Electronic Cash, Decentralized Exchange, and the Constitution

Peter Van Valkenburgh

March 2019

Coin Center Report

FIAT IVSTITIA.

COIN CENTER
coincenter.org

Peter Van Valkenburgh, *Electronic Cash, Decentralized Exchange, and the Constitution*, Coin Center Report, Mar. 2019, available at https://coincenter.org/entry/e-cash-dex-constitution

Abstract

Regulators, law enforcement, and the general public have come to expect that cryptocurrency transactions will leave a public record on a blockchain, and that most cryptocurrency exchanges will take place using centralized businesses that are regulated and surveilled through the Bank Secrecy Act. The emergence of electronic cash and decentralized exchange software challenges these expectations. Transactions need not leave any public record and exchanges can be accomplished peer to peer without using a regulated third party in between. Faced with diminished visibility into cryptocurrency transactions, policymakers may propose new approaches to financial surveillance. Regulating cryptocurrency software developers and individual users of that software under the Bank Secrecy Act would be unconstitutional under the Fourth Amendment because it would be a warrantless search and seizure of information private to cryptocurrency users. Furthermore, any law or regulation attempting to ban, require licensing for, or compel the altered publication (*e.g.* backdoors) of cryptocurrency software would be unconstitutional under First Amendment protections for speech.

Author

Peter Van Valkenburgh
Coin Center
peter@coincenter.org

About Coin Center

Coin Center is a non-profit research and advocacy center focused on the public policy issues facing open blockchain technologies such as Bitcoin. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using blockchain technologies. We do this by producing and publishing policy research from respected academics and experts, educating policymakers and the media about blockchain technology, and by engaging in advocacy for sound public policy.

Acknowledgements

Thank you to Andrea Castillo who provided invaluable research assistance, and to my Coin Center colleagues Neeraj Agrawal, James Foust, Robin Weisman, Alex Strernhell, and Jerry Brito for indispensable discussions and comments on early drafts of this paper. Sincere thanks to those who provided comments on a draft of this paper, including Brandon G. Goodell, Jason Somensatto (0x Project), Alexander Zaidelson (Beam), Elena Nadolinski (Beanstalk), Ron Bernstein (Coinbase), Rainey Reitman & Jamie Lee Williams (Electronic Frontier Foundation), Silke Elrifai (Gnosis), Daniel Lehnberg (Grin), Alex Gladstein (Human Rights Foundation), Steven Waterhouse (Orchid Labs), Marvin Ammori (Protocol Labs), Alan Curtis (Radar), Zooko Wilcox (Zcash), and Josh Cincinnati (Zcash Foundation). Special thanks to Shane Glynn, Joshua Goldbard, and Nathana Sharma (MobileCoin) for helping organize a workshop for this paper.

Table of Contents

I. Introduction and Executive Summary

Cryptocurrencies have been around now for just over a decade.[1] Users and regulators have come to understand that they are far less anonymous than originally perceived.[2] This has been a boon to law enforcement,[3] but it has also dramatically curtailed the legitimate privacy interests of law-abiding persons who wish to use cryptocurrencies or related open blockchain technology.[4] The present-day lack of cryptocurrency privacy is not, however, likely to last much longer.

Proposals to alter the software libraries powering existing cryptocurrencies[5] as well as a range of next-generation cryptocurrencies[6] promise to provide users with much greater transactional privacy while still enabling public certainty over the integrity of these systems. In essence, these systems can hide, or not record at all, the salient details of any particular transaction while still assuring users and the public generally that, across all transactions, there is no counterfeiting and transactions can only be authorized by persons who have previously received coins.[7] In practice, using these cryptocurrencies is like using cash, *i.e.* tangible currency. In both cases, two people can pay each other without the need to trust an intermediary, and no information about these two people or the transaction they've just made need be released to the public or shared with any third party. These new cryptocurrencies truly offer users *electronic cash*. For clarity we will refer to these new technologies as *electronic cash* and to transactions made using them as *electronic cash transactions*.[8]

[1] The "Genesis block" of the first cryptocurrency, Bitcoin, was broadcast on January 3, 2009. *See*: Block 0. Main chain. 2009-01-03. Hash 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f, https://blockexplorer.com/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f.

[2] Adam Ludwin, "How Anonymous is Bitcoin?" *Coin Center* (Jan. 20, 2015) https://coincenter.org/entry/how-anonymous-is-bitcoin.

[3] Joon Ian Wong, "The woman who led crypto policing in the US guesses what's next for regulation," *Quartz* (Apr. 12, 2018), https://qz.com/1236501/the-woman-who-once-policed-the-crypto-world-for-the-us-government-says-a-crackdown-is-coming/.

[4] As Praveen Jayachandran of IBM notes: "Another disadvantage is the openness of public blockchain, which implies little to no privacy for transactions and only supports a weak notion of security. Both of these are important considerations for enterprise use cases of blockchain." *See*: Praveen Jayachandran, "The difference between public and private blockchain," *Blockchain Pulse: IBM Blockchain Blog* (May 31, 2017) https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain.

[5] *See*, *e.g.*: Greg Maxwell, "Confidential Transactions" https://people.xiph.org/~greg/confidential_values.txt.

[6] Some noteworthy examples of privacy-focused cryptocurrency projects are Monero, Zcash, Grin, and Beam.

[7] *See* Appendix: Integrity and Privacy: The Quarrelsome Core Design Goals of Cryptocurrencies pp. 55-8

[8] Jerry Brito, "The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society," *Coin Center* (Feb. 2019) https://coincenter.org/entry/the-case-for-electronic-cash.

Similarly, regulators have come to expect that any exchange from one cryptocurrency to another will—by necessity—occur through trusted third parties, informally called cryptocurrency exchanges, which hold cryptocurrency for their users and match buyers and sellers of several currency pairs.[9] As entities that accept and transmit currency substitutes[10] for their users, these exchanges are regulated as "financial institutions" for purposes of the Bank Secrecy Act,[11] and regulators have access to customer information from these exchanges.[12] While this is unlikely to change with regard to exchanges between sovereign currencies and cryptocurrencies (due to the need for a trusted legal entity to maintain banking relationships in order to deal in sovereign currencies), it will soon no longer be the case for exchanges between cryptocurrencies and any other assets that are similarly blockchain-based.

Blockchain-based assets can be exchanged peer to peer without trusted intermediaries, with little friction, and with minimized counterparty risk thanks to the advent of blockchain-based smart contracts.[13] Such smart-contract software can even facilitate the automatic creation of order books, the automatic matching of willing buyers and sellers on those books, and the

[9] Coinbase and Kraken are two examples of prominent cryptocurrency exchanges.

[10] The Financial Crimes Enforcement Network (FinCEN) of the Treasury Department has established that "any exchanger that uses its access to the convertible virtual currency services provided by the administrator to accept and transmit the convertible virtual currency on behalf of others, including transfers intended to pay a third party for virtual goods and services" is a money transmitter, and subject to all according regulations. *See*: US Department of the Treasury, Financial Crimes Enforcement Network, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," Guidance FIN-2013-G001 (Mar. 18, 2013) https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

[11] *Id.*

[12] Exchanges may be required to divulge customer information through several regulatory avenues. For example, the Bank Secrecy Act requires financial institutions to file "Suspicious Activity Reports" (SARs) on acts of suspected money laundering or fraud with FinCEN. In July of 2014, FinCEN's SAR statistics report started to include cryptocurrency transactions. The popular exchange service Coinbase was also compelled to divulge personal data for 13,000 customers without warrants and based merely on the volume of their transactions. *See*: "SAR Stats: Technical Bulletin," Financial Crimes Enforcement Network (Jul. 2014) https://www.fincen.gov/news_room/rp/files/SAR01/SAR_Stats_proof_2.pdf; The IRS has compelled the popular cryptocurrency exchange Coinbase to divulge data on certain high-volume customers. *See*: *U.S. v. Coinbase,* Case No.17-cv-01431-JSC (N.D. Cal. Nov. 28, 2017) https://casetext.com/case/united-states-v-coinbase-inc.

[13] Several cryptocurrency projects are developed as platforms for smart contracts. As I wrote in a comment to the CFTC: "All cryptocurrencies are programmable money. The primary impetus for developing Ether and the Ethereum Network was to make a new cryptocurrency that would be more easily programmable and capable of executing transactions of arbitrary complexity (*i.e.* if you can imagine it in logic, then you can code it as an ethereum transaction and the blockchain will execute it). These complex transactions are often referred to as smart contracts because they may involve similar logic to traditional legal contracts: if one party performs, the other is paid the negotiated price. However, this terminology can be confusing given that a smart contract may not necessarily be a legally binding contract (depending on the circumstances) and given that several poorly written smart contracts, whose bugs or aberrant behavior have earned them some infamy, hardly warrant the adjective 'smart.'" *See*: Peter Van Valkenburgh, "Comments to the Commodity Futures Trading Commission in Response to the Request for Input on Crypto-asset Mechanics and Markets," *Coin Center* (Feb. 11, 2019) https://coincenter.org/files/cftc-ether-rfi-coin-center.pdf.

settlement of trades without a third-party escrow provider.[14] This allows for so-called *decentralized exchange*. During decentralized exchange, users retain custody of their cryptocurrency (rather than keep it with a trusted third party) and use smart contracts to trade them peer to peer. In essence, all the functions of a trusted third-party exchange can now be accomplished directly by the trading partners via software-based smart contracts and public blockchains capable of executing the logic of those smart contracts.[15]

The cumulative effect of these advances in technology is significantly less visibility into cryptocurrency transactions for the public, regulators, and law enforcement. Thanks to electronic cash transactions, data that would otherwise be available on a public blockchain may now be private to the transacting parties, and, thanks to decentralized exchange, many users seeking to exchange their cryptocurrencies for other cryptocurrencies may do so directly with each other rather than through a regulated third party, which could collect customer information.

Again, neither electronic cash nor decentralized exchange require trusted intermediaries of any kind. At the heart of these innovations lie only two types of parties:

1. Users who employ software tools and public blockchain networks to transact and exchange; and,
2. Software developers who research, author, publish, and distribute source code that can be employed by the users to transact and exchange.

Users are, of course, culpable for their own illegal acts. However, aside from self-reporting their tax liabilities,[16] they are not regulated and forced to collect and report to law enforcement information about their own lawful behavior or the lawful behavior of their commercial counterparties.[17]

Software developers are not culpable for unlawful acts committed by others using their research if they are unaware of those acts and lacked any intent to facilitate crimes.[18] Indeed,

[14] Will Warren, “What is a decentralized exchange?” *Coin Center* (Oct. 10, 2018) https://coincenter.org/entry/what-is-a-decentralized-exchange.

[15] *See infra* II. B. Decentralized Exchange Means No Trusted Third Party, pp. 12-15.

[16] Internal Revenue Service, “Virtual Currencies,” Notice 2014-21 (2014) https://www.irs.gov/pub/irs-drop/n-14-21.pdf.

[17] The BSA applies only to financial institutions, not to individuals. BSA implementing regs 31 USC § 5312(a)(2)(Y).

[18] For instance, the CFTC must assiduously demonstrate a defendant’s intention to commit some violation, like “spoofing” algorithmic trading, as explained by Commissioner Rostin Behnam. Commissioner Brian Quintenz has clarified that publishing software alone is not grounds for CFTC enforcement; rather, the agency should limit itself to “instances where developers knowingly design code that can be used for unlawful purposes, and intend that code by used for such purposes.” *See*: Rostin Behnam, “Delivering a Message on Relationship Patterns,” Remarks before Energy Risk USA in Houston, TX (May 15, 2018) https://www.cftc.gov/PressRoom/SpeechesTestimony/opabehnam6; Brian Quintenz, “How the CFTC can take a pro-innovation posture while maintaining orderly markets,” *Coin Center* (Feb. 12, 2019)

software developers, to the extent they limit their activities to the publication of source code, are engaged in a protected speech act that cannot be regulated unless the government can prove a compelling state interest that could not be achieved through any less restrictive policy.[19]

Neither users nor developers are "financial institutions" as defined in the Bank Secrecy Act (BSA)—a financial surveillance statute the mandates recordkeeping and reporting in the U.S.[20] The Secretary of Treasury can, through rulemaking, define a new category of financial institution that includes either users or developers.[21] However, such a rulemaking would likely be unconstitutional under the Fourth Amendment of the U.S. Constitution.[22]

The Fourth Amendment prohibits warrantless search and seizure of information over which persons have a reasonable expectation of privacy.[23] Existing BSA recordkeeping and reporting requirements are constitutional despite collecting large amounts of information without warrants because bank customers are said to lose their reasonable expectation of privacy when they voluntarily hand this information over to a third party in furtherance of a legitimate business purpose of that third party.[24] If users do not voluntarily hand this information to a third party because no third party is necessary to accomplish their transactions or exchanges,

https://coincenter.org/entry/how-the-cftc-can-take-a-pro-innovation-posture-while-maintaining-orderly-markets.

[19] *See infra* IV. Electronic Cash, Decentralized Exchange, and the First Amendment, pp. 32-52.

[20] As defined in the BSA 31 U.S.C. 5312(a)(2), a "financial institution" includes: an insured bank; a commercial bank or trust company; a private banker; an agency or branch of a foreign bank in the United States; a credit union; a thrift institution; an SEC-registered broker or dealer; a securities or commodities broker or dealer; an investment banker or company; a currency exchange; an issuer, redeemer, or cashier of travelers' checks, checks, money orders, or similar instruments; a credit card system operator; an insurance company, a dealer in precious metals, stones, or jewels; a pawnbroker; a loan or finance company; a travel agency; a licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system; a telegraph company; a business engaged in vehicle sales (automobiles, airplanes, and boats); persons involved in real estate closings and settlements; the United States Postal Service; An agency of the United States Government or of a State or local government carrying out a duty or power of a business described in this paragraph; and a casino or gaming establishment with an annual gaming revenue of more than $1,000,000. Additionally, FinCEN can consider any entity as a financial institution if it engages in activities similar enough to those undertaken by the entities above. *See*: Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114-4 (1970) (codified as amended in scattered sections of 12 U.S.C., 18 U.S.C., and 31 U.S.C.). Regulations for the Bank Secrecy Act and other related statutes are 31 C.F.R. §§ 103.11-103.77.

[21]"any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage; or any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters." *See*: 31 C.F.R. Section 5312(a)(2)(Y).

[22] *See infra* III. Electronic Cash, Decentralized Exchange, and the Fourth Amendment, pp. 17-31.

[23] U. S. Const. Amend. IV.

[24] *California Bankers Assn. v. Shultz*, 416 U.S. 21 (1974) https://supreme.justia.com/cases/federal/us/416/21/; *United States v. Miller*, 425 U.S. 435 (1976) https://supreme.justia.com/cases/federal/us/425/435/.

then they logically retain a reasonable expectation of privacy over their personal records and a warrant would be required for law enforcement to obtain those records. Users cannot be forced to record and report their lawful activities without violating the 4th Amendment's warrant requirement.[25]

Similarly, financial institutions can be forced to record and retain customer data because their customers willingly hand that data over to them and because that data are essential to their conduct of legitimate business purposes.[26] Developers of electronic cash and decentralized exchange software have no legitimate business purpose for collecting that data and users do not volunteer that information to developers when they use their software tools. Indeed, a software developer will likely be even less aware of who is using their tools than the author of a book would know who has bought a copy and read it. Deputizing software developers to collect this information as a prerequisite to publishing their software tools would be unconstitutional under the Fourth Amendment because it would constitute a warrantless seizure of information over which users have a reasonable expectation of privacy.

Faced with both (a) a decline in readily surveillable data on public blockchains and from BSA-regulated exchanges, and (b) the inability to constitutionally deputize new entities as BSA-obligated surveilors, regulators may seek to outlaw the publication of electronic cash or decentralized exchange source code, or permission its publication on inclusion of backdoors that surreptitiously collect and report information to the government. Source code, the language by which developers communicate scientific and engineering ideas to each other and the world, is protected speech as described in the First Amendment.[27] The government cannot ban the publication of types of speech nor can it require a person to speak unless it can prove a compelling state interest that could not be achieved through any less restrictive policy.[28] Indeed, laws that require content-based licensing of speech carry a strong presumption of unconstitutionality that must be rebutted by the government when challenged in court.[29] Any attempt to ban the publication of electronic cash and decentralized exchange source code, or any attempt to compel developers to rewrite their source code according to government strictures, would thus likely be found unconstitutional under the First Amendment.

In general, the emergence of electronic cash and decentralized exchange software challenges several assumptions of what is and is not regulated under existing law, and what can and cannot be regulated constitutionally even if Congress decided to create new law. This report is not aspirational or hypothetical. It does not advocate for new constitutional jurisprudence (*e.g.* the weakening of the third-party doctrine, or heightened scrutiny for compelled commercial speech). Rather, this report explains how new technologies fit or do not fit into uncontroversial statutory interpretations and existing, well-settled constitutional jurisprudence. The resulting analysis may be surprising to some who, for policy reasons, wish for greater regulatory

[25] *See infra* III. Electronic Cash, Decentralized Exchange, and the Fourth Amendment, pp. 17-31.
[26] *Id.*
[27] *See infra* IV. Electronic Cash, Decentralized Exchange, and the First Amendment, pp. 32-52.
[28] *See infra* note 235.
[29] *See infra* note 240.

authority over activities performed using this software, or others who are concerned about the effect that the emergence of electronic cash and decentralized exchange could have on law enforcement's ability to find and apprehend criminals. Indeed the results may be especially surprising to those who harbored the incorrect belief that these technologies are no different than previous tools and therefore do not pose novel legal questions.

We will begin with a description of the technology behind electronic cash and decentralized exchange. Later, we will review the relevant constitutional law and analyze the constitutionality of certain hypothetical attempts to impose financial surveillance obligations onto software developers and users.

II. Technology Background

Rather than offer a comprehensive survey of the technology behind electronic cash or decentralized exchange, this section will be limited to a description of the aspects of the technology that are relevant to our discussion of constitutional law. At root, three aspects of these technologies are relevant to that discussion:

1. Unlike early transactions made with cryptocurrencies, electronic cash transactions can be completely private to the transacting parties and may leave no useful public record of the transaction on the blockchain.
2. Unlike a transaction made through a centralized cryptocurrency exchange, a decentralized exchange may be strictly peer-to-peer and may have no legal or business entity that powers the exchange service.
3. Both electronic cash and decentralized exchange originate from published software written in different computer languages. When that software is executed by diverse and unaffiliated persons around the world it can facilitate an electronic cash transaction or decentralized exchange between participants. However the development of that software is a separate activity (authorship) from the execution of that software (use) and the parties involved, authors and users, are distinct.

For more comprehensive information on these technologies we have added an Appendix to this report. The Appendix will be useful for readers who do not yet have a base of knowledge in cryptocurrencies and who wish to learn more about electronic cash and decentralized exchange, specifically: what they do, how they function, who builds them, and what that building process entails.

A. Electronic Cash Means Completely Private, Cash-Like Transactions

A typical bitcoin transaction leaves a plaintext[30] record on the Bitcoin blockchain that includes:

1. The bitcoin address or addresses the sender is using to fund the transaction,

[30] Plaintext is ordinary, machine-readable text that is not encrypted, formatted, tagged, or written in code.

2. The recipient’s bitcoin address or addresses,
3. The amount sent, and
4. A digital signature that proves the sender’s control over the sending addresses.

Anyone with a computer and an internet connection can freely download a copy of the blockchain and view the entirety of this transactional data for every bitcoin transaction that has ever been made since the network’s inception in 2009.[31] Public websites provide free tools for exploring this massive data set,[32] and specialty blockchain analysis companies provide even more user-friendly solutions for visualizing this data and linking these addresses and their transactional history with real world identities and organizations.[33] In short, despite several incorrect headlines and reports,[34] bitcoin transactions are not at all anonymous; They are, in fact, far less private than transactions made using a bank or credit card. As former DOJ prosecutor and Silkroad investigator Katie Haun has remarked, “If you wanted to cover your tracks and you were a good criminal, Bitcoin or cryptocurrency is one of the last things you should use.”[35] It’s also the last thing you should use if you are a law abiding person who does not want the world at large to see and potentially scrutinize your entire financial history.

As we describe in depth in the Appendix, this level of publicity about transactions exists in part to allow the entire network of cryptocurrency users to independently verify that transactions are valid.[36] As Bitcoin was originally designed, verifying the integrity of the blockchain necessitated public visibility into the details of every transaction.[37]

[31] To download the blockchain directly from the peer-to-peer Bitcoin network, one must install the Bitcoin Core software on an internet-connected computer and allow the software to sync with the larger network. *See*: The Bitcoin Core GitHub repository (https://github.com/bitcoin/bitcoin).

[32] *See, e.g.*: blockchain.info.

[33] Thomas Brewster, “Why Investors Are Betting Millions On Bitcoin Surveillance,” *Forbes* (Apr. 15, 2018) https://www.forbes.com/sites/thomasbrewster/2018/04/05/snooping-on-bitcoin-is-big-business/#4191a5072d19.

[34] *See, for example*: Matthew O’Brien, “Bitcoin Is No Longer a Currency,” *The Atlantic* (Apr. 11, 2013) https://www.theatlantic.com/business/archive/2013/04/bitcoin-is-no-longer-a-currency/274859/ (“The idea is to create money that central banks can't debase and governments can't tax. In other words, digital gold. Actually, make that *anonymous* digital gold.”); James J. Angel, “Don’t get bitten by Bitcoins,” *CNN* (Apr. 12, 2013) https://www.cnn.com/2013/04/11/opinion/angel-bitcoin-currency/index.html (“The near anonymity built into the Bitcoin system keeps funds away from the prying eyes of tax collectors, who are getting ever better at shutting down tax havens. This potential for anonymity makes the currency ideal for drug smugglers, terrorists and money launderers, as well as the merely paranoid.”); Quentin Fottrell, “To secure your bitcoins, print them out,” *MarketWatch* (Feb. 26, 2014) https://www.marketwatch.com/story/to-secure-your-bitcoins-print-them-out-2014-02-26 (“Bitcoin was created to provide an anonymous, digital currency free from government control or physical existence.”).

