend uses masternode quorums to instantly lock transactions in a way that makes them irreversible.[98] Once a quorum exists, the transaction inputs are locked and become spendable only with that specific transaction. Once consensus of the lock is reached by a masternode quorum and broadcasted to the network, no conflicting transactions are accepted since they would need to match the exact transaction ID on the lock in place.[99] The masternodes then broadcast this information to the Dash network, thereby ensuring that the transaction will be included in subsequently mined blocks and prohibiting any spending of the inputs during the confirmation time period.[100]

## bitcoin Transactions using CoinJoin

As explained in our overview of Dash's PrivateSend feature, CoinJoin can be applied to any transparent blockchain and does not require modification to certain protocols, including the Bitcoin protocol.[101] Bitcoin transactions that use CoinJoin therefore offer privacy enhancements that are substantially similar to PrivateSend transactions on the Dash protocol. Bitcoin users have used CoinJoin ever since it was proposed in mid-2013 to address Bitcoin's privacy shortcomings and have done so at an increasing rate in recent years.[102] As of mid-2019, one study estimated that CoinJoin was used in approximately 4% of all Bitcoin transactions, a roughly three-fold increase from the previous year.[103]

While this white paper does not further analyze Bitcoin as a "privacy coin," we briefly raise this example to show that the world's largest cryptocurrency has long enabled users to conduct privacy-enhancing transactions and to demonstrate that Bitcoin is as much of a "privacy coin" as any other coin that allows for privacy-enhanced transactions via CoinJoin.[104]

---

[98] *Id.*
[99] *Id.*
[100] *See* Dash, *Features* (last visited July 17, 2020), https://docs.dash.org/en/stable/introduction/features.html.
[101] *See* Bitcoin Wiki, *CoinJoin* (last visited July 17, 2020), https://en.bitcoin.it/wiki/CoinJoin.
[102] *See* Landon Manning, Bitcoin Magazine, *Percentage of CoinJoin Bitcoin Transactions Triples Over Past Year*, Yahoo Finance (May 1, 2019), https://finance.yahoo.com/news/percentage-coinjoin-bitcoin-transactions-triples-205017559.html.
[103] *Id.*
[104] CoinJoin is not the only available method for conducting privacy-enhanced Bitcoin transactions. *See, e.g.*, Lucas Nuzzi, *Schnorr Signatures & The Inevitability of Privacy in Bitcoin*, Medium (Mar. 13, 2019), https://medium.com/digitalassetresearch/schnorr-signatures-the-inevitability-of-privacy-in-bitcoin-b2f45a1f7287 (discussing increasing use of a privacy-enhancing method known as Schnorr signatures in Bitcoin transactions). Other widely traded cryptocurrencies, including Ethereum and Litecoin, have likewise supported or plan to support methods for privacy-enhanced transactions. *See* Jon Buck, *Ethereum Upgrade Byzantium Is Live, Verifies First ZK-Snark Proof*, Cointelegraph (Sept. 21, 2017), https://cointelegraph.com/news/ethereum-upgrade-byzantium-is-live-verifies-first-zk-snark-proof; Jack Martin, *Litecoin Mimblewimble Integration Sees Test Build and Codebase Progress*, Cointelegraph (May 4, 2020), https://cointelegraph.com/news/litecoin-mimblewimble-integration-sees-test-build-and-codebase-progress.

# Part 3

## Approaches to AML Regulation of Privacy Coin Use

Regulators take evolving approaches in how they handle, monitor, and enforce AML and related regulations as they pertain to persons and businesses transacting with privacy coins. We focus on the approaches that each of the following regulators—the Financial Crimes Enforcement Network ("FinCEN"), the New York Department of Financial Services ("NYDFS"), the Japanese Financial Services Agency ("JFSA"), and the British Financial Conduct Authority ("FCA") (collectively, "Regulators")—take with regard to privacy coin uses and then turn to the AML and related issues that those Regulators may have with privacy coin transactions. Lastly, we discuss the AML recommendations developed by the Financial Action Task Force ("FATF") and how those recommendations apply to privacy coins.

As mentioned in the Introduction, we reiterate that the following content is *for informational purposes only and may not be relied upon by any party as legal advice. VASPs, and other persons engaged in privacy coin-related activities, should contact qualified counsel for advice regarding the laws and regulations that may apply to their activities.*

### FINANCIAL CRIMES ENFORCEMENT NETWORK (FINCEN)

FinCEN promulgates and administers AML regulations under the Bank Secrecy Act ("BSA"), which is the principal U.S. federal statute aimed at preventing money laundering and the financing of terrorism. The BSA and FinCEN's implementing regulations require various entities, including money transmitters, to register with FinCEN as money services businesses ("MSBs").[105] FinCEN regulations require an MSB to develop, implement, and maintain a risk-based anti-money laundering program ("AML Program") that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities.[106] An AML Program must include policies and procedures to (a) verify customer identities (i.e., know-your-customer, or "KYC"), (b) identify and report suspicious activity, and (c) comply with transaction recordkeeping requirements.

FinCEN has established and clarified its regulatory approach to virtual currencies, and privacy coins specifically, over the course of two significant guidance documents, one in 2013 (the "2013 FinCEN Guidance") and another in 2019 (the "2019 FinCEN Guidance"). We discuss those in turn:

#### 2013 FINCEN GUIDANCE

In the 2013 FinCEN Guidance, FinCEN established that it would regulate certain virtual currency activities as a form of money transmission.[107] Under FinCEN's regulations, a money transmitter is defined as a person that (a) accepts "currency, funds, or other value that substitutes for currency from one person" and transmits "currency, funds, or other value that substitutes for currency to another location or person by any means," or (b) is "engaged in the transfer of funds."[108]

[105] 31 C.F.R. § 1022.380 (2016). Money transmitters are a regulated category of MSBs in the United States, which reside under the general umbrella of VASPs, as used throughout this white paper.
[106] 31 C.F.R. § 1022.210 (2011). In addition, an AML Program must designate an individual responsible for assuring ongoing compliance with the AML Program, providing for compliance training, and providing for independent monitoring and review of internal AML Program compliance.
[107] FinCEN Guidance issued on March 18, 2013 (FIN-2013-G001).
[108] 31 C.F.R. § 1010.100(ff)(5)(i)(A) (2014).

The 2013 FinCEN Guidance provides that any "convertible virtual currency," which means a virtual currency that has "an equivalent value in real currency, or acts as a substitute for real currency," is value that substitutes for currency.[109] FinCEN defines "virtual currency" as "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency."[110]

Further, the 2013 FinCEN Guidance categorizes the participants in virtual currency arrangements as "users," "exchangers," and "administrators." According to the 2013 FinCEN Guidance, "A *user* is a person that obtains virtual currency to purchase goods or services on the user's own behalf. An *exchanger* is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. An *administrator* is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency."[111] FinCEN has clarified that exchangers and administrators of CVCs are money transmitters, and thus parties engaging in exchanger or administrator activities must register as MSBs and comply with applicable regulations.

2019 FINCEN GUIDANCE

In the 2019 FinCEN Guidance, FinCEN consolidated current FinCEN regulations, and related administrative rulings and guidance issued since 2011, including the 2013 FinCEN Guidance, and applied these rules and interpretations to common business models involving convertible virtual currencies in addition to expressly addressing its regulatory approach to privacy coins.[112]

In the 2019 FinCEN Guidance, the FinCEN categorized privacy coins as those "specifically engineered to prevent their tracing through distributed public ledgers" and confirmed that a VASP that operates in privacy coins "is subject to the same regulatory obligations as when operating in currency, funds, or non-anonymized" cryptocurrencies, while making clear that a "money transmitter cannot avoid its regulatory obligations because it chooses to provide money transmission services using" privacy coins.[113]

FinCEN also made a critical distinction in the 2019 FinCEN Guidance between those who provide anonymizing services and those who merely supply anonymizing software.[114] Specifically, FinCEN views those that provide anonymizing services (e.g., mixers and tumblers), whereby persons accept cryptocurrency and retransmit such in a manner designed to prevent others from tracing the transmission to the source—as being regulated money transmitters and thus MSBs.[115] These anonymizing service providers are, therefore, obligated to register with FinCEN as MSBs and comply with FinCEN regulations.

