Boston University School of Law Scholarly Commons at Boston University School of Law

Faculty Scholarship

5-25-2020

A Proposal for Taxing Cryptocurrency In the Midst of the COVID-19 Pandemic

Richard Thompson Ainsworth

Xiuyuan (Tony) Hu

Follow this and additional works at: https://scholarship.law.bu.edu/faculty_scholarship



Volume 98, Number 8 📕 May 25, 2020

A Proposal for Taxing Cryptocurrency In the Midst of the COVID-19 Pandemic

by Richard T. Ainsworth and Xiuyuan (Tony) Hu

Reprinted from Tax Notes International, May 25, 2020, p. 921

VIEWPOINT

tax notes international[®]

A Proposal for Taxing Cryptocurrency In the Midst of the COVID-19 Pandemic

by Richard T. Ainsworth and Xiuyuan (Tony) Hu





Richard T. Ainsworth

Xiuyuan (Tony) Hu

Richard T. Ainsworth is an adjunct professor at the Boston University graduate tax program and the New York University graduate tax program. Xiuyuan (Tony) Hu is a tax LLM student at New York University.

In this article, the authors present the case for a globally effective remedial tax on cryptocurrency transactions that could help fund multinational relief efforts, such as providing aid to jurisdictions affected by the COVID-19 virus and countries fighting the opioid crisis.

The COVID-19 pandemic cannot last forever.

When it is behind us, the world will probably ask China to pay for huge economic and humanitarian losses based on the belief that the spread of disinformation pertaining to COVID-19 caused the world to underestimate its severity.¹ If China does not pay (and it likely will not), the international community should look for a global revenue source to help fund the response to health emergencies. A globally effective remedial tax on cryptocurrency could help fund much-needed humanitarian assistance to jurisdictions debilitated by COVID-19 — and it could help the world prepare for the inevitable pandemics that seem all too likely to occur in the future.²

It is no secret that criminals have been dealing drugs³ and conducting other illicit business on the dark web for years.⁴ These transactions and the income they produce are notoriously untaxed largely because cryptocurrency is the preferred medium of exchange. Much like cash transactions, the use of cryptocurrencies on the dark web can leave no trace of the transacting parties' identities.⁵ Occasionally law enforcement can track down illicit activities, including by using undercover agents to pose as potential buyers on the dark web or following credible leads from informants,⁶ but they lack a systematic means to pierce through criminals' anonymity. This leaves the vast majority of wrongdoers uncaught, their

¹See Ken Ritter, "Lawsuit: China Hid Virus Information, Should Pay Billions," Associated Press, Mar. 24, 2020. See also Sadanand Dhume, "Delhi Isn't Buying Beijing's Coronavirus Hero Act," The Wall Street Journal, Apr. 2, 2020.

²See Hiroshi Kaneko, "Proposal for International Humanitarian Tax – A Consumption Tax on International Air Travel," *Tax Notes Int'l*, Dec. 14, 1998, p. 1911 (proposing, more than 20 years ago, a humanitarian tax on international air travel with the funds used to provide relief for disaster victims).

³See testimony of Kirsten D. Madison, assistant secretary, Bureau of International Narcotics and Law Enforcement Affairs, before the Senate Caucus on International Narcotics Control, "Stopping the Poison Pills: Combating the Trafficking of Illegal Fentanyl From China" (Oct. 2, 2018).

⁴See Peter D. Hardy, Alicia M. Went, and Shauna Pierson, "IRS CI Highlights International Efforts to Tackle Cryptocurrency Abuse, Money Laundering and Tax Evasion," Ballard Spahr LLP Money Laundering Watch blog, Dec. 9, 2019.

See Caitlin Reilly, "Cryptocurrencies Complicate Effort to Stop Opioid Dealers," Roll Call, Oct. 29, 2019.

