**CHAPTER 4: The Government Takes Crypto Seriously**  
  
The best status to have vis-a-vis the state is none at all—that is, to go unnoticed as you live your life in peace and freedom. Invisibility is a difficult or expensive  
  
status to achieve, however, and the government delivers stiff punishment to those who try unsuccessfully. Crypto has lost the legal invisibility it initially enjoyed from being arcane or dismissed as a flash in the pan. It is being taken seriously and “seen” by authorities. Drawing the state’s attention is probably what Satoshi meant when he lamented the prominence Bitcoin attained through its association with Wikileaks. The technology was young and in early development; the last thing it needed was to be taken seriously by government. As Satoshi commented, “WikiLeaks has kicked the hornet's nest, and the swarm is headed towards us.”  
  
The goal of the swarming state is predictable—control—but the reaction of authorities varies. Some politicians and bureaucrats perceive a threat; others glimpse the fresh plunder that is possible; still others see a means by which to update an inefficient and unpopular central banking system; many want to use it to springboard into a cashless society that they digitally control. Whatever differences in perspective exist, however, the same conclusion is reached: crypto needs to be under their centralized authority.  
  
**A State Strategy to Control Crypto**  
  
A popular state strategy for dominating crypto is to reclassify it as money and to apply the same stringent laws that cover fiat. A bill currently stalled in the United States Senate embodies common aspects of this tactic, which is far from confined to American shores. Examining the bill is a way to understand how this strategy is likely to play out and how the process would destroy crypto, if successful.  
  
On Tuesday, November 28, 2017, [Senate Bill 1241](https://www.congress.gov/bill/115th-congress/senate-bill/1241/text) was heard by the Congressional Committee on the Judiciary. The bill was held in committee where it remains. It is an alarm bell ringing in the night.  
  
Some crypto enthusiasts will applaud this development because they believe regulation means crypto is going mainstream and achieving a respectability that brings more profit. Some of the applauders want to benefit from licenses (government approvals), which could eliminate free-market competitors. Other crypto zealots will just shrug because they think free-market crypto cannot be controlled and the statist efforts will fail. The shruggers may be correct—I hope they are—but lives can be destroyed by the state’s attempt to dominate, and the destruction of good people is a nonshrugging matter. The prudent approach to state intrusion is neither applause nor dismissal but preparation. The government is coming, and it wants more than money. It wants to make hard-hitting examples of crypto users in order to dissuade others from seeking financial freedom.  
  
The “Combating Money Laundering, Terrorist Financing and Counterfeiting Act” (S.1241) is an anti-money laundering bill that regulates cryptocurrency on a federal level. This means there would be a uniformity of crypto’s legal status and treatment across America.  
  
Again, some crypto enthusiasts will applaud this move for providing the situation with clarity. This is a misguided response on several levels. For one thing, control is not clarity; it is the centralization and surrender of choice. And clarity has no intrinsic value apart from the content being clarified; a murderer can be very clear on how he intends to kill you, but this not something to cheer about or seek out. For another thing, if legal inconsistencies in the treatment of crypto cause problems, then the appropriate response is to remove the laws, not to call for more.  
  
Moreover, inconsistencies in the law can be useful because they can work to the advantage of those who seek freedom. This strategy is sometimes called the “parallel institution” approach. Parallel institutions such as Church and State can act as bulwarks against each other’s power, allowing individuals to breathe more deeply in the divide. The concept of church sanctuary was traditionally available for criminals and run-away slaves, for example, though it was not offered reliably. On the other hand, people with the “wrong” religious or political beliefs can sometimes escape persecution by fleeing to the sanctuary of a politically friendlier area.  
  
The parallel institution strategy is employed every day across the global. In America, people move from states with high taxes to ones with low or no taxes. The British rich move to tax havens. Marijuana aficionados shift from Texas, with its draconian drug laws, to Colorado, where marijuana is legal. Around the world, people flee for their own reasons.  
  
Freedom does not benefit from the homogenization of government law but from the presence of alternatives. Federalizing law on crypto to eliminate inconsistency also eliminates the ability of users to move to whichever state-level jurisdiction is friendliest to their purpose. Federalizing law also expands government into areas that are not yet addressed on the state level; this includes border and customs control. Consistency may bring clarity, but it does not bring choice. Another word for consistency in the law is centralization.  
  