[109] FinCEN Guidance issued on March 18, 2013 (FIN-2013-G001).
[110] *Id.*
[111] *Id.*
[112] *See generally* FinCEN Guidance issued on May 9, 2019 (FIN-2019-G001).
[113] *Id.* at § 4.5.
[114] *Id.* at § 4.5.1.
[115] *Id.*

However, FinCEN stated that those who merely supply anonymizing software, including those that develop privacy-preserving cryptocurrency software, are not regulated money transmitters[116] because FinCEN regulations exempt from the definition of *money transmitter* those persons providing "the delivery, communication, or network access services used by a money transmitter to support money transmission services."[117] This result stems from the distinction that anonymizing software suppliers are engaged in trade, not money transmission.[118]

Developers of privacy coins may still qualify as regulated MSBs and money transmitters under FinCEN regulations if those developers also create, issue, or sell privacy coins while operating as administrators of a centralized payment system.[119] Likewise, developers who also create, issue, or sell privacy coins on a decentralized payment system may be money transmitters if those developers engage in the business of accepting and transmitting the privacy coins they developed.[120] And businesses that exchange privacy tokens are regulated as money transmitters, as has been clear since the 2013 FinCEN Guidance.[121] Contrarily, FinCEN has stated that, in general, a person who uses privacy coins "to pay for goods or services on his or her own behalf would not be a money transmitter."[122]

Developers of privacy coins may still qualify as a regulated MSB and a money transmitter under FinCEN regulations

In the 2019 FinCEN Guidance, FinCEN expressly noted that cryptocurrency transactions are subject to the FinCEN's Funds Travel Rule, which requires MSBs and other regulated financial institutions to share certain information when executing funds transfers with another financial institution.[123] FinCEN stated that this requirement applies "regardless of how a money transmitter sets up their system for clearing and settling transactions," adding in a footnote that "a person that chooses to set up a transaction system that makes it difficult to comply with existing regulations may not invoke such difficulty as a justification for non-compliance."[124] Notably, the Funds Travel Rule and similar "tracking"-oriented obligations, which were initially implemented for compliance of non-cryptocurrency services, do not mandate that this tracking and sharing of required transaction information occur via blockchain analysis and surveillance.[125]

---

[116] Individuals that merely deploy anonymizing software may not be considered anonymizing software providers as a threshold matter; however, if FinCEN takes the position that mere deployment of anonymizing software constitutes providing anonymizing software, then the individual should still not be considered a money transmitter because the individual is engaged in trade and not money transmission.

[117] 31 C.F.R. § 1010.100(ff)(5)(ii) (2014).

[118] *See* FinCEN Guidance issued on May 9, 2019 (FIN-2019-G001), § 4.5.1(b); *see also* FinCEN Guidance issued on January 30, 2014 (FIN-2014-R002).

[119] *See* FinCEN Guidance issued on May 9, 2019 (FIN-2019-G001), § 4.5.2(a) (noting that this determination holds true while the system works on a centralized basis but may change once the system transitions to a decentralized basis).

[120] *Id.* at § 4.5.2(c).

[121] FinCEN Guidance issued on March 18, 2013 (FIN-2013-G001).

[122] *See* FinCEN Guidance issued on May 9, 2019 (FIN-2019-G001), § 4.5.2(b)-(c).

[123] *See* 31 C.F.R. § 1010.410(f) (2016). Among other things, the Funds Travel Rule requires the transmitting institution or intermediary to include the name of the transmittor and the amount of the transmittal order. The 2019 FinCEN Guidance also stated that related recordkeeping requirements in the Funds Transfer Rule, 31 C.F.R. § 1010.410(e) (2016), apply to cryptocurrency transactions. We analyze only the Funds Travel Rule in this white paper because of its requirements to transfer information between VASPs and the relatively more significant compliance challenges that such requirements pose for VASPs.

[124] FinCEN Guidance issued on May 9, 2019 (FIN-2019-G001), § 2.1.

[125] Some industry participants have questioned the applicability of the Funds Travel Rule and Funds Transfer Rule to cryptocurrency transactions and have requested that FinCEN commence a notice and comment rulemaking to confirm and clarify such applicability. *See* Letter from Chamber of Digital Commerce, *Re: Comments to FinCEN Guidance: 'Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies,' FIN-2019-G001 (May 9, 2019)* (Nov. 26, 2019), https://digitalchamber.org/wp-content/uploads/2019/12/Chamber-of-Digital-Commerce-Comment-Letter-to-FinCEN-

## NEW YORK DEPARTMENT OF FINANCIAL SERVICES (NYDFS)

The NYDFS supervises and regulates the activities of VASPs with the mission to keep pace with the rapid and dynamic evolution of the financial industry, to guard against financial crises, and to protect consumers and markets from fraud.[126] The NYDFS is among the first and most active state regulators in developing a regulatory framework for cryptocurrency business activities, starting with its "BitLicense" regulation in 2015.[127] Since then, many of the largest cryptocurrency custodians and exchanges have obtained BitLicenses or limited purpose trust company charters from the NYDFS, thus solidifying NYDFS's role as a leading U.S. regulator in the industry. In keeping with that role, the NYDFS announced in July 2019 a new division tasked with the responsibility of licensing and supervising cryptocurrencies.[128] The NYDFS has imposed AML-related requirements on privacy coins in the state of New York in several key ways, including through the BitLicense regulation and a separate set of transaction monitoring and filtering requirements.[129]

### THE BITLICENSE

The NYDFS regulates certain privacy coin business activities, but not (a) the development and dissemination of software, or (b) merchants and consumers that use privacy coins solely for the purchase or sale of goods or services or for investment purposes.[130] Notably, NYDFS does not allow those with a BitLicense ("BitLicensees") to engage in, facilitate, or knowingly allow the transfer or transmission of privacy coins when such action will obfuscate or conceal the identity of an individual customer or counterparts, unless such identity is already known to all parties involved.[131] Moreover, the NYDFS requires that BitLicensees verify each customer's identity upon opening an account or upon establishing a service relationship.[132]

BitLicensees are not prohibited from effectuating transactions that are obfuscated from the general public, so long as required information can be made available to NYDFS regulators.

However, there is no requirement that BitLicensees make available to the general public the fact or nature of the movement of privacy coins by individual customers or counterparties.[133] In other words, BitLicensees are not prohibited from effectuating transactions that are obfuscated from the general public so long as required information can be made available to NYDFS regulators. For example, the NYDFS granted an exchange permission to provide custodial and listing services for Zcash.[134] Furthermore, the privacy-enhancing

Guidance1.pdf. As of the date of this white paper, FinCEN has not publicly articulated any change in its position that such rules apply to cryptocurrency transactions, and no rulemaking has commenced. Thus, this white paper assumes that VASPs remain subject to such rules in accordance with the 2019 FinCEN Guidance.

[126] *See* NYDFS, *About Us* (last visited July 17, 2020), https://www.dfs.ny.gov/our_mission.

[127] 23 N.Y.C.R.R. 200 (2015).

[128] *See* Daniel Kuhn, *New NYDFS Division to Oversee Licensing for Cryptocurrency Startups*, Coin Center (July 23, 2019), https://www.coindesk.com/a-new-nydfs-division-will-oversee-licensing-for-crypto-startups.

[129] 3 N.Y.C.R.R. 504 (2017).

[130] *See* 23 N.Y.C.R.R. 200.3(a) and (c)(2) (2015). For illustrative purposes, we focus on privacy coin-related obligations on BitLicensees in this white paper, although we note that many of the same obligations apply to New York limited purpose trust companies as well.

[131] *See* 23 N.Y.C.R.R. 200.15(g) (2015).

[132] *See* 23 N.Y.C.R.R. 200.15(h) (2015).

[133] *See* 23 N.Y.C.R.R. 200.15(g) (2015).

[134] *See* Press Release, NYDFS, *DFS Authorizes Gemini Trust Company to Provide Additional Virtual Currency Products and Services* (May 14, 2018), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1805141.

features of privacy coins do not prevent any BitLicensee from complying with their customer identification and verification requirements under New York law.

The approach that NYDFS takes towards regulating privacy coins aligns with its stated mission and enables New York regulators the ability to review required information, while simultaneously allowing privacy coin users the benefit of financial privacy.

## TRANSACTION MONITORING, FILTERING, AND RECORDKEEPING REQUIREMENTS

The NYDFS clarified required attributes of BitLicensees and other licensed financial service providers that relate to transaction monitoring and filtering via regulation.[135] Specifically, these regulations are intended to ensure that BitLicensees can sufficiently identify the parties to transactions and validate that their services are not being used for illicit purposes.[136]

With regard to privacy coins, these requirements are gatewayed by a BitLicense obligation that requires BitLicensees to make publicly obfuscated information available to NYDFS regulators, as discussed above.[137] While not initially developed with privacy coin attributes in mind, the transaction monitoring and filtering requirements apply equally to transparent and privacy coins. Among other requirements, transaction monitoring and filtering programs must be reasonably designed to monitor violations of the BSA and to comply with suspicious activity reporting obligations. They must also include certain screening requirements imposed by the U.S. Treasury's Office of Foreign Assets Control ("OFAC") to ensure that prohibited transactions do not occur.[138] Like FinCEN with the AML Program, the NYDFS outlines certain requirements on the rigorousness of these programs, but it similarly does not require the use of on-chain surveillance tools. When these on-chain surveillance tools are not available, regulated companies can still meet their compliance obligations through other robust means of off-chain information sharing.