[°]See Chainalysis Team, "Chainalysis in Action: Analyzing a Fentanyl Dealer's Cryptocurrency Transactions," Chainalysis blog, Oct. 1, 2019.

illicit profits untaxed, and their victims unaided and alone.⁷

From a revenue perspective, law enforcement's obsession with unveiling criminals' identity is somewhat misguided. Anonymity (or relative anonymity) is a magnet that draws criminals into the cryptocurrency world, which is a world that actually allows authorities to gauge the value of the illicit goods being exchanged as long as the transactions are recorded on the cryptocurrency's public ledger. Imposing a flatrate sales tax on dark web transactions based on the value exchanged becomes easy, and it is particularly desirable if the funds are used to purchase medical supplies during a pandemic like COVID-19 or provide humanitarian assistance in its aftermath. These funds can be used more generally for a range of apt, publicspirited ends such as reducing opioid overdoses, helping survivors of human trafficking, curtailing global dissemination of child pornography, and responding to terrorist attacks.

In this remedial model, cryptocurrency's perceived financial anonymity functions as a bait that lures criminals to feed. The tax authorities may not know exactly who the criminals are or even what illicit goods they exchanged, but nonetheless the authorities can still collect a tax on their sales proceeds and put the revenue to good use. Without anonymity, criminals would be scared away and would leave the tax authorities little to work with.

'Catch Me if You Can'

Probably as part of a publicity campaign to simultaneously boost the public's confidence in the government and discourage criminals from using cryptocurrencies, law enforcement has been touting the fact that some of the most widely used cryptocurrencies, such as bitcoin, are only pseudo-anonymous. This means they can be traced using forensic analysis.

Forensic analysis starts with a bitcoin address's transaction history.⁸ From there, law

enforcement focuses on points of vulnerability that is, times when the investigator might discover the criminal's identity, such as when the cryptocurrency is exchanged for fiat currency.⁹ Because U.S.-registered cryptocurrency exchanges must comply with know-yourcustomer and anti-money-laundering (AML) regulations, authorities can subpoen the exchange to obtain information about specific users under investigation.¹⁰

Many non-U.S.-registered exchanges, however, do not necessarily comply with U.S. AML regulations because their home jurisdictions may have different — and often more lax rules.¹¹ Without effective coordination between jurisdictions, cross-jurisdictional investigations are likely to end in deadlock.

In 2019 three researchers based in Australia – Sean Foley, Jonathan R. Karlsen, and Tālis J. Putniņš – estimated that there are at least \$76 billion worth of illegal activities per year involving bitcoin, which translates to about 46 percent of all bitcoin transactions.¹² Their study took a sample composed of previously identified bitcoin users associated with dark web activities and used information regarding these known bad actors to estimate the total amount of illicit activity involving bitcoin.

Despite its popularity, bitcoin is not the only cryptocurrency gaining traction in the dark web world. In a 2018 study requested by the European Parliament, two Belgium-based researchers, Robby Houben and Alexander Snyers, made policy recommendations to the EU based on their study of 10 altcoins that had the highest market capitalization at the time.¹³ They suggested that the EU to create more weak spots by subjecting more players in the cryptocurrency market, such

⁷ See Robby Houben and Alexander Snyers, "Cryptocurrencies and Blockchain: Legal Context and Implication for Financial Crime, Money Laundering and Tax Evasion," European Parliament TAX3 Committee (July 2018).

⁸*See* Chainalysis Team*, supra* note 6.

⁹See Matthew Cronin, "Hunting in the Dark: A Prosecutor's Guide to the Dark Net and Cryptocurrencies," 66(4) Atty's Bull. 65 (July 2018).

¹⁰For example, in *United States v. Coinbase Inc.*, No. 3:17-cv-01431 (N.D. Cal. 2017), a court granted the IRS's request for information about some of Coinbase's customers because the IRS had reason to suspect some users did not report gains. Coinbase was responsible for keeping the data because of AML regulations.

¹¹See Craig Adeyanju, "What Crypto Exchanges Do to Comply With KYC, AML and CFT Regulations," Cointelegraph, May 17, 2019.