[35] Katie Haun, “3 Common Myths People Have About Crypto,” *a16z YouTube channel* (Nov. 2, 2018) https://www.youtube.com/watch?v=JDD9TsgUNPY.

[36] By valid we mean that the transaction is not an attempt to send coins one has not received previously or to counterfeit new coins outside the established rules for coin creation.

[37] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” (Oct. 31, 2008) https://bitcoin.org/bitcoin.pdf (“The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method.”).

Since Bitcoin's inception in 2009, several technical proposals have emerged that would improve privacy for Bitcoin users without sacrificing public verification of the blockchain.[38] Some of these proposals involve changes to wallet software that people would use to access the Bitcoin network and store their bitcoins,[39] others involve new networking protocols built on top of the Bitcoin network that could shuffle bitcoins amongst several addresses and transactions,[40] and some involve fundamental changes to the core Bitcoin protocol software itself.[41] Several of these proposals have been developed and allow Bitcoin users greater privacy than would be found in typical transactions. While the Bitcoin developer community has yet to incorporate any of the proposals that would necessitate comprehensive changes into the Bitcoin Core software itself, several of these proposals have been developed and launched as separate, standalone cryptocurrencies and associated networks.[42]

The details of this technological evolution are described in the Appendix. For our purposes, however, it is sufficient to know that this work is ongoing and that it allows for peer-to-peer cryptocurrency transactions that leave no plaintext record of sender or recipient addresses and no plaintext record of the amount sent on the blockchain. This information, if it is available to anyone at all, is kept private to the transacting parties who, in some of these systems, may also be able to share it with others (effectively decrypting otherwise unreadable information on the

[38] *See, e.g.*: Ian Miers, et. al, "Zerocoin: Anonymous Distributed E-Cash from Bitcoin," *IEEE Symposium on Security and Privacy* (2013) http://zerocoin.org/media/pdf/ZerocoinOakland.pdf; Tom Elvis Jedusor, "MIMBLEWIMBLE" (Jul. 16, 2016) https://scalingbitcoin.org/papers/mimblewimble.txt.

[39] *See, e.g.*: Wasabi Wallet (https://wasabiwallet.io/) and Dark Wallet (https://www.darkwallet.is/).

[40] *See, for example*: Felix Konstantin Maurer, Till Neudecker, and Martin Florin, "Anonymous CoinJoin Transactions with Arbitrary Values," *IEEE Trustcom/BigDataSE/ICESS* (2017) https://www.comsys.rwth-aachen.de/fileadmin/papers/2017/2017-maurer-trustcom-coinjoin.pdf; Ethan Heilman, et al., "TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub," *NDSS Symposium* (2017) https://eprint.iacr.org/2016/575.pdf.

[41] *See supra* note 31.

[42] For example, the ZeroCoin proposal has been developed into the Zcash cryptocurrency. *See*: Eli Ben-Sasson, et. al, "Zerocash: Decentralized Anonymous Payments from Bitcoin," *IEEE Symposium on Security and Privacy* (2014) http://zerocash-project.org/media/pdf/zerocash-oakland2014.pdf. The cryptocurrency Monero is a version of bitcoin with coinjoin and other privacy enhancements added to the core software. *See:* Kurt M. Alonso and KOE "Zero to Monero: A Technical Guide to a Private Digital Currency; For Beginners, Amateurs, and Experts (v1.0.0)" (Jun. 26, 2018) https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf. The Mimblewimble proposal is actively being developed into at least two cryptocurrencies, Grin and Beam. *See*: Aaron van Wirdum, "What We know About Grin and Beam's Mimblewimble," Bitcoin Magazine (Oct.1, 2018) https://bitcoinmagazine.com/articles/battle-privacycoins-what-we-know-about-grin-and-beams-mimblewimble/. *For a general discussion of how new cryptocurrency projects fork off from older ones, see*: Peter Van Valkenburgh, "What are Forks, Alt-coins, Meta-coins, and Sidechains?" *Coin Center* (Dec. 8, 2015) https://coincenter.org/entry/what-are-forks-alt-coins-meta-coins-and-sidechains. *For a visualization of how different projects have forked from Bitcoin and other cryptocurrencies, see:* Map of Coins (https://mapofcoins.com/).

blockchain) using so-called view keys.[43] This functionality is generally referred to as selective disclosure.[44]

Despite this lack of transaction publicity, mathematical proofs built into these software projects allow the public at large to verify the integrity of the blockchain without learning the details of any specific transactions.[45] Trust in the scarcity of the underlying coins and the provenance of transactions is generated by an open set of impartial validators around the world just like Bitcoin's miners.[46] Unlike Bitcoin, however, privacy is guaranteed in these protocols by neglecting to share any information about transactions with these validators or the public at large except for the minimized amount of information necessary to prove scarcity and provenance. Additionally, selective disclosure systems ensure that counterparties and third parties can be given visibility into the details of any particular transaction whenever the initiator (and the initiator alone) wishes to be transparent or is compelled to be transparent by regulation or law.

There's no widely accepted term for these software projects or the private transactions that they can enable. For clarity we will refer to this category of software as "electronic cash software" and this category of transactions as "electronic cash transactions." Like cash, these new tools allow payments to be made directly, person to person, without leaving any authoritative record of the parties involved or how much money changed hands.[47]

B. Decentralized Exchange Means No Trusted Third Party

One can only make electronic cash transactions if one has obtained the underlying cryptocurrency of that blockchain (bitcoins if using Bitcoin with additional software to augment privacy, or some other cryptocurrency such as Zcash or Monero if using a new, privacy-focused blockchain). There are only two ways to obtain these cryptocurrencies: (1) participate in the blockchain consensus mechanism and receive rewards for your contributions in the form of newly minted cryptocurrency (*i.e.* mining),[48] or (2) receive cryptocurrency from someone who already has it, either as a gift, payment as wages, or in exchange for other valuables (*i.e.* exchange).

[43] For example, in Zcash, "every shielded address comes with what we call a view key that is generated for the holder of the address. She can choose to share this view key with anyone else in the world. With that view key a person can get the details about the particular transactions sent from that address; they can see the recipient addresses and the amounts sent. Not only can they see these details, they can prove them with the certainty of a blockchain data structure." *See*: Zooko Wilcox and Peter Van Valkenburgh, "What is Zcash?" *Coin Center* (Dec. 8, 2016) https://coincenter.org/entry/what-is-zcash.

[44] *Id*.

[45] *Id*.

[46] *Id*.

[47] Jerry Brito, "The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society," *Coin Center* (Feb. 2019) https://coincenter.org/entry/the-case-for-electronic-cash.

[48] Peter Van Valkenburgh, "Why is Bitcoin Mining, and Why is it Necessary?" *Coin Center* (Dec. 15, 2014) https://coincenter.org/entry/what-is-bitcoin-mining-and-why-is-it-necessary.

Historically, mining is not an activity well-suited to non-technical individuals and may even be cost-prohibitive for all but the most expert mining entrepreneurs when the relevant blockchain is secured by a highly competitive proof-of-work consensus mechanism (*e.g.* Bitcoin).[49]

Therefore, the vast majority of cryptocurrency users will obtain their coins through an exchange. It is, of course, possible to find and meet individuals—either in person or over the internet—who would willingly sell some of their cryptocurrency holdings in exchange for cash or various other forms of electronic value transfer. In this scenario, the seller would transfer the cryptocurrency directly to the buyer making a blockchain transaction to an address generated by a software wallet on the buyer's phone or other device. The buyer would pay the seller however is convenient. This approach, however, can carry risks. One party could take payment and fail to carry out the exchange, in-person meetings could result in robbery or other injury should one of the parties turn out to be criminal, and—even in the best circumstances—it may be difficult to find a counterparty with the amount and type of cryptocurrency one wishes to purchase.

Frictions associated with such direct exchange have resulted in the emergence of several so-called centralized cryptocurrency exchanges.[50] These are, speaking generally, legally incorporated businesses with websites and banking relationships for accepting payments. Through their websites, these businesses allow users to establish accounts, fund those accounts with sovereign currencies through ACH or similar transfers, and then may serve as either a broker for persons wishing to buy cryptocurrencies or a matcher of buyers and sellers on their platform.

These centralized exchanges will also secure cryptocurrencies on behalf of their customers. These are often referred to as *custodial wallets* as contrasted with user-secured *software wallets*. In the context of a software wallet, cryptocurrency is received and kept in blockchain addresses that have associated cryptographic keys generated and secured directly on the user's phone or computer. A custodial wallet will secure cryptocurrency in blockchain addresses whose matching cryptographic keys are safeguarded by the centralized exchange rather than by its customers.

As entities that accept and transmit currency substitutes[51] for their users, these centralized cryptocurrency exchanges are regulated as financial institutions under the Bank Secrecy Act in

[49] Aaron Hankin, "Here's how much it costs to mine a single bitcoin in your country," *MarketWatch* (May 11, 2018). https://www.marketwatch.com/story/heres-how-much-it-costs-to-mine-a-single-bitcoin-in-your-country-2018-03-06.

[50] There are many centralized exchanges. Some prominent examples are Coinbase, Gemini, Kraken, and Binance.

[51] *See supra* note 10.

the United States,[52] and regulators have access to customer information from these exchanges.[53]

Decentralized exchange is best understood as a verb rather than a noun. Our earlier description of a direct person-to-person exchange is a decentralized exchange in the sense that two parities somehow find each other and trade their valuables without relying on any trusted third party in between. Advances in cryptocurrency software, however, can streamline this process and mitigate the risks otherwise associated with meeting a stranger and trusting them to honor their side of a bargain. We describe this software briefly below, but first a caveat: these software-powered decentralized exchanges are only possible for cryptocurrency-to-cryptocurrency trades. To trade sovereign currencies will always require either (A) some trusted third party with banking relationships or (B) physical cash, which necessitates in-person dealing.

Decentralized exchange software falls under the general umbrella of so-called *smart contracts*.[54] For our purposes, a smart contract is simply a transaction made using cryptocurrency that has associated rules governing its execution, wherein these rules are enforced by the underlying blockchain itself rather than by some outside arbiter or legal entity. These rules could be as simple as: *using bitcoin at address x, pay one bitcoin to address Y, if and only if the 567,238th block has been added to the Bitcoin blockchain.* These rules would be expressed in computer code rather than English and would need to be in the particular coding language native to the blockchain on which the smart contract is meant to execute.[55] Bitcoin blocks come around every 10 minutes on average and, as of writing, the blockchain is 565,222 blocks long. Therefore this transaction message is, in effect, a one bitcoin check payable to address Y that is post-dated to about two weeks in the future. Unlike a post-dated check, however, where we would rely on a bank to only cash it if the date was current, this transaction does not rely on any third party to execute its rules. If the recipient has the signed transaction message, she can submit it to the Bitcoin network and miners will put it in the blockchain when it is current and *only* once it is current. Any miner attempting to put it in the blockchain before block 567,238 would have her block automatically rejected by the rest of the network because it would contain an invalid transaction according to the rules of Bitcoin's computing language. A contract-like conditional payment is made even though no third party is required to judge or enforce the condition; though it is simple, this is the essence of a smart contract.

Software for facilitating decentralized exchange is not much more advanced than this simple example. The computer code would simply describe a payment that is conditional on proof of some other payment being recorded on the blockchain. Various additional rules and conditions can be written as well, for example:

[52] *Id.*

[53] *See supra* note 17.

[54] *See supra* note 15.

[55] In our example we are using bitcoin, so that language is called Bitcoin Script.

- A rule to cancel the payment of either party (returning the cryptocurrency to the sending address), if and only if their counterparty fails to make their payment within a set time period,
- A set of rules that make the contract an open-ended offer from the buyer at a set price. Anyone who finds the buyer's signed transaction message (perhaps it's posted on social media) can become the buyer's seller if and only if they are the first to do so on the blockchain.

Some blockchain computing languages will even allow for rules that reference data on other blockchains such that payments on both chains are mutually codependent. This allows for so-called *cross-chain atomic trades* wherein a decentralized exchange could take place between users of two different blockchain networks (*e.g.* an exchange of bitcoin for ether).

Finally, decentralized exchange software can even be written that allows trading parties to store and access buy and sell offer information (*i.e.* an orderbook) in the blockchain or some other decentralized data store, and to utilize a matching engine whose logic is also executed by the blockchain so that trades happen automatically whenever signed offers to buy and sell overlap.

Some decentralized exchange software may rely on certain centralized parties to perform certain functions within the otherwise decentralized exchange. For example, centralized parties could be relied upon to store orderbook data or to actively match buyers and sellers. Then, once matched, the trade itself takes place directly and peer-to-peer using the smart contract. The cryptocurrency community will often call this arrangement a decentralized exchange even though there were certain centralized components, because the cryptocurrency always stayed in the custody of the participants and no third party ever had to be trusted to keep it safe. This quasi-centralization has also led to regulatory consequences for persons playing the centralized role within otherwise decentralized exchanges.[56] We do not argue in this paper that there are constitutional barriers to regulating these centralized parties (we also do not intend to suggest there are not). Instead, this paper focuses exclusively on the users of electronic cash and decentralized exchange software and the authors of that software.

C. Electronic Cash and Decentralized Exchange are Powered by Software

At heart, developing electronic cash or decentralized exchange software is an academic engineering challenge like any other. There's prior work from which to draw inspiration: decades of computer science research,[57] cryptographic literature,[58] and existing cryptocurrency

[56] *See, for example*: In the Matter of ZACHARY COBURN, Securities Exchange Act of 1934 Release No. 84,553, Fed. Sec. L. Rep. (AP) ¶ 18,888 (Nov. 8, 2018) https://www.sec.gov/litigation/admin/2018/34-84553.pdf.

[57] Arvind Narayanan and Jeremy Clark, "Bitcoin's Academic Pedigree," *Communications of the Association for Computing Machinery*, Vol. 60, No. 12 (Dec. 2017): pgs. 36-45, https://users.encs.concordia.ca/~clark/papers/2017_cacm.pdf.

software, which for all major networks is open-source and available without payment or licensing.[59] There's creative and innovative work to be done: forging new mathematical proofs, translating old ideas into new languages, and combining past work into novel and useful arrangements. As with any scientific inquiry, this process is ongoing and never-ending, and thousands of people around the world are actively contributing to the body of research.[60] Periodically there are published results, both academic papers written in prose that describe new software tools as well as the software itself, written in a range of common coding languages.

Those published results, on their own, do not create electronic cash or decentralized exchange. Instead, the published software explains—in exacting detail—how one would make an electronic cash transaction or a decentralized exchange. Software is not self-executing; it's a set of instructions, like a recipe for a meal or a musical score for a performance. Once published, it's up to people around the world to follow those instructions.[61] Software makes this a bit easier than performing a Beethoven sonata or baking a soufflé, because the instructions are so complete that they require little skill or improvisation and because their users can exploit a machine that can read the instructions, a computer, to do most of the work. But the users are essential nonetheless: they must run the software on their internet-connected computers, and it's only once those computers start working together as a network[62] that some usable functionality, like electronic cash or decentralized exchange, becomes possible.

The primary effect of these advances in technology are cryptocurrency networks that protect the privacy of their users. Developers and advocates genuinely believe that such tools are necessary to protect human dignity and autonomy, and argue that they are of profound political and societal importance in a world where transactions are increasingly surveilled and controlled by a handful of private financial intermediaries and powerful governments.[63] A secondary effect of these advances is significantly less visibility into cryptocurrency transactions for regulators and law enforcement. Thanks to electronic cash transactions, data that would otherwise be public on a blockchain may now be private to the transacting parties, and, thanks to decentralized exchange, many users seeking to exchange their cryptocurrencies

[58] *See, e.g.*: Leslie Lamport, Robert Shostak, and Marshall Pease, "The Byzantine Generals Problem," *ACM Transactions of Programming Languages and Systems*, Vol. 4, No. 3 (Jul. 1982): pgs. 382-401, https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf.

[59] *See, e.g.*: The Bitcoin Core GitHub repository (https://github.com/bitcoin/bitcoin).

[60] Bitcoin and Ethereum core client software alone have over 1000 individual contributors and that number does not include the countless developers working on compatible software for wallets, miners, smart contracts, or countless developers working on other cryptocurrencies. Nor does that number include the several academic authors who have published peer-reviewed research on these systems.

[61] You can try it for yourself by following the directions to install Bitcoin here: https://bitcoin.org/en/getting-started.

[62] You can see a visualization of the global nodes on the Bitcoin network at Bitnodes: https://bitnodes.earn.com/nodes/network-map/?ipv6_bits=56.

[63] Jerry Brito, "The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society," *Coin Center* (Feb. 2019) https://coincenter.org/entry/the-case-for-electronic-cash.

for other cryptocurrencies may do so directly with each other rather than through a regulated third party, which could collect customer information.

Faced with this reduction in surveillable information, governments may seek to extend Bank Secrecy Act obligations to electronic cash or decentralized exchange software developers or to the users of this software. This would be unconstitutional under the Fourth Amendment. Similarly, governments may seek to ban or permission the distribution electronic cash software or compell developers to introduce surveillance-friendly vulnerabilities or backdoors into their software; this would be unconstitutional under the First Amendment. Each of these arguments will be discussed in turn.

III. Electronic Cash, Decentralized Exchange, and the Fourth Amendment

The Fourth Amendment prohibits warrantless search or seizure of a person's home and private papers.[64] However, since 1971, a financial surveillance law, the Bank Secrecy Act, has mandated the bulk collection of customer information by banks and other financial institutions as well as automatic reporting of that data to regulators and law enforcement.[65] This sweeping surveillance regime is arguably both a seizure and search of private financial information and it operates without warrants.[66] The Supreme Court found this to be constitutional because customers willingly hand their information over to banks and banks have a legitimate business purpose that requires the collection and retention of that information; thus, the banks' customers lose their reasonable expectation of privacy with respect to that information and no warrant is required for its seizure by government or by private entities deputized by government (*e.g.* banks).[67]

As we have just described, electronic cash and decentralized exchange work without the need to trust an intermediary like a bank or other financial institution and may leave little or no information about user transactions public on the blockchain for use by law enforcement.[68] If regulators wish to impose Bank Secrecy Act obligations upon entities in the electronic cash or decentralized exchange space, the only possible targets would be the software developers of electronic cash protocols and decentralized exchange smart contracts or the persons running that software on the internet. Would the imposition of such obligations upon these parties be constitutional under current Fourth Amendment jurisprudence?

A. Fourth Amendment Protections Apply to Electronic Messages

The Fourth Amendment reads:

[64] U. S. Const. amend. IV.

[65] Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114-4 (1970) (codified as amended in scattered sections of 12 U.S.C., 18 U.S.C., and 31 U.S.C.).

[66] *California Bankers Assn. v. Shultz,* 416 U.S. 21 (1974) https://supreme.justia.com/cases/federal/us/416/21/.

[67] *Id.*; *United States v. Miller*, 425 U.S. 435 (1976) https://supreme.justia.com/cases/federal/us/425/435/.

[68] *See supra* II. Technology Background, pp. 9-16.

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[69]

Generally speaking, the Fourth Amendment prohibits warrantless searches and requires that warrants only be issued for searches of particularly described places with probable cause.

Much jurisprudence has been devoted to determining precisely when actions taken in a police or other government investigation constitute a search and therefore require a warrant.[70] For many years, this inquiry hinged on an Anglo-Saxon common law interpretation of privacy that focused on physical trespass.[71] When novel questions of electronic surveillance, such as wiretapping, emerged in the 1960s, the Supreme Court had to determine whether intrusions upon persons' otherwise private communications constituted a search even if there was no physical trespass onto the property or person of the searched individual.[72] Similarly, the Court had to grapple with whether the bulk collection of data made possible by electronic surveillance violated the Fourth Amendment's "particularity requirement" clause, which requires that warrants only be granted for searching places that are "particularly described."[73]

In the landmark 1967 case on these questions, *Katz v. United States*, the Court held that "[t]he Fourth Amendment protects people and not simply 'areas' against unreasonable searches and seizures, and... [the] Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[74] The Court concluded that even immaterial intrusions using technology could qualify as a search and created a new test to determine when the Fourth Amendment's protections should apply: whenever a person has a "reasonable expectation of privacy."[75]

Also in 1967, the Court in *Berger v. New York* held that statutes authorizing sweeping eavesdropping via electronic surveillance may violate the particularity requirement[76] of the Fourth Amendment and therefore constitute impermissibly general warrants unless they provide procedural safeguards to prevent overcollection.[77] The opinion of the Court "condemns electronic surveillance, for its similarity to the general warrants out of which our Revolution sprang and allows a discreet surveillance only on a showing of 'probable cause.' These

[69] U. S. Const. amend. IV.
[70] *See, generally*: John Kaplan, "Search and Seizure: A No-Man's Land in the Criminal Law," 49 *Calif. L. Rev.* 474 (1961), https://doi.org/10.15779/Z38V48G.
[71] *Ibid.*
[72] *Katz v. United States*, 389 U.S. 347 (1967) https://supreme.justia.com/cases/federal/us/389/347/.
[73] For instance, in *Berger v. New York*, the Court held that a statute permitting general eavesdropping was unconstitutional and violative of the Fourth Amendment in its broadness. *See*: *Berger v. New York*, 388 U.S. 41 (1967) https://supreme.justia.com/cases/federal/us/388/41/.
[74] *Katz v. United States.*
[75] *Id.*
[76] *See supra* note 73.
[77] *Berger v. New York.*

safeguards are minimal if we are to live under a regime of wiretapping and other electronic surveillance."[78]

Further, the Court in *Berger* suggested that if it is not possible to narrow the scope of electronic data collection to fit the warrant requirement then such evidence will simply be inadmissible. The Court reasoned: "It is said that neither a warrant nor a statute authorizing eavesdropping can be drawn so as to meet the Fourth Amendment's requirements. If that be true, then the 'fruits' of eavesdropping devices are barred under the Amendment."[79]

The Court also addressed the concerns of law enforcement losing visibility and failing to prevent crimes, effectively urging investigators to try harder with other, less invasive techniques and suggesting that sometimes privacy must trump security in order to preserve freedom. The moral panic identified by the Court in many ways resembles that of present-day concerns over encryption, cryptocurrencies, and "going dark."[80]

As the Court reasoned,

> It is said with fervor that electronic eavesdropping is a most important technique of law enforcement, and that outlawing it will severely cripple crime detection. … In any event, we cannot forgive the requirements of the Fourth Amendment in the name of law enforcement. … [I]t is not asking too much that officers be required to comply with the basic command of the Fourth Amendment before the innermost secrets of one's home or office are invaded. Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices. Some may claim that, without the use of such devices, crime detection in certain areas may suffer some delays, since eavesdropping is quicker, easier, and more certain. However, techniques and practices may well be developed that will operate just as speedily and certainly and—what is more important—without attending illegality.[81]

When making an electronic cash or a decentralized exchange transaction, a person's private 'papers' and 'effects' may now be data in the form of encoded messages sent over the internet. As with the early examples of electronic communications in *Katz* and *Berger*, the mere fact that these messages are electronic and exist outside the home poses no barrier to their continued protection against warrantless search, so long as the person to whom they belong has a reasonable expectation of their privacy.