The BitLicense imposes several additional transaction-based compliance requirements of note. BitLicensees must not only maintain information regarding customers who are parties to a transaction but also, "to the extent practical," must maintain "the identity and physical addresses of . . . any other parties to the transaction."[139] Furthermore, when a virtual currency transaction (or series thereof) exceeds $10,000 in one day and is not subject to federal currency transaction reporting requirements (i.e., because there is not a fiat currency component), a BitLicensee must report that transaction or series of transactions to the Department.[140]

[135] *See* 3 N.Y.C.R.R. 504.1 (2017); *see generally* 3 N.Y.C.R.R. 504 (2017).
[136] *Id.*
[137] *See generally* 23 N.Y.C.R.R. 200.15(g). (2015)
[138] *See* 3 N.Y.C.R.R. 504.3 (2017). We note that, even if a virtual currency business is not a regulated BitLicensee or other form of VASP, U.S. OFAC regulations (and sanctions regulations of other jurisdictions) still apply to its activities where applicable. Because this white paper focuses on AML regulation, we do not address OFAC and other sanctions regulations in detail.
[139] 23 N.Y.C.R.R. 200.15(e)(1)(i) (2015).
[140] 23 N.Y.C.R.R. 200.15(e)(2) (2015).

## JAPANESE FINANCIAL SERVICES AGENCY (JFSA)

The JFSA is the primary financial regulator in Japan. Services related to the use of privacy coins in Japan are primarily regulated by the JFSA under two key acts: (a) the Payment Services Act ("PSA"); and (b) the Act on Prevention of Transfer of Criminal Proceeds (Act No. 22 of 2007) ("Act 22").

### PAYMENT SERVICES ACT (PSA)

The PSA requires any person engaged in providing virtual currency exchange services ("VCES")[141] in Japan to be registered with the Prime Minister.[142] Like BitLicensees in the United States, VCES Providers[143] have several regulatory obligations imposed. For example, VCES Providers must maintain records and report on their transactions,[144] subject themselves to on-site inspections,[145] maintain certain information security standards[146] and undertake the duty to notify the Prime Minister upon the occurrence of certain events,[147] among other things. While the PSA does not impose restrictions or limitations that affect privacy coins specifically, it does provide the foundation for government registration and oversight.

In the context of privacy coins, the PSA requires exchanges, certain privacy coin wallets, and various intermediaries, among others, to register with the Prime Minister. Furthermore, the PSA obligates these privacy coin participants to maintain certain transaction records and sufficiently secure their customers' and users' data.

### ACT ON PREVENTION OF TRANSFER OF CRIMINAL PROCEEDS (ACT 22)

Japan promulgated Act 22 with the purpose of, among other things, preventing the transfer of criminal proceeds and enforcing international treaties concerning the prevention of terrorism financing.[148]

Act 22 obligates VCES Providers to verify customer and user data including the customers' and users' representatives (if applicable).[149] For natural persons, this includes the verification of their name, domicile, and date of birth, whereas for legal entities, the VCES Provider need only verify the company name and main office location.[150] Notably, the VCES Provider must retain the information obtained for at least seven years.[151]

Similar to the PSA, Act 22 also obligates VCES Providers to maintain certain transaction records for at least seven years.[152] All transactions, along with customer verification information, and other proceeds suspected of criminal origination or intent must be reported to authorities as "suspicious transactions."[153] Like suspicious activity reports ("SARs") in the United States, VCES Providers cannot divulge the fact that they intend to file or actually have filed a suspicious transaction report.[154]

---

[141] *Virtual Currency Exchange Services* includes those in the business of (i) purchase and sale of virtual currency or exchange with another virtual currency, (ii) intermediary, brokerage, or agency services for the activities in (i), and (iii) management of users, money, or virtual currency, carried out by persons in connection with their acts set forth in (i) or (ii). *See* PSA, Ch. III-2, Article 2(7). For purposes of this white paper, VCES falls under the definition of VASPs used herein.
[142] *See* PSA, Ch. III-2, Article 63-2.
[143] VCES Providers are persons and entities registered with the Prime Minister that provide VCES.
[144] *See* PSA, Ch. III-2, Article 63-14.
[145] *Id.* at Article 63-15.
[146] *Id.* at Article 63-8.
[147] *Id.* at Article 63-6.
[148] *See* Act 22, Article 1.
[149] *Id.* at Article 4(1).
[150] *Id.* at Article 4(1).
[151] *Id.* at Article 6(2).
[152] *Id.* at Article 7(1) and (3).
[153] *See generally* Act 22, Article 9.
[154] *See id.* at Article 9(2).

## RECENT JFSA REGULATORY DEVELOPMENTS RELATING TO PRIVACY COINS

In 2018, the JFSA began pressuring certain virtual currency exchanges to stop handling various privacy coins in an effort to prevent money laundering, the sale of illicit goods, and ransom payments, despite the fact that it was legal to exchange many of the privacy coins at issue.[155] In March 2019, the JFSA submitted a bill to amend how the PSA and Japan's Financial Instruments and Exchange Act regulate the purchase and sale of virtual currencies and VCES Providers ("JFSA Amendment").[156] On May 31, 2019, the JFSA Amendment passed and came into effect in April 2020.[157]

The new JFSA Amendment requires custodians of privacy coins[158] that do not offer exchange or intermediary services to register under the PSA.[159] It also requires each exchange operating in Japan to segregate its users' funds from the exchange's own cash flow. Moreover, when a VCES Provider manages a user's money, it must either (a) store the virtual currency in a cold wallet, or (b) if using a hot wallet, maintain the same kind and same quantity of virtual currency as the user's virtual currency as a form of security to reimburse stolen or misappropriated funds.[160]

Additionally, the JFSA Amendment increases the customer identify verification and related anti-money laundering obligations imposed, while simultaneously fortifying data security and customer protection requirements. Furthermore, it requires each VCES Provider to obtain approval to list and subsequently trade each virtual currency.

## UNITED KINGDOM FINANCIAL CONDUCT AUTHORITY (FCA)

The FCA's objective is to protect consumers, protect financial markets, and promote competition.[161] In setting forth its regulatory perimeter, the FCA noted that certain cryptocurrencies pose a risk of money laundering and terrorist financing and specifically noted that privacy features on certain cryptocurrencies are attractive for facilitating criminal activity, an issue that the FCA intends to address.[162]

[155] *See* Jake Adelstein, *Japan's Financial Regulator Is Pushing Crypto Exchanges To Drop 'Altcoins' Favored By Criminals*, Forbes (Apr. 30, 2018), https://www.forbes.com/sites/adelsteinjake/2018/04/30/japans-financial-regulator-is-pushing-crypto-exchanges-to-drop-altcoins-favored-by-criminals/#18eda68a1b8a.
[156] *See* Nagashima Ohno & Tsunematsu, *Amendments to Payment Services Act*, Lexology (Apr. 26, 2019), https://www.lexology.com/library/detail.aspx?g=bca6f924-7902-4283-9b3c-11f05df88e40.
[157] *See* Marie Huillet, *Japan Officially Approves Bill to Amend National Legislation Governing Crypto Regulation*, Cointelegraph (May 31, 2019), https://cointelegraph.com/news/japan-officially-approves-bill-to-amend-national-legislation-governing-crypto-regulation; *see also* Kevin Helms, Japan Implements Significant Changes to Cryptocurrency Regulation Today, Bitcoin (Apr. 30, 2020), https://news.bitcoin.com/japan-changes-cryptocurrency-regulation/.
[158] This requirement applies to other virtual currencies as well.
[159] *See* Hitashi Oki, *Japan Hopes to Set Global Crypto Law Benchmark With Latest Regulatory Update*, Cointelegraph (June 5, 2019), https://cointelegraph.com/news/japan-hopes-to-set-global-crypto-law-benchmark-with-latest-regulatory-update.
[160] *Id.*
[161] *See* Cryptoassets Taskforce: Final Report, Appendix A, § A.1 (Oct. 2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf.
[162] *Id.* at § 4.12 and § 5.7.