¹²See Foley, Karlsen, and Putniņš, "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?" 32(5) Rev. Fin. Stud. 1798 (May 2019).

¹³See Houben and Snyers, supra note 7.

as miners, virtual currency exchange services, and custodian wallet providers, to the EU's due diligence and registration requirements.

While blockchain technology has largely eliminated the role of financial institutions in transactions, Houben and Snyers propose inserting regulated intermediaries at various points in cryptocurrency transactions so that AML regulations attach to identifiable persons. This will give law enforcement more opportunities to pierce through the anonymity that is a feature of so many cryptocurrencies.

Notably, Houben and Snyers' plan is philosophically incompatible with the vision of Satoshi Nakamoto, the pseudonymous author of the white paper "Bitcoin: A Peer-to-Peer Electronic Cash System," which was released simultaneously with the bitcoin application, and sought to create "a purely peer-to-peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without going through a financial institution."¹⁴ If implemented, Houben and Snyers' proposal would effectively nullify the most innovative aspects of the blockchain technology.

In practice, however, the regulatory reforms that they propose may not be enough to complete the transformation of cryptocurrencies into fiat currencies that rely on financial institutions acting as trusted third parties. As the pair acknowledge, the use of forensic analysis to uncover a user's identity cannot be made into:

a standardized approach to tackle money laundering, terrorist financing and tax evasion more widely: discovering identities in this way is too complex and costly to become the general answer to tackling this issue — and moreover, it will not certainly lead to any result.¹⁵

While Houben and Snyers' policy recommendations would certainly give law enforcement more tools to work with, their study — taken together with the work of the three Australian researchers — ultimately suggests that without credible leads from informants or undercover agents to narrow down the targets, law enforcement is unlikely to have the bandwidth to conduct comprehensive investigations on the millions of cryptocurrency addresses that might be linked to illicit activities. After all, Foley, Karlsen, and Putniņš estimate that, as of August 2017, at least 27 million bitcoin market participants were using the cryptocurrency primarily for illegal purposes to conduct some 37 million transactions each year.¹⁶

The optimism surrounding the use of forensic analysis to fight cryptocurrency-enabled crime is disproportionate to its practical utility. The vast majority of criminals using cryptocurrencies are daring, in some cases even taunting, law enforcement: "Catch me if you can."

The Remedial Tax Proposal

The Question of Value

Not only does the remedial model work better with blockchain technology's decentralizing feature, it is also more administrable in practice than relying on forensic analysis. Although the remedial tax alone does not provide justice to the victims of crypto crimes, it does ensure funds are readily available to make a real and positive impact on their lives. The key to taxing illicit goods is finding a reliable and accurate indicator of the value of goods transacted.

Transaction size might be a starting point for value. Taking bitcoin as an example, a byte is the measuring unit of the size of a bitcoin transaction. Transaction size, however, is not directly reflective of the amount of funds transferred.

We can calculate the size of a bitcoin transaction as follows:¹⁷ If our transaction has *in* inputs and *out* outputs, the transaction size (in bytes) will be:

in x 180 + *out* x 34 + 10 *plus or minus in*

If our transaction has one input and two outputs, then the transaction size should be 258 bytes as follows:

1 *x* 180 + **2** *x* 34 + 10 + - **1**

TAX NOTES INTERNATIONAL, MAY 25, 2020

¹⁴Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (Oct. 31, 2008).

¹⁵Houben and Snyers, *supra* note 7.

¹⁶See Foley, Karlsen, and Putniņš, supra note 12.

¹⁷ See Kai Sedgwick, "How to Calculate Bitcoin Transaction Fees When You're in a Hurry," Bitcoin.com, Nov. 27, 2017.

Here, "input" is related to the source or origin of the bitcoins used in the transaction, while "output" denotes the number of recipients. Notably, there is a transaction fee associated with each bitcoin transaction. The fee is not related to the amount transferred; instead, it is based on how the sender received the funds in the first place and the number of recipients.