[78] *Ibid.*, 64.
[79] *Ibid.*, 63.
[80] *See, for exampl*e: Matthew Olsen, Bruce Schneier, Jonathan Zittrain, et al., "Don't Panic: Making Progress on the 'Going Dark' Debate," *The Berkman Center for Internet and Society at Harvard University* (Feb. 1, 2016) https://cyber.harvard.edu/pubrelease/dont-panic/.
[81] *Berger v. New York*, 61, 62, 63.

B. The Third-Party Doctrine

In *Katz*, the Court held that data knowingly exposed to the public would not be protected, for the subject of the search would have lost her reasonable expectation of privacy. The Court held that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[82]

Thus any information that a cryptocurrency user shares publically, say by posting transaction data to a blockchain, will, of course, be freely available to regulators and law enforcement to search without any warrant or particularized suspicion. An electronic cash transaction may not, however, result in much publicly available information being recorded on the blockchain. In essence, the blockchain records encrypted data and displays it publicly in an unintelligible form; as in *Katz*, it is "preserved as private" but is displayed "in an area accessible to the public." It follows that this private but accessible information will be constitutionally protected.

In *United States v. Miller* (a case about bank records that we will return to in greater detail below) and *Smith v. Maryland* (a case about telephone company records) the Court further fleshed out the reasonable expectation standard, holding that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[83] This has come to be known as the *third-party doctrine*[84] and is currently used to justify warrantless data collection from electronic intermediaries such as Google or Amazon.[85]

Recently, the third-party doctrine has come under attack from justices and legal scholars who believe it is predicated on an outmoded understanding of the modern information landscape and who fear that it is today used to enable truly massive private data collection with little to no judicial process or accountability.[86] As people increasingly hand the entirety of their private correspondence and data over to cloud service providers and other online intermediaries, there grows, effectively, a gaping hole in our once comprehensive Fourth Amendment protections.[87] As Justice Sotomayor wrote in a concurrence to the 2012 *United States v. Jones* case,

[82] *Katz v. United States*, 351.

[83] *Smith v. Maryland*, 442 U.S. 735 (1979) https://supreme.justia.com/cases/federal/us/442/735/.

[84] *For a general discussion of the development of third-party doctrine, see*: Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477 (2006).

[85] *See, generally*: Andrew William Bagley, *Don't Be Evil: The Fourth Amendment in the Age of Google, National Security, and Digital Papers and Effects*, 21 Alb. L. J. Sci. & Tech. 153 (2011) https://heinonline.org/HOL/P?h=hein.journals/albnyst21&i=153.

[86] *See, e.g.*: Michael W. Price, *Rethinking Privacy: Fourth Amendment Papers and the Third-Party Doctrine*, 8 J. Nat'l. Sec. L. & Pol'y 247 (2016) https://heinonline.org/HOL/P?h=hein.journals/jnatselp8&i=254; *United States v. Jones*, 565 U.S. 400 (2012) https://supreme.justia.com/cases/federal/us/565/400/ (Sotomayor, S., concurring).

[87] David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 Minn. L. Rev. 2205 (2009), https://heinonline.org/HOL/P?h=hein.journals/mnlr93&i=2217.

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.[88]

Adjacent to the third-party doctrine is the question of whether the third party in question has a legitimate business purpose to collect information about their customers in the first place, and whether the customer voluntarily provided the information. This question is pertinent because it speaks to the customer's reasonable expectation of privacy. If I am willing to keep my private files unencrypted with a data storage provider, then I have reason to believe they may no longer be private. If, however, I am surreptitiously recorded by my doctor while being examined, I have no reason to believe that this interaction should *not* be private. Again, as stated in *Katz*, "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[89] Thus the question of whether personal information obtained by a third party is protected by a warrant requirement under the Fourth Amendment is not merely: Is the information still private to the searched party or has it been obtained by a third party? It must also ask: If obtained by a third party, did the third party have a legitimate business purpose to seek and retain that information and did the person voluntarily provide it?

This question was central to the *Smith v. Maryland* decision, although it was dealt with swiftly in that context.[90] The controversy in *Smith* centered on whether law enforcement can collect records of phone numbers dialed (not recordings of phone conversations had) from telephone companies without a warrant or particularized suspicion of certain subscribers.[91] The Court reasoned that whenever a caller dials numbers into her phone, she "voluntarily convey[s]"[92] that information to the phone company as a necessary and obvious step in making a call. Moreover, phone companies have "legitimate business purposes"[93] for recording that information. The Court therefore found that "although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret."[94] Without that reasonable expectation of privacy, the records of numbers dialed were deemed unprotected by the Fourth Amendment.

In *United States v. Miller* the Court dealt with the same question in the context of bank records. [95] It found that bank customers could "assert neither ownership nor possession"[96] of the

[88] *United States v. Jones*, 565 U.S. 400 (2012) https://supreme.justia.com/cases/federal/us/565/400/.
[89] *Katz v. United States*, 351.
[90] *Smith v. Maryland*, 442 U.S. 735 (1979) https://supreme.justia.com/cases/federal/us/442/735/.
[91] *Ibid*.
[92] *Id*., 745.
[93] *Id*., 743.
[94] *Ibid*.
[95] *United States v. Miller*, 425 U.S. 435 (1976) https://supreme.justia.com/cases/federal/us/425/435/.
[96] *Id*., 440.

documents; they were “business records of the banks.”[97] The particular nature of the records and the necessity of their revelation in order to conduct business was, again, core to the customers’ privacy expectations. The Court found that the “contents of the original checks and deposit slips” are not private correspondence, but rather they are “negotiable instruments to be used in commercial transactions.”[98] As with the phone numbers dialed in *Smith*, bank customers understand that they must hand this information over to the third party as a means to conducting business, else how would the phone company know to whom they wish to speak or the bank to whom they wish to pay? As the Court found, “all the documents obtained contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.”[99]

A recent case before the Court brought the question of legitimate business purposes and the third-party doctrine to a head. In *Carpenter v. United States* the Court refused to extend the reasoning behind the third-party doctrine to cellular phone location data collected by telecommunications providers.[100] Instead, the Court found that a warrant was required to search or seize this data from cellular service providers.[101] Cell phone users reveal their location to service providers because the radios on their devices regularly connect to multiple cell phone towers simultaneously (even when the user is not making a call). Thus it is a simple matter of triangulating signal strength in order to determine with high accuracy where the customer’s phone is at all times. To find that this third-party location data was protected unlike checks and phone number data in *Smith* and *Miller*, the Court had to distinguish why such data was either not voluntarily provided or went beyond a legitimate business purpose.

On the question of volition, the Court reasoned that the information was never voluntarily “shared” by customers because of the ubiquity of cell phones, their necessity to everyday life, and the fact that they simply cannot be used without revealing that data.[102] The Court found that “Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily assume the risk of turning over a comprehensive dossier of his physical movements.”[103]

On the question of legitimate business purposes, the Court noted that in both *Miller* and *Smith* the records in question were at the core of the legitimate business purpose of the third party.[104] A phone company *must know* the number that their customer wishes to reach. The bank *must know* the name of the person the customer wishes to pay. The warrantless data collection in those cases was limited to those key items that customers must understand as *essential* to their use of the business’ services; items that a reasonable customer would expect the third party to

[97] *Ibid*.
[98] *Id*., 442.
[99] *Id*., 435.
[100] *Carpenter v. United States*, 585 U.S. __ (2018) https://supreme.justia.com/cases/federal/us/585/16-402/.
[101] *Ibid*.
[102] *Ibid*.
[103] *Ibid*.
[104] *Ibid*.

have and retain. With cellular location data, however, the Court found that “there are no comparable limitations on the revealing nature” of the information sought.[105] A cell phone company need not know the customer's location at all times to connect calls, and subscribers would not expect them to have and retain this information as a condition of receiving cell service.

Customers understand that the numbers they ask to be connected with must be shared in order to be connected in a call. They do not contemplate trading the full revelation of their day-to-day movements merely because they wish to check their email. Interestingly, this holding does not argue that there is no legitimate business purpose that could justify the telecommunications providers collecting and retaining that data (surely knowing where your customers are is important to providing them with good mobile phone connectivity).[106] Instead, it argues that the data sought by law enforcement was ancillary to the data that a customer would reasonably expect to provide within the context of the business relationship.[107] It is data that may be legitimate for the business to obtain, but it is not essential to the provision of the service and is beyond the business purpose as the customer understands it and therefore within her reasonable expectation of privacy.[108]

The technology behind a digital cash transaction or a decentralized exchange is designed to obviate the need for users to hand any personal data over to any third party. Indeed, these systems are designed such that no trusted third party need even exist for the the transaction or exchange to take place. Therefore, it would be impossible to argue that the users of these systems voluntarily hand any personal data over to any third party when they transact. A user will construct her electronic messages to be compatible with the electronic cash protocol or decentralized exchange smart contract that she chooses to use, but this data alone will likely not be useful to regulators or law enforcement[109] and it will certainly not include typical financial transaction data like the name or physical address of the user. Regardless of its lack of usefulness to law enforcement, this is the only data that a user of these protocols must provide in order to obtain the desired result and, consequently, it is the only data for which the user would no longer have a reasonable expectation of privacy.

No third party within these systems *must know* any additional information about the user for the transaction to take place; thus, it would be impossible to argue that such extra data was essential to the conduct of any supposed third party's business purposes.[110] Arguing in the opposite is equivalent to suggesting that envelope manufacturers have a legitimate business purpose in learning what letters people mail, or that safe manufacturers have a legitimate business purpose in learning what valuables people keep in their safes.

[105] *Ibid*.
[106] *Ibid*.
[107] *Ibid*.
[108] *Ibid*.
[109] Paige Peterson, “Anatomy of A Zcash Transaction,” *Electric Coin Company blo*g (Nov. 23, 2016) https://z.cash/blog/anatomy-of-zcash/.
[110] *Ibid.*

Lacking publicly available information about the user's transaction and lacking a third party to whom the user has voluntarily revealed information pursuant to a legitimate business purpose, the only constitutional path to a search of information in an electronic cash transaction or decentralized exchange must, by necessity, go through the user herself, and that must require particularized suspicion of the user and a warrant from a judge.

Faced with these limitations, regulators may seek to deputize some other third party to collect additional information about these transactions. Again, because electronic cash and decentralized exchange transactions can be performed by the user(s) alone with nothing more than software and an internet connection, the only possible target for such deputization would be the software developers who invented the tools that the users employ.[111] This would be a radical shift from the current administration of financial surveillance statutes. As we shall see in the next subsection, the Bank Secrecy Act has always taken for granted the existence of a third party that would already have a business-customer relationship and would already be in possession of customer transaction data. The question of surveillance now turns on whether regulators can impose similar reporting obligations on parties that would otherwise have no more connection to an illegal transaction than a car manufacturer would have to a bank robbery getaway vehicle.

C. The Bank Secrecy Act

The Bank Secrecy Act (BSA)[112] is a federal law that orders financial institutions to collect and retain certain information about their customers and share that information with the Department of the Treasury.[113]

The BSA applies to "financial institutions, " but the statute only offers loose definitions of various subcategories of financial institution,[114] and grants power to the Secretary of the Treasury to craft new or more specific definitions through notice and comment rulemaking, thus expanding the range of businesses subject to the Act.[115] The statute also does not spell out what sorts of records or reports must be made, but rather it authorizes the Secretary to prescribe by regulation certain recordkeeping and reporting requirements. The Secretary may mandate that financial institutions "require, retain, or maintain" as well as "report" to Treasury any records determined to have a "high degree of usefulness in criminal, tax, or regulatory investigations or proceedings."[116]

[111] One could suggest deputizing the user but then, of course, the third-party doctrine would not apply because the user is not a third party to her own transactions.

[112] 31 USC §§ 5311-5332.

[113] FinCEN is a Bureau within the Treasury established by order of the Secretary of the Treasury (Treasury Order Numbered 105-08).

[114] 31 USC § 5312(a)(2).

[115] 31 USC § 5312(a)(2)(Y).

[116] 31 USC § 5311.

The regulations implementing the Bank Secrecy Act[117] (henceforward the “implementing regulations”) thereby determine both its breadth (which businesses are financial institutions) and depth (what degree of recordkeeping and reporting are required). These regulations have evolved over the years. With respect to domestic financial transactions made by customers of regulated financial institutions, the original implementing regulations only included insured banks within the ambit of financial institutions and only required recording and maintenance of identity information for their customers and those with signing authority, copies of checks drawn against the bank for over $100, and any extension of credit exceeding $5,000.[118] The original implementing regulations also only required financial institutions to make reports to Treasury whenever a customer made a deposit, withdrawal, or other transfer involving “a transaction in currency of more than $10,000.”[119] Thus for domestic transactions involving constitutionally protected U.S. persons, only those made with physical cash necessitated reports. These reports are referred to as Currency Transaction Reports or CTRs.

Today, the implementing regulations have significantly expanded. The definition of “financial institution” has grown from banks and a handful of similar businesses[120] to include securities broker-dealers, telegraph companies, casinos, dealers in foreign exchange, check cashers, issuers or sellers of traveler's checks or money orders, providers and sellers of prepaid access, money transmitters, and the U.S. Postal Service.[121] The domestic reporting obligations also expanded in 1996 to include “suspicious activity reports” or SARs.[122] SARs must be filed for every transaction or series of structured transactions over $5,000 (if the reporting financial institution is a bank) or over $2,000 (otherwise) whenever the financial institution “knows, suspects, or has reason to suspect” that the transaction:

1. “involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities,”
2. is designed to evade any requirements of regulations promulgated under the Bank Secrecy Act; or
3. “has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage…”[123]

[117] 31 USC §§ 5311-5332.
[118] 31 USC § 5312(a)(2).
[119] 31 USC § 5316(a)(2).
[120] The original text only addressed “any person engaging in the business of carrying on any of the following functions: (1) Issuing or redeeming checks, money orders, travelers' checks, or similar instruments, except as an incident to the conduct of its own nonfinancial business. (2) Transferring funds or credits domestically or internationally. (3) Operating a currency exchange or otherwise dealing in foreign currencies or credits. (4) Operating a credit card system. (5) Performing such similar, related, or substitute functions for any of the foregoing or for banking as may be specified by the Secretary in regulations.” *See*: Bank Secrecy Act, Pub. L. No. 91-507 (1970) https://www.govtrack.us/congress/bills/91/hr15073/text.
[121] 31 USC § 5312(a)(2).
[122] 31 USC § 5312(a)(2)(Y).
[123] 31 CFR § 1020.320(a)(2)(i-iii).

The inclusion of SAR reporting has spurred a massive increase in the amount of data reported under the Bank Secrecy Act to Treasury. SAR reporting has grown from around 60,000 SARs per year in 1996 when the rule was promulgated to 3,000,000 per year in 2017.[124]

Aside from SARs and CTRs, any additional information sought by Treasury from financial institutions will be released only via "existing legal process."[125] In other words, any examination of other records the collection of which is mandated under the BSA but the reporting of which is not required would necessitate either a judge-issued warrant (if the Fourth Amendment applies, which we will discuss next) or a mere subpoena (if the Fourth Amendment does not apply). SARs and CTRs do not require warrants or any other form of judicial process and must be automatically filed by regulated financial institutions with Treasury.

In short, the Bank Secrecy Act mandates the collection of an incredible amount of personal financial data and the reporting of that data to the government for purposes of criminal investigation without any particularized suspicion, finding of probable cause, or warrant. It is a program of warrantless mass surveillance. How is it constitutional?

D. The Constitutionality of the Bank Secrecy Act

It is unknown if the Bank Secrecy Act as currently applied is constitutional. Two cases brought not long after the law's passage in 1970, *California Bankers Association v. Shultz*[126] and *United States v. Miller*,[127] found that it passed constitutional muster as applied in the implementing regulations of the day. As was just explained, however, the scope of the implementing regulations has expanded tremendously since that time.

In *Shultz*, the plaintiffs—a trade association of California bankers joined by the ACLU—argued that the BSA's recordkeeping requirements were unconstitutional because they effectively made financial institutions agents of the government surveillance apparatus and directed them to seize records containing the personal information of their customers. The Court articulated why the third-party doctrine excluded those records from a customer's reasonable expectation of privacy and therefore obviated any warrant requirement for such a seizure:

> Plaintiffs urge that, when the bank makes and keeps records under the compulsion of the Secretary's regulations, it acts as an agent of the Government, and thereby engages in a 'seizure' of the records of its customers. But **all of the records which the Secretary requires to be kept pertain to transactions to which the bank was itself a party.** .... The fact that a large number of banks voluntarily kept records of this sort before they were required to do so by regulation is an indication that the records were

[124] Jenna Danko, "The Effectiveness of Suspicious Activity Reports," *Oracle Financial Services Blog* (Feb. 16, 2018) https://blogs.oracle.com/financialservices/the-effectiveness-of-suspicious-activity-reports
[125] S. REP. No. 1139, 91st Cong., 2d Sess. 5 (1970); H.R. REP. No. 975, 91st Cong., 2d Sess. 10 (1970).
[126] *California Bankers Assn. v. Shultz*, 416 U.S. 21 (1974) https://supreme.justia.com/cases/federal/us/416/21/.
[127] *United States v. Miller*, 425 U.S. 435 (1976) https://supreme.justia.com/cases/federal/us/425/435/.

> thought useful to the bank in the conduct of its own business, as well as in reflecting transactions of its customers.[128]

As with telephone numbers, the nature of checks and other negotiable instruments is such that customers must make certain pertinent facts available to their bank in order for any meaningful business to be accomplished. For example, a check must say who is paying whom in order to be cashed, or a series of dial tones must describe the called number in order to be connected. Furthermore, the Court reasoned that because the recorded information (presumably still held privately by the banks) would only be obtained by investigators by way of "existing legal process," and because no such particular process (*e.g.* a subpoena for records) was yet being challenged (plaintiffs were challenging the statute and the implementing regulations generally), it could not find any constitutional defect with the recordkeeping scheme as implemented.[129] This would not be the only instance in the *Shultz* opinion that the Court punted on a critical issue because of standing and ripeness.

Plaintiffs also argued that the *reporting* requirements violated the Fourth Amendment as a warrantless search, but the Court found that neither plaintiff could bring such a claim. The bankers association could not claim to represent the rights of customers harmed by the reporting requirement,[130] and the ACLU, while it did have accounts with BSA-regulated banks, had not engaged in any currency transactions over $10,000, and therefore would never have been the subject of a CTR report.[131] No harm no foul. These claims would have to wait for the next case, *Miller*, to be tested.

However, in separating the analysis between the seizure of records, which was discussed in *Shultz*, and the search, which would have to wait for *Miller*, the Court may have prejudged the outcome. As Justice Marshall, in a scathing dissent from the *Shultz* majority, wrote:

> The seizure has already occurred, and all that remains is the transfer of the documents from the agent forced by the Government to accomplish the seizure to the Government itself. Indeed, it is ironic that, although the majority deems the bank customers' Fourth Amendment claims premature, it also intimates that, once the bank has made copies of a customer's checks, the customer no longer has standing to invoke his Fourth Amendment rights when a demand is made on the bank by the Government for the records. By accepting the Government's bifurcated approach to the recordkeeping requirement and the acquisition of the records, the majority engages in a hollow charade whereby Fourth Amendment claims are to be labeled premature until such time as they can be deemed too late.[132]

[128] *Id.* 52.
[129] *Id.* 51-54.
[130] *Id.* 59-70.
[131] *Ibid.*
[132] *Id.* 97.