## OVERVIEW OF UK CRYPTOASSETS TASK FORCE

In March 2018, the government of the United Kingdom brought together the HM Treasury, the FCA, and the Bank of England to launch the Cryptoassets Taskforce to address the risks associated with cryptoassets that fall within existing regulator frameworks.[163] The existing frameworks require, among other things, that certain businesses apply risk-based customer due diligence measures and take steps to prevent services from being used for money laundering or terrorist financing.[164]

These frameworks note the importance of the full traceability of the transfers of funds resulting from the need to prevent, detect, and investigate money laundering and terrorist financing, opining that it would be appropriate to request information on both the payor and the payee for anonymous transfers.[165]

…unregulated tokens must still adhere to applicable AML and CFT requirements that exist…

In July 2019, the FCA finalized its guidance on cryptoassets, which further clarified which tokens fell under its jurisdiction.[166] Specifically, the FCA defined unregulated tokens as those that do not provide rights or obligations akin to specified investments (e.g., exchange tokens).[167] Exchange tokens, as defined by the FCA, are those that are not issued or backed by any central authority and that are intended and designed to be used as a means of exchange.[168] Notably, the FCA expressly stated that unregulated tokens can be privacy coins.[169] However, the FCA noted that any token that qualifies as a security token or e-money token remains regulated under each respective regime[170] and that unregulated tokens must still adhere to the applicable AML and countering financing of terrorism ("CFT") requirements that exist, including those to be implemented by the EU Fifth Anti-Money Laundering Directive ("5AMLD").

## 5AMLD AND OTHER CONTEMPLATED REGULATIONS FROM THE UK CRYPTOASSETS TASKFORCE

In January 2020, the United Kingdom established the FCA as the supervisor of a cryptoasset AML and CFT regime that goes beyond the 5AMLD and brings certain cryptoasset businesses into regulation.[171]

---

[163] *Id.* at Foreword.
[164] *See* FCA Publication: Money laundering and terrorist financing, updated February 16, 2018; *see generally The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017* (2017 No. 692) (June 26, 2017), https://www.legislation.gov.uk/uksi/2017/692/pdfs/uksi_20170692_en.pdf.
[165] *See* Regulation (EU) 2015/847.
[166] *See generally* Guidance on Cryptoassets, Feedback and Final Guidance to CP 19/3 (July 2019).
[167] *Id.* at § 43 (stating that exchange tokens currently fall outside the regulatory perimeter and that transferring, buying, and selling exchange tokens, including the commercial operation of cryptoasset exchanges for exchange tokens, are activities not currently regulated by the FCA).
[168] *See* Guidance on Cryptoassets, Consultation Paper 19/3, § 2.5 (January 2019).
[169] *See* Guidance on Cryptoassets, Feedback and Final Guidance to CP 19/3, § 35 (July 2019).
[170] *Id.* at § 36.
[171] *See* FCA, *FCA becomes AML and CTF supervisor of UK cryptoasset activities* (Jan. 10, 2020), https://www.fca.org.uk/news/news-stories/fca-becomes-aml-and-ctf-supervisor-uk-cryptoasset-activities.

Currently, providers engaged in exchange services between cryptoassets and fiat currencies as well as custodian wallet providers are under no European Union-imposed obligation[172] to identify suspicious activity.[173]

The 5AMLD, which went into effect on January 10, 2020, brought certain cryptoasset products and services under regulation and requires that providers of cryptoasset exchange services and custodian wallet providers (types of VASPs) be registered.[174] Additionally, the Cryptoassets Taskforce will consult on the prevention of anonymous layering of funds that mask the funds' origin and the functionality of peer-to-peer exchanges that enable anonymous transfers between individuals.[175] The 5AMLD requires certain cryptoasset businesses to submit SARs and perform KYC processes in addition to obtaining addresses and identities of cryptoasset owners at the national level so that authorities can identify account holders in a timely manner.[176] Other measures include, in some cases, determining the source of wealth and source of income for users of exchanges and custodial wallets.[177]

These regulations do not directly limit the functionality of privacy coins themselves. Instead, the FCA and related EU regulations impose obligations on the businesses that facilitate token use by requiring their users to provide personal information and satisfy certain conditions.

### FINANCIAL ACTION TASK FORCE (FATF)

FATF is an independent intergovernmental organization that was founded in 1989 at the G7 Summit to develop policies to combat money laundering.[178] Today, there are over 200 countries and jurisdictions committed to implementing the policy recommendations created by FATF, which aim to ensure a coordinated global response to prevent organized crime, corruption, money laundering, terrorism, and other illicit activities ("FATF Recommendations").[179]

FATF periodically evaluates member jurisdictions for compliance with the FATF Recommendations and places jurisdictions with "strategic deficiencies" on "increased monitoring." Such jurisdictions are identified on what FATF refers to as the "grey list."[180] With that said, FATF recognizes that countries have a diverse set of legal frameworks and financial systems that do not allow identical measures to be taken from jurisdiction to jurisdiction.[181]

The FATF Recommendations were last updated in June 2019.[182] At that time, FATF also released a separate "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" ("FATF Virtual Asset

---

[172] EU law will still apply in accordance with the overall withdrawal agreement until at least the end of December 2020. *See* Guidance on Cryptoassets, Feedback and Final Guidance to CP 19/3, § 1.33 (July 2019).
[173] *See generally* Directive (EU) 2015/849; *see also* Directive (EU) 2018/843.
[174] *See* Directive (EU) 2018/843.
[175] *See* Cryptoassets Taskforce: Final Report, § 5.7 (Oct. 2018).
[176] *See generally* Directive (EU) 2018/843.
[177] *Id.*
[178] *See* International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations (June 2019), p. 6.
[179] *See* FATF, *About* (last visited July 17, 2020), https://www.fatf-gafi.org/about/.
[180] *See* FATF, *Jurisdictions under Increased Monitoring – 30 June 2020* (2020), http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-june-2020.html.
[181] *See* International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations (June 2019), p. 6.
[182] As a result of its recent June 2020 plenary, FATF agreed to a public consultation of modifications to Recommendation 1 and its corresponding Interpretive Note, which aim to strengthen the requirements for jurisdictions and private sector entities to identify, assess, and mitigate the risks of potential breaches, non-implementation, or evasion of the targeted financial sanctions related to financing of weapons of mass destruction. *See* FATF, *Outcomes FATF Virtual Plenary, 24 June 2020* (2020), http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-fatf-plenary-june-2020.html.

Guidance") to help member jurisdictions understand specifically how the FATF Recommendations apply to virtual asset activity. In June 2020, FATF completed a 12-month review of member countries' and service providers' compliance with such recommendations on VASPs. In summarizing the key findings of its review,[183] FATF found that "overall, both the public and private sectors have made progress in implementing the revised FATF Standards" in addition to concluding that FATF need not amend its revised Standards on virtual assets and VASPs at this time.[184] FATF also stated that it would continue its enhanced monitoring of virtual assets and VASPs by undertaking a second 12-month review by June 2021 and consider whether further updates to the FATF Standards are necessary.[185]

## INITIAL RISK ASSESSMENT, CUSTOMER DUE DILIGENCE, AND PREVENTION AND MITIGATION MEASURES

The FATF Recommendations endorse essential measures that guide countries to effectively identify risks and develop policies, pursue money laundering and terrorist financing, apply preventive measures for the financial sector, establish governmental powers and enforcement authority, enhance transparency and availability of beneficial ownership information, and facilitate international cooperation.[186]

FATF further recommends that countries identify, assess, and understand the money laundering and terrorist financing risks from virtual asset activities and the operations of VASPs.[187] Based on that assessment, a risk-based approach should be applied to ensure that prevention and mitigation measures are commensurate with the risks identified.[188] FATF notes that countries should require these VASPs to "identify, assess, and take effective action to mitigate their money laundering and terrorist financing risks."[189]

The FATF Virtual Asset Guidance mentions that "[virtual asset] products or services that facilitate pseudonymous or anonymity-enhanced transactions also pose higher [money laundering or terrorist financing] risks, particularly if they inhibit a VASP's ability to identify the beneficiary. The latter is especially concerning in the context of [virtual assets], which are cross-border in nature. If customer identification and verification measures do not adequately address the risks associated with non-face-to-face or opaque transactions, the [money laundering or terrorist financing] risks increase, as does the difficulty in tracing the associated funds and identifying transaction counterparties."[190]

Consequently, FATF recommends that VASPs should consider, among others, the following elements when "identifying, assessing, and determining how best to mitigate the risks associated with covered [virtual asset] activities and the provision of VASP products and services . . . any unique features of each [virtual asset], such as [anonymity-enhanced cryptocurrencies ("AECs")], embedded mixers or tumblers, or other products and services that may present higher risks by potentially obfuscating the transactions."[191] FATF encourages regulators to determine whether a "VASP can manage and mitigate the risks of engaging in activities that involve the use of anonymity-enhancing technologies or mechanisms, including but not limited to AECs," and if "the VASP cannot manage and mitigate the risks posed by engaging in such activities, then the VASP should not be permitted to engage in such activities."[192]

---

[183] FATF, *12 Month Review of Revised FATF Standards – Virtual Assets and VASPs* (July 7, 2020), http://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html.