The chief technology officer and one of the founders of Ripple, a U.S.-based technology company that primarily serves as a currency exchange and remittance network, David Schwartz, explains:

Imagine if you walk into a candy store and are told that a candy bar is 35 cents, but then when they rang you up, they tacked on a 15 cent fee. When you asked them what it was for, they explained that the previous customer had paid them all in pennies, and in order to give you your change, they'd have to count all those pennies, and that takes more time.¹⁸

So if the buyer obtained the bitcoins used in the transaction from several different sources, the input number would be larger and, based on the formula above, there would be a higher transaction fee. In short, bitcoin bases its transaction fee on how the funds are structured; it has nothing to do with the value of the transaction itself and thus is not a useful indicator of such.

A better indicator of the value of goods exchanged is the difference between the sender's starting balance and the funds in the sender's change address after the transaction. In a bitcoin transaction, if A has a balance of BTC 3 and wants to pay BTC 0.5 to B, A cannot simply send BTC 0.5 and keep the remaining BTC 2.5 in her wallet.¹⁹ Instead, A must spend the whole BTC 3 and designate BTC 0.5 to B while sending the remaining BTC 2.5 back to a change address that A controls. Originally, bitcoin wallets asked users to designate a change address if they were not spending their whole balance. Now, so-called deterministic wallets automatically generate change addresses. To preserve bitcoin users' privacy, these automatically generated change addresses are different from the users' initial addresses (see Figure 1 for an illustration).

In Figure 1, transactions 1-5 involve an anonymous user who starts with a net balance of BTC 11.852428 and repeatedly sends BTC 0.8 to another bitcoin address. For each transaction, after the deduction of 0.8 BTC plus transaction fees, the remaining balance is returned to a change address that the sender controls.

Although it is unclear what the BTC 0.8 in this example is spent for, if it is used to purchase illicit goods then the dollar value corresponding to BTC 0.8 at the time of the transaction is the best indication of the actual purchase price. A flat rate remedial tax should be attached to the BTC 0.8 purchase price. This is akin to consumers paying a sales tax in the United States. In the remedial model proposed herein, the BTC 0.8 purchase price would be subject to a flat rate tax.

Thus, instead of using transaction size as a yardstick, the difference between a bitcoin user's starting and remaining balance — even if these amounts are technically in two different accounts — is a more reliable and accurate benchmark of the illicit goods' actual value.

Example: Bitcoin's Blockchain

Although the transacting parties' identities are private on bitcoin's blockchain, the details of their transactions are not. In Figures 2 and 3 (a randomly chosen record of a bitcoin transaction on its blockchain), an anonymous user with a starting balance of \$1,590.10 spends \$272.54 and ends up with \$1,308.81 in her change address.

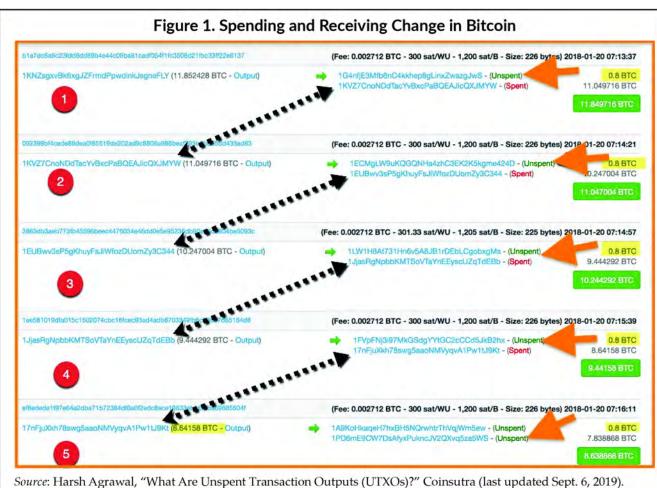
Again, the records do not show what this user received for the \$272.54. However, if the money is used for illicit purposes, the remedial tax should apply to this dollar amount because it is best reflection of the actual purchase price of the goods or services that the user obtained.