Justice Marshall's concern proved prescient. In *Miller*, the respondent had been indicted, effectively, for conspiracy to make moonshine, and the evidence at stake in the indictment was a series of transactions he had made through his bank for cargo van rentals, radio equipment, and metal piping.[133] The bank had records of these transactions that it retained as per the implementing regulations of the BSA, and, when subpoenaed by the Treasury Department's Alcohol, Tobacco and Firearms Bureau, the bank turned these records over to investigators.[134]

Again, the Court held that Miller had no reasonable expectation of privacy over these records because he had knowingly revealed this information to the bank during the usual course of business; the records were as much the bank's information as Miller's, and the bank was free to share them with law enforcement through the usual, warrantless legal processes:

> The checks are not confidential communications, but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.[135]

The Court refused to entertain Miller's arguments that it was the combined compulsion of the bank by the government to collect the information in the first place and the subsequent subpoena of that information once collected that constituted a search and seizure. Instead it merely analyzed, separately, whether Miller had a reasonable privacy expectation over the copies of the checks (no, because they are business records) or the original checks that were copied (no, because they were willingly handed over to a third party).[136]

Again, Justice Marshall lambasted the bifurcated analysis as a sham:

> Today, not surprisingly, the Court finds respondent's claims to be made too late. Since the Court in [*Shultz*] held that a bank, in complying with the requirement that it keep copies of the checks written by its customers, "neither searches nor seizes records in which the depositor has a Fourth Amendment right," [] there is nothing new in today's holding that respondent has no protected Fourth Amendment interest in such records. A fortiori, he does not have standing to contest the Government's subpoena to the bank. … I wash my hands of today's extended redundancy by the Court.[137]

In a separate dissent, Justice Brennan warned of the danger inherent in permitting such broad and judicially unchecked surveillance. Especially prescient was his concern over the characterization of persons' provision of information to banks as "voluntary." He wrote:

> For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate

[133] *United States v. Miller*, 425 U.S. 435 (1976) https://supreme.justia.com/cases/federal/us/425/435/.
[134] *Ibid*.
[135] *Id*. 442.
[136] *United States v. Miller*.
[137] *Id*. 455-456.

> in the economic life of contemporary society without maintaining a bank account. In the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography. ... Development of photocopying machines, electronic computers and other sophisticated instruments have accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds. Consequently, judicial interpretations of the reach of the constitutional protection of individual privacy must keep pace with the perils created by these new devices.[138]

This analysis, although it is in a dissent and carries no legal authority, states almost exactly the concern that ultimately swayed the court in *Carpenter* some 40 years later:

> Cell phone location information is not truly 'shared' as one normally understands the term. In the first place, cell phones and the services they provide are "such a pervasive and insistent part of daily life" that carrying one is indispensable to participation in modern society. ... [I]n no meaningful sense does the user voluntarily "assume the risk" of turning over a comprehensive dossier of his physical movements.[139]

Finally, it is important to remember that the constitutionality of the BSA as adjudged in *Shultz* and *Miller* was only "as applied" in the implementing regulations of the 1970s.[140] As noted above, since the 1970s the BSA's reach has expanded both in the number of businesses it treats as financial institutions and in the quantity and type of transaction reports those financial institutions are required to file. To our knowledge, for example, the constitutionality of domestic SARs has never been challenged or vindicated. Neither has the application of the BSA to businesses that are not traditionally understood to be financial institutions, such as casinos or retail sellers of prepaid cards.

The tenuous nature of the BSA's constitutionality is underscored by the vote count in *Shultz*. The majority opinion of the Court is matched with a concurrence authored by Justice Powell and joined by Justice Blackmun. Had these two justices sided with the dissenters the outcome would have been 5-4 against the BSA's constitutionality. Powell's concurrence specifically says that his opinion is predicated on the narrow application of the BSA that existed at the time:

> A significant extension of the regulations' reporting requirements, however, would pose substantial and difficult constitutional questions for me. In their full reach, the reports apparently authorized by the open-ended language of the Act touch upon intimate areas of an individual's personal affairs. Financial transactions can reveal much about a person's activities, associations, and beliefs. At some point, governmental intrusion upon these areas would implicate legitimate expectations of privacy. Moreover, the

[138] *Id*. 451-452.

[139] *Carpenter v. United States*, 585 U.S. __ (2018) https://supreme.justia.com/cases/federal/us/585/16-402/.

[140] *California Bankers Assn. v. Shultz*, 78-79.

> potential for abuse is particularly acute where, as here, the legislative scheme permits access to this information without invocation of the judicial process. In such instances, the important responsibility for balancing societal and individual interests is left to unreviewed executive discretion, rather than the scrutiny of a neutral magistrate.[141]

Powell subsequently authored the majority opinion in *Miller*, but made clear that constitutionality was predicated on the narrowness of the investigation into Miller's moonshine operation and the judicial process that accompanied it:

> We are not confronted with a situation in which the Government, through "unreviewed executive discretion," has made a wide-ranging inquiry that unnecessarily "touch[es] upon intimate areas of an individual's personal affairs." California Bankers Assn. v. Shultz, 416 U.S. at 416 U. S. 78-79 (POWELL, J., concurring). Here the Government has exercised its powers through narrowly directed subpoenas duces tecum subject to the legal restraints attendant to such process.[142]

With the introduction of SARs in the 1990s, the question alluded to above becomes: Is the automatic reporting of over three million transactions and associated personal details a "wide-ranging inquiry that unnecessarily touches upon intimate areas" of Americans' personal affairs? Is it "unreviewed executive discretion" when this flow of personal data is the direct result of new implementing regulations that do not require investigators to seek a single subpoena or engage in any other judicial process?[143]

E. Regulating Software Developers Under the BSA Would be Unconstitutional

The surveillance obligations imposed on financial institutions by the BSA have only been found constitutional as they were applied in the 1970s implementing regulations. Since then, we've seen a substantial expansion in the number of businesses categorized as financial institutions as well as the depth of the domestic reporting requirements they must undertake.

The constitutionality of that regime as it currently stands is predicated on the third-party doctrine. Justices have already substantially weakened that doctrine with respect to location data and cellular service providers.[144]

Under the BSA, the Secretary of Treasury could, in theory, classify developers of electronic cash and decentralized exchange software as financial institutions through rulemaking and attempt to mandate their compliance with BSA recordkeeping and reporting obligations. In effect, the regulator would be ordering these developers to alter the protocols and smart contract software they publish such that users must supply identifying information to some third party on the network in order to participate and such that suspicious transactions are reported to the

[141] *Ibid.*
[142] *United States v. Miller*, footnote 6.
[143] *Ibid.*
[144] *Carpenter v. United States*.

regulator and potentially blocked as per a reasonably calibrated anti-money laundering program.

It is unclear whether this would even be technologically feasible short of merely turning a decentralized cryptocurrency network into, in effect, a centralized payments provider like a custodial money transmitter or a bank. It's also stunning to imagine that the BSA could be used to force a person to entirely change their line of business from being a developer who authors software tools and releases them to the public to becoming a centralized financial services provider with all of the attendant regulatory burdens. In effect, it's like asking a novelist to stop merely publishing stories and now, instead, become a improvisational actor willing to participate in every reader's experience of their books.

It is clear that this would be tantamount to an unconstitutional warrantless seizure and search of information over which users of electronic cash and decentralized exchange have a legitimate privacy expectation—an expectation that has not been abrogated by handing said information over to any third parties. These technologies are explicitly designed to operate without third parties. Developers are not third parties to transactions nor to any other interaction with users. They never have control over customer funds (indeed they may have no customers), nor need they even have any actual interaction with the peer-to-peer networks their software make possible.

It is true that the BSA placed obligations on banks to collect and retain information that they may have not otherwise collected, and one could argue that an obligation on software developers to collect cryptocurrency-user information would be no different. However, the holdings of *Shultz* and *Miller* are very clear. In those cases the mandate was not a seizure of customer records because the mandate *only* "pertain[ed] to transactions to which the bank was itself a party."[145] It involved *only* information voluntarily handed over to the bank from its customers and that information was limited to conducting the legitimate business purpose of operating a bank (*e.g.* signatures on negotiable instruments, payment instructions, and the like).[146]

A developer of electronic cash or decentralized exchange software does not have any legitimate business purpose to collect information about the users of their software. Indeed, such collection is anathema to the business purpose in which the developer has presumably engaged: the publication of software with strong privacy and security guarantees (*e.g.* no back doors or surveillance). Nor would users be voluntarily providing this information to the developer if they were operating under the misapprehension that the electronic cash or decentralized exchange software was delivering upon its stated purpose of enabling private transactions or cryptocurrency exchange without an intermediary. In effect, the users' information would be surreptitiously captured while they operated under the false belief that the tools they were using honored their expectations of privacy.

[145] *California Bankers Assn. v. Shultz*, 52.
[146] *Ibid*.

If a developer of electronic cash or decentralized exchange software publicly announced that they were voluntarily incorporating BSA-style surveillance into their tools, users who continued to use those tools would likely lose their reasonable expectation of privacy over any information they provided when they used those tools. However, it is hard to imagine that *every* developer of electronic cash or decentralized exchange software would suddenly choose to voluntarily surveil the users of their software, even under pressure from law enforcement (many are not located in the U.S.). It is even more unbelievable that users would continue to use tools that had known backdoors if previous versions of the software without backdoors continued to exist in online archives or on peer-to-peer file sharing networks, or if other developers continued to offer more private alternatives.

If a developer refused to comply with a regulator's demand that they add surveillance backdoors into their tools and the regulator either ordered them to cease publishing their software or compelled them to add the backdoor through a legal order then two additional constitutional questions would surface:

1. Is a licensing requirement or ban on the publication of electronic cash or decentralized exchange source code an unconstitutional prior restraint on protected speech?
2. Is an order to only publish electronic cash or decentralized exchange source code with surveillance backdoors unconstitutionally compelled speech?

To answer these questions and the perfunctory matter of whether electronic cash or decentralized exchange source code is constitutionally protected speech, we must turn from the Fourth Amendment to the First.

IV. Electronic Cash, Decentralized Exchange, and the First Amendment

The First Amendment prohibits the content-based regulation of expressive speech unless the government can prove a compelling state interest that could not be achieved through any less restrictive policy.[147] If electronic cash or decentralized exchange source code is expressive speech, then a publication ban or licensing requirement on developers would be presumed unconstitutional unless the government can prove in court that banning that software or licensing its publication achieves a compelling state interest that could not be achieved through any less restrictive policy. Similarly there would be a presumption of unconstitutionality if a law or regulation attempted to compel developers to rewrite their source code to include backdoors.[148]

Rarely do courts faced with bans on speech of a certain type or content find that the government's interest is truly compelling and not achievable through less restrictive policies. Therefore, cases usually hinge on whether the speech is indeed protected and what level of protection it deserves. The remainder of this report argues that electronic cash and

[147] This judicial review standard is known as "strict scrutiny" and is used to evaluate constitutionality. *For more, see*: Richard H. Fallon, Jr., *Strict Judicial Scrutiny*, 54 UCLA L. Rev. 1267 (2006-2007).
[148] *See infra* IV. C. iii. Compelling Developers to Write Backdoors Would be Unconstitutional, pp. 51-52.

decentralized exchange source code is protected speech and that laws banning or requiring licensing for its publication, as well as laws compelling developers to alter their speech, should be presumed unconstitutional and must face strict scrutiny, rather than a lower standard such as intermediate scrutiny, upon judicial review.

A. Computer Code is Protected Speech

The Supreme Court has yet to hold generally that programs written in computer code are protected speech. However, holdings in cases dealing with novels, musical scores, and blueprints strongly suggest that computer code would be protected speech, and two recent cases related to video games and prescription datasets establish broad tests for whether any electronic data (software included) would qualify as protected speech. Lower courts have taken varied approaches, and some have found that computer code is protected speech because it is expressive conduct, like flag burning or nude dancing. As we shall discuss, this conduct-based approach has split the circuits, is misguided, offers lesser protection from regulation, and has no support in Supreme Court precedent.

i. Computer Code Expresses Ideas for Political and Social Change

In *Roth v. United States*, the Supreme Court found that "the First Amendment was fashioned to assure unfettered interchange of ideas for the bringing about of political and social changes desired by the people."[149] Generally, the particular medium through which ideas are expressed is inconsequential to First Amendment protection. If it is an idea of at least modest "political and social" significance, the Court certainly does not discriminate.[150] It protects ideas regardless of the medium in which they are presented, even if it is gibberish or visual chaos. As the Court has found, the category of "unquestionably shielded" speech includes a "painting of Jackson Pollock, music of Arnold Schöenberg, or Jabberwocky verse of Lewis Carroll."[151]

As discussed earlier,[152] open source computer code shared over the internet is directly intended to convey the scientific and engineering ideas of a given project to other developers, including current collaborators, potential future collaborators, researchers, and the general public who may wish to use these tools and seek assurances of their correct operation, which can only be achieved through publicity and transparency. If digital tools derived from this science and engineering will be employed to, for example, organize social behavior on the internet, then their source code certainly holds at least as much social and political significance in the 21st century as a schematic of a steam engine or a blueprint for an amphitheater would have held in previous ages.

[149] *Roth v. United States*, 354 U.S. 476 (1957) https://supreme.justia.com/cases/federal/us/354/476/.
[150] *Ibid.*
[151] *Hurley v. Irish-American Gay, Lesbian & Bisexual Group of Boston,* 515 U.S. 557, 569 (1995) https://supreme.justia.com/cases/federal/us/515/557/.
[152] *See supra* II. C. Electronic Cash and Decentralized Exchange are Powered by Software, pp. 15-17.

Indeed, the “unfettered interchange of ideas”[153] found in computer code is the primary motivation behind open source software development as a practice. Rather than cloister one’s software project within the developer staff of a single corporation by enforcing copyrights, trade secrets, and other restrictions on dissemination through a proprietary software model, open source software development principles eschew copyrights and restrictive licenses, push for better ways to clearly and publicly display source code for review, and seek to solicit the widest possible audience in order to increase the odds that a member of that audience will catch errors that would otherwise go undetected or find opportunities for innovation that would otherwise have been ignored. This ethos is long established and well-captured in developer Eric Raymond’s landmark 1997 essay *The Cathedral and the Bazaar*.[154] All major electronic cash and decentralized exchange software projects rigorously adhere to this open source model of development. Canonical changes to that software are only made after an exhaustive round of public sharing and discussion of the code itself.[155]

Moreover, computer code underlies systems we rely upon daily to organize our society—from email clients to traffic lights, police surveillance cameras to social networking websites and—more recently—private decentralized money and exchange. Everything we do (and cannot do) on those platforms and with those tools is mediated by software and ideas expressed in

[153] *Roth v. United States*, 484.

[154] In the essay, Raymond explains several emergent rules in the open source developer community: “Every good work of software starts by scratching a developer's personal itch.” The majority of developers in an open source project are motivated primarily because they want to use the product they are making. They aren’t under contract to build something for someone else; they have a personal need and they are addressing it. This leads to greater motivation and it brings intimate personal knowledge about the problem to bear. “Good programmers know what to write. Great ones know what to rewrite (and reuse).” When development happens in the open, redundancy can be avoided, a division and specialization of knowledge and expertise achieved, and troublesome, complicated, or redundant code identified and simplified. “When you lose interest in a program, your last duty to it is to hand it off to a competent successor.” People come and go within an open source project depending on their interests and expertise. No one gets stuck working on projects they no longer care about and fresh minds appear to offer different perspectives on longstanding problems or new avenues for development. “Treating your users as co-developers is your least-hassle route to rapid code improvement and effective debugging.” Many of the people who use the open source code will also be able to identify and flag issues, and may even be able to offer solutions. The line between a consumer and a producer of open source software blurs because production happens transparently in full view of the public and participation in production is available to all. “Given a large enough beta-tester and co-developer base, almost every problem will be characterized quickly and the fix obvious to someone.” This has come to be known as Linus’s Law after Linus Torvalds, the original creator and longtime principal developer of Linux. When development is not open, all developers may share a certain blind spot or fail to notice a certain error. Wider development amongst sophisticated users with idiosyncratic perspectives increases the likelihood that bugs are discovered and addressed, thus making open source software more resilient and secure. *See*: Eric S. Raymond, *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. Cambridge, MA: O’Reilly, 1999.

[155] *See, e.g.*: the so-called block size debate among the Bitcoin community. *For an overview, see*: Aaron van Wirdum, “Segregated Witness, Part 3: How a Soft Fork Might Establish a Block-Size Truce (or Not),” *Bitcoin Magazine* (Dec 29, 2015) https://bitcoinmagazine.com/articles/segregated-witness-part-how-a-soft-fork-might-establish-a-block-size-truce-or-not-1451423607/.

code. Anyone can learn to read the languages in which this code is written in order to elevate and formulate their view of debates surrounding these technologies, and anyone who has learned those languages can invent and suggest new and different ideas, including alternatives to the systems of today. Developers may learn these skills because they think they can build better, safer tools for organizing society, enabling individual freedom, or limiting the freedom of those who would do others harm.

Say what one will about the deservedly mocked mantra of Silicon Valley, "make the world a better place," but software does make the world.[156] Source code and the creative and scientific expression it contains now represents a substantial quantity of the world's "ideas for the bringing about of political and social changes desired by the people."[157] Many remain surprised and even alarmed that a new language—many new languages in fact—are actively being used to fundamentally reshape the landscape of human interaction. But to deny this fact is to deny everything that has changed in our lives since the advent of digital computing. Similarly, to deny statements made in coding languages like C++[158] or Rust[159] the same protections we would grant statements made in English would make no more sense than to deny novels protection when they are written in French, symphonies protection because they are written in musical notation, or scientific papers protection because they tend to be filled with arcane graphs and formulae.

At least under the broad standard articulated by the Court in *Roth*, electronic cash and decentralized exchange software should be protected speech. A rigorous analysis, however, is not that simple. As we shall unpack in the next two subsections, some lower courts have muddled what should be a straightforward analysis by treating code as expressive conduct rather than speech, meaning it is subject to weaker First Amendment protections. By contrast, recent Supreme Court cases have eschewed this conduct-based approach and articulated extremely broad tests for what qualifies as strongly protected speech in the digital age. Later we will describe the different levels of protection (*i.e.* strict vs. intermediate scrutiny) to which various types of expression (*i.e.* expressive conduct vs. speech) are entitled, and the importance of this seemingly academic debate will be clear: if electronic cash or decentralized exchange software is found to be expressive conduct rather than speech it is entitled to substantially weaker protections.

ii. Publishing Computer Code is a Speech Act, Not Symbolic Conduct

The Supreme Court has yet to hold generally that programs written in computer code are protected speech. That said, it has also never explicitly found that short stories written in Russian are protected speech or that oboe concerti written in musical notation are protected

[156] *See, e.g.*: "Silicon Valley, TechCrunch Disrupt Parody," *goodlaugh182 YouTube Channel* (May 25, 2014) https://www.youtube.com/watch?v=J-GVd_HLlps.
[157] *Roth v. United States, 484.*
[158] *See, generally:* Bjarne Stroustrup, "The Essence of C++," *The University of Edinburgh YouTube Channe*l (May 4, 2014) https://www.youtube.com/watch?v=86xWVb4XIyE.
[159] *See, generall*y: Steve Klabnik and Carol Nichols, *The Rust Programming Language*, San Francisco, CA: No Starch Press (2018) *available at* https://doc.rust-lang.org/book/ch00-00-introduction.html.

speech. Some lower courts have begun to analyze this question under the jurisprudence of expressive conduct.[160] These cases rely on the *Spence*[161] and *O'Brien*[162] tests for expressive conduct developed in earlier holdings from the Court. As we will argue later at length, these lower-court applications of *Spence* and *O'Brien* are misguided approaches to the question of whether computer code is protected speech. Those cases dealt with actions, not mere ideas: hanging a flag upside down in *Spence*,[163] and burning a draft card in *O'Brien*.[164] Actions may be expressive, but they can also have more immediate and dangerous consequences than mere words. Burning a building down may express someone's feelings about that building, but it also presents obvious risks to life and property. Therefore, even if a expressive action, like burning a flag, is found to be speech, it will often be entitled to less-strict protection from regulation.

Computer code, however, is not an expressive or symbolic action. It is, quite literally, a written series of symbols themselves, *i.e.* letters and numbers or, once compiled, 0s and 1s. It is not like a musical performance, but rather like the printed score for an orchestra's conductor or the printed roll for a player piano. While it is true that people will use computer source code to perform actions (just as one might use the musical score to perform music), the act of writing and sharing the code is an entirely separate act from the act of executing the code. Each or both may be protected speech, but they must be analyzed separately: analysis of the act of executing the code must use the *Spence* and *O'Brien* tests for expressive conduct, and analysis of the act of writing and sharing the code must use the same standards we use for authorship of novels or musical scores as articulated in *Roth*.[165] To conflate the analysis and judge both the authorship and execution of code under *Spence* and *O'Brien* is to treat an impromptu performance of the 1812 Overture (cannons and all) the same as the moment Tchaikovsky put pen to paper on his musical score. The potentially disruptive performance should rightly and constitutionally be subject to somewhat prescriptive regulation, while the mere act of writing the music in notes and clefts on paper should not.

As we have discussed, making electronic cash or decentralized exchange transactions involves executing computer code. We do not argue in this report that the act of executing that code and actually transmitting or exchanging cryptocurrency is protected speech. (It may be protected speech in several contexts, but if we were making this argument we would likely need to use the *Spence* and *O'Brien* tests to determine whether a symbolic action is protected speech.) This report is concerned only with the developers of computer code and whether they can be banned from publishing code, made to get a license to publish it, or compelled to alter the code they publish such that it has surveillance backdoors. Although it is unlikely, a developer of electronic cash or decentralized exchange software may go her whole life without making an electronic cash transaction or a decentralized exchange. The question of whether she deserves

[160] *Universal City Studios, Inc. v. Corley* , *Junger v. Daley*, and *Karn v. US Dept. of State*.
[161] *Spence v. Washington,* 418 U.S. 405 (1974) https://supreme.justia.com/cases/federal/us/418/405/.
[162] *United States v. O'Brien,* 391 U.S. 367 (1968) https://supreme.justia.com/cases/federal/us/391/367/.
[163] *Spence v. Washington*.
[164] *United States v. O'Brien*.
[165] *Roth v. United States*.