**What is S.1241?**  
  
S.1241 was introduced into the Senate Committee covertly. An alert bitcoiner noticed that the Senate Judiciary meeting had been listed on the official webpage at 10 a.m. on the 28th—the same day as the hearing—after being [added](https://www.cryptocoinsnews.com/us-senate-judiciary-to-hold-panel-hearing-on-aml-laws-today-focusing-on-digital-currencies/) to the Hearing page at 6 p.m. the previous evening. This maneuver effectively precluded media coverage, public feedback, or protests. Actions to control crypto are likely to follow this pattern—abrupt, unseen, and unexpected. S.1241 can be viewed as a template for how governments intend to proceed. Whither the U.S., much of the world will follow.  
  
S.1241 seeks to amend [31 U.S. Code § 5312](https://www.law.cornell.edu/uscode/text/31/5312), which addresses definitions and their application to money and finance. It sounds dry, but the impact would be dramatic. The purpose of the bill is to include “digital currencies” in the definition of “monetary instruments” and “any digital exchanger or tumbler of digital  
  
currency” in the definition of “financial institution.” $10,000 is the trigger amount. In the U.S., $10,000 triggers a personal declaration at the border; it is the point at which financial institutions complete a state-mandated currency report that can cause accounts to be frozen or confiscated regardless of whether there is evidence of a crime.  
  
S.1241 is a tightening noose.  
  
Section 2: “Transportation or Transhipment of Blank Checks in Bearer Form” declares that any check entering or leaving the U.S. which is “drawn on an account containing more than $10,000” and has no dollar amount specified is “valued in excess of $10,000 for reporting purposes.” Since crypto can be difficult to assess and rarely has a dollar amount specified, the “no dollar amount” allows customs agents to evaluate crypto at the reportable amount.  
  
Section 3: “Increasing Penalties for Bulk Cash Smuggling” addresses the concealment of $10,000 or more in currency or monetary instruments when crossing the border. Maximum punishment is ten years imprisonment with fines increasing by an unspecified amount. When the state punishes a petty offense in a draconian manner, it means authorities have no other solution to a situation except the barrel of a large gun.  
  
Section 4: “Section 1957 Violation Involving Commingled Funds and Aggregated Transactions” deals with “the transfer of criminal proceeds…without the need to demonstrate” criminal intent. Two existing loopholes would close. 1) $10,000 in funds in which allegedly dirty money is commingled with clean money becomes $10,000 of dirty money. 2) A series of transactions under $10,000 that is “closely related in time, the identity of the parties, the nature of the transactions, or the manner in which they are conducted” collectively meet the $10,000 threshold. Legal money that is in the presence of ‘criminal’ money is criminalized through guilt by association, allowing officials to confiscate everything. Undeclared or improperly declared crypto makes all wealth—crypto or not—fair game.  
  
Section 5: “Charging Money Laundering as a Course of Conduct” simplifies the process of charging a person with money laundering and includes “conspiracies to violate…[the] prohibition of unlicensed money transmitting businesses as money laundering conspiracies.” Plans to transmit crypto can be punished as though the act had occurred. It is not clear whether the co-conspirators will also be charged or have their money confiscated.  
  
Section 6: “Illegal Money Services Businesses” makes It a crime for unregistered businesses to send “proceeds abroad.” Ignorance of the need to register is no defense. The term “money transmitting business” is replaced with “money services business” to include “entities…such as check cashiers” that “do not transmit money.” Penalties and fines increase.  
  
Section 7: “Concealment Money Laundering” applies to “couriers or mules.” The Supreme Court ruled in the past that a defendant needs to know the  
  
transportation of funds is clandestine and why the funds are being “so transported” for a courier to be guilty of a crime. Those requirements are diluted or eliminated. Again, ignorance is not a defense.  
  
Section 8: “Freezing Bank Accounts of Persons Arrested for the Movement of Money Across International Borders.” A 30-day hold is instituted on the accounts of those charged and could be extended “for good cause.” This seems to apply to the full amount within an account.  
  
Section 9: “Prohibiting Money Laundering through Hawalas, Other Informal Value Transfer Systems, and Closely Related Transactions” redefines what constitutes a money laundering offense when it involves “a set of parallel or dependent transactions.” All would be considered to be “a single plan or arrangement,” which might well bring the collective transaction up to prosecutable levels.  
  