A Supranational Body to Administer the Tax

As illustrated above, bitcoin's blockchain does not disclose transacting parties' IP addresses. Therefore, if the tax was administered at a

¹⁸This quote is from Schwartz's answer to a StackExchange discussion thread started by the user macintosh264 titled "How to Calculate Transaction Size Before Sending (Legacy Non-Segwit – P2PKH/P2SH)." Both the question and answer were first posted on Sept. 22, 2011.

¹⁹See Harsh Agrawal, "What Are Unspent Transaction Outputs (UTXOs)?" Coinsutra (last updated Sept. 6, 2019).



Source: Harsh Agrawal, "What Are Unspent Transaction Outputs (UTXOs)?" Coinsutra (last update Reprinted with permission.

national level, jurisdictions would be likely to make competing claims to the collected proceeds. At a minimum, resolving potential jurisdictional conflicts would require knowledge of the transacting parties' tax residences. Intrusive disclosures like this would ruin the privacy appeal of cryptocurrency. It is, however, worth noting that not all users of cryptocurrency are motivated by anonymity; there are subsets who primarily seek currency stability and others who like the digital mobility of cryptocurrency.

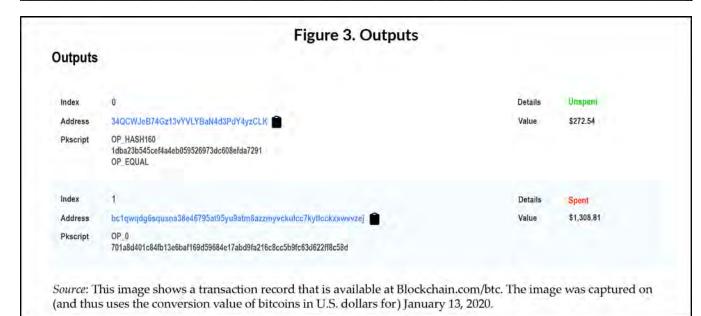
To avoid the extra headache, it would be preferable to have a supranational body like the United Nations administer the remedial tax and distribute the funds according to a particular jurisdiction's needs. For example, when a jurisdiction is battling an opioid pandemic — a plight often associated with cryptocurrency — it could apply to the administering body for appropriate funds proportionate to the scale and severity of the crisis, and use the funds to reduce instances of overdosing and develop more advanced technology to detect opioids at port of entry. Similarly, the funds can provide relief for the economic impact of COVID-19 and other health epidemics. It would not be necessary for a health emergency to be directly associated with cryptocurrency transactions on the dark web for a jurisdiction to be eligible to receive remedial funds, but the health crisis would need to be multinational and not simply local.

Successful implementation of the remedial tax would require strong international cooperation and political will.

Considering Legal Uses of Cryptocurrency

Exceptions would not be needed if cryptocurrencies were used solely for illicit purposes. However, approximately half of all bitcoin transactions are not (at least on their face) associated with dark web activities or known bad