[184] However, FATF did note the eventual need for additional guidance on virtual assets and VASPs generally. *See* FATF, *Outcomes FATF Virtual Plenary, 24 June 2020* (2020), http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-fatf-plenary-june-2020.html.

[185] *Id.*

[186] *See* International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations (June 2019), p. 6.

[187] *Id.* at Interpretative Note to Recommendation No. 15.

[188] *Id.*

[189] *Id.*

[190] FATF, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (June 2019), paragraph 28.

[191] *Id.* at paragraph 31.

[192] *Id.* at paragraph 110.

In the context of virtual assets like privacy coins (or AECs as defined by FATF), FATF recommends that AML and CFT regulations apply to virtual assets and VASPs in addition to requiring those VASPs to be licensed and to comply with relevant financial regulations.[193] For situations involving a higher risk of money laundering or terrorist financing, FATF also recommends taking enhanced due diligence measures that are consistent with the risks identified.[194] In that regard, FATF emphasizes the need for enhanced due diligence of business relationships and transactions with natural and legal persons from higher-risk countries in the case of virtual assets (given their cross-border nature).[195]

Additionally, FATF recommends that jurisdictions ensure that all VASPs be required to file SARs (which FATF refers to as "suspicious transaction reports") as appropriate.[196] FATF notes that "[SARs] that reference [virtual assets] have proven invaluable in furthering law enforcement investigative efforts as well as for improving the [financial intelligence unit's] ability to better understand and analyse both providers and activities in the [virtual asset] ecosystem," mentioning specifically that VASP SARs "enabled U.S. law enforcement to take action in 2017 against BTC-e" by "helping them to identify [virtual asset] wallet addresses used by BTC-e and detect different illicit streams of activity moving through the exchange."[197]

## LICENSING AND REGULATORY OVERSIGHT

FATF recommends that VASPs be required to license or register and be subject to certain application requirements.[198] However, a separate licensing or registration system is not necessary for persons already licensed or registered as financial institutions within the country that subjects those financial institutions to the applicable obligations under the FATF Recommendations.[199]

In addition, FATF notes that countries should ensure that VASPs are subject to adequate regulation and supervision or monitoring for AML and CFT concerns and that the VASPs are effectively implementing the FATF Recommendations to mitigate money laundering and terrorist financing risks emerging from virtual assets.[200] These regulation and monitoring requirements are placed on the VASPs and not the individual virtual assets. As for supervision, FATF recommends that VASPs be supervised by a competent authority and not a self-regulating body.[201] These supervisory authorities should have "adequate powers to supervise or monitor and ensure compliance by VASPs with requirements to combat money laundering and terrorist financing" and include the authority to conduct inspections, compel the production of information, and impose sanctions.[202]

## THE FATF TRAVEL RULE

To prevent terrorists and other criminals from having unfettered access to wire transfers for moving funds, and for detecting certain misuses upon occurrence, the FATF Recommendations include a rule similar to the Funds Travel

---

[193] *See* International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations (June 2019), Recommendation No. 15; *see also id.* at Recommendation No. 26 (recommending that financial institutions be subject to adequate regulation and supervision in addition to effectively implementing the FATF Recommendations); *see also id.* at Interpretative Note to Recommendation No. 15 (recommending that countries should apply relevant measures to the virtual assets and the VASPs).

[194] *Id.* at Interpretative Note to Recommendation No. 10.

[195] FATF, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (June 2019), paragraph 123.

[196] *Id.* at paragraph 124.

[197] *Id.* at paragraph 126.

[198] *See* International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations (June 2019), Interpretative Note to Recommendation No. 15.

[199] *Id.*

[200] *Id.*

[201] *Id.*

[202] *Id.*

Rule, known as the FATF Travel Rule.[203] The FATF Travel Rule recommends that financial institutions be required to pass certain information to the next financial institution for qualifying funds transmittals that involve more than one financial institution.[204]

This information generally includes the name of the originator, the originator's account number or unique transaction reference number that permits traceability, the originator's information,[205] the beneficiary's name, and the beneficiary's account number.[206] Notably, however, if the information for domestic transmittals can be made available to the beneficiary financial institution and appropriate authorities by other means, then the ordering financial institution need include only the account number (or unique transaction reference number), so long as that number permits the transaction to be traceable to the originator or the beneficiary.[207]

In the context of virtual assets and privacy coins, the FATF Recommendations make clear that the FATF Travel Rule should apply to all VASPs for virtual asset transmittals as well.[208] However, the FATF Recommendations expressly mention that this information, with respect to VASPs and virtual asset transmittals, "can be submitted either directly or indirectly. It is not necessary for this information to be attached directly to the virtual asset transfers."[209]

The FATF Virtual Asset Guidance elaborates on this requirement, noting that FATF "does not expect that VASPs and financial institutions, when originating a [virtual asset] transfer, would submit the required information to individual users who are not obliged entities." However, FATF stated that "VASPs receiving a [virtual asset] transfer from an entity that is not a VASP or other obliged entity (e.g., from an individual [virtual asset] user using his/her own [distributed ledger technology] software, such as an unhosted wallet), should obtain the required originator information from their customer."[210]

[203] *Id.* at Recommendation No. 16.
[204] *Id.* (requiring compliance in addition to recommending that records be retained for at least five years in accordance with Recommendation No. 11). The FATF Recommendations contemplate a *de minimis* threshold for cross-border wire transfers (no higher than $1,000), below which a financial institution would be required to pass a more limited set of transaction information to the next financial institution.
[205] The originator's information includes, for example, the originator's address, identification number, or date and place of birth.
[206] *See* International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations (June 2019), Recommendation No. 16.
[207] *Id.* at Interpretative Note to Recommendation No. 16 (requiring that this information should be able to be made available within three business days of receiving a request to do so).
[208] *Id.* at Interpretative Note to Recommendation No. 15 (referring to the obligations in Recommendation No. 16).
[209] *Id.* (referring to the submission of information obligations set forth in Recommendation No. 16).
[210] FATF, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (June 2019), paragraph 117.

# Part 4

## Targeted AML Regulation of VASPs Works

In AML and related areas, legislation and Regulator implementation and enforcement focuses on VASPs to prevent money laundering, terrorism financing, and other financial crimes. This focus has been largely embodied in the FATF Recommendations as well. Broadly speaking, VASPs generally include businesses acting as the middleman between parties in a financial transaction and those engaged in the business of dealing with financial and monetary transactions in certain capacities.[211]

Regulators impose specific AML obligations on VASPs that provide services and facilitate transactions to assist them with carrying out their respective legislative mandates, because the financial system is "the most effective sector when it comes to detecting signs of money laundering."[212] These VASPs often accept their role in preventing financial crimes and view it as a benefit to society. The same is true for cryptocurrency businesses, and more specifically privacy coin-related businesses, when providing services substantially similar to those historically offered only by traditional financial intermediaries and financial institutions.

> Even in the case of privacy coins, VASPs should and will remain the primary subject of AML and CFT regulations, just as they do in traditional financial transactions.

Even in the case of privacy coins, VASPs should and will remain the primary subject of AML and CFT regulations, just as they do in traditional financial transactions. The current regulatory structure provides suitable protections for both consumers and investors in addition to promoting fairness and preventing crime. This structure should be adapted as much as possible to new technologies, like privacy coins, so that compliance expectations are known and innovation remains unstifled.

### COMPLIANT VASPS CAN ALREADY SATISFY REGULATOR MANDATES

In general, cryptocurrencies, including privacy coins, fit within and can comply with the current financial regulatory structure.[213] Like government-issued fiat currency, many cryptocurrencies serve as a medium of exchange existing entirely in intangible form.[214] However, cryptocurrencies are not recognized as legal tender but can substitute for such.[215] While cryptocurrencies allow for peer-to-peer transactions, they are essentially convertible to legal tender and other cryptocurrencies through the intermediaries that maintain, transfer, and exchange the cryptocurrencies.

---

[211] *See* James Chen, *Financial Intermediary*, Investopedia (Mar. 14, 2020), https://www.investopedia.com/terms/f/financialintermediary.asp; *see also* Adam Hayes, *Financial Institution (FI)* (Apr. 21, 2020), https://www.investopedia.com/terms/f/financialinstitution.asp; *see e.g.* 31 C.F.R. § 1010.100(t) (2014).
[212] *See* Ana Cabirta, *Anti-money laundering challenges in the financial sector*, BBVA (Jan. 3, 2019), https://www.bbva.com/en/anti-money-laundering-challenges-in-the-financial-sector/.
[213] *See, e.g.*, FinCEN Guidance issued on May 9, 2019 (FIN-2019-G001) (stating that FinCEN's May 9, 2019, guidance does not establish any new regulatory expectation or requirements for cryptocurrencies).
[214] *See* Sarah Jane Hughes & Stephen T. Middlebrook, *Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries*, Yale Journal on Regulation, Volume 32, Issue 2 (2015), http://www.cs.yale.edu/homes/jf/Hughes.pdf.
[215] *Id.*

The key difference between most cryptocurrencies and privacy coins is that most cryptocurrencies rely on a transparent public ledger, whereas privacy coins obfuscate certain transaction details and history from the public. These privacy features, however, do not prevent VASPs from complying with regulations in various jurisdictions.

## PRIVACY COINS CAN BE SUPPORTED WITHIN A RISK-BASED AML PROGRAM

As described above, VASPs[216] are required to implement a risk-based AML Program, which is typically based on a risk assessment. When conducting an AML risk assessment, a VASP is generally expected to analyze (a) the inherent AML risk of its customers, geographies, products, and operations, (b) the controls it applies to mitigate such inherent risks, including enhanced due diligence, and (c) the residual AML risk that the VASP faces.[217] As FATF has emphasized, its recommendations "do not predetermine any sector as higher risk," and different entities "within a sector may pose a higher or lower risk depending on a variety of factors, including products, services, customers, geography, and the strength of the entity's compliance program."[218]

### *Inherent AML Risk of Privacy Coins, in a Comparative Context*

An analysis of relevant FATF/FinCEN factors shows that privacy coins pose inherent AML product risks roughly comparable to (and in any event, not materially greater than) other cryptocurrencies or higher risk traditional payment types, such as cash, that are routinely supported by VASPs as part of a risk-based AML Program.

FATF and FinCEN have long identified, as factors tending to increase AML risk, products or services that inherently favor anonymity or products that can readily cross international borders, such as cash, online money transfers, stored value cards, money orders, and international money transfers by mobile phone. When assessing how the inherent AML risk of privacy coins under these factors compares to other cryptocurrencies and traditional currency and payment instruments, it is important to distinguish between the "anonymity" and "ease of crossing borders" factors.

Regarding the "anonymity" factors, privacy coins and other cryptocurrencies provide greater anonymity than account-based currency equivalents (such as bank-issued payment instruments) since the transaction identifier is recorded using a cryptographically generated address, rather than personal information. But they still provide levels of anonymity nearing bearer instruments, like cash, card, or paper payment instruments, because the transactions are executed using networked distributed ledger technology and therefore are (to varying degrees) pseudonymous rather than truly anonymous. Depending on the privacy coin or cryptocurrency, addresses can be traced to natural persons using forensic technology, or permissions can be given to VASPs (e.g., view keys) enabling them to see transaction data and related addresses, as discussed below.

With regard to the "ease of crossing borders" factor, privacy coins and other cryptocurrencies present a higher inherent AML risk than cash, which is physically bulky and therefore more difficult to transport across borders, because large amounts of cash would require sufficient physical transportation and passing government border security. But privacy coins and other cryptocurrencies arguably pose a lower risk, in this respect, than cash, card, or paper payment instruments, which can cross borders with no transfer record at all (i.e., not even a publicly broadcast blockchain transaction).

---

[216] Examples of VASPs are cryptocurrency administrators, exchanges, and hosted wallet providers, including MSBs in the United States.

[217] FATF, *Guidance for a Risk-Based Approach for Money or Value Transfer Services*, paragraph 40 (2016), http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-money-value-transfer-services.pdf.

[218] FATF, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (June 2019), paragraph 25.

FinCEN and FATF also highlight, as a related product risk factor, "the global reach of the product or service offered." Here, too, privacy coins and other cryptocurrencies have attributes that are comparatively higher and lower risk when viewed against other payment types. Cryptocurrencies are technically capable of worldwide reach, given that any person with an internet connection and relevant software could obtain them. But they are generally not recognized as legal tender or accepted as a medium of exchange, unlike fiat currency and other traditional payment types. These limitations substantially mitigate their practical utility and reach on a global basis. For example, holders of cryptocurrencies cannot widely exchange them for goods or services. In other words, if a person were to obtain such assets when conducting illicit activity, such person could not readily convert them into cash without engaging a VASP and transacting through the VASP's platform. Such VASP engagement presumably would result in the holder being identified and the transaction being monitorable.

If anything, privacy coins pose lower inherent AML risk than other cryptocurrencies when considering evidence of illicit use in practice. A recent study by the RAND Corporation found that, while most transactions made with cryptocurrencies are legitimate, Bitcoin is "widely documented to be the most dominant cryptocurrency on the dark web." [219] According to RAND, more than 90% of the cryptocurrency addresses mentioned on dark web markets or forums were Bitcoin addresses. Together, Dash, Monero, and Zcash accounted for just 0.3%.[220]

… the critical takeaway here is that privacy coins do not pose an inherent AML risk that is uniquely or unmanageably high…

Other commonly cited AML product risk factors, such as whether products permit the exchange of cash for a negotiable instrument or whether products have a high or no transaction limit, do not (unlike the factors discussed above) turn on inherent characteristics of the product. These can generally be mitigated, or accentuated, for any product depending on how a VASP chooses to offer it. Thus, privacy coins and other cryptocurrencies do not present structurally higher (or lower) AML risks under these factors as compared to traditional payment types.

Viewing these product AML risk factors on balance, it appears that privacy coins pose inherent AML risks in the approximate range of high-risk traditional payment types, such as cash, other cryptocurrencies, or card or paper payment instruments. To be sure, we anticipate that VASPs supporting privacy coins would likewise classify them as inherently high-risk products (as they commonly classify other cryptocurrencies). But the critical takeaway here is that privacy coins do not pose an inherent AML risk that is uniquely or unmanageably high, since that risk does not appear materially greater than other high-risk traditional products that VASPs have long supported in a responsible and compliant manner. Just as with those traditional products, appropriate controls can in fact yield a substantially lower and manageable AML risk for privacy coins, as we discuss next.

[219] Silfversten, Erik, Marina Favaro, Linda Slapakova, Sascha Ishikawa, James Liu, & Adrian Salas, *Exploring the use of Zcash cryptocurrency for illicit or criminal purposes*. Santa Monica, CA: RAND Corporation (2020), https://www.rand.org/pubs/research_reports/RR4418.html.
[220] *Id.*

### *Appropriate Controls Can Mitigate Inherent AML Risk of Privacy Coins*

A VASP can effectively mitigate the inherent AML risk of privacy coins through a variety of potential controls, which we summarize below. Given the individualized, risk-based nature of AML Programs, it should be emphasized that our summary of these controls is for illustrative purposes only, and certain controls may not be appropriate or necessary for any given VASP.

#### *Enhanced Due Diligence*

The most important control in mitigating privacy coin AML risk, in many cases, is likely enhanced due diligence on VASP customers who wish to transact in privacy coins. Standard customer due diligence at onboarding, to take FinCEN rules as an illustration, requires collection and verification of a customer's name, date of birth, address, and identification number.[221] But FATF, FinCEN, and other national regulators expect appropriate enhanced due diligence measures to be applied in contexts of higher inherent AML risk, as would be the case if a customer wished to transact in privacy coins.

To target and lessen the anonymity-related risks of privacy coins, appropriate enhanced due diligence would likely include measures to prove a customer's source of funds, place of residence, and profession. Other measures may include a requirement that customers describe in detail their purpose for transacting privacy coins (e.g., the holder is a cryptocurrency trader or operates a business in which cryptocurrency is accepted as payment), along with anticipated privacy coin transaction volumes and anticipated privacy coin transaction counterparties. This information would not only help VASPs determine whether a customer is unlikely to use privacy coins for money laundering but also help construct a robust and detailed customer profile against which the customer's ongoing activity could be assessed.

#### *Limitations on Types of Customers and Geographies*

As noted above, a VASP's overall inherent AML risk consists of not only its product risk but also the risks posed by types of customers and geographies. For example, certain categories of customers (e.g., politically exposed persons) and certain geographies (e.g., jurisdictions on FATF's "grey list") pose a presumptively higher inherent AML risk. Although it would be a blunter instrument for risk mitigation than per-customer analysis, a VASP could reasonably and effectively lessen the overall AML risk of a privacy coin offering by categorically prohibiting customers who are in higher risk categories or geographies from accessing the privacy coin offering.[222]

#### *Ongoing Transaction Monitoring and Diligence*

Collecting additional customer information on a per-transaction basis, as appropriate, would further mitigate the AML risk of privacy coins. After creating certain predefined thresholds (e.g., based on transaction size, asset type, or divergence from customer profile), a VASP could require supplemental information from a customer before processing a privacy coin transaction (e.g., details regarding the purpose of a transaction, the name and address of the recipient, and contact information for the recipient). Collecting this information could help deter illicit activity in the first instance, provide verifiable data that could assist the VASP's recordkeeping and audit processes, and in some cases satisfy regulatory obligations.[223] The privacy-preserving features of privacy coins would not, as compared to other cryptocurrencies, make it any more difficult for a VASP to obtain this information about a privacy coin transaction and its beneficiary.

---

[221] 31 C.F.R. § 1022.210(d)(1)(iv) (2011).

[222] These steps could also be done in conjunction with per-customer analysis.

[223] BitLicensees, for example, are required to maintain for each customer transaction "the names, account numbers, and physical addresses of: (i) the party or parties to the transaction that are customers or accountholders of the Licensee; and (ii) to the extent practicable, any other parties to the transaction." 23 N.Y.C.R.R. 200.12(a)(1) (2015).

Additionally, a VASP can implement technological, privacy coin-specific controls to obtain additional visibility into the amounts and addresses associated with privacy coin transactions. A VASP could require that a customer accept and agree to comply with these controls, which are detailed on a per-coin basis below, as a condition of transacting in specified privacy coins.

Other controls may involve monitoring of transactions through on-chain surveillance and other software-based tools. On-chain surveillance tools are being increasingly used by law enforcement and have been mentioned as a helpful way for VASPs to detect suspicious patterns of cryptocurrency activity. These tools, however, currently have limited effectiveness when applied to privacy coin transactions. On-chain surveillance tools provided by Chainalysis, for example, can analyze Dash transactions, but not shielded Zcash transactions or transactions in Monero or Grin.[224] Where on-chain surveillance tools cannot be used, a VASP would still have ample controls to address AML risks of privacy coin transactions. All other controls would still be available, and there is no analogue to on-chain surveillance for traditional bearer instruments (like cash) that are widely supported within financial institutions' AML Programs. And even where a VASP can use on-chain surveillance tools, it is important that such tools function as a supplemental, rather than a primary, AML control measure. Without a detailed understanding of what a customer's typical activity is, even the best technical tools are of limited use in detecting suspicious activity.

Where on-chain surveillance tools cannot be used, a VASP would still have ample controls to address AML risks of privacy coin transactions.

Should a VASP determine that its particular mix of controls does not sufficiently reduce the inherent AML risk of a given privacy coin, it could take the additional step of limiting all incoming and outgoing transactions involving such coin to originating or receiving addresses that the accountholder demonstrably controls. This is another blunt measure that should generally not be necessary, if other controls are adequate. But we mention it to show the full extent of potential controls that could enable VASPs to support privacy coins within a prudent, risk-based AML Program.

Finally, a VASP can (and should) have a robust procedure for reevaluating the effectiveness of its controls as the volume and composition of its privacy coin products change and as AML regulatory requirements and expectations evolve, given the rapid pace of development in the industry.

In sum, each VASP can implement and comply with an effective, risk-based AML Program that specifically considers privacy coins and mitigates the possibility that privacy coins are being used for money laundering, the financing of terrorism, or other illicit activity, just like traditional financial intermediaries and institutions.

[224] Chainalysis began conducting forensics on the Dash and Zcash protocols as of June 8, 2020. *See* Chainalysis Insights, *Introducing Investigation and Compliance Support for Dash and Zcash* (June 8, 2020), https://blog.chainalysis.com/reports/introducing-chainalysis-investigation-compliance-support-dash-zcash.

## THE TRAVEL RULE IN THE PRIVACY COIN CONTEXT

In the United States, the Funds Travel Rule requires, among other things, the transmitting financial institution or intermediary to include the name of the transmittor and the amount of the transmittal order for transmittal orders to another financial institution.[225]

A common misconception is that the privacy-preserving features of privacy coins prevent exchanges and other MSBs from complying with FinCEN's Funds Travel Rule.[226] We believe this misconception stems, at least in part, from the assumption that Funds Travel Rule information must accompany the funds transfer in the same system, which is possible in traditional funds transfer systems like Fedwire but generally impractical or impossible in blockchain-based systems.[227] The text of the Funds Travel Rule lends itself to this misconception, providing that a transmitter's financial institution "shall *include in any transmittal order* for a transmittal of funds in the amount of $3,000 or more, information as required" by the rule.[228]

However, FinCEN clarified in the 2019 FinCEN Guidance that "the parties to the transmittal of funds are not required to use the same system or protocol for both the actual transmission of value and the reception or transmission of the required regulatory information."[229] This clarification was substantially mirrored by the FATF Recommendations whereby required transmittal information pursuant to the FATF Travel Rule (together with the FinCEN Funds Travel Rule, the "Travel Rule") does not need to be attached directly to the transfer of the virtual asset.[230]

As a practical matter, this enables a sender's VASP to execute its customer's privacy coin transaction on the blockchain while transmitting the required Travel Rule information through an alternative information channel with the beneficiary's VASP. The sender's VASP will already know the required information about the sender (its customer) through its own KYC process and can require the sender to provide all other required transactional and beneficiary information as a prerequisite to executing the transaction. Notably, the Travel Rule applies only to transactions involving more than one regulated VASP, so an exchange is not required (for example) to transmit a sender's Travel Rule information to a beneficiary's unhosted privacy coin wallet. Since the sending and receiving VASPs are required to conduct KYC on their respective customers prior to providing services, the privacy-preserving nature of privacy coins therefore does not hinder compliance with the Travel Rule.

To be sure, the Travel Rule presents certain logistical challenges to VASPs that support privacy coins and other cryptocurrencies. These challenges principally include determining whether a customer's transaction is covered by the Travel Rule (i.e., that the transaction involves another VASP), coordinating with other VASPs so that Travel Rule information is shared in a uniform manner, and ensuring that customer Travel Rule information is transmitted securely and immediately to a recipient financial institution. But as detailed below, these challenges are applicable to cryptocurrencies in general (i.e., they are not unique to privacy coins), and various private sector solutions have already emerged to address them.

---

[225] *See* 31 C.F.R. § 103.33(g) (2011).

[226] *See* 31 C.F.R. § 1010.410(f) (2016). Among other things, the Funds Travel Rule requires the transmitting institution or intermediary to include the name of the transmittor and the amount of the transmittal order.

[227] It is worth emphasizing that this issue is not specific to privacy coins, since it also applies to transfers of nonprivate cryptocurrency, cash, and any other types of funds where there is no system (like Fedwire) that allows Funds Travel Rule information to be included with the transfer itself.

[228] *See* 31 C.F.R. § 1010.410(f) (2016) (emphasis added).

[229] FinCEN Guidance issued on May 9, 2019 (FIN-2019-G001), § 2.1.

[230] *See* International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations (June 2019), Interpretative Note to Recommendation No. 15 (referring to the submission of information obligations set forth in Recommendation No. 16).

Because a cryptocurrency transaction is subject to the Travel Rule only when two VASPs are involved, a VASP must have a means of determining whether a customer's transaction is from or to another VASP. As noted above, one way of addressing this issue is to require that the customer provide information regarding the origin or destination of the transaction before execution, including sufficient detail to allow the VASP's compliance team to verify accuracy if needed. If a customer is truly involved with a transaction to or from another regulated financial institution (such that the Travel Rule would apply), there does not appear to be an obvious motive for such customer to provide inaccurate information regarding the origin or destination of funds (e.g., telling the VASP that an outbound transfer is to an unhosted wallet instead of another exchange). This is especially true if the VASP makes clear in its terms that providing inaccurate information could be grounds for account termination.

There are also third-party providers that assist with facilitating off-chain Travel Rule compliance via innovative technical solutions, like Netki's TransactID service and the Travel Rule Information Sharing Architecture ("TRISA").[231] To illustrate: TRISA, which is an open source and available for any VASP to use, relies on the well-understood certificate authority model (which underpins most "secure website" designations) to enable VASPs to reliably identify and verify each other. TRISA also features mutual authentication procedures to help ensure that VASPs do not send customer information to the wrong VASP. Finally, TRISA is compatible with a variety of emerging messaging standards for Travel Rule information, such as the interVASP Messaging Standard.[232] It should be emphasized that Netki, TRISA, and interVASP are presented by way of illustration only; other information sharing architectures and messaging standards have been developed as well, and it is too early to predict which ones will be most widely used.[233] However, as TRISA and interVASP illustrate, private entities have taken meaningful steps to address the coordination and privacy-related concerns that Travel Rule compliance presents for VASPs. So long as the leading solutions remain committed to broad interoperability, the existence and use of multiple solutions should not materially hinder VASP coordination and compliance efforts.