Section 10: “Restoring Wiretap Authority for Certain Money Laundering and Counterfeiting Offenses” allows the state to monitor those people it suspects of criminal activity.  
  
Section 11: “Applying the International Money Laundering Statute to Tax Evasion” defines the use of foreign accounts to evade taxes as money laundering. Because crypto flows so easily across borders, users tend to frequent “foreign” exchanges —a practice that could be labeled “tax evasion” unless it can be proven otherwise.  
  
Section 12: “Conduct in Aid of Counterfeiting” includes the use of new technology, “materials, tools, or machinery.” This provision takes specific aim at crypto, digital money, and the tools that provide privacy to them.  
  
Section 13: “Prepaid Access Devices, Stored Value Cards, Digital Currencies, and Other Similar Instruments” amends current law to explicitly include “any digital exchange or tumbler of digital currency” as well as any “issuer, redeemer or cashier” of a “digital currency.” Funds stored in a digital format are explicitly subject to money laundering reporting requirements.  
  
Section 14: “Administrative Subpoenas for Money Laundering Cases” expands the availability and ease of administrative subpoenas.  
  
Section 15: “Obtaining Foreign Bank Records from Banks with U.S. Correspondent Accounts” strengthens “this existing investigative tool.” Foreign banks can be subpoenaed for records related to any “civil forfeiture action,” and they can be punished for noncompliance. Remember: S.1241 includes “any digital exchanger or tumbler of digital currency” in the definition of “financial institution,” which leaves foreign exchanges vulnerable to subpoenas.  
  
Section 16: “Danger Pay Allowance” provides special compensation to a wide range of law enforcement agencies. It is unclear what constitutes “danger” but, presumably, agencies will have a vested interest in defining situations in a manner that draws more funding.  
  
Section 17: “Clarification of Secret Service Authority to Investigate Money Laundering” expands police authority.  
  
Section 18: “Prohibition on Concealment of Ownership of Account” makes it a crime for a person “to knowingly conceal, falsify or misrepresent, from or to a financial institution” their identity or “a fact concerning the ownership or control of an account or assets held in an account.” This is particularly relevant to crypto users who routinely employ anonymity or pseudonymity. It becomes a crime to not reveal identities or specific transfers over the blockchain.  
  
Section 19: “Prohibition on Concealment of Source of Assets in Monetary Transaction” allows the government to pursue assets even if the person is not charged with an offense. Instead, their money can be confiscated simply because its source is not stated or unclear.  
  
Lawyer Ballard Spahr explains, “If passed in its present form, S.1241 ironically will take the one kind of offense which Congress has historically *not* allowed to form the predicate for money laundering—i.e., “garden variety” tax fraud not involving illegal proceeds—and turn things on their head. That is, transactions promoting a tax crime, so long as they involve a cross-border transaction, will be the one and only kind of transaction that can constitute a money laundering offense when the proceeds represent otherwise entirely legal funds.”  
  
Those who wish to prepare against the coming crackdown should study S.1241. **Protecting People From Freedom**  
  
Money laundering and tax evasion are two justifications that the state proclaims when it reaches out to control crypto. Arguably, these broad and vague justifications are not viewed with general sympathy because it often looks like a blatant money grab.  
  
Other rationales are more successful. The crypto community, government argues, is rife with drug dealers, blackmailers, sex traffickers, child porn producers, gun dealers, and other miscreants. The state points to the “dark web” as proof of perfidy. This is the part of the web that is accessed only by special software, allowing users to remain anonymous or untraceable. Controlling crypto is said to be necessary in order to protect people from dark web crime. In doing so, the state argues it is protecting vulnerable drug users, exploited women and children, gun victims, compliant taxpayers, law-abiding citizens, and a scrolling list of other “victims” of the monetary outlaws.  
  
There are myriad ways to refute this claim, including the fact that it is flatly false. Some crypto users are undoubtedly violent criminals; the same is true of some people who use cash and credit cards. Crypto is a currency and a payment method. Like anything else useful in life, it is a tool that can be employed for good or bad purposes. But the overwhelming majority of people with crypto or with  
  
cash are peaceful human beings who are being criminalized for preferring one payment method over another. The justification for doing so boils down to the claim that their economic choices are dangerous to public welfare.  
  