First Amendment protection hinges not on what actions others may use her software to perform but merely on whether she, simply by publishing, has engaged in protected speech.

iii. Electronic Cash and Decentralized Exchange Software Are Protected Speech

In two cases, *Brown v. Entertainment Merchants Association*[166] and *Sorrell v. IMS Health Inc.*,[167] the Supreme Court has found that some computer programs and some digital data are worthy of protection as speech. It did not use the *Spence* or *O'Brien* test in either determination.

In *Brown*, the court found that video games were protected speech and even violent ones could not be banned from sale. Some scholars believe that *Brown* articulated a new, narrow standard for when novel modes of expression would be entitled to First Amendment protections.[168] For example, lawyer Andrew Tutt writes:

> Rather than reach beyond video games to software generally, the Court zeroed in on video games and held that they were speech because they communicated ideas through familiar literary devices. The Court reasoned that video games were speech because they expressed ideas in familiar ways: "Like the protected books, plays, and movies that preceded them, video games communicate ideas—and even social messages—through many familiar literary devices (such as characters, dialogue, plot, and music) and through features distinctive to the medium (such as the player's interaction with the virtual world)."[169]

Tutt views the Court's failure to analyze the underlying code itself, and its focus on the analogous content between video games and more traditional entertainments, as indicative of a narrow standard: "*Brown's* test is probably best read as defining 'new speech' as that which is directly analogous in presentation and mode to 'old speech.'"[170] Tutt, however, makes too much of this holding. The Court does not at any point hold that it is identifying a new standard that conflicts with or narrows previous interpretations, such as those in *Roth*. Instead, the Court holds that it is *sufficient* for a finding of protected speech that new modes of expression are analogous to old modes. At no point does the Court suggest that it is *necessary* for the new mode to bear this resemblance. As the Court held, resemblance "*suffices* to confer First Amendment protection."[171] Even if resemblance was now necessary rather than sufficient, open

[166] *Brown, et al. v. Entertainment Merchants Assn. et al.*, 564 U.S. 786 (2011) https://supreme.justia.com/cases/federal/us/564/786/.
[167] *Sorrell, et al. v. IMS Health Inc., et al.*, 564 U.S. 552 (2011) https://supreme.justia.com/cases/federal/us/564/552/.
[168] *See*, *e.g.*, Andrew Tutt, *Software Speech*, 65 Stan. L. Rev. Online 72 (2012) https://www.stanfordlawreview.org/online/software-speech/.
[169] *Ibid.*
[170] *Ibid.*
[171] Emphasis added. *Brown, et al. v. Entertainment Merchants Assn. et al.*, 788.

source software would easily be analogous to scientific publications shared amongst experts, which are protected as speech.[172]

In *Sorrell*, the Court articulated a surprisingly broad standard of what constitutes protected speech. It found that the mere "creation and dissemination of information" constitutes speech within the meaning of the First Amendment.[173] *Sorrell* dealt with a law that "on its face" enacted "content- and speaker-based restrictions on the sale, disclosure, and use of prescriber-identifying information."[174] The Court found that a Vermont law limiting sales of and access to records of which medicines doctors prescribe "disfavors marketing, that is, speech with a particular content" and "disfavors specific speakers, namely pharmaceutical manufacturers."[175] Vermont contended that the sale, transfer, and use of prescriptions data was conduct and not speech (as we discussed earlier and will return to in the next section), but the Court rejected this argument out of hand, adding that:

> Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs. There is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes.[176]

The computer code within electronic cash and decentralized exchange systems is heavily laden with facts that advance human knowledge and allow us to conduct human affairs. If the essential factual nature of discrete logarithms was not well understood, to give one example, we would struggle to engage in any secure electronic conversations.[177] Bank records, government secrets, and copyrighted content would all be up for grabs if not for pioneering advances in the science of applied cryptography. These are advances that, by and large, have always been best uncovered and expressed in computer code.

Therefore, even though there is no conclusive holding from the Supreme Court on the specific topic of computer code's classification as protected speech, we can reasonably assume, based on older cases such as *Roth*[178] as well as recent holdings such as *Sorrell,* that the issue would be

[172] *See, e.g., FCC v. Pacifica Foundation*, 438 U.S. 726, 746 (1978) (words which lack literary, political, or scientific value are not entirely outside first amendment protection); *Miller v. California*, 413 U.S. 15, 34 (1973) ("The First Amendment protects works which, taken as a whole, have ... scientific value, regardless of whether the government or a majority of the people approve of the ideas these works represent."); *Roth v. United States*, 354 U.S. 476, 484 (1957) (quoting a letter of the Continental Congress identifying scientific progress as a reason for protecting speech).
[173] *Sorrell, et al. v. IMS Health Inc., et al.*
[174] *Ibid.*
[175] *Ibid.*
[176] *Ibid.*
[177] Kevin S. McCurley, "The Discrete Logarithm Problem," *Proceedings of Symposia in Applied Mathematics*, Vol. 42 (1990): pgs. 49-74, http://www.mccurley.org/papers/dlog.pdf.
[178] As the Court held in *Roth*, "all ideas having even the slightest redeeming social importance—unorthodox ideas, controversial ideas, even ideas hateful to the prevailing climate of opinion—have the full protection of the guaranties, unless excludable because they encroach upon the limited area of more important interests." *Roth v. United States*, 354 U.S. 476, 484, 77 S.Ct. 1304, 1 L.Ed.2d 1498 (1957).

non-contentious: it's protected. Setting aside the issue of expressive conduct vs. speech, every court of appeals to rule on this issue has held that code is protected expression worthy of at least some First Amendment protections.[179]

However, as we shall see in the next two sections, the finding that code is protected expression does not mean that it cannot be regulated. Much depends on the nature of the speech and the concomitant level of scrutiny that regulations impacting that speech will face.

B. Strict vs. Intermediate Scrutiny for Regulation of Protected Speech

As we have discussed, electronic cash and decentralized exchange software is protected under the First Amendment. However, not all protected expression is protected equally. For our purposes, there are two standards of review that courts may use to judge the constitutionality of laws regulating electronic cash or decentralized exchange software: strict scrutiny and intermediate scrutiny.

Strict scrutiny is formulated such that a law or regulation will be found unconstitutional unless it is "narrowly tailored to serve a compelling state interest."[180]

[179] For example, in *Universal City Studios v. Corley*, the Second Circuit held that "[c]ommunication does not lose constitutional protection as 'speech' simply because it is expressed in the language of computer code. Mathematical formulae and musical scores are written in 'code,' *i.e.*, symbolic notations not comprehensible to the uninitiated, and yet both are covered by the First Amendment." Similarly in *Junger v. Daley*, the Sixth Circuit explained that "[b]ecause computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment." *See*: *Universal City Studios v. Corley*, 273 F.3d 429 (2d Cir. 2001); *Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000).

[180] *See, e.g.*, *Austin v. Michigan Chamber of Commerce*, 494 U.S. 652, 655 (1990). Constitutional scholar Eugene Volokh has expertly captured the sweep of strict scrutiny jurisprudence. Eugene Volokh, Freedom of Speech, Permissible Tailoring and Transcending Strict Scrutiny, 144 U. Pennsylvania L. Rev. 2417 (1997). We will include the salient parts here:

As Volokh writes, "The Court has set forth four general principles related to compelling interests."

1. Compelling interests cannot privilege certain broad social or political interests over others. As Volokh has observed, "The mere interest in furthering a subset of [economic, social, and political] speech (for instance, labor picketing) "without more, cannot justify [a content-based] exemption" for such speech.
2. The fact that restricting speech would avoid offence or squelch unpopular and disagreeable ideas cannot be a compelling interest. Volokh offers flag burning as an example, citing *Texas v. Johnson*.
3. An interest may reveal itself as non-compelling if the government refused to pass laws that would more effectively address the issue. Volokh offers the example of an Illinois law that attempted to ban labor protests. When the state attempted to justify the law by virtue of ensuring residential privacy, the Court found the lack of similar laws addressing disruptive protests for other political causes evidence that the residential privacy interest was not compelling.
4. An interest may reveal itself as non-compelling if the government's attempt to address it is woefully underinclusive. Volokh cites a case wherein a law prohibiting criminals from publishing memoirs was justified as preventing criminals from profiting from their crimes. The Court found that there were so many other ways to prevent such profiting left unaddressed, that the government evinced a lack of seriousness with respect to its purported compelling interest.

Intermediate scrutiny, on the other hand, is an easier hurdle for laws and regulations to clear. As the Second Circuit found in *Universal City Studios, Inc. v. Corley*, under intermediate scrutiny:

> The regulation must serve a substantial governmental interest, the interest must be unrelated to the suppression of free expression, and the incidental restriction on speech must not burden substantially more speech than is necessary to further that interest.[181]

While this test may not appear drastically different from the strict scrutiny formulation above, in practice its application is significantly less charitable to speech. As constitutional scholar Ashutosh Bhagwat writes,

> [I]n applying intermediate scrutiny to reconcile governmental interests with free speech claims, the appellate courts have tended to systematically favor the government. Although the balance that the courts have drawn in individual cases is often perfectly defensible, and indeed may be an inevitable consequence of the form of analysis mandated by the intermediate scrutiny test, [we] show that the aggregate consequence of this governmental preference is the suppression of substantial amounts of important, socially valuable speech.[182]

Symbolic conduct, like burning a flag, is only entitled to intermediate scrutiny because of the obvious public safety issues inherent in actions rather than words. When the standard of review is intermediate scrutiny, laws regulating speech tend to be upheld as constitutional and speech can be suppressed.[183] Advocates for continued research and development of electronic cash and decentralized exchange software should not, therefore, accept that these tools are protected because they are symbolic conduct. Instead, they must argue that these tools are not conduct, but speech, and that their publication by developers is an entirely separate matter from their use by other persons to perform actions in the world. Aside from being more likely to garner strong constitutional protection, this approach is also correct.

With one exception, lower court judges have found that computer code is a hybrid of speech and conduct because it is "functional."[184] This a misguided approach that has not been adopted

Volokh, however, finds that the majority of strict scrutiny cases turn on the question of narrow tailoring, and recounts Court-articulated factors pertaining to that analysis:

1. A narrowly tailored law should, in fact, advance the compelling interest, but scientific proof is not required.
2. A narrowly tailored law must not restrict a significant amount of speech unrelated to the government interest.
3. If there is a less restrictive means to achieve the interest, then the law is not narrowly tailored.

[181] *Universal City Studios, Inc. v. Corley,* 273 F.3d 429 (2d Cir. 2001).

[182] Ashutosh Bhagwat, *The Test That Ate Everything: Intermediate Scrutiny in First Amendment Jurisprudence*, 2007 U. Ill. L. Rev. 783 (2007).

[183] *Id.*

[184] The exception is *Bernstein v. Dep't of State*, 176 F.3d 1132, 1136 (9th Cir.), *vacated for rehearing en banc*, 192 F.3d 1308 (1999), *available at* https://cr.yp.to/export/1996/1206-order.txt, *Cf. Universal City Studios, Inc. v. Corley*, *Junger v. Daley*, and *Karn v. US Dept. of State*, 925 F. Supp. 1 (D.D.C. 1996) https://law.justia.com/cases/federal/district-courts/FSupp/925/1/2294325/.

by the Supreme Court[185] and that should be avoided by electronic cash and decentralized exchange advocates.

For example, in *Junger v. Daley* the Sixth Circuit held that "[t]he fact that a medium of expression has a functional capacity should not preclude constitutional protection. Rather, the appropriate consideration of the medium's functional capacity is in the analysis of permitted government regulation."[186] At root, *Junger* suggests that if the code is functional then it is both conduct and expression. As expressive conduct, laws regulating its publication and distribution would be subject only to intermediate scrutiny thereby permitting more restrictive government regulation.

Some commentators[187] suggest that these lower court judges have misunderstood how software works by failing to understand the difference between source code, which is primarily used by developers to *express* new systems and share their ideas with other developers, and object code, the compiled form of source code that will actually trigger a computer to do something *functional*.[188]

Even if that was the case, and even if we accept that judges should be better at discriminating between the two types of code, why should object code be expressive conduct rather than speech? After all, object code is merely a unique and often important arrangement of digits or bits.[189] Returning to the musical metaphor, source code would be the composer's score, a piano roll would be the object code, and the player piano would be the computer. Object code can in fact be read by particularly sophisticated developers in order to understand a message.[190] Piano rolls too are used by musicians to share music; some may even be more adept at reading this

[185] *See Sorrell, et al. v. IMS Health Inc., et al.*

[186] *Junger v. Daley*.

[187] *See*: L Jean Camp, "Code as Speech: a discussion of Bernstein v. USDOJ, Karn v. USDOS, and Junger v. Daley in light of the U.S. Supreme Court's recent shift to Federalism" *Ethics and Information Technology*, March 2001. Vol. 1, No. 2 *available at* http://www.ljean.com/files/CODE_FEDERALISM.pdf
("Judge Gwin's assertion that 'source and object code are essentially interchangeable' is simply wrong. His very next statement that 'source code is not directly executable by a computer' exposes his error. The error in Judge Gwin's understanding of how software works is further exposed in the footnote of the previously quoted passage: 'Software in source code, a 'high level language,' is unintelligible to most, but it can be understood by computer scientists, mathematicians, programmers, and others with knowledge of the particular language in which the program is written.")(*citing Junger v. Daley*).
See also: Adrianna Oddo, *Being Forced to Code in the Technology Era as a Violation of the First Amendment Protection Against Compelled Speech* 67 Cath. U. L. Rev. 211 (2018) ("With respect to questions regarding computer code, courts must further distinguish whether the speech in question is source code or object code.").

[188] *Ibid.* L Jean Camp.

[189] It might look like this: 01101111 01110000 01100101 01101110 00100000 01110100 01101000 01100101 00100000 01110000 01101111 01100100 00100000 01100010 01100001 01111001 00100000 01100100 01101111 01101111 01110010 01110011.

[190] David S. Touretzky, "Source vs. Object Code, A False Dichotomy," *Carnegie Mellon University* (Jul. 12, 2000) https://www.cs.cmu.edu/~dst/DeCSS/object-code.txt.

style of musical notation than a traditional score.[191] Regardless of whether we're discussing dots and dashes on a roll of paper or 1s and 0s in a computer file,[192] how can the creation and dissemination of these unique arrangements of data be anything but the "creation and dissemination of information,"[193] which is the Supreme Court's standard for speech in *Sorrell*? The Oxford English Dictionary defines "information" as "what is conveyed or represented by a particular arrangement or sequence of things."[194]

Again, counter to the lower court in *Junger*, the Court in *Sorrell* felt no need to address Vermont's argument that prescription data was conduct, and held that "if the acts of 'disclosing' and 'publishing' information do not constitute speech, it is hard to imagine what does fall within that category, as distinct from the category of expressive conduct."[195]

In *Corley*, at least, the district court judge (who was praised and quoted heavily by the Second Circuit)[196] did not appear to misunderstand software but rather felt that the ease with which an otherwise purely expressive piece of source code could be compiled into object code and executed by the user of a computer meant that, for all intents and purposes, the code should be regulated as conduct as well as expression.

As the district judge wrote:

> Computer code, … no matter how functional, causes a computer to perform the intended operations only if someone uses the code to do so. Hence, one commentator, in a thoughtful article, has maintained that functionality is really 'a proxy for effects or harm' and that its adoption as a determinant of the level of scrutiny slides over questions of causation that intervene between the dissemination of a computer program and any harm caused by its use.
>
> The characterization of functionality as a proxy for the consequences of use is accurate. But the assumption that the chain of causation is too attenuated to justify the use of functionality to determine the level of scrutiny, at least in this context, is not.
>
> Society increasingly depends upon technological means of controlling access to digital files and systems, whether they are military computers, bank records, academic records, copyrighted works or something else entirely. There are far too many who, given any opportunity, will bypass those security measures, some for the sheer joy of doing it, some for innocuous reasons, and others for more malevolent purposes. Given the

[191] *See, e.g.*: "Boogie Woogie - Piano roll QRS #7882," *Pianola & Jazzy Stuff YouTube Channel* (Oct. 28, 2010) https://www.youtube.com/watch?v=biZdjPI9akY.
[192] As James Foust reminds me, this is more accurately described as "high and low voltage memory cells that represent 1s and 0s."
[193] *Sorrell, et al. v. IMS Health Inc., et al.*
[194] *Information*, Oxford English Dictionary Online (2019) http://www.oed.com/viewdictionaryentry/Entry/95568.
[195] *Sorrell, et al. v. IMS Health Inc., et al.*
[196] *Universal City Studios, Inc. v. Reimerdes*, 82 F.Supp.2d. 211 (S.D.N.Y. 2000) aff'd 273 F.3d 429 (2d Cir. 2001).

> virtually instantaneous and worldwide dissemination widely available via the Internet, the only rational assumption is that once a computer program capable of bypassing such an access control system is disseminated, it will be used.[197]

While that rationale appears sensible, it also means that the the perpetrator of the expressive conduct (executing the code) will be treated under the law as equivalent to the person who originally authored speech that was later used in that conduct. This has significantly more complicated consequences than the expressive conduct cases upon which these lower court judges rely where the only "speaker" in question is the person actually performing the conduct.

To illustrate the absurdity of this approach, let's apply the reasoning of these lower court opinions to the facts in *Texas v. Johnson,*[198] an expressive conduct case that used the *Spence* and *O'Brien* analysis to strike down state laws banning flag burning. According to the analysis in *Corley*, laws affecting Betsy Ross's freedom to stitch the first American flag would be judged using the same intermediate scrutiny as laws affecting Johnson's freedom to burn said flag in front of the 1984 Republican National Convention. It may be that we should judge both laws strictly and protect both forms of expression. However, it is absurd to suggest that Ross, in her solitary act of patriotic creativity, carries any responsibility for Johnson's potentially dangerous street protest. Flags have several uses other than being burned, and Ross surely did not have this future public safety hazard in mind when she was sewing. Diminishing Ross's First Amendment rights (by qualifying them with intermediate rather than strict scrutiny review) simply because her flag was subsequently used in a burning "slides over questions of causation,"[199] to quote the judge in *Corley*.

This is not a stretched metaphor in the context of electronic cash and decentralized exchange software. Just like flags, that software is capable of at least as many non-subversive and legal uses as it is subversive or illegal uses. Similarly, the author of that software will likely have as little knowledge or awareness of what people are actually doing with her code as a flag designer will know of her flags. It is more logically consistent to say that a software developer produces speech (strongly protected under standards from *Roth* and *Sorell*), and that any person who runs that code is engaged in conduct (expressive or not), which is less protected under standards from *O'Brien* and *Spence*.

As some scholars have remarked, the expressive conduct cases may be an attempt "to reconcile the constitutional promise of expressive freedom with the practical need for governmental regulation."[200] Surely this is true, and people who blow up buildings in order to express political views should not enjoy First Amendment protection from prosecution. But is it right to deny protections to researchers whose chemical descriptions of dynamite made it, all other things being equal, much easier for someone those researchers had never met to commit an act of

[197] *Ibid*.

[198] 491 U.S. 397 (1989)

[199] *Id.*

[200] Genevieve Lakier, *The Invention of Low-Value Speech*, 128 Harv. L. Rev. 1 (2015) https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=11976&context=journal_articles.

terror? Is it legitimate to police harmful conduct by denying constitutional rights to persons who had no knowledge of the crime or the criminal, nor any intent to facilitate the crime?

Nonetheless, three out of four lower courts looking at the question of whether software is speech have confused the analysis between speech and conduct. This confusion could perhaps be reconciled by suggesting that the *Corley* line of thinking represents some new form of judge-made contributory liability for software developers; again, the judge in *Corley* found that "functionality is really 'a proxy for effects or harm.'"[201] If this is true, then it is an unheard of form of contributory liability that does not require knowledge of- or intent to aid the illegal act, and can even go so far as to abrogate otherwise protected constitutional rights. After all, if I publish code in a textbook that could potentially be used to violate copyright law (say it decrypts content protected with digital rights management tools) but nobody ever uses it, then there's no conduct and, presumably, it's now just speech and should be afforded the strongest First Amendment protection. If, however, one person uses my code to violate someone's copyright, then I no longer receive my full First Amendment rights (through no fault or action of my own). This would, we believe, be a rather unprecedented constitutional construct with no support from Supreme Court jurisprudence that we can find.

Indeed, the judge's reasoning sounds more like policymaking in response to a changed world than it does constitutional interpretation. Perhaps these policy changes *are* necessary now that "society increasingly depends upon technological means of controlling access to digital files and systems."[202] But that decision would be up to Congress[203] or the States,[204] and if it involved abrogating established constitutional rights it would require an amendment to the Constitution.[205] That's a far cry from tweaking the test for what types of expression qualify for protection under intermediate or strict scrutiny review.