Figure 2. Inputs		
		HEX ASM
0'	Details	Output
bc1qwqdg6squana38e46795at95yu9atm8azzmyvckulec7kyllockxawvvzej	Value	\$1,589.01
OP_0		
3044022051d2942683f83e6d9a867ba260f8c01765070a5e4451f6c6e0f9b8cfc0f60bdf02202dc6a 128e7413064801	aa7c7abc00683691fce8a6e96	c5cb766554182d3806b52f8
304402206187f8cc2f3f0ef3b6c7f78aa2f114b3324af055cc0e75a40fa9ff90d75e329b02200da5f2t 8f62f96ec01	5e9829771922f491283f97433	97fc4920d236fc1d139b1394
52210375e00eb72e29da82b89367947f29ef34afb75e8654f6ea368e0acdfd92976b7c2103a1b263 74496feff2103c96d495bfdd5ba4145e3e046fee45e84a8a48ad05bd8dbb395c011a32cf9f88053ae		559d8cac749a0e53d70eff018
	0 bc1qwqdg6sqlisna38e46795at95yu9atm8azzmyv6kujdc7kyllockxawvvzej OP_0 3044022051d2942683f83e6d9a867ba260f8c01765070a5e4451f6c6e0f9b8cfc0f60bdf02202dc6a 128e7413064801 304402206187f8cc2f310ef3b6c7f78aa2f114b3324af055cc0e75a40fa9ff90d75e329b02200da5f2l 8f62f96ec01 52210375e00eb72e29da82b89367947f29ef34afb75e8654f6ea368e0acdfd92976b7c2103a1b263	0 Details bc1qwqdg6sqlisna38e46795at95yu8atm8azzmyvckujdc7kyllockxxwvvzej Value OP_0 3044022051d2942683f83e6d9a867ba260f8c01765070a5e4451f6c6e0f9b8cfc0f60bdf02202dc6aa7c7abc00683691fce8a6e96 3044022051d2942683f83e6d9a867ba260f8c01765070a5e4451f6c6e0f9b8cfc0f60bdf02202dc6aa7c7abc00683691fce8a6e96 3044022051d2942683f83e6d9a867ba260f8c01765070a5e4451f6c6e0f9b8cfc0f60bdf02202dc6aa7c7abc00683691fce8a6e96 3044022051d2942683f83e6d9a867ba260f8c01765070a5e4451f6c6e0f9b8cfc0f60bdf02202dc6aa7c7abc00683691fce8a6e96 3044022051d2942683f83e6d9a867ba260f8c01765070a5e4451f6c6e0f9b8cfc0f60bdf02202dc6aa7c7abc00683691fce8a6e96 3044022051d2942683f83e6d9a867ba260f8c01765070a5e4451f6c6e0f9b8cfc0f60bdf02202dc6aa7c7abc00683691fce8a6e96 30440220513f620f8c01765070a5e4451f6c6e0f9b8cfc0f60bdf02202dc6aa7c7abc00683691fce8a6e96 304402206187f8cc2f3f0ef3b6c7f78aa2f114b3324af055cc0e75a40fa9ff90d75e329b02200da5f2be9829771922f491283f974338 38f62f96ec01 52210375e00eb72e29da82b89367947f29ef34afb75e8654f6ea368e0acdfd92976b7c2103a1b26313f430c4b15bb1fdce663207 38f62f96ec01



actors.²⁰ Obviously, given the nature of the inquiry, data regarding the prevalence of illicit use of all crypto coins are limited. Still, it seems reasonable to say that not all cryptocurrency transactions involve illegal purposes. Thus, a sweeping remedial tax encompassing all cryptocurrency transactions seems excessive. There are two main categories of legitimate uses of cryptocurrencies. The first group includes those who use cryptocurrencies to escape the repercussions of particular actions amid authoritarian regimes and minorities who want financial secrecy to avoid prejudice or peer pressure. For example, some individuals living under a repressive regime may want to purchase virtual private networks to gain uncensored access to the internet; in doing so, they must avoid leaving a trail of financial information that could lead to their arrest or even imprisonment.

For these individuals — those who use cryptocurrencies to preserve financial privacy —

²⁰See Foley, Karlsen, and Putniņš, supra note 12. But see Chainalysis, "The 2020 State of Crypto Crime" (Jan. 2020). Chainalysis released a report in January estimating that only about 1.1 percent of cryptocurrency transactions are for illicit purposes. However, in our opinion, the report does not adequately explain why its limited sample of a few known bad actors is representative of or proportional to the cryptocurrency ecosystem at large.

the remedial tax can be viewed as a premium. From an enforcement point of view, it would be difficult to distinguish illicit uses of cryptocurrency's privacy features from legitimate ones without destroying the desired anonymity. Because anonymity is a function that fiat currency does not provide, paying a premium for financial privacy makes sense from a consumer's point of view.