Clamping down on allegedly exploitative but nonviolent economic practices is a tremendous violation of the rights of vulnerable people; it does not protect them. I know. My life could have been ruined by one measure that was intended to prevent a so-called form of economic exploitation that repulses most people— child labor. When I was 16 years old, I ran away from home and lived on the street for as short a period as I could manage. I refused to go to a shelter or seek government assistance for the same reason as many run-away teens; when teenagers prefer the cement to home, it means adults have betrayed them. The only safety is to take care of yourself.  
  
I was luckier than many. I was barely 16, but this meant I could work legally. I could stand behind the warm counter in a fast food restaurant or, in my case, I could sit in the office of a family-owned furniture store where I did years worth of backed-up paperwork during the day and slept on a couch downstairs during the night. The owner paid me minimum wage and gave me a safe place to sleep. As a result, I worked far longer than the eight hours a day for which I was paid. I saved enough to move into a boarding house and, when I moved on to a filing job in a bank, I had a reference. My future hinged on having those opportunities.  
  
What if I had been one month or one year younger than the legal working age? The store owner would not have risked his business by hiring me. Nor should he have. He was correct to insist upon inspecting and xeroxing my I.D. before offering me the job; he was correct to wait until he knew me a bit better to offer me the basement couch. Why should he put his family’s income and future in peril to help a stranger? And that’s what he did; he did not exploit me. He *helped* me.  
  
Without the ability to make money legally, my life may have turned out badly rather than well. In the name of humanitarianism, the law would have closed off my one path back into the mainstream of society, and it would have done so self- righteously. How would I have fed myself then? Stealing, begging, sex work, and drug dealing come to mind. But I wanted a way *of* the street, not a way to make it or prison my permanent address.  
  
Closing off nonviolent economic options does not protect vulnerable people. Just as raising the mandatory minimum wage makes it difficult for those starting out to find employment, economic “protections” cut off vulnerable people from being able to climb upward. In my case, not being able to support myself would have created a criminal and a victim, decreasing the public good. If there is violence involved in an economic option, then address the violence. If there isn’t, then leave it alone. This principle is the way to help everyone who wants earn their own money and spend it as they see fit. The state does not shield victims or society by taking economic options away from people who have done no demonstrable harm but happen to fall into a category that is either protected or reviled.  
  
Oddly enough, the law’s response to both categories is much the same: deny economic rights. As a run-away teen, I was in the “protected” category, and I came within a hair of losing my right to earn a living. Peaceful crypto users are in the “reviled” category, and many may be stripped of the right to retain money they have earned.  
  
To benefit the vulnerable and society, the state needs to do nothing more than get out of the way. The French phrase “laissez faire” is most often associated with “laissez-faire capitalism.” It is said to have originated during a 1681 meeting between Jean-Baptiste Colbert, the French Controller-General of Finances, and a group of businessmen. Colbert asked how the state could assist the men in their businesses. The head of the group, M. Le Gendre, reportedly replied, “laissez nous faire" (leave it to us). Leave us alone.  
  
**A Second Control Strategy: Government-issued Crypto**  
  
Some states plan or attempt to issue their own crypto. Central Bank-Issued Digital Currency (CBDC) refers to a national cryptocurrency that issues from a central bank. It is the crypto counterpart to a physical fiat such as the U.S. dollar or the British pound.  
  
It is also a bitter irony. A monetary wildcat that was designed to undermine the financial system is being redefined to serve the status quo. At least, this is what the status quo hopes will happen. In fairness, some world leaders understand this development is not possible. [Putin famously said](https://news.bitcoin.com/putin-cryptocurrency-has-its-place-no-state-can-have-own-crypto/) that a national cryptocurrency is not viable because crypto is an international phenomenon. Other nations are actively exploring the development of CBDCs, however. Japan has launched the digital money [J-Coin](https://news.bitcoin.com/tag/j-coin/), for example. It is a digital currency rather than a crypto  
  
[based on a blockchain](https://coinnounce.com/japan-launches-j-coin-pay-not-a-cryptocurrency-though/), but it serves the purpose of moving Japan closer to a cashless society; it makes tracking digital coin users into a trivial matter; and it allows the state to crack down on real crypto users with greater ease and less backlash. These are three of the main goals of a national e-currency.  
  