This conduct-speech confusion may also be understood if one assumes that these courts have begun their analysis with the wrong case law. *Corley*, *Junger*, and *Karn* all begin with the premise that one must look to the line of cases dealing with expressive conduct in order to determine whether the code in question is protected at all (under either strict or intermediate scrutiny). This prejudices the later question: is the expression worthy of intermediate or strict scrutiny? Again, the Supreme Court found no need to inquire into whether buying and selling data about prescriptions was conduct in *Sorrell*, but rather started from the proposition that the data was speech because it was information.[206]

The only lower court to avoid confusing conduct and speech in the context of software, the district court in *Berstein*,[207] articulated the strangeness of the alternative approach with

[201] *Universal City Studios v. Corley*.
[202] *Ibid*.
[203] U.S. Const. Art. I Sec. I.
[204] U. S. Const. Amend. X.
[205] U.S. Const. Art. V.
[206] *Sorrell, et al. v. IMS Health Inc., et al.*
[207] *Bernstein v. Dep't of State*, 176 F.3d 1132, 1136 (9th Cir.), *vacated for rehearing en banc*, 192 F.3d 1308 (1999), *available at* https://cr.yp.to/export/1996/1206-order.txt.

aplomb: “A computer program is so unlike flag burning and nude dancing that defendants' reliance on conduct cases is misplaced. It would be convoluted indeed to characterize [code for an encryption program] as conduct in order to determine how expressive it is when, at least formally, it appears to be speech.”[208]

Putting this all together:

1. Electronic cash and decentralized exchange software is assuredly some kind of protected expression, either expressive conduct or mere speech.[209]
2. Expressive conduct receives weakened protection from regulation under intermediary scrutiny while plain speech receives robust protection under strict scrutiny review.[210]
3. Electronic cash and decentralized exchange software is published to express facts that advance human knowledge and allow us to conduct human affairs.[211]
4. This publication is entirely separate from the execution of the code by users when they make electronic cash transactions or conduct decentralized exchanges.[212]

Therefore, the publication of electronic cash and decentralized exchange software is protected as plain speech rather than expressive conduct, and it follows that laws governing its publication are subject to strict scrutiny review. In the final section we will look at how that review could unfold if regulators attempted to ban, require licensure for, or compel the inclusion of surveillance backdoors in the publication of electronic cash or decentralized exchange software.

C. Regulating Publication of Electronic Cash and Decentralized Exchange Software

First, an aside: We do not argue that electronic cash and decentralized exchange are wholly unregulated activities. Several activities, when performed using cryptocurrencies or smart contracts, are certainly regulated (*e.g.* accepting and transmitting cryptocurrency on behalf of others,[213] issuing new cryptocurrencies in a public sale with promises of future efforts to create profits,[214] trading cryptocurrency derivatives such as swaps or futures[215]) and several activities are simply illegal (laundering the proceeds of crime through cryptocurrency networks,[216]

[208] *Ibid.*

[209] *See supra* part IV. A. i. Computer Code Expresses Ideas for Political and Social Change, pp. 33-35.

[210] *See supra* part IV. B. Strict vs. Intermediate Scrutiny for Regulation of Protected Speech, pp. 39-45.

[211] *See supra* part IV. A. iii. Electronic Cash and Decentralized Exchange Software Are Protected Speech, pp. 37-39.

[212] *See supra* part IV. B. Strict vs. Intermediate Scrutiny for Regulation of Protected Speech, pp. 39-45; and part II. C. Electronic Cash and Decentralized Exchange are Powered by Software, pp. 15-17.

[213] US Department of the Treasury, Financial Crimes Enforcement Network, “Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies,” Guidance FIN-2013-G001 (Mar. 18, 2013)
https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdfFincen Guidance

[214] *SEC v. Howey Co.*, 328 U.S. 293 (1946), https://supreme.justia.com/cases/federal/us/328/293/; Peter Van Valkenburgh, “Framework for Securities Regulation of Cryptocurrencies,” *Coin Center* (Aug. 2018) https://coincenter.org/entry/framework-for-securities-regulation-of-cryptocurrencies.

[215] 7 U.S.C. ch. 1 §§ 4a-27f.

[216] 18 U.S.C. 1960.

sending cryptocurrencies to sanctioned persons[217]). Merely developing and publishing cryptocurrency software, however, is not at present an activity that triggers any regulation.

Electronic cash and decentralized exchange software is, to put it mildly, radically new. And like many new things, existing laws did not contemplate it, let alone prohibit or regulate it. A fundamental premise in Anglo-Saxon common law is *nulla poena sine lege* or "no penalty without law." As it stands, writing this type of software is not the subject of law and therefore it is, of course, allowed.

As discussed, the emergence of electronic cash and decentralized exchange will make transacting using cryptocurrencies more private and will, in many cases, eliminate the need to use BSA-regulated institutions in order to move from one cryptocurrency to another. If policymakers seek to subject these activities to greater financial surveillance, they will need to find new parties to regulate. As discussed earlier, regulating software developers as Financial Institutions under the BSA would result in a warrantless search and seizure violating the Fourth Amendment rights of the users of these networks. Without the ability to deputize these developers as agents of the U.S. financial surveillance regime, we can imagine calls to place restrictions on the publication and dissemination of electronic cash and decentralized exchange software.

To our knowledge, no policymaker has yet proposed a ban on, a licencing requirement for, or the compelled inclusion of a surveillance backdoor in the publication of electronic cash and decentralized exchange software. Nonetheless, should a law or regulation be put in place that attempts to do so, it would be unconstitutional under the First Amendment.

i. Banning Publication Would be Unconstitutional

Electronic cash and decentralized exchange software is constitutionally protected speech. Like all computer code, it should be understood properly as unadulterated speech and not as expressive conduct.[218] Supreme Court precedent provides no grounds for treating it as expressive conduct. Indeed, *Sorrell* advocates for pure speech treatment for data that is significantly less communicative.[219] Lower court opinions to the contrary engage in a dangerous process of judicial policymaking.[220] The emergence of electronic cash and decentralized exchange, as well as myriad other marvels of the still-recently connected world, may well necesitate new tradeoffs. But where those tradeoffs deal in policy they should be made by

[217] *See*: Office of Foreign Assets Control, "OFAC FAQs: Sanctions Compliance," *Department of Treasury*, https://www.treasury.gov/resource-center/faqs/sanctions/pages/faq_compliance.aspx ("Yes, the obligations are the same [for virtual currency.] U.S. persons...must ensure that they block the property and interests in property of persons named on OFAC's SDN List or any entity owned in the aggregate, directly or indirectly, 50 percent or more by one or more blocked persons, and that they do not engage in trade or other transactions with such persons.").
[218] *See supra* IV. A. Computer Code is Protected Speech, pp. 33-39.
[219] *Ibid*.
[220] *Id*.

Congress, and where those tradeoffs weaken constitutional rights they must be made through the process of constitutional amendment.

Regulations or laws that would ban the development or publication of electronic cash and decentralized exchange software would be prior restraints on speech. Prior restraint refers to restrictions on publication or distribution of speech made by government in advance of that publication or distribution. It can be contrasted with punishment-after-the-fact, wherein publication is allowed to proceed but may carry legal liability should the speech prove unprotected and unlawful. Regulations imposing prior restraint are usually unconstitutional and face extreme scrutiny. As the Supreme Court held in *Bantam Books v. Sullivan*, "Any system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity."[221]

To rebut this presumption, the government faces strict scrutiny review of their policy. Again, this almost always means that the policy will be found unconstitutional. Nevertheless, we will run through the analysis here. Under strict scrutiny the government must prove that the ban is narrowly tailored to achieve a compelling interest.[222] A narrowly tailored policy must, in fact, advance the stated interest, it must not restrict a significant amount of speech unrelated to the interest, and there must not be a less restrictive means to achieve the interest.[223] The government may fail to show that its interest is compelling if the policy appears transparently incapable of achieving that interest,[224] and the government's interest cannot be an interest in privileging certain scientific and political ideas over others, even if this would, indeed, be compelling to government.[225]

Electronic cash and decentralized exchange software includes a broad class of published research and innovations with far-reaching potential to alter the way we organize society. Its developers and advocates genuinely believe that these scientific and engineering advances will, on net, improve the human condition and better guarantee human dignity and individual autonomy than alternative centralized and surveillance-accommodating tools for payments and exchange.[226]

A primary motivation behind the development of this technology is the global decline of cash transactions (which are inherently private and lacking in intermediaries).[227] This decline has been matched with the rise of powerful, private financial technology intermediaries that can systematically surveil their users and arbitrarily exclude them from economic life simply by closing their account. Such private surveillance and arbitrary power, argue electronic cash

[221] *Bantam Books v. Sullivan*, 372 U.S. 58, 70 (1963).

[222] Eugene Volokh, "Freedom of Speech, Permissible Tailoring and Transcending Strict Scrutiny," 144 U. Pennsylvania L. Rev. 2417 (1997). *Available at* http://www2.law.ucla.edu/volokh/scrutiny.htm#12.

[223] *Ibid.*

[224] *Ibid.*

[225] *Ibid.*

[226] Jerry Brito, "The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society," *Coin Center* (Feb. 2019) https://coincenter.org/entry/the-case-for-electronic-cash.

[227] *Ibid.*

advocates, contravenes the rule of law. In nation states with weaker human rights guarantees, governments can and are actively partnering with these intermediaries to obtain greater control over their populations.[228] If cash disappears, advocates claim, only electronic cash and decentralized exchange technologies can serve as a safety valve against imminent payments-technology-enforced totalitarianism.[229]

One does not need to personally subscribe to these views in order to grasp the gravity of the constitutional law at hand. It is sufficient to believe that electronic cash and decentralized exchange software developers earnestly believe these views and publish their software to express them (rather than for some other cynical purpose). If this much is true, then bans on software publication wade dangerously into the territory of stifling a vibrant and consequential debate.[230]

Government may present its compelling interest for a ban as the prevention of crime, terrorism, or money laundering, rather than as an impermissible interest in stifling such debate. Other less restrictive policies, however, would both better advance that interest and burden substantially less speech. Banning publication would not prevent money launderers, terrorists, or criminals from using previously published or international versions of electronic cash or decentralized exchange software. The narrow way to address crime, terrorism, and money laundering is to more aggressively investigate, pursue, and apprehend money launders, terrorists, and criminals, not to ban dissemination of tools that criminals may use in their crimes, especially if those tools have non-criminal uses and if the developers have altruistic motivations and no knowledge of or intent to facilitate crime.

Courts have found that a policy's evident failure to effectively address the stated government interest is often indicative of there being some other undisclosed and impermissible government interest at play.[231] Again, a ban on electronic cash would self-evidently be an attempt to stifle the development of these tools and the beliefs that motivate that development. Such a ban thus privileges certain scientific and political ideas over others, and that cannot be an acceptable government interest.[232]

[228] *Id.*

[229] *Id.*

[230] *C.f.* Abrams v. United States, 250 U.S. 616, 630 (1919)(Holmes, J., dissenting) ("Persecution for the expression of opinions seems to me perfectly logical. If you have no doubt of your premises or your power and want a certain result with all your heart you naturally express your wishes in law and sweep away all opposition...But when men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas... . The best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out.")

[231] *See Florida Star v. B.J.F.*, 491 U.S. 524, 542 (1989) (Scalia, J., concurring in part and in the judgment); *Carey v. Brown*, 447 U.S. 455, 465 (1980).

[232] *See Carey*, 447 U.S. at 467; *see also* Consolidated Edison Co. v. Public Serv. Comm'n, 447 U.S. 530, 537-38 (1980).

Government interest aside, a ban would not qualify as a narrowly tailored policy. A narrowly tailored policy must not restrict a significant amount of speech unrelated to the government interest. Electronic cash and decentralized exchange promise a multitude of legitimate uses—not the least of them being a bulwark against totalitarian regimes.[233] Significant research, creativity, and non-criminal, non-money-laundering activities would be stopped or significantly chilled here in the U.S. if such a ban was to occur. Assuredly, some, if not most, electronic cash and decentralized exchange users are not engaged in crimes but simply want to try new technologies and protect their privacy and security. A ban would deprive this audience of the research and innovations provided by developers at least as much, if not more, than it would deny these tools to criminals, who would be less reticent to find and use a banned technology. The primary result would be a massive reduction in the freedom of law-abiding citizens. This is not narrow tailoring. As Justice Douglas wrote in the Fourth Amendment context, "I am not yet ready to agree that America is so possessed with evil that we must level all constitutional barriers to give our civil authorities the tools to catch criminals."[234]

Lacking narrow tailoring and a convincingly compelling government interest, a blanket ban on the publication of electronic cash and decentralized exchange software would be unconstitutional.

ii. Licensing Regimes for Publication Would be Unconstitutional

A licensing regime is not a ban *per se*, and we can imagine a law or regulation that purported not to ban the publication of electronic cash and decentralized exchange software but merely license it. Perhaps the regulator would grant licenses only to software that included backdoors to enable surveillance of the resultant cryptocurrency networks, or perhaps the license would only be granted to certain 'qualified' developers as judged at regulator's discretion. These licensing schemes, however, would be unconstitutional for the same reasons that an out-and-out ban would be unconstitutional.

Speech licensing schemes, although they are not blanket bans, remain clear examples of regulations imposing prior restraint. As the Supreme Court held in *Lakewood v. Plain Dealer Publishing Co.*, "even if the government may constitutionally impose content-neutral prohibitions on a particular manner of speech, it may not condition that speech on obtaining a license or permit from a government official in that official's boundless discretion."[235]

The Supreme Court set out three factors for determining the constitutionality of licensing schemes in *Freedman v. Maryland*:

[233] *See* Jerry Brito, "The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society," *Coin Center* (Feb. 2019) https://coincenter.org/entry/the-case-for-electronic-cash; and Alex Gladstein, "Why Bitcoin Matters for Freedom" *Time* (December 28, 2018) http://time.com/5486673/bitcoin-venezuela-authoritarian/.

[234] *California Bankers Assn. v. Shultz*. (Douglas, J., dissenting).

[235] *Lakewood v. Plain Dealer Publ. Co.*, 486 U.S. 750 (1988) https://supreme.justia.com/cases/federal/us/486/750/.

1. Any restraint must be for a specified brief period of time,
2. There must be expeditious judicial review,   and
3. The censor must bear the burden of going to court to suppress the speech in question and must bear the burden of proof.[236]

One of the lower court cases dealing with restrictions on distributing encryption code, *Bernstein v. Dep't of State*, analysed prior restraint and the constitutionality of a software publishing licencing scheme under the Arms Export Control Act (AECA) and its implementing regulations, the International Traffic in Arms Regulations (ITAR). The judge in *Bernstein* looked to the *Freedman* factors and found that the licensing scheme was unconstitutional.[237]

In *Bernstein*, the licensing scheme lacked any real standard or process of review apart from the discretion of the censor.[238] But even if there was a clear standard and process of review for our hypothetical scheme to limit publication of electronic cash and decentralized exchange software, conditioning approval on the presence of surveillance backdoors would be unconstitutional.

According to *Freedman*'s third factor, the censor bears the burden of going to court and defending every restraint on publication (*i.e.* denied license), and—in our hypothetical—each denial is predicated merely on the fact that the software does not incorporate a backdoor for identifying users. Therefore, each license denial and subsequent review should unfold as if it were a content-based ban on speech.

As discussed in the previous section, such a ban self-evidently seeks to privilege certain scientific and political ideas over others.[239] Each ban is a deliberate attempt to stymie valuable discussion concerning whether (both technologically and politically) we can and should have the ability to transact privately or exchange valuables over the internet without the need to rely

[236] *Freedman v. Maryland*, 380 U.S. 51 (1965) https://supreme.justia.com/cases/federal/us/380/51/.

[237] *Bernstein v. Dep't of State*, 176 F.3d 1132, 1136 (9th Cir.), *vacated for rehearing en banc*, 192 F.3d 1308 (1999), *available at* https://cr.yp.to/export/1996/1206-order.txt.
"The ITAR scheme, a paradigm of standardless discretion, fails on every count. This court finds nothing in the ITAR that places even minimal limits on the discretion of the licensor and hence nothing to alleviate the danger of arbitrary or discriminatory licensing decisions. Pt. 123, lays out an extensive list of requirements for those seeking a license but places no constraints on the ODTC in approving or denying a license. First, there is no limit to the time in which the ODTC must make a licensing decision. Second, not only does the ITAR not provide for judicial review of licensing decisions, prompt or otherwise, the AECA makes the initial designation of items as defense articles unreviewable. ... Finally, given there is no recourse for someone denied a license, there is no burden on the ODTC to go to court to justify the denial. Moreover, applications for licenses can be disapproved and approved licenses can be revoked, suspended or amended without prior notice in the interests of national security or whenever it "is otherwise advisable". ... While the court is mindful of the problems inherent in judicial review of ODTC licensing decisions regarding cryptographic software, both with respect to the sophistication of the technology and the potentially classified nature of the licensing considerations, there must still be some review available if the export controls on cryptographic software are to survive the presumption against prior restraints on speech." *Id.*

[238] *Id.*

[239] *See supra* IV. B. Strict vs. Intermediate Scrutiny for Regulation of Protected Speech pp. 39-45.

on a trusted intermediary. There is nothing inherently illegal with making a private payment or trading a valuable asset, and the mere publication of information that enables or describes how one might enable those activities is, by its nature, an act of scientific and political discussion. As with a blanket ban, a licensing restriction would face strict scrutiny review and be found unconstitutional for its lack of a truly compelling interest and narrowly tailored approach to achieving that interest.

iii. Compelling Developers to Write Backdoors Would be Unconstitutional

Courts have long imposed a strong presumption against the constitutionality of any content-based ban on speech.[240] A similar presumption exists against laws that would compel persons to speak content they would otherwise avoid.[241] As Justice Jackson wrote in *West Virginia State Board of Education v. Barnette*, “If there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion or force citizens to confess by word or act their faith therein.”[242] *Barnette* concerned a state school board requirement that students must salute the flag at the start of each school day; the court found this requirement to be unconstitutionally compelled speech.

As with bans and licensing, however, the question of whether the expression being compelled is conduct or speech is often the decisive factor. In *Rumsfeld v. Forum for Academic and Institutional Rights, Inc.*, for example, the court acknowledged as true “the principle that freedom of speech prohibits the government from telling people what they must say.”[243] The Court, nonetheless, upheld an order that compelled schools to include military recruiters at job fairs. The Court reasoned that the order compelled schools to engage in conduct rather than the expression of a view. Schools would need to admit these military recruiters to their fairs alongside any other employers they invited, but they were not required to express any endorsement or approval of military employment. Thus, the order faced only intermediate scrutiny, and, as is typical with intermediate scrutiny in speech cases, it was upheld as constitutional.

Rumsfeld underscores the need to correctly analyze electronic cash and decentralized exchange software as speech rather than conduct, following Supreme Court precedent rather than the lower court opinions in *Corley*, *Junger*, and *Karn*, as discussed earlier.[244] Under such an analysis, a law compelling developers to publish software of a certain specification would face strict scrutiny and the state would bear the burden of proving that the law is narrowly tailored to achieve a compelling interest.

[240] *Bantam Books v. Sullivan*, 372 U.S. 58, 70 (1963).

[241] *West Virginia State Bd. of Educ. v. Barnette*, 319 U.S. 624 (1943) https://supreme.justia.com/cases/federal/us/319/624/.

[242] *Ibid.*

[243] *Rumsfeld v. Forum for Academic and Institutional Rights, Inc.*, 547 U.S. 47 (2006) https://supreme.justia.com/cases/federal/us/547/47/.

[244] *See supra* part IV. B. Strict vs. Intermediate Scrutiny for Regulation of Protected Speech, pp. 39-45.

An order that developers must write code that includes surveillance backdoors is tantamount to forcing developers to express a particular view in ongoing political and societal debates over privacy and security. Developers publish electronic cash and decentralized exchange software because they fervently wish to teach others *how* these private and person-to-person interactions are technologically possible and *why* they are essential to preserving human dignity and individual autonomy. Forcing such a developer to publish software that does the opposite—that compromises both the privacy of transacting parties with information-sharing and the autonomy of parties by reintroducing an intermediary—goes well beyond a simple order instructing a child to salute a flag. It is on par with forcing an academic to recant their previously published research and publish new, bogus research in its place or forcing a political organizer to condemn her constituency and form an opposition party. To paraphrase Justice Jackson, it prescribes what shall be orthodox in payments technology and forces developers to confess by word and act their faith therein.

An order to write such software is at least as coercive as an order that private parade organizers must include participants who would express beliefs not shared by the organizer[245] or an order that drivers must display the state motto on their license plate even if they find it objectionable.[246] In all of these cases, the court has consistently held that the order at issue is unconstitutional.[247]

As with a ban or license requirement, such an order would not be narrowly tailored—by forcing participants in a genuine debate to express views counter to their own, it would profoundly impact ongoing discussions about privacy and security, cause persons not engaged in any illegal act to use tools they otherwise would avoid, and introduce vulnerabilities into those tools that could be exploited by malicious persons other than the government.

As with a ban or license requirement, such an order would also fail to achieve the government interest at stake: uncompromised software would continue to be available to criminals via the internet, and privacy-protecting tools would be denied to those who are law abiding citizens. The government has a strong interest in preventing crime and money laundering. However, compelling hundreds or thousands of law-abiding developers of electronic cash and decentralized exchange software to affirm views they do not genuinely hold and publish

[245] *See, e.g.*, *Hurley v. Irish-American Gay, Lesbian, & Bisexual Group of Boston*, 515 U.S. 557 (1995).
[246] *See, e.g.*, *Wooley v. Maynard,* 430 U.S. 705 (1977).
[247] The compelled speech doctrine does have a narrow exemption that allows the state to order businesses to make "purely factual and uncontroversial information" disclosures about their products. This is why, for example, mandatory cigarette health warnings and nutrition fact labeling is constitutional. An order to publish software with surveillance backdoors is, however, expressive rather than factual and it would be anything if not uncontroversial. Indeed, even in the context of cigarettes, certain mandatory labeling efforts have been found non-factual and therefore unconstitutional. This is why American cigarette cartons lack the graphic photos of smoking-related disease that often can be found on cartons internationally. *See Zauderer v. Office of Disciplinary Counsel of Supreme Court of Ohio*, 471 U.S. 626 (1985)

software they would never otherwise write is not a narrowly tailored approach to addressing those ills.