A second group of legal uses of cryptocurrencies includes many large-volume transactions undertaken for speculative purposes.²¹ Opportunistic investors often hold cryptocurrencies as investment assets. For these individuals and investment companies, financial privacy is not a key factor. Rather, they hope to generate sizeable returns, and the fact that they are investing in cryptocurrency is usually not a secret.

It seems unfair to apply the remedial tax to these investors. This problem, however, could be remedied by offering refunds or tax credits to investors who are not looking for financial privacy. They could either seek refunds directly from the administering body or claim tax credits from their local tax authorities. For investors, the tradeoff is that they must disclose financial information to gain tax benefits. Unfortunately, refunds are hard to oversee and prone to fraud.

Alternatively, an exemption can apply to all transactions for which the taxpayer can show a local sales tax or VAT has been imposed and paid. All transactions would be assessed the remedial tax, but the transactions would not be specifically identified. If an individual did not want to claim an exemption for local taxes, then, by default, the user would pay the remedial tax on all transactions whether legal or illicit. The individual's identity and activity would remain relatively private but, by paying the remedial tax, the user would contribute significantly to global relief activities. Compliant cryptocurrencies could imbed the remedial tax directly into their protocols as a condition of using the product, and the systems would automatically add the tax to each transaction. The administering body would be responsible for certifying that the modification

²¹See Foley, Karlsen, and Putniņš, supra note 12.

worked, but the cryptocurrency companies would withhold tax on its behalf. In effect, the remedial tax would be a cost of conducting business using cryptocurrencies.

This proposal necessarily requires jurisdictions to cede taxing authority over cryptocurrencies to a supranational authority. The concession would be conditional. If the national tax authority were able to impose a tax on cryptocurrency transactions conducted by its resident nationals, the remedial tax would be extinguished and the funds returned to the cryptocurrency provider and, eventually, the users. In this respect, the remedial tax would facilitate domestic compliance in one of the most difficult enforcement areas.

Monero: A Game Changer?

A Cryptocurrency Designed for Privacy

Although the chance that a crypto criminal will actually be caught is slim, the mere possibility is enough to cause some sleepless nights. Because there is a market for crypto coin that is even more private, those with the technical know-how (and a desire to make money) invented Monero.

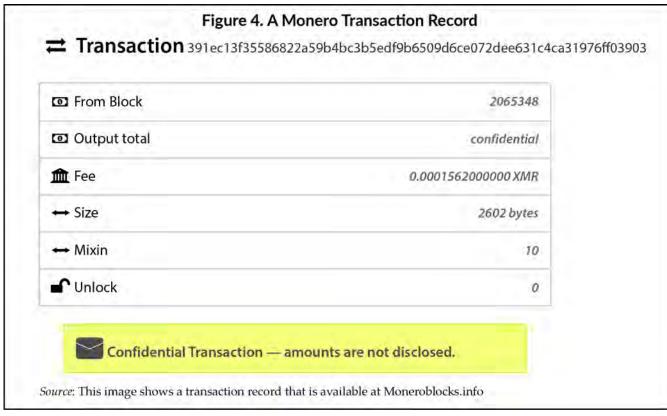
Developed in 2014, Monero uses three techniques to promote financial secrecy. The first involves stealth addresses — Monero generates new addresses for every transaction.²² Address reusage is a major privacy flaw in bitcoin because it enables law enforcement or another party to track the various incoming and outgoing transactions from a single address.²³ To solve this problem, Monero obscures destination addresses in its blockchain.

Monero's second privacy technique, ring signature, mixes the identity of the actual signer of a transaction with that of other possible signers.²⁴ These possible signers — essentially, decoys — are selected from past transaction outputs on Monero's blockchain to form a distinctive ring signature that makes it

²² See The Monero Project, "Stealth Addresses: The Basics," Moneropedia (last accessed Mar. 31, 2020).

²³ See Chainalysis Team, supra note 6 (address reusage made it possible for Chainalysis to conduct a forensic analysis of a drug dealer's bitcoin transactions).

²⁴ See The Monero Project, "The Basics of Ring Signature," Moneropedia (last accessed Mar. 31, 2020).



exponentially more difficult, if not impossible, for an observer to trace the transaction back to the actual signer.²⁵

The third technique – ring confidential transactions or RingCT – hides the amount transferred in a Monero transaction so that it does not appear on its blockchain.²⁶ Monero achieves this by using a Pedersen commitment, a tool that uses randomly generated variables to obscure the actual amount of funds transferred.²⁷ This scheme allows the user to keep a piece of data - such as the actual amount transferred - secret, but commit to it so that the user cannot later change his mind. In other words, even if the commitment value is public, no one knows the actual amount transferred. Meanwhile, the commitment scheme keeps the transacting parties honest, allowing the Monero protocol to ensure the integrity of its blockchain's bookkeeping.

Monero's first two privacy features can coexist with the remedial tax because they merely add more layers of protection to ensure its users' financial privacy. However, Monero's third privacy feature cannot — it is specifically designed to obfuscate the amount of funds transferred, making it impossible to gauge the value of goods exchanged. Figure 4 illustrates what a Monero transaction looks like on its blockchain.

The transaction amount is concealed because of Monero's RingCT technology. Unless there is another means by which to gauge the transaction amounts, Monero presents an existential threat to the feasibility of the remedial tax.

Reconciling the Remedial Tax With Monero

Because of Monero's special features, cryptocurrency users would be drawn to Monero to gain privacy and avoid the remedial tax, thereby significantly shrinking the revenue pool. To reconcile Monero with the remedial tax, the administering body would need to negotiate with Monero's core development team and ask them to change the protocol and reveal transaction amounts. If these negotiations stalemate, the

²⁵See id. See also Bisade Asolo, "Monero Ring Signature Explained," Mycryptopedia, Nov. 1, 2018.

²⁶ See Asolo, "Monero Ring Confidential Transactions (RingCT)," Mycryptopedia, Nov. 1, 2018.

^{2'} See Shen Noether, Adam Mackenzie, and Monero Core Team, "Ring Confidential Transactions," Monero Research Lab (Feb. 2016).

administering body may consider banning financial institutions from dealing with Monero altogether. Because cryptocurrencies are merely computer codes with no intrinsic value except for the value that is widely accepted by others, Monero would become worthless if it cannot be exchanged for fiat currency.

Ideally, a compromise would be reached that would allow Monero to continue its use of stealth addresses and ring signatures. It would, however, need to make a concession and reveal transaction amounts or at least propose an alternative plan that would allow the transactions to be subject to the remedial tax.

Conclusion

The remedial tax is a compromise. It recognizes and respects an individual's legitimate financial privacy interest, but it also recognizes that financial anonymity will inevitably attract criminals. Legal and illegal uses of cryptocurrency are (and would remain) indistinguishable. While not perfect, the remedial tax offers a workable solution. It would assess a global tax on all cryptocurrency transactions with the proceeds kept in reserve for global emergencies, and it would accomplish this in a manner that respects legitimate local taxing interests. Ultimately, the remedial tax would only be imposed on transactions that, for whatever reason, a resident jurisdiction is unable to tax. Jurisdictions would conditionally cede the authority to impose the proposed remedial tax proposed to the U.N. or another supranational agency to achieve a level of justice not reachable today.

taxnotes



Need nexus info? Get Nexus Tracker.

Check out our state nexus tool featuring an interactive map and state-by-state comparison table, included with all *Tax Notes State* and *Tax Notes Today State* subscriptions.

taxnotes.com/nexus-tracker

Tax Notes gives you the inside track.

TAX NOTES INTERNATIONAL, MAY 25, 2020