By using alternative information channels, exchanges can and do satisfy the Travel Rule for qualifying transactions by sending the required information to a beneficiary or intermediary VASP in a contemporaneous message by another means.[234] In June 2020, FATF specifically noted the development progression of these technological solutions and alternative information channels for VASPs in implementing and complying with the Travel Rule.[235] Indeed, the availability of multiple alternative compliance solutions to the Travel Rule logically eliminates any need for an outright ban or limiting regulation. As referenced above, off-chain compliance solutions can be developed by and among the VASPs that offer services involving privacy coins that can directly or indirectly share the information necessary for protecting against transfers for illicit purposes and meeting applicable compliance obligations.

Indeed, the availability of multiple alternative compliance solutions to the Travel Rule logically eliminates any need for an outright ban or limiting regulation.

[231] *See* TRISA, *Decentralized Cryptocurrency Travel Rule Compliance* (last visited July 17, 2020), https://trisa.io/; Netki, *TransactID - The Proven Travel Rule Solution* (last visited July 17, 2020), https://netki.com/transactid/.
[232] *See* interVASP Messaging, *interVASP Messaging Standard Overview*, https://intervasp.org/.
[233] Examples include OpenVASP and BIP75 (messaging standards) and Sygna Bridge (information sharing architecture).
[234] *See* FinCEN Guidance issued on November 9, 2010 (FIN-2010-G004), § 2.
[235] *See* FATF, *Outcomes FATF Virtual Plenary, 24 June 2020* (2020), http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-fatf-plenary-june-2020.html.

Although we expect VASPs to primarily or exclusively use off-chain solutions for Travel Rule compliance, at least in the near term, we note that there are also potential on-chain solutions available for VASPs that facilitate privacy coin transactions. For example, some privacy coins already have an encrypted memo field that can be used to transmit information along with a transaction, as discussed further below.

Ultimately, privacy coins present no incremental challenges or requirements to already compliant VASPs, other than the need to collect, retain, and transmit certain customer and transaction information to the recipient VASP.[236] These requirements are not unique to VASPs providing privacy coin services, and thus those VASPs should remain subject to the same standards as traditional financial institutions.

### PRIVACY COIN FEATURES PROVIDE SUPPLEMENTAL WAYS FOR ENABLING AML COMPLIANCE

Certain features and inherent characteristics of various privacy coins can provide supplemental ways for VASPs to satisfy their respective AML compliance obligations. As noted above, these VASPs can already comply with various KYC, AML, and sanctions-related compliance obligations via traditional methods (i.e., because they can require whatever information they choose, in accordance with their AML Program, from customers using their services, regardless of the characteristics or features and aspects of any cryptocurrency or privacy coin). But it is worth emphasizing these supplemental methods of compliance to underscore that privacy coins, far from being technologically incompatible with AML compliance, can facilitate such compliance through certain features.

If VASPs serve as custodians of the private keys of their users, they will be able to see the amount of privacy coins received by their users or the amounts their users transact with. These VASPs will also be able to report on suspicious activity, pursuant to and in compliance with their respective AML Programs, should such activity be identified. Lastly, the privacy coins discussed in Part 2 each enable VASP compliance in supplemental and unique ways. We look at a few mechanisms that each privacy coin currently uses below.


The privacy features embodied in Monero allow the transaction participants to obfuscate their identities and hide the amounts transferred from third parties, except for those they designate. This feature protects commercial and individual privacy by preventing unwanted third parties from being able to view transaction details, while leaving the door open for the transacting parties to assist with financial intermediary compliance.

Users can reveal an XMR transaction's details that are specific to their account via key-based functionality that is built into the Monero protocol. Specific view keys can be shared with any third party to grant insight into the account associated with the view keys. This enables users and VASPs to disclose certain transaction details associated with a given account to a third party without publicly disclosing that user's transactional information. In addition, VASPs can require up-front disclosures as part of their registration process and on an ongoing basis to meet their obligations.

[236] *See* 31 C.F.R. § 103.33(g) (2011).

The PrivateSend feature complicates transactions by merging DASH tokens with at least three other parties during the transmission process in a way that cannot be readily reverse-analyzed at a later date to determine originations. However, both the sending party and the receiving party will have their own transactional data, which further supplements VASPs' ability to comply with their respective compliance obligations. This information, combined with VASPs being able to require sufficient disclosures during the registration process and on an ongoing basis, enables VASP compliance.

Like transactions on the Monero network, the Grin network uses privacy features that automatically create opaque transactions that are verifiable, yet publicly hidden. Unlike transactions on the Monero network, however, Grin transactions enable verification through the use of blinding factors and other features, as discussed in Part 2 above. While the Grin network's privacy features obfuscate the identity of the sending party, the VASPs can still determine the identity and amounts received by their users because they can require specific information during onboarding and as part of each user's continued use of their services.

Moreover, the employment of the Dandelion relay and cut-through technique further provides privacy in addition to increasing the efficiency of the Grin network. The use of these two concepts does not deteriorate the VASPs' ability to meet their respective compliance obligations, given that these techniques merely obfuscate the originating user from the public and remove unnecessary transaction verification data from the network. When the transaction is first effectuated, the sending user's VASP will be able to determine who sent Grin coins and how much, while the receiving user's VASP will be able to determine how many Grin coins were received and who received it, because in both cases, the VASPs can require upfront and ongoing disclosure requirements.

The zero-knowledge proof privacy enhancement to certain ZEC transactions allows for verification of transactions without revealing certain information to the public. However, users that send or receive ZEC from or to their z-address (private address) have the ability to reveal the transaction's details that are specific to their account via a viewing key. The viewing key can be shared with any third party and enables full transparency with regard to the account associated with that viewing key. This enables users and VASPs to disclose certain transaction details associated with a given account to a third party, without publicly disclosing that user's transactional information.

Additionally, sending users can include a brief memo with each transaction that only the recipient can see. This enables users to share information that may be necessary in a given transaction. For example, when required, users may include certain information in the memo that is necessary for VASPs to comply with the Travel Rule (where implemented). Furthermore, users can elect to transact without using any of the above-mentioned privacy features,

making certain transactional data visible to the public.[237] Lastly, VASPs can require up-front disclosures during the registration process and on an ongoing basis to satisfy KYC obligations.

### FOCUSED AML REGULATION CREATES CERTAINTY, MITIGATES CRIME, AND FOSTERS INNOVATION

Keeping AML regulation focused on VASPs will create more certainty in markets, while simultaneously mitigating crime and fostering innovation. This has been the traditional approach taken and remains the only proven and effective method. Imposing AML regulatory requirements on peer-to-peer, commercial transactions for privacy coins would be a radical departure from that proven approach, resulting in significantly greater (and unwarranted) government involvement in personal and business matters. Such regulatory requirements, at least in the United States, would likely necessitate major changes to underlying AML legislation in order to withstand judicial scrutiny. If prohibitive or unduly burdensome obligations that are specific to select aspects of cryptocurrencies are imposed, Regulators and society may experience unintended consequences, and such action will likely stifle investment, innovation, and advancement in that area.

Applying AML-related regulation only to VASPs is particularly important at this stage because cryptocurrencies, and specifically privacy coins, are still in the embryonic phase of their evolution. It is difficult to tell which direction and what technological advancements may ultimately result from the current technologies that privacy coins possess. Moreover, some Regulators have already espoused the benefits of cryptocurrencies and blockchain technology and see the potential they have in enhancing economic efficiency, mitigating centralized systemic risk, defending against fraudulent activity, and generally improving data quality and governance.[238] Ultimately, absent evidence that existing AML regulations cannot adequately address the risks posed by privacy coins, there is no reason to impose new and overbroad AML requirements that specifically target privacy coins.

# Conclusion

Privacy coins reflect a nascent, but important, effort to safeguard our fundamental interest in personal and commercial financial privacy. The AML risks of privacy coins, while real, do not require specific, tailored regulations that may pose an unnecessary risk of stifling privacy coins' growth. Rather, VASPs can adequately address those AML risks by maintaining an effective, risk-based program. Allowing VASPs to support privacy tokens under current, tested AML regulations strikes the appropriate policy balance between preventing money laundering and allowing beneficial, privacy-preserving technology to develop.

[237] Public ZEC transactions are viewable by the public, just like regular Bitcoin transactions.

[238] *See, e.g.,* U.S. Commodity Futures Trading Commission, *Written Testimony of Chairman J. Christopher Giancarlo before the Senate Banking Committee, Washington, D.C.* (Feb. 6, 2018), https://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo37.