V. Conclusion

Electronic cash and decentralized exchange software development is essential for preserving human dignity and autonomy as the world moves increasingly toward fully intermediated payments technologies like Alipay or Wechat.[248] This report explained why anonymous electronic cash and decentralized exchange software is the endgame for all cryptocurrency networks, and how this evolution will result in much less publicly available information about cryptocurrency transactions. Postulating that this shift could trigger calls for more aggressive financial surveillance policies, we analyzed why two potential policy responses would be unconstitutional:

1. Regulating cryptocurrency software developers and individual users of that software under the Bank Secrecy Act, a federal surveillance statute, would be unconstitutional under the Fourth Amendment because it would be a warrantless search and seizure of information private to cryptocurrency users.
2. Furthermore, any law or regulation attempting to ban, require licensing for, or compel the altered publication (*e.g.* backdoors) of cryptocurrency software would be unconstitutional under First Amendment protections for speech.

We looked at over fifty years of U.S. case law, uncovering long-ignored questions about how the Fourth Amendment's warrant requirement can and cannot be reconciled with the Bank Secrecy Act, and why there is reason to doubt the full constitutionality of that law as currently applied. We investigated why lower court opinions from the Crypto Wars of the 1990s[249] are often misguided (even though many did protect encryption code as speech) and why recent Supreme Court case law provides a more robust shield against any attempt to regulate persons who are merely engaged in developing software.

There are many activities performed using electronic cash and decentralized exchange software that will be regulated, and some uses that will even be illegal. Nonetheless, an aggressive attempt to regulate software developers and individual users, as postulated in this report, would be a severe and unconstitutional overreach into our privacy and speech rights. Drawing that line will mean reduced tools for crime fighters and regulators, but that tradeoff has always been fundamental to American values and to open societies.

[248] *See*: Jerry Brito, "The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society," *Coin Center* (Feb. 2019) https://coincenter.org/entry/the-case-for-electronic-cash; and Alex Gladstein, "Why Bitcoin Matters for Freedom" *Time* (December 28, 2018) http://time.com/5486673/bitcoin-venezuela-authoritarian/.

[249] Specifically, *Universal City Studios, Inc. v. Corley* , *Junger v. Daley*, and *Karn v. US Dept. of State*. The Crypto Wars refers to broad debates over regulation of encryption in the 1990s. *See generally,* Paul Detrick, "How Government Lost the Crypto Wars (At Least for Now)" *Reason* (Mar. 1, 2018) https://reason.com/reasontv/2018/03/01/crypto-wars-how-encryption-went-mainstre.

As Benjamin Franklin put it, “Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.”[250] And as Justice Douglas remarked in a dissenting opinion in the case that found the Bank Secrecy Act to be constitutional: “I am not yet ready to agree that America is so possessed with evil that we must level all constitutional barriers to give our civil authorities the tools to catch criminals.”[251]

Nor does this report suggest that law enforcement should have *no* path to the information it needs to investigate crime effectively. However, the correct path involves particular suspicion and a judge-granted search warrant, not the indiscriminate collection of electronic data or an order to developers that they must weaken the tools they work so diligently to make secure. As Justice Clark wrote in a case finding warrantless electronic eavesdropping unconstitutional,

> [W]e cannot forgive the requirements of the Fourth Amendment in the name of law enforcement. … [I]t is not asking too much that officers be required to comply with the basic command of the Fourth Amendment before the innermost secrets of one’s home or office are invaded. Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices.[252]

And as Justice Douglas wrote,

> It would be highly useful to governmental espionage to have like reports from all our bookstores, all our hardware and retail stores, all our drugstores. These records too might be ‘useful’ in criminal investigations.
>
> One's reading habits furnish telltale clues to those who are bent on bending us to one point of view. What one buys at the hardware and retail stores may furnish clues to potential uses of wires, soap powders, and the like used by criminals. A mandatory recording of all telephone conversations would be better than the recording of checks under the Bank Secrecy Act, if Big Brother is to have his way.
>
> The records of checks—now available to the investigators—are highly useful. In a sense, a person is defined by the checks he writes. By examining them, the agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, the papers and magazines he reads, and so on ad infinitum. These are all tied to one's social security number; and now that we have the databanks, these other items will enrich that storehouse and make it possible for a bureaucrat—by

[250] “Franklin’s Contributions to the Conference on February 17: Four Drafts, 1775,” Founders Online, National Archives, version of January 18, 2019, https://founders.archives.gov/documents/Franklin/01-21-02-0269. [Original source: The Papers of Benjamin Franklin, vol. 21, January 1, 1774, through March 22, 1775, ed. William B. Willcox. New Haven and London: Yale University Press, 1978, pp. 495–499.]

[251] *California Bankers Assn. v. Shultz* (Douglas, J., dissenting).

[252] *Berger v. New York* at 60.

> pushing one button—to get in an instant the names of the 190 million Americans who are subversives or potential and likely candidates.[253]

The world Douglas described is now real, embodied by China and other repressive surveillance states that depend on financial intermediaries for their window into peoples' lives.[254] Fortunately, America has yet to fully travel down this road and our constitution bars us from choosing that path whenever moral panics over new technologies drive some to seek safety and control over human dignity and individual autonomy.

Appendix: Building Electronic Cash and Decentralized Exchange Software

These technologies *are truly novel* and therefore it is essential to understand, at least on a surface level, what they do, how they function, who builds them, and what that building process entails, in order to comprehend the relevant statutory and constitutional law at play. We will begin with an overview of the objectives behind developing cryptocurrency software, then move to a description of early attempts at achieving electronic cash, and finally progress to newer tools.

This Appendix is not intended to be a technical audit of any of the projects described below. We will often take the claims of the developer communities building these tools at face value in order to analyze the legal and regulatory consequences that would stem from those claims. No one should read this Appendix hoping to learn which tools are most likely to guard their privacy or which cryptocurrencies are wise investments. This Appendix is, instead, aimed at helping policymakers and regulators come to grips with the emergence of electronic cash and decentralized exchange and helping them understand why several of these technologies lack typically surveilled administrators or typically surveillable public data.

Integrity and Privacy: The Quarrelsome Core Design Goals of Cryptocurrencies

Much of the usefulness of open blockchain networks and the cryptocurrencies they can power stem from two guarantees of integrity that these systems generally offer their users:

1. **Integrity of Scarcity**: Digital units described by a blockchain cannot be duplicated or counterfeited. They are created only according to ex-ante specified rules in the protocol. The fact that there will only ever be as many as described in these rules makes them economically scarce and rivalrous, more like gold or silver than abundant and non-rivalrous goods like atmosphere or sunlight.

   For example, according to the Bitcoin protocol, new bitcoins are only ever created when

[253] *California Bankers Assn. v. Shultz* (Douglas, J., dissenting) at 84.

[254] *See*: Jerry Brito, "The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society," *Coin Center* (Feb. 2019) https://coincenter.org/entry/the-case-for-electronic-cash; and Alex Gladstein, "Why Bitcoin Matters for Freedom" *Time* (December 28, 2018) http://time.com/5486673/bitcoin-venezuela-authoritarian/.

they are released to miners who provide a valid proof-of-work. They are released according to a schedule that is roughly 50 coins every 10 minutes for four years, then half that every 10 minutes for the next four years, and then halving again and again every four years until new coin creation is insignificant and the total supply is just short of 21 million coins in total. Bitcoins cannot be created any other way and once created they cannot be duplicated.

2. **Integrity of Provenance**: Digital units described by a blockchain can be transferred person to person but they can only be sent by persons who have previously received them. A transfer of a bitcoin should be trusted in the same manner that a transfer of a deed to land is trusted: because the record of previous ownership and transfers has integrity going back through history all the way to the beginning of the asset.

   There are, however, no real-life identifiers in the blockchain, therefore this guarantee is more accurately stated as: digital units can be transferred from one pseudonymous address to another, but only addresses that have previously received units can send them to other addresses and a verifiable digital signature proving control over the sending address is required for the transaction to be valid. You can't send someone else's coins unless you steal their cryptographic credentials and can create that verifiable digital signature.

   For example, Bitcoin uses addresses that are derived from public keys in elliptic curve cryptography (ECC) key pairs.[255] A bitcoin address is like a username and the corresponding ECC private key is like a password. To make a valid Bitcoin transaction the user must specify which bitcoins they are using to fund the transaction (inputs) and sign a message with the private key or keys that correspond to the bitcoin address or addresses which previously received those coins. This signed transaction message must also describe the bitcoin address or addresses the sender wishes to be the recipient of the transaction and the amount or amounts she wishes to send. The recipient can then send those coins to a future recipient by proving control over that corresponding private key, and so on and so forth.

These twin goals—integrity of scarcity and integrity of provenance—are at the core of public blockchain technology. Other digital assets (*e.g.* copyrighted music or money in a savings account) rely on trusted third parties (*e.g.* banks or governments) to guarantee scarcity and provenance. Bitcoin's invention is significant because it represents the first time that a *digital* asset can be relied upon as scarce and a transfer as having provenance without the need to trust

[255] ECC key pairs are widely used across the internet and other computing systems for authentication. They consist of two very large numbers: a random but unique number called a private key and the corresponding public key that is derived from the private key by elliptic curve point multiplication. This transmutation of the private key into the public key is a mathematical operation that is easy to perform in one direction (private key => public key) but so difficult to perform in reverse (public key => private key) that it is effectively impossible (even with supercomputers or computers likely to be developed in the future should trends continue).

a third party. Less like downloading a licensed Kindle e-book from Amazon, more like accepting a gold coin in the hand. Speaking generally, however, open blockchain networks also attempt to offer two additional guarantees, beyond integrity of scarcity and provenance, to their users:

3. **Privacy**: Transfers of digital units should not unnecessarily reveal to the general public the identities and full transaction histories of the participants. Many projects wish to enable users to be public when they wish to make public declarations: *e.g.* a tax-exempt non-profit could prove that their donations are being spent on projects that further their charitable purpose.

   In general, however, payment systems—even blockchain-based ones—should not reveal to the general public every transaction by default. No one wants their every purchase of a politically tendentious book or their every receipt of a holiday bonus to be instantly and always public knowledge.

4. **Fungibility**: Digital units should be indistinguishable from one another and be of equal value. Some blockchain networks now enable users to create and trade deliberately non-fungible tokens that are sought as unique collectibles. In general, however, the primary goal behind most systems is the creation of digital cash or other fungible financial instruments like equity shares or subway tokens. Cash and other fungible instruments work efficiently in economies because the recipient of the note can reasonably assume that it is equal in value to all others of the same denomination. This minimizes transaction costs associated with uncertainty and subjective valuation.

   Without fungibility, the recipient would need to investigate the full history of the asset, be on the lookout for defects in quality or in legal title, and contemplate the unique attributes that could make this particular unit either especially risky or peculiarly undervalued as compared to others of its kind. With fungibility, all units are the same and no such costly appraisal or assumption of risk is necessary. The inability to distinguish one unit from another is what fosters this fungibility.

Perceptive readers may have already noticed the potential for contradiction between our so-called core goals and these additional goals. Integrity of scarcity and provenance rely on verifiable public knowledge about the entire history of all digital unit minting and transfer activities. Else how could we know that the supply is finite and that the units we’ve received have a bona fide origin?

Privacy and fungibility, however, rely on these same records being either concealed or never recorded from the start. How can the system be private if the general public learns my specific transaction history along with the full history of the network? And how can the digital units be fungible if that history reveals unique facts about the history of the particular units I have just received?[256]

How public blockchain projects balance these goals or find ways of achieving them simultaneously is key to understanding the technological landscape and the motivations of those who work tirelessly to improve it. We now present a short history and a brief look into the future.

Early Attempts at Electronic Cash

Satoshi Nakamoto, Bitcoin's pseudonymous inventor, understood the tradeoff between integrity and privacy even before they published the Bitcoin network software. In the 2008 white paper, Nakamoto wrote:

> The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method[.][257]

Bitcoin's blockchain is deliberately transparent in order to guarantee integrity across the entire transaction history of the network. Every bitcoin transaction that has ever occured is listed in the blockchain such that users can be assured that all transactions follow the consensus rules of the protocol. Again, there are no human-readable names in the Bitcoin blockchain but there are persistent Bitcoin addresses associated with all transactions. These addresses are effectively pseudonyms, and they can be linked to real persons and used to track their payment history on the blockchain.

Nakamoto stressed the importance of avoiding this linkage between real-world identifying information and bitcoin address pseudonyms:

> [P]rivacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone.[258]

And Nakamoto ultimately admitted that a lack of privacy would likely be a very real risk to Bitcoin users:

[256] For example, imagine I have just received 10 units in a blockchain transaction. What if the same 10 units were fraudulently pledged as collateral in a loan obtained by a person who held them some 3 transactions earlier in the history of the blockchain? I do not know this person and obtained the units in an entirely legal and non-fraudulent exchange. Who has the better claim on these units that I hold today through no fault of my own? Me or the bank attempting to foreclose on collateral? Are these tainted digital units worth less than pristine units? Their unique history could mean they now come with a risk discount and their fungibility has been eroded.

[257] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," (Oct. 31, 2008) https://bitcoin.org/bitcoin.pdf.

[258] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," (Oct. 31, 2008) https://bitcoin.org/bitcoin.pdf.

> Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.[259]

Nakamoto's concerns were justified. Ten years on and a typical Bitcoin user should expect effectively no privacy when they transact using Bitcoin. Here is why.

Many if not the majority of Bitcoin users transact via cryptocurrency exchanges rather than directly through the peer-to-peer network. These exchanges generate addresses for their users and collect bank-grade know-your-customer (KYC) information about their users. An exchange can match that KYC information with the addresses they create for users and retain a clear picture of their transactions. These exchanges therefore know at least as much about their user's bitcoin transactions as a bank would know about its customers' transactions. As with banks, if these centralized institutions are hacked or mismanaged, that private data could be exposed. Additionally, this information can be subpoenaed by law enforcement without a warrant.

On the blockchain level, attempts to offer greater privacy by mixing payments between several addresses (so-called bitcoin tumblers or mixing services) carry risks for the user—the administrator of the tumbler may be able to run-off with the users' bitcoins—and do not offer robust guarantees of privacy, especially when there are not several users tumbling their coins together or when one user of the tumbler represents an outsized share of the coins.

Finally, specialist big data analysis firms have perfected tools to simplify the process of tracking transactions on the blockchain and identifying clusters of Bitcoin addresses that belong to particular persons. These tools are called blockchain analysis, and they match addresses in bitcoin transactions with additional data about the users of those addresses. They may obtain that additional off-chain data by monitoring the Bitcoin peer-to-peer messaging network (*e.g.* to note that certain addresses are often listed as the sender in transaction messages originating from certain IP-addresses), the larger internet (*e.g.* to find websites or message boards where people have previously posted their bitcoin address), or by obtaining data from partners such as law-enforcement, exchanges, or wallet-providers (*e.g.* an exchange has created this address for a customer whose name is Francis etc.).

[259] *Ibid*.

While the bitcoin blockchain may merely show you a transaction between two addresses, *e.g.*:

Sender	Recipient	Amount; Time (block number, date and time it was mined)
1LhwgrCmiuWZrWfdRq59pdkWXtQh3yHY12	1AVzBTPoTcFxi8mKHr1uj2t89Uhr8Ns45n	3 Bitcoin; 237886 2013-05-25 16:30:55

Blockchain analysis services can match those addresses with additional data that they have collected, *e.g.*:

Sender	Recipient	Amount; Time (block number, date and time it was mined)
1LhwgrCmiuWZrWfdRq59pdkWXtQh3yHY12	1AVzBTPoTcFxi8mKHr1uj2t89Uhr8Ns45n	3 Bitcoin; 237886 2013-05-25 16:30:55
Address has been used in transaction messages likely originating from this ip-address: 212.77.0.223 (within the Vatican City block of IP Addresses)	Address posted by the Electronic Frontier Foundation to accept the donation described here: https://www.eff.org/deeplinks/2013/05/thank-you-bitcoin-community	

In this simplified fictional example, the blockchain told us only that someone sent 3 bitcoins to someone else (or possibly even to themselves at another address) on May 25, 2013. However, data surfaced by a blockchain analysis firm told us that, in all likelihood, our fictional transaction was a donation to the Electronic Frontier Foundation from the Holy See.

Blockchain analysis firms will also map how addresses pay other addresses on the blockchain and use clustering analysis techniques in order to determine, with reasonable accuracy, whether a set of bitcoin addresses all belong to the same person or group. In our fictional example, we could open a visualization tool and see other transactions to or from the EFF or the Holy See even if they were made using addresses other than the ones used in our donation transaction.

Generally speaking, the end result of combining Bitcoin's transparent blockchain with big data analysis is a reliable, searchable, highly-detailed, and user-friendly visualization of the entire history of all bitcoin transactions accompanied by a wealth of personal data about the persons transacting. Several companies provide these tools. They are, of course, available to law-enforcement but also to anyone curious and willing to purchase access.

Altogether, these developments mean that Bitcoin (at least as currently specified) affords its users little to no privacy. In several ways, transacting with bitcoin is far *more* public than transacting using the legacy financial system. Banks, although obligated under law to identify customers, may nonetheless (A) keep imperfect records of transactions; they may (B) fail to maintain records from many years ago; and (C) there will be several banks with independent records in unique data formats that must be obtained, aggregated, and merged in order to get a full picture of a person's financial history. Bitcoin, by contrast, (A) has a *perfect* record of all transactions made globally (because if a transaction is not in the blockchain it does not exist), (B) has a record that is maintained from the start of the network in 2009 to the present with full copies kept redundantly across several tens-of-thousands of independently owned computers the world-over, and (C) has a single record that is complete rather than partial records scattered across several institutions. Finally, it goes without saying that Bitcoin transactions are *far* more transparent than physical cash transactions, which leave no record whatsoever.

Several forks of Bitcoin, as well as other derivative cryptocurrency projects, have emerged over the years, and the majority do not meaningfully improve privacy for users. Most projects that are direct forks of the Bitcoin protocol like, Litecoin and Dogecoin, as well as many bespoke public blockchain networks, like Ethereum and Ripple's XRP Ledger, all have blockchains that expose the addresses and amounts sent in every historic transaction in order to guarantee scarcity and provenance.

These major cryptocurrencies, at least in their present configuration, do not offer privacy to their users. Anyone transacting with them should assume that the entire world can and will learn about their transactions, including who they have paid, who has paid them, and how much. However this may soon change; several proposals have been made to improve the privacy capabilities of these early cryptocurrencies and several next generation cryptocurrencies that are built to protect user privacy have launched or are being launched.

Brief Overview of Electronic Cash Efforts Thus Far

Next generation cryptocurrencies seek to limit full public visibility of three pieces of data in any transaction: the addresses or pseudonyms of the sender and recipient, the amount sent, and the transaction graph or full pattern of transactions that a user of the protocol leaves behind. These are efforts to create true electronic cash.

Pioneering advances in obscuring the transaction graph began with efforts to augment bitcoin's privacy by creating software tools and protocols that change *how* users constructed their bitcoin transactions rather than changing the bitcoin core protocol itself. The fruits of these efforts include software tools such as the CoinJoin,[260] Coin Shuffle,[261] Tumblebit and other

[260] Blockchain.info, SharedCoin and other CoinJoin implementations: Uses and Limitations (Jun. 10, 2014)
https://blog.blockchain.com/2014/06/10/sharedcoin-and-other-coinjoin-implementations-uses-and-limi

similar protocols. These tools facilitate the shuffling of bitcoins between several addresses in a manner that makes it difficult to link a set of addresses and transactions to any one particular user. Unlike traditional Bitcoin tumblers which are centralized tools wherein the users must hand over control and trust to a third party in order to mix the coins, these tools are powered by automated processes, so-called smart contracts, which can be entered into by the participants peer-to-peer and without risk that they will lose their cryptocurrency. These tools essentially allow a group of bitcoin users to collaboratively write and commit to a transaction message that will automatically move bitcoins between the participants once they've committed their funds and will automatically refund the participants if any participant attempts to renege on the deal (*i.e.* receive funds from the pool without adding their own).

Research has also led to the development of so-called stealth addresses for Bitcoin and other cryptocurrencies. Stealth addresses are created using cryptographic primitives and a protocol that differs from how run-of-the-mill bitcoin addresses are generated. The details of this protocol are beyond the scope of this report but the end result is that a person who wishes to receive bitcoin payments can publish a single fixed address, but each payment made to that address will arrive at a different and unique bitcoin address over which the recipient will already have control. Each payor only learns the one address where their particular payment arrived and the public blockchain does not record any link between the several addresses unique to each payment. This does not, however, solve any issues with respect to making the transaction graph more private because a bitcoin user will eventually recombine amounts of bitcoin in her several addresses in order to send a transaction to someone else. Nor do stealth addresses obscure the amounts sent, which can be valuable data points in identifying and clustering addresses and transactions (*e.g.* I witnessed someone buy groceries costing exactly $123.87 and a bitcoin transaction of equivalent value has just been published on the blockchain, therefore I can assume this is their address).

Thus far we have only described cryptographic tools that can add a level of privacy to bitcoin transactions without requiring any fundamental changes to the Bitcoin protocol itself. Researchers have also developed proposed changes to the Bitcoin protocol that would obscure the value of each transaction as it appears in the blockchain, a project referred to as Confidential Transactions.[262] As of this report, Confidential Transactions has yet to be incorporated into the Bitcoin protocol. More recently, some security researchers have proposed that key concepts from the Confidential Transactions and CoinJoin protocols, could be combined and used to build a cryptocurrency protocol that would obscure both the value and the participant addresses to every transaction in the blockchain while still ensuring that all transactions maintain integrity of provenance and scarcity. This new research has been referred

tations/.