CBDCs may seem to parallel free-market crypto, but they are the anti-crypto. Consider just some of the technical differences:  
  
• Bitcoin is decentralized; CBDCs would [centralize](https://themerkle.com/is-there-a-future-for-central-bank-digital-currencies/) all aspects of digital currency, often in the hands of one agency or system of agencies that are  
  
heavily regulated.  
  
• Bitcoin is peer-to-peer between individuals; CBDCs would be administered by trusted third parties in the worse sense of this term.  
  
• Bitcoin is open-source; CBDCs would be patented, proprietary, and not transparent.  
  
• Bitcoin is mined; CBDCs would be issued by a central authority.  
  
• Bitcoin is limited to 21 million coins; CBDCs’ cap would be whatever the authority wished it to be.  
  
• Bitcoin is on a transparent blockchain; CBDCs may not use a blockchain, and probably would not.  
  
• Bitcoin users possess their own private keys; private keys for CBDCs would be owned by a trusted third party that would control the wealth.  
  
• Bitcoin is anonymous; CBDCs would [track](https://www.technologyreview.com/s/603505/paper-problem/) both the identities of users and how they spent the currency.  
  
• Bitcoin severs the connection between currency and central banks; CBDCs would cement it.  
  
Free-market crypto and CBDCs also have antagonistic goals. Crypto obsoletes the central bank’s status as a trusted third party and eliminates the money monopoly. CBDCs are the central-banking system’s bid to retain its trusted third party status and the monetary monopoly.  
  
Free-market crypto and CBDCs may have one goal in common, however: the ultimate elimination of physical fiat. But, again, the reasons are antagonistic. Crypto rejects a corrupt currency that steals from honest people. CBDCs want to rescue the status quo for the benefit of financial elites by creating a digital fiat.  
  
**Why the Push for a Cashless Society?**  
  
Cold cash has always been the enemy of government. In his [article](https://mises.org/library/why-government-hates-cash-0) “Why Governments Hate Cash,” the Economics Professor Joseph Salerno writes:  
  
Now the reason given by our rulers for suppressing cash is to keep society safe from terrorists, tax evaders, money launderers, drug cartels, and other villains real or imagined. The actual aim of the flood of laws restricting or even prohibiting the use of cash is to force the public to make payments through the financial system. This enables governments to expand their ability to spy on and keep track of their citizens’ most private financial dealings, in order to milk their citizens of every last dollar of tax payments that they claim are due.  
  
The problem confronting authorities: When cash leaves the bank and goes into the pockets of individuals, the government loses track of how it is spent. Individuals can buy and sell with an anonymity that blocks the collection of taxes, fees, and other revenue for the state. Government wants to “solve” this. [Currency tracking sites](https://en.wikipedia.org/wiki/Currency_bill_tracking) can record the serial numbers of fiat, for example, and allow the circulation to be monitored—that is, as long as the serial number is re-entered at every stage. The system requires a high degree of unlikely cooperation.  
  
The drive toward trackable fiat will inevitably fail because of noncooperation. Fortunately for governments and central banks, digital cash is a perfect substitute for physical cash because traceability is built into the design. If governments manage to make digital money work, then the resulting currencies will be a nightmare for freedom. They will combine the efficiency of crypto with the totalitarianism of government. The trusted third party problem that Bitcoin was created to eliminate will be back on steroids.  
  
The state’s hostility to cash will cause some nations to move from physical to digital fiat with alacrity. The process is likely to resemble some version of the following:  
  
First: A government explores the possibility of digital cash while it gradually removes physical cash from circulation.  
  
Second: A database for digital currency—probably not based on a blockchain—is written in proprietary code and implemented in a nontransparent manner.  
  
Third: A digital cash is issued and sold as an alternative to both cash and free- market crypto. To encourage its adoption, government regulates free-market crypto which is driven underground or forced to flee to friendlier climes. Fourth: Automatic taxation is embedded into the new digital currency. The absolute tracking of every unit of currency, which is linked to real identities, gives government an unprecedented control over the flow of wealth.  
  
Fifth: Central banks inflate the supply of digital currency at will, devaluing each unit in circulation. This inflicts a huge, hidden tax on every owner.  
  
The CBDC also gives government [greater precision in manipulating](https://news.bitcoin.com/the-satoshi-revolution-chapter-3-do-you-want-a-government-fiat-crypto-part-4/) the economy. In an article entitled “Why Governments Want a Central Bank-Issued Digital Currency,” the Austrian economist Xiong Yue observes:  
  
[G]iven that these digital currencies are programmable, the government can even control exactly how to spend this new money using scripts. For example, if the government plans to subsidize certain farms, say some corn farms, to support this sector of agriculture, they can directly add a certain amount of money to the wallets of some farms, for instance 100 million dollars and program this money to be sent to certain fertilizer merchants at a certain time, and that each can only spend maximum of 10 million dollars per year.  
  
In short, a CBDC could facilitate a more efficient centralized state. This is hardly a good thing.  
  
Another agenda item of government and central banks is negative interest rates. Negative interest occurs when depositors do not receive interest on money kept in their accounts; instead, they pay interest to the bank for holding their money. This is a money maker for the banks. It also encourages people to spend because the money erodes if it sits unspent, and consumer spending is seen to prop up the economy.  
  
The 2015 [bank crisis in Greece](https://news.bitcoin.com/can-the-bitcoin-economy-help-greeks-hide-their-wealth/) provides an example of how negative interest works. To avoid bank runs, Greece imposed a surcharge of one euro per 1,000 euros in cash withdrawals. Salerno observes, “It doesn’t seem very big, but the *principle* at work is extremely big because what they’re in effect doing is breaking the exchange rate between a unit of bank deposits and a unit of currency.” Salerno continues, “To make the calculations easier…let’s say that the Greek ‘surcharge’ is ten dollars for every 100 dollars withdrawn. Now, instead of being  
  
able to convert one euro in your checking account into one euro in cash, on demand, you will only be able to buy one euro in cash by spending 1.10 euros in your bank accounts. That’s a negative 10-percent rate in some sense….So, you would only really get ninety cents for every dollar that you wanted to withdraw and that’s very significant because this means it will be more expensive to buy an item with cash than with bank deposits.” Predictably, people were driven away from cash. There was an incentive to pay bills out of bank accounts which made all payment trackable.  
  
The main problem with a scheme of negative interest for government and central banks is that people will keep their cash outside of the financial system. Large amounts will stay beyond government’s reach. If digital cash is fully adopted, however, then government can insist that people use it instead of physical money for payments such as taxes. This means the wealth will be trapped within the financial system.  
  
**The Strategy of Centralized Exchanges**  
  
The root problem with conventional currency is all the trust that’s required to make it work…We have to trust them [third parties] with our privacy, trust them not to let identity thieves [including government] drain our accounts—[Satoshi Nakamoto](http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source)  
  
The one thing CBDCs cannot survive is free-market competition. This is why every state that seeks a CBDC will make a concerted effort to eliminate or cripple free- market alternatives. An interesting aspect of this repression is that there is one form of non-state crypto that most governments will tolerate: digital currencies issued by licensed financial institutions. These currencies are no challenge to the central banking system because the issuing institutions are regulated to act as though they were affiliate banks. Licensed exchanges become the outer lobby of the central banking system. The lobby mimics the free market in some ways, but it bears no real relationship to it.  
  
A standard definition of a centralized exchange: “Centralized cryptocurrency exchanges are online platforms used to buy and sell cryptocurrencies. They are the most common means that investors use to buy and sell cryptocurrency holdings.” A [centralized exchange](https://news.bitcoin.com/blocknet-centralized-exchanges/) is a marketplace for trading or converting assets through a single location or service. The definition does not capture the problems that centralized exchanges present to the Satoshi model, however.  
  
But, first, what are problems that centralized exchanges solve? Why did they come into existence? There is a market demand to speculate, to trade in currencies, and to perform other sophisticated financial transactions for which peer-to-peer structures—decentralized exchanges—are not yet adequately equipped. There is also a demand for convenience and access to crypto that does not require technical knowledge or effort. For some, centralized exchanges also have the comforting familiarity of banks. Centralized exchanges fill a niche or else  
  
they would not be popular. They currently dominate much of the crypto world, with a majority of users entrusting exchanges with their wealth and privacy.  
  
The niche occupied by centralized exchanges comes from blending the functions of a stock market and a bank. In many ways, they are similar to the New York Stock Exchange. Currencies can be traded, shorted, and cashed out for fiat, for example; margin trading, stop loss, and lending are also available. In other ways, centralized exchanges resemble traditional banks. After purchasing crypto from an exchange, many customers choose to leave their coins in an account rather than transfer them to private wallets on their own hard drives. Centralized exchanges become trusted third parties; this means they present a terrible danger to the wealth and well-being of account holders. Consider one aspect of the risk. Most centralized exchanges hold the private keys of account holders. But private keys **are** the crypto. The coins have no physical presence, only algorithmic ones. When an exchange controls the keys, it de facto owns the coins. The customer has nothing more than a promise of access to them upon demand in the same way banks promise access to physical money upon an account holder’s demand.  
  
Recently, the risks associated with centralized exchanges increased exponentially and for one reason: the exchanges are increasingly complying or partnering with the state to enforce laws and reporting requirements on customers. A February, 2018 [*Forbes* article](https://www.forbes.com/sites/kellyphillipserb/2018/02/28/coinbase-notifies-customers-that-it-will-turn-over-court-ordered-data/#4b9de1921431) announced the inevitable regarding the world’s largest centralized exchange.  
  
It’s finally happening: The much-ballyhooed turnover of documents in the battle between the Internal Revenue Service (IRS) and Coinbase, a company which facilitates transactions of digital currencies like Bitcoin and Ethereum, is moving ahead. Coinbase has announced that it has notified affected customers that it will comply with a court order regarding the release of specific data.  
  
2018 was the year in which American tax agencies got serious about crypto profits and holdings. Governments around the world are watching as Coinbase turns in data on its customers, which will almost certainly lead to audits and/or high-profile prosecutions. Specifically, Coinbase is reporting all customers with transactions of $20,000 or more in a single year between 2013 and 2015. Taxpayer IDs, real names, dates of birth, street addresses, and all transaction records will be delivered. The wealth of data is available because Coinbase, like every other licensed exchange, complies with Know Your Customer and Anti- Money Laundering laws which destroy financial privacy.  
  
Coinbase has become extremely aggressive about gathering information and verifying identities. The exchange uses [facial-recognition technology](https://support.coinbase.com/customer/en/portal/articles/2909168-how-to-enable-a-webcam), for example, to compare a real-time face shot from a webcam or smart phone with whatever ID an applicant submits. Expect aggressive intrusion to become the norm for centralized exchanges because they prize their licenses and relationships with government. Expect them to act as data-gathering arms of the state. The danger is not only freezing and confiscation of accounts, but also legal proceedings  
  
against and imprisonment of account holders. The IRS [states](https://news.bitcoin.com/irs-reminds-taxpayers-report-virtual-currency-earnings/) that “anyone convicted of tax evasion is subject to a prison term of up to five years and a fine of up to $250,000. Anyone convicted of filing a false return is subject to a prison term of up to three years and a fine of up to $250,000.”  
  
Fortunately, the market demand for stock market and banking functions can be satisfied (or soon will be) without sacrificing privacy and safety. A decentralized exchange is a marketplace that does not rely on third party services. Trades are peer-to-peer; they are direct transfers between people who use an automated process to facilitate the exchange. They are trustless. They are transparent with software and transactions being open source. They are Satoshi.  
  
A [decentralized exchange](https://news.bitcoin.com/championing-decentralized-exchanges-now-might-be-the-perfect-time-for-bisq/) allows individuals to hold their own private keys which makes it a less attractive target for hackers. It also requires a minimal amount of personal or financial data to establish an account and to conduct commerce. Often, only an email address is requested, and it can be one that is generated specifically to register, with no connection to a real identity.  
  
Decentralized exchanges employ a wide variety of strategies to facilitate peer-to- peer transfers. Some create proxy tokens; others employ a multi-signature escrow. Peer-to-peer banking uses an auction-type dynamic to facilitate loans of a specific amount and at an agreed-upon rate between members. Smart contracts can assume the traditional functions of banks. *Technology Review* [explains](https://www.technologyreview.com/s/609621/cryptocurrency-exchanges-can-be-pretty-sketchy-places-the-solution-a-blockchain-of-course/) :  
  
Switching back and forth between fiat money and cryptocurrency will require a traditional point of exchange for the foreseeable future. But some technologists say an alternative model for trading crypto that would give people more control over their wealth is possible. Its metaexchanges can be decentralized, they say, using a blockchain. The idea hinges specifically on so-called smart contracts, software code that can be stored in a blockchain and set up to programmatically govern transactions. Imagine, for example, you want to send your friend some cryptocurrency automatically at a specific date and time. You could use a smart contract to do that.  
  
The point here is *not* to advocate a particular decentralizing tactic. It is to offer a sense of the rich and evolving alternatives to centralized exchanges. Many people will still choose a centralized exchange because the platforms are easy to access and use; they are sanctioned by government and this means respectability to some people; and they offer the familiar, advanced functions of a stock market. People have every right to make this choice with their own money, of course. But for those who prize privacy, it is an unacceptable alternative. (More on decentralized exchanges later.)  
  
An analogy illustrates the stark difference in how privacy and rights fare under a centralized and decentralized system: social media.  
  
“’Want To Freak Yourself Out?’ Here Is All The Personal Data That Facebook/Google Collect.” This is a March 2018 headline at *Zero Hedge*. The types of data collected  
  
are too extensive to enumerate. An indication: Android cellphone users who downloaded specific Facebook apps have had data on their personal calls logged by Facebook for years.  
  
A relatively undiscussed cause of social media’s privacy hemorrhage and its abridgment of free speech is the centralization of information and discussion that accompany corporate behemoths, like Facebook and Google. Large corporations form alliances of convenience and reciprocal profit with government. An intriguing article in *The Federalist* asks, “[Was Social Media A Mistake?](http://thefederalist.com/2018/03/19/social-media-mistake-heres-experiment-find/)” The author, Robert Tracinski, harks back to the 2000s—the golden age of blogs, when everyone and their grandmothers expressed themselves through blogging.  
  
Tracinski writes, “It felt like liberation. The era of blogging offered the promise of a decentralized media. Anybody could publish and comment on the news and find an audience…We were bypassing the old media gatekeepers. And we had control over it! We posted on our own sites. We had good discussions in our own comment fields, which we moderated.” It was a whirlwind of free speech, but it was also a bastion of privacy because individuals retained control. Individual control of data and expression is freedom.  
  
Then social media arrived like a juggernaut, and the mom-and-pop blogs migrated their diaries and information to Facebook, Google, Twitter, and other trusted third parties. Like centralized exchanges, the social media giants were relatively easy to access and use; they offered sophisticated software and functions that individual bloggers lacked the technical knowledge or money to implement; social media slid seamlessly onto cell phones via apps that seemed to open up the world. In reality, they closed down personal freedom.  
  
Tracinski notes the result.  
  
A few of the best and most interesting blogs became full-fledged online publications, but a lot of the small, quirky, one-person amateur bloggers moved onto social media. That turned out to be a big mistake, because the era of social media has *recentralized* the media. Instead of a million blogs— what Glenn Reynolds of Instapundit fame called an ‘[Army of Davids](https://www.amazon.com/Army-Davids-Technology-Ordinary-Government/dp/1595551131) ’—we now have a social media economy mostly controlled by three big companies: Twitter, Facebook, and Google.  
  
The price tag of centralizing personal writing has become apparent. The left- leaning politics of social media giants means that they purge (suspend accounts) or punished (throttled accounts) of those who hold “wrong” views. This is akin to banks and other financial institutions refusing to deal with porn, pot, or gun industries due to political pressure from government. “The old media gatekeepers” have been replaced by the equally intrusive Silicon Valley Puritans. Although both may be preferable to direct government intervention, their quasi- monopolies are bolstered by tax privileges, by favorable regulation, and by direct tax funding. In short, they may not be government, but they are certainly state  
  
cronies and owe their loyalty to it. As a result, individuals have lost control of their own work and data. Perhaps it is more accurate to say they relinquished it.  
  
Nowhere is the price tag of centralizing personal expression more glaring than with personal data. In return for convenience, all social media asked was to know and to market every detail of customers’s lives. The role of centralization in this rape of privacy was key to its effectiveness.  
  
Privacy is the front-line defense of individual freedom. Decentralization is the social condition under which privacy thrives. No one can or should tell individuals which strategy to use. But, if you value privacy and safety, stay private and decentralize.