[261] Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin," *Computer Security - European Symposium on Research in Computer Security (ESORICS). Lecture Notes in Computer Science*, Vol 8713, No. 2 (2014): pgs. 345-364, https://crypsys.mmci.uni-saarland.de/projects/CoinShuffle/coinshuffle.pdf.

[262] The Elements Project, "Confidential Transactions," accessed February 26, 2019, https://elementsproject.org/features/confidential-transactions.

to, whimsically, as Mimblewimble (from the Harry Potter books) and it is now being developed into a standalone cryptocurrency called Grin, which, as of this report, has made significant development progress but has yet to launch.[263]

Separately, zero-knowledge proofs are a cryptographic primitive for proving some important fact about otherwise encrypted data without revealing any other information aside from the proof.[264] Integrating zero-knowledge proofs into a public consensus blockchain could potentially allow a decentralized, open set of transaction validators to verify that all recent transactions have been appropriately funded, signed, and not double-spent, without revealing any additional information about addresses or amounts sent. Unlike Confidential Transactions protocols described above, these technologies do not rely on users mixing their coins with sufficiently large groups of other users because the entirety of transactional data on the blockchain can be encrypted and a mathematical proof can nonetheless verify integrity of provenance and scarcity.

Cryptographers at Johns Hopkins University first published research proposing a protocol that could integrate zero knowledge privacy into Bitcoin, the Zerocoin protocol, in 2013. That integration has not occurred as of this report, however a group of developers and researchers housed variously within several universities, a private company, and a non-profit public charity, have collaborated on Zcash, a standalone cryptocurrency protocol employing these zero-knowledge techniques. The Zcash software was officially released in 2016 and the resultant public peer-to-peer network has developed a community of users. Not only is Zcash testing the viability of a fully encrypted blockchain, the protocol also allows users to selectively disclose information about their transactions to whomever they choose.

> Zcash transactions automatically hide the sender, recipient and value of all transactions on the blockchain. Only those with the correct view key can see the contents. Users have complete control and can opt-in to provide others with their view key at their discretion.[265]

Since its launch in 2014, Monero, another standalone cryptocurrency, has also made strides toward greater privacy for users. The Monero software is developed by several individual developers coordinating over the internet, and it employs stealth addresses as well as a version of the Confidential Transactions protocol first developed for use in Bitcoin. Like Zcash, Monero also allows users to unblind their transactions selectively by sharing view keys at their discretion.

This is not a complete list of projects to create standalone next generation cryptocurrencies or privacy improvements to the Bitcoin protocol. Several other efforts are underway. Indeed

[263] Grin, “Grin, the Tech,” accessed February 26, 2019, https://grin-tech.org/.

[264] *See* Wilcox *supra* note 79.

[265] Giulio Prisco, “Zcash Creator on the Upcoming Zcash Launch, Privacy and the Unfinished Internet Revolution,” *Bitcoin Magazine* (Aug. 30, 2016) https://bitcoinmagazine.com/articles/zcash-creator-on-the-upcoming-zcash-launch-privacy-and-the-unfinished-internet-revolution-1472568389.

nearly every major cryptocurrency and open blockchain network has a development roadmap that includes research into either zero knowledge proofs, better protocols for mixing or address randomization, or other means of limiting the degree of public knowledge about blockchain transactions to the bear minimum: what is needed to prove provenance and scarcity of token transfers, and any additional information users choose to share about their own transactions at their own discretion using view keys.

Nor is this a complete discussion of the uses that such cryptographic tools can have. Just as these technologies can be used to balance verification and privacy with respect to financial systems they could also have massively positive implications for other systems that require widespread trust over data but would benefit from not having full public revelation of that data. Take for example identity systems. A zero knowledge proof or some similar cryptographic construction could allow a young person to give a bartender verifiable proof that she has a valid license attesting that her age is over 21 and that she can legally drink in the United States. That proof could be relied upon to show the bartender *only* that pertinent information without exposing her home address or other sensitive information that could jeopardize her safety if the bartender proved unscrupulous.

For cryptocurrencies these technologies are in many ways ideal: Trust in the scarcity of the underlying tokens and the provenance of transactions is generated by an open set of impartial validators around the world just like bitcoin. Unlike bitcoin, however, privacy is guaranteed in these protocols by neglecting to share any information about transactions with these validators or the public at large except for the minimized amount of information necessary to prove scarcity and provenance. Additionally, selective disclosure ensures that counterparties and third parties can be given visibility into the details of any particular transaction whenever the initiator wishes to be transparent or is compelled to be transparent by regulation or law.

Characterizing the Development Process

The core design challenge for electronic cash software remains unchanged from how we specified it earlier: how can you assure the users of the protocol that there is integrity in scarcity and integrity in provenance without publicly revealing the identities of persons behind specific transactions, their complete transaction histories, and without compromising the fungibility of the units.

At heart this is an engineering challenge like any other. There are candidate raw materials, possible arrangements of materials (systems), and there are usable results. Those results are blueprints and technical schematics, it's then up to people around the world to build the resulting program on their internet connected computers and its only once those computers start working together and following the same protocol that a usable service—generally a peer-to-peer messaging network and a verifiable blockchain ledger—emerges.

An Example of What Gets Built: Digital Signature Schemes

To help you understand what is going on when someone helps engineer new electronic cash software, let's look at just one part of bitcoin's software, the digital signature scheme that allows us to create addresses and verify the provenance of transactions. This protocol is all written down and has several authors, and even several versions (like editions of a great textbook), and translations (into different computing languages). You can look at one version of it here: https://github.com/bitcoin/bitcoin/tree/master/src/secp256k1.

For those unfamiliar with cryptography and software design, think of it like a system in your home, say heating and cooling. There are various primary goals: cool in the summer, warm in the winter. There are secondary goals: humidity control and air purification. There are choices of system: forced air vs. radiators. There are choices of underlying materials: copper piping, pex/plastic piping, cast iron radiators, freon, gas, *etc*.

Cryptographic raw materials are mathematical functions instead of metals and plastics. Like metals and plastics, however, these raw mathematical materials obey fundamental laws and exhibit unique an unalienable properties. By way of example, a fundamental class of cryptographic raw materials is the class of so-called one-way-lock functions.

These are functions that take a random number as an input and give the user an output that also looks random but, in fact, bears an important and verifiable relationship to the input. Calculating the output number from the input is trivially easy, like multiplying two numbers together. But if you are only given the output and want to reverse engineer the input, then suddenly the mathematics becomes very hard, like finding the prime factorization of a large number. There's no shortcut that will reverse a well-constructed one-way-lock function and the best chance you have at solving for the input is by guessing and then checking a large number of potential inputs, running them forward through the function, and then seeing if you get your desired output. If the input number is very large and truly random, then you (or more realistically a powerful computer) will likely need to make trillions upon trillions of guesses before finding the right one.

For example, Bitcoin's public addresses (at which users can receive funds) are random-looking numbers that are derived from a user's randomly generated private key by running the key through a well-known one-way-lock function called the elliptic curve digital signature algorithm.

For scale, here is a bitcoin private key expressed in decimal form:

105627842363267744400190144423808258002852957479547731009248450467191077417570

That is a very big number. Using a similarly large number randomly generated for their own purposes, a bitcoin user's computer would multiply this number by a set of points on a known elliptic curve in order to get their public key. By curve we truly mean just a geometric function. You may remember simple geometric functions from grade school, for example $y = x^2$ is a basic quadratic function and when you graph it in two dimensions you get a curved parabola shape, rather like the light and shadow that come from the top of a lamp. Elliptic curves are no different from these simpler curves except that their unique symmetries and shapes allow you to do certain interesting mathematical operations using points on the curve.

Unless you plan on heading to graduate school for cryptography, don't be concerned with understanding exactly how elliptic curve functions work. Remember, these are raw materials: just as the unique arrangement of molecules in copper makes it a good choice for some building applications (*e.g.* conducting electricity through wires or fresh water through pipes) and a poor choice for other applications (*e.g.* insulating the walls of a house from heat loss), so too can the unique arrangement of numbers in a particular elliptic curve make it a good choice for building useful computational structures like one-way-locks. You don't need to understand the molecular structure of copper to understand its usefulness in building a house, just its general properties.

So returning to our example key from above, if we run that number through the elliptic curve function we will get a corresponding public key which can be further manipulated using another cryptographic primitive (raw material) called a hash function in order to shorten it into a unique number that can serve as the user's public payment address. The end result of all of those functions is something like this if it is expressed using character encoding (an established way of representing numbers as unique strings of letters and other characters):

1LhwgrCmiuWZrWfdRq59pdkWXtQh3yHY12

The person who generated that address from their corresponding private key can now announce their bitcoin address to the world, effectively saying "this address is mine." Remember, however, that this address is the product of a one way function. So when they make this announcement they reveal essentially zero information that would help adversaries guess their private key. If you wanted to guess it, you'd have to quite literally guess and check all the possible private keys by running them through the same elliptic curve function. Taking our decimal form private key example from above, you might start with:

0000000000000000000000000000000000000000000000000000000000000000000000000001

And then try:

0000000000000000000000000000000000000000000000000000000000000000000000000002

Continuing on, eventually you might get to:

0000000000000000000000000000000000000000000000000000000000000000000000010000

But even the fastest computer in the world today would, on average, only ever guess the correct private key once in 5,194,882,658,574,989,737,995,779,322,992,527,357,514,014 years. For scale, the universe is, so far, probably only 13,800,000,000 years old. You should probably give up.

The person who generated that address can also do something else very useful with their private key. They can use it to digitally sign messages. The rest of the world can compare those signed messages to the previously announced public address and verify with mathematical certainty that the message could only have been produced by someone in possession of the private key that matches the public key. How do they know this? Because they know that there should be a deterministic mathematical relationship between keys and signatures and they can check the authenticity of the signed messages by running these bits of data through the same cryptographic primitives used to generate the key pairs—hash functions and elliptic curves—in order to compare the results. The output of those signature checking functions should be the message text and the public key of the sender. If it is not, then the signature is invalid and you can't trust that the message came from its purported sender.

So when the person who generated public address:

1LhwgrCmiuWZrWfdRq59pdkWXtQh3yHY12

wants to send bitcoins to another bitcoin address, say:

1AVzBTPoTcFxi8mKHr1uj2t89Uhr8Ns45n

They can simply write a message that includes their address, the recipient address, and the amount they'd like sent. They can convert all that into a number and then combine that number with their private key through a series of functions and the resulting signed message will look something like this:

ScriptSig:
PUSHDATA(72)[30450220741f735595f00dd061ff8572cd5d880986b0191337c5c5add2fdca29f8b6
f0b4022100a0dd1c544c7afe7490401cbd62ac857adddea0852f625c172c8f9358cae42ce501]
PUSHDATA(65)[043e16ed0777ffb43117503a67318a2c14bb4b287f3eb90a29f6b5cfa7c96cb08fd88
ed6af1e2168b066b9c121e8d692b4f96e1997e2d12b2face74b0d3b0ba0aa]

Which, when verified according to the the same signature schemes, outputs the message and their public address. We now know that only the person who has the private key matching address:

1LhwgrCmiuWZrWfdRq59pdkWXtQh3yHY12

Could have asked to move these bitcoins to 1AVzBTPoTcFxi8mKHr1uj2t89Uhr8Ns45n

If the sender's address has sufficient bitcoins to fund the transaction, then the transaction is valid and will be added to the blockchain.

This complex arrangement of cryptographic primitives and the protocol for how to use them to achieve a result (signature verified, public key generated, etc.) is called a cryptosystem. Anyone can invent one by assembling a series of primitives that will, when performed in the prescribed order with any other prescribed constants, parameters or inputs, do some useful work. In practice it's very difficult work and requires a great amount of prior knowledge, disciplined effort, and creativity. Again, it's rather like building a blueprint for a beautiful house that specifies all the essential systems from lighting to plumbing, and all the raw materials from copper pipes to mud bricks. Once that blueprint is out in the world, people are free to use it how they will.

Cryptosystems are nothing new to Bitcoin, they have long been employed in computing networks and over the internet (*e.g.* when you send your credit card information online it is encrypted using public key cryptography powered by the same elliptic curves we've just described). They predate digital computers, as exemplified by the mechanical enigma machines used by the Germans to send secret messages during World War II. Indeed some cryptosystems are truly ancient, and their antiquated simplicity can make it easier to understand the category. Long before digital computers and the cryptographic primitives we've discussed thus far, some cryptosystems were quite literally engineered out of wood and parchment. Take, for example, the ancient Greek *scytale* cryptosystem as described by Plutarch:

> This scroll is made up thus: When the Ephors send an admiral or general on his way, they take two round pieces of wood, both exactly of a length and thickness, and cut even to one another; they keep one themselves, and the other they give to the person they send forth; and these pieces of wood they call Scytales. When, therefore, they have occasion to communicate any secret or important matter, making a scroll of parchment long and narrow like a leathern thong, they roll it about their own staff of wood, leaving no space void between, but covering the surface of the staff with the scroll all over. When they have done this, they write what they please on the scroll, as it is wrapped about the staff; and when they have written, they take off the scroll, and send it to the general without the wood. He, when he has received it, can read nothing of the writing, because the words and letters are not connected, but all broken up; but taking his own staff, he winds the slip of the scroll about it, so that this folding, restoring all the parts into the same order that they were in before, and putting what comes first into connection with what follows, brings the whole consecutive contents to view round the outside. And this scroll is called a staff, after the name of the wood, as a thing measured is by the name of the measure.[266]

The lengths of parchment, the thickness of the wooden dowel, the direction it should be wrapped, these are parameters and functions in a cryptosystem. The imposing and complicated systems we use today may seem alien by contrast but they are no different. They are made up of static parameters, functions, and procedures that can be written down in a book, shared with

[266] Plutarch, *Lysander* (75 A.C.E.) (Translated by John Dryden) *Available at* http://classics.mit.edu/Plutarch/lysander.html.

the world, and employed for secret keeping, message authentication, and now even for making electronic cash transactions and decentralized exchanges.

Who builds these tools and what does the process actually look like? We'll discuss this briefly in the next subsection.

Who Builds this Software?

Satoshi Nakamoto is responsible for Bitcoin in the same way that Thomas Edison is responsible for the electric light bulb. What is critical about both Nakamoto and Edison is that they created a working prototype. In both cases, however, it is important to not overstate their importance to the respective fields.

Neither worked alone; they assembled breakthroughs in other disciplines and from other inventors in order to create their prototypes. To build the lightbulb you need to understand breakthroughs in electricity, materials science, and other fields. To build the Bitcoin protocol you need to understand prior breakthroughs in peer-to-peer networking, consensus mechanism design, cryptography, and economics. You may have imagined that the first inventor of the cryptosystem described in the previous section was Nakamoto. That is not true. Whitfield Diffie and Martin Hellman were the first to notionally describe a digital signature scheme of this sort in 1976. You might have imagined that Nakamoto was responsible for the discovery that a digital signature cryptosystem could be used to do cash-like payments person to person. That is also not true. David Chaum was the first to publish research on a signature-scheme-powered electronic cash in 1982. Nakamoto actually had little to do with the digital signatures involved in the Bitcoin protocol; his seminal contribution was in describing a proof-of-work public blockchain to prevent users from double-spending coins. The fact that it would use signatures as a form of authentication among participants was taken as wrote. As the white paper says at the start:

> A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. *Digital signatures provide part of the solution*, but the main benefits are lost if a trusted third party is still required to prevent double-spending.[267]

Another useful comparison to Edison is what happens after the invention of the prototype. Today, neither Edison (his estate) or Nakamoto maintain a monopoly on the fruits of their prototype, nor did they control how people used their prototype. Edison's patents eventually expired and Nakamoto never even applied for any. More importantly the world of electric lights became much larger than Edison or any of his business associates. Ultimately there were lively competitive markets for selling bulbs and eventually new innovations from other inventors like halogen lamps, fluorescents, and light emitting diodes. Similarly the world of Bitcoin has become much larger than Nakamoto. Bitcoin's reference client, Nakamoto's prototype, is still

[267] Emphasis added. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," (Oct. 31, 2008) https://bitcoin.org/bitcoin.pdf.

actively maintained and tweaked to this day by no fewer than 587 code contributors. That reference client itself is merely that, a reference or blueprint from which other developers can build bitcoin compatible software for their own needs, whether they are creating a mobile wallet to run on smartphones or mining the blockchain with server warehouses.

The final comparison may seem comically obvious but it is worth stating. Neither Edison's lightbulb nor Nakamoto's bitcoin client were ongoing services, they were new things made of new ideas that suddenly existed in the world because of discovery. With light bulbs it's obvious, a lightbulb is a device you can have in your home, you don't need an ongoing service contract with Edison for it to work. All you need is commonly available resources like electricity. Once folks understand the lightbulb's operation they can, if creative and so-inclined, riff on the idea freely and build new things from traffic lights to tanning beds. With bitcoin it's less obvious but no less accurate. When people started using bitcoin they were employing the core invention, the software, and benefitting from or building atop the brilliantly creative ideas—blockchains, proof-of-work, etc.—but they were not using a service provided by Nakamoto or anyone else to send money across oceans. They were doing it themselves with new tools and inventions they had obtained. Nakamoto and Edison can and did eventually disappear and yet their inventions continued to enrich our lives. The important thing that they did was create an idea; not run an industry or organize a consumer-oriented service.

Today, scores of brilliant people carry on this work. As stated earlier, the fundamental challenge in building next generation cryptocurrencies is an engineering one, not a question of building a profitable business or providing an ongoing service to customers, but rather a question of whether someone can figure out a way to combine cryptographic primitives into new cryptosystems such that public blockchain transactions can have integrity without sacrificing user privacy. Some next generation cryptocurrencies are developed by individual volunteers who cooperate using tools like GitHub, Slack, Internet Relay Chat (IRC), in order to coordinate. Other next generation cryptocurrencies are actively being developed by companies and non-profit organizations. Some are still developed by persons who, like Nakamoto, would rather not publicly share their identity; others have well-known developers. In all cases, however, the work being done is software development and fundamental cryptographic and scientific research. It is a creative and expressive endeavor.

The most fundamental way that groups of developers coordinate their creative efforts is by sharing the source code that ultimately describes a particular cryptosystem and their proposed revisions to that source code. When source code is compiled to object or machine-readable code and executed by a computer user, it may perform an action. In the example of our digital signature scheme above, a computer user can download source code known as OpenSSL from various sources. The user can compile this source code on her machine and then she will be able to, from a standard command line interface, sign messages or verify the signatures on messages she has received. The compiled program is a useful tool, but the source code is a set of instructions for the tool's creation and use. Source code for widely used open-source cryptosystems, like OpenSSL, is shared to facilitate coordination between the hundreds and sometimes thousands of software developers, cryptographers, and security researchers who work together to ensure that the science and engineering behind these tools is sound, to hunt for bugs, and to bring creative and new derivative projects to life. If this expressive activity was not essential to the continued progress of computer science then there'd be little reason to share code in this uncompiled form.

Cryptocurrencies are no different. Source code is shared amongst large developer communities using tools like GitHub. Cumulatively these developers do the creative and scientific work of improving that code. Persons interested in using the cryptocurrency can download the source code, compile it on their device, and begin communicating with others to join the resultant peer-to-peer messaging networks, send and receive transactions, and—if they wish—play a role in storing, validating, and updating a copy of the resultant distributed ledger or blockchain. Nakamoto's singular moment of invention has spurred countless iterations: new versions of bitcoin, derivative projects, and entire global communities of users.

Arguing that this inventive work should not continue because it could lead to some tools and inventions that will do harm is like arguing that Alfred Nobel should never have been allowed to invent dynamite. That perspective naively ignores the fact that tools and technologies are purpose agnostic and will inevitably be used for both good and evil. Worse, it assumes that if one person, say Nobel, simply hadn't been allowed to invent something like dynamite that no one else would have invented it in his stead. The truth is, of course someone would have, and it would have self-evidently been someone with less respect for law and order, maybe even someone who would be *happy* to see their invention do harm in the world.

Nor should we assume an adversarial posture between cryptographers and government. As one scholar has remarked, "In fact, we as citizens owe at least a small debt to the science of encryption for the birth of our nation. From the Revolutionary War to WWII encryption code has been critical for our nation."[268]

Hopefully this Appendix has offered a richer picture of how and why research into electronic cash and decentralized exchange is taking place. These technologies are as powerful as they are contentious. It is not wrong to be concerned about their misuse by criminals or those who would seek to harm our nation or its people. Neither is it wrong to be skeptical of these technologies or even to believe that they are fundamentally unnecessary for the continued flourishing of human society. However, as with any attempt to forcibly stifle a debate rather than engage, it is wrong to say that research into these technologies should be stopped, banned, or allowed only at the government's discretion. As Justice Oliver Wendell Holmes famously wrote,

> Persecution for the expression of opinions seems to me perfectly logical. If you have no doubt of your premises or your power and want a certain result with all your heart you naturally express your wishes in law and sweep away all opposition...But when men

[268] L. Jean Camp and K. Lewis, "Code as Speech: a discussion of Bernstein v. USDOJ, Karn v. USDOS, and Junger v. Daley in light of the U.S. Supreme Court's recent shift to Federalism," *Ethics and Information Technology*, Vol. 3, No. 1 (Mar. 2001): pgs. 21-33, http://www.ljean.com/files/CODE_FEDERALISM.pdf.

> have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas… . The best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out.
>
> That, at any rate, is the theory of our Constitution. It is an experiment, as all life is an experiment. Every year, if not every day, we have to wager our salvation upon some prophecy based upon imperfect knowledge. While that experiment is part of our system, I think that we should be eternally vigilant against attempts to check the expression of opinions that we loathe and believe to be fraught with death, unless they so imminently threaten immediate interference with the lawful and pressing purposes of the law that an immediate check is required to save the country.[269]

[269] *Abrams v. United States*, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting).