Financial Freedom and Privacy in the Post-Cash World

Alex Gladstein

The future of currency is digital. The majority of transactions made every day are already electronic and controlled by banks or tech companies. These payments are easily surveillable, confiscatable, and censorable. Physical cash still functions as an essential savings mechanism and privacy tool for millions of people worldwide. With cash, individuals can buy goods and services or save without sharing their identity with a third-party merchant or custodian. But as banknotes fade from daily use, the future of financial freedom and privacy comes into serious jeopardy.

Users of platforms like Visa, Apple Pay, WeChat, or PayPal trade their freedom and privacy for convenience. Quick daily purchases done through phone apps or credit cards bear little resemblance to purchases done with cash. Transactions are no longer an exchange of bearer instruments but modified entries in a tech company's ledger. Personal information is demanded and shared rather than protected. For those without identification documents, these systems are inaccessible.

Beyond corporate money, two types of currency will most likely compete in the coming years to replace banknotes and their social function. One is central bank digital currency (CBDC): a digital central bank liability issued by governments across the world for citizens

---

Cato Journal, Vol. 41, No. 2 (Spring/Summer 2021). DOI:10.36009/CJ.41.2.7.

Alex Gladstein is Chief Strategy Officer at the Human Rights Foundation.

to hold and use directly in mobile wallet apps. The other is bitcoin: the world's most dominant, robust, liquid, valuable, and convertible cryptocurrency, distinguished by its monetary policy, which operates outside the control of governments and corporations. Both CBDCs and bitcoin could replace cash, but each system faces challenges in implementation, regulation, and adoption.

This article will take a global view on the civil liberties implications of both CBDCs and bitcoin as potential heirs to paper cash. According to the Human Rights Foundation (2020), approximately 4.2 billion people across 93 countries live today under authoritarian regimes. These individuals have little to no ability to push peacefully for reform concerning economic problems such as state corruption, currency debasement, and financial surveillance. Cash is a vital tool of savings and privacy for them. Once it is gone, the nature of whatever replaces it will, in no small way, dictate their freedom.

Financial Repression on the Rise

In countries like the United States and the United Kingdom, individuals have some protections against state or corporate abuse of financial power. Citizens in liberal democracies can petition effectively for change through their elected representatives, they can write op-eds to spark change in independent media, and they can even sue the government. Such accountability can trigger reform. For example, in the United States, after the global financial crisis, laws like Dodd-Frank (H. R. 4173 [2010]) were passed to prevent banks from gambling client funds. Central banks in electoral democracies also typically have some degree of independence from the executive branch, ostensibly shielding monetary policy from country's rulers' often-myopic whims. In addition, consumer protection laws, such as the Right to Financial Privacy Act in the United States, provide nominal defense against financial surveillance (FDIC 1978). But the truth is, even in liberal democracies where citizens can—in theory—protect themselves, corruption thrives and financial privacy is on the verge of extinction.

As revealed in the FinCEN files leak, in September 2020, Western banks are involved in the flow of hundreds of billions of dollars of dirty and corrupt money, much of which ends up in the coffers of the Davos elite, at the expense of the average citizen, with virtually none of the money launderers going to prison (FinCEN Files Reporting

Team 2020). A 2018 investigation by the *Financial Times* revealed that outside of a handful of executives from Iceland, Ireland, and Spain, only four bankers in the world were sentenced to jail time for their role in the global financial crisis (Noonan et al. 2018). And only one Wall Street executive—Credit Suisse senior trader Kareem Serageldin—actually went to prison. Even in democracies, financial actors at the top of the food chain have immunity, while lower- or middle-class people face a proliferation of financial restrictions.

In the United States, citizens are ruled by the Bank Secrecy Act (BSA), which forces financial institutions to disclose information about their customers to the federal government in an increasingly intrusive way. The BSA created a $10,000 daily cash reporting threshold in 1970, but authorities never adjusted for inflation. This means more transactions fall under surveillance every year. When the threshold was first created, only transactions that were more than approximately $60,000 (in today's dollars) were monitored, but now, as a result of gradual inflation, payments six times smaller are tracked (Bureau of Labor Statistics 2020). Ironically, the U.S. government's FinCEN *fines* are adjusted for inflation (Financial Crimes Enforcement Network 2020).

In general, very little American economic activity is protected from the eyes of the government. In 1976, the Supreme Court case *United States v. Miller*, 425 U.S. 435 (1976) ruled that bank records are not protected under the Fourth Amendment, establishing the "third-party doctrine" holding that citizens who voluntarily provide financial information to banks have no expectation of privacy. This doctrine enables the government to collect financial data from banks without a warrant or probable cause.

The digital currency–focused nonprofit CoinCenter points out that, when the BSA was rendered constitutional in the United States in 1971, dissenting justices voiced major concerns about privacy leaks that would happen when Americans transacted through intermediaries (Brito and Valkenburgh 2020). The BSA still stands, but compared to 1971, when most small transactions were done with paper money, today nearly every transaction an American makes is done through an intermediary, available for the government to peruse.

The situation in the United States is an example of how even some of the world's most empowered citizens—protected by a Bill of Rights, an independent judiciary, and a free press—struggle to challenge the creeping erosion of their financial rights.

In dictatorships and authoritarian regimes, the prospects for financial freedom and privacy are darker still. There are no accountability mechanisms like independent media or an independent Supreme Court in countries like China, Saudi Arabia, Russia, and Turkey. Such regimes often abuse their money printing abilities to satisfy short-term aims with no public accountability, they conspire with the heads of commercial banks to commit massive fraud, and they trespass on the financial transactions of their citizens with no fear of penalty.

Ironically, the Chinese, Saudi Arabian, Russian, and Turkish governments are all part of the Financial Action Task Force (FATF), a multilateral organization responsible for crafting recommendations and customs for global financial policy. These regimes stand diametrically opposed to values like freedom and privacy, yet can influence FATF recommendations, steering the whole world toward more financial restrictions and state immunity.

These regimes routinely win seats on the United Nations Human Rights Council. There is significant public protest against this hypocrisy, but there is virtually no opposition to these same regimes being allowed to govern financial bodies. One FATF recommendation worth mentioning is the "Travel Rule," which urges money transmitters to share customer information, creating an international financial dragnet.

In October 2020, in the United States, FinCEN and the Federal Reserve Board opened the door for a new, more invasive interpretation of this rule. Today, American financial institutions are obligated to share information about transactions of more than $3,000. The proposed rule would mean surveillance for any international transaction of more than $250 (Board of Governors 2020). This crackdown is in line with general government sentiment following last September's FinCEN files leak, where authorities have called for more restrictions and less privacy to "solve" the problem of corruption.

Given expected future U.S. inflation, this trend of decreasing the surveillance threshold is especially troublesome, leading to more and more transactions under watch. As CoinCenter notes, "The current threshold for 'travel rule' obligations ($3,000) was in 1971 roughly equivalent to $20,000 in today's money adjusted for inflation. The newly proposed $250 threshold would equate to a $40 threshold in 1971 when these warrantless data collection mandates were last constitutionally scrutinized" (Brito and Valkenburgh 2020: 4).

While there still may be a slim hope that citizens can push and lobby to keep some vestiges of financial freedom in electoral democracies, this possibility is nonexistent for the billions of people who live under dictatorships. Because of the great global digital transformation, even that slim hope for citizens of the free world is rapidly shrinking.

The War on Cash

Society is currently undergoing a historic shift away from paper-based, bearer asset daily money toward completely electronic, corporate ledger daily money. This change is part of a long trend of disuse of all bearer instruments, like stock certificates and bearer bonds.

Decades ago, small daily transactions were predominantly made with coins or notes, which disclosed nothing about the buyer to the seller. Cash is an excellent privacy tool, capable of fully anonymous transactions—for example, a donation to a community collection box. Cash also permits citizens to save securely. Putting money under a mattress may be widely mocked, but banknotes and especially dollar bills are still commonly stored in this manner in countries around the world.

Credit cards, on the other hand, are an excellent tool for surveillance and control. Increasingly, individuals make purchases with credit cards, smartphones, and even wearables, revealing a tremendous amount of information about them to merchants, third parties, and governments. Funds in bank accounts or phone apps are freezable and seizable. Given existing trends, where only about a quarter of daily transactions in the United States are still done with cash, it is not hyperbole to say that children born today are unlikely to use paper money as adults in the 2040s and beyond (Board of Governors 2019).

As the monetary historian Brett Scott explains, there are three traditional varieties of money in use today: (1) central bank or public money, in the form of reserves issued to banks and banknotes or coins given to the public; (2) commercial money, dispensed by those big banks; and (3) "fintech" money, private ledgers operated by tech companies using commercial bank accounts (Scott 2020).

Scott observes a "war on cash" where the (bearer asset) public money notes and coins that the world has used in the past few hundred years are being replaced primarily by commercial digital money. This was accelerated in 2020 by the Covid-19 crisis, where a Bain

analysis indicated that the pandemic could trigger a 10 percent reduction in cash payments in the coming five years (Gringoli et al. 2020). The World Bank, meanwhile, has publicly called for more digital payments for the sake of "social protection" against banknotes that could transmit disease (Rutkowski et al. 2020).

Undoubtedly, the commercial and fintech monies that Scott describes are on the rise. While a 2019 Consumer Payment Choice study showed cash still being used in 26 percent of daily American transactions, that number is down 5 percent over the previous two years alone (Board of Governors 2019). Elsewhere, from London to Seoul to Berlin to Caracas, cash plays an even smaller role in people's daily lives. Increasingly, consumers rely on debit cards, credit cards, and phone apps built by a variety of fintech and tech companies to transact (Kumar and O'Brien 2019).

Individuals transact more and more on corporate ledgers based on, for example, dollars, euros, or renminbi. Moving forward, they could very well also be based on currencies issued by companies. The early failure of Facebook's Libra project should not distract us from the potential future of independently run corporate currency.

According to fintech analyst Nic Carter, as of October 2020, $20 billion of stablecoins are in circulation, with that number only projected to increase in the coming months and years (Carter 2020). While these "stablecoins'" are virtual assets mainly pegged to fiat currencies, they are controlled by nonstate corporate actors and operate as a kind of shadow banking system.

No matter the form, corporate money—whether traditional fintech or new stablecoins—is censorable, trackable, subject to regulatory capture, and is an inadequate replacement for paper money and its role as a savings and privacy tool.

Central Bank Digital Currency

In the war on cash, whatever money is not replaced by Apple, Ant Financial, or a new corporate stablecoin may be replaced by a digital form of public money. Governments worldwide seek to replace cash with a new form of central bank liability known as central bank digital currency. Today, central bank liabilities exist in the form of digital reserves given to commercial banks and in the form of banknotes distributed to the public. CBDCs would be digital central bank liabilities distributed directly to the public.

An operational CBDC system could, hypothetically, allow central banks to have fine-grained control over fiscal stimulus, delivering cash to specific subsections of the population at the press of a button. In a world where citizens couldn't extract physical banknotes out of their deposit accounts, CBDCs could allow the widespread introduction of negative interest rates, where citizens would be forced to pay a fee to save their money. CBDCs could also help governments more easily confiscate funds from political opponents or even auto fine people who violate certain laws.

Already in 2020, the world's biggest governments were openly experimenting with CBDCs. As of October 2020, the Federal Reserve said it was undertaking "active research" in this area (Brainard 2020), with Fed chair Jerome Powell describing a cautious yet serious approach to CBDCs in recent public remarks (Hayashi 2020). U.S. lawmakers have proposed that reserve banks create "digital dollar" wallets (S. 3571 2020), and MIT's Digital Currency Initiative has started a research effort to explore the design of CBDCs in cooperation with the Federal Reserve Bank of Boston (Narula 2020). Elsewhere, CBDC projects are being rolled out everywhere from Beijing to Brussels to London. According to a recent survey conducted by the Bank of International Settlements, 20 percent of central banks are likely to launch a digital currency by 2025, and 80 percent of central banks are actively researching a CBDC (Auer et al. 2020).

As digital currency scholar Michel Rauchs observes, CBDCs aren't primarily about digitizing payments (Rauchs 2020). Again, most money is already digital. He argues that the real goal is to nationalize or rein in financial infrastructure and the commercial banking sector. The public sector "has effectively outsourced the creation, management, and distribution of money to the private sector," and CBDCs present a challenge to and possible reversal of this system.

There are two main visions for CBDCs: token-based and account-based systems. As monetary historian Lawrence H. White points out, account-based CBDCs would mean that "households and businesses have retail checking accounts directly" on central bank balance sheets (White 2020). He argues, convincingly, that a government bureaucracy would be spectacularly bad at handling the customer service needs of tens or hundreds of millions of new clients.

A token-based system is a more widely discussed option. This would mean that households and businesses hold central bank

liabilities (Fedcoins or digital dollars) in smartphone or computer wallets likely designed by third-party tech companies. A high-profile research and policy group called the "Digital Dollar Project" is already lobbying for a token-based model in the United States (Giancarlo and Gorfine 2019).

Regardless of the format, CBDCs will face resistance. As the *Wall Street Journal* recently reported, commercial banks are worried about CBDCs limiting their source of customer deposits and shrinking their businesses (Sindreu 2020). Some central bankers are even worried that citizens will take their commercial deposits and swap them for CBDCs, in what could amount to a massive slow-motion global bank run (Alloway and Weisenthal 2020).

CBDCs and Financial Freedom

If CBDCs can launch successfully, the big question remains: Will they function like cash and be anonymous bearer assets, not leaking anything about buyers and sellers, or will they function like commercial money and pair transactors to names and addresses and share that sensitive information with third parties? For now, governments seem united in saying they won't design CBDC systems with full anonymity. While a payment in one of these systems may protect against leaking transaction data to the general public, backdoors would be built-in, allowing government access to the data.

In December 2019, the European Central Bank (ECB) published a paper exploring anonymity in central bank digital currencies, where they describe a "simplified CBDC payment system that allows users some degree of privacy for lower-value transactions, while still ensuring that higher-value transactions are subject to mandatory AML/CFT checks" (ECB 2019). This would be a "hybrid privacy" model (Koning 2020), which is to say, privacy would be discretionary and up to the authorities. In October 2020, the ECB noted that anonymity "may have to be ruled out" in the design of a CBDC euro (Lagarde and Panetta 2020: 27).

In the United States, the architects of the Digital Dollar Project say they will "support a balance between individual privacy rights and necessary compliance and regulatory processes." Moreover, according to Loretta Mester, president of the Federal Reserve Bank of Cleveland, American digital cash "would be just like the physical currency issued by central banks today, but in a digital form and,

potentially, without the anonymity of physical currency" (Mester 2020: 9). The Bank for International Settlements has been perhaps the most unequivocal—noting that "full anonymity [for CBDCs] is not plausible" (BIS 2020: 6). Not often mentioned is that anonymity is a costly feature to build in a digital system and requires strong motivations to pay that cost.

In 2005, several central bank advisers, including Charles Kahn, wrote that the key social function of cash is to protect the purchaser's identity and that, even though banknotes may get displaced, users would push for their survival (Kahn, McAndrews, and Roberds 2005). However, the ensuing decade seemed to change Kahn's mind. In 2017, he wrote,

> When central banks first took on the job of note issuance they became privacy providers. . . . As they try to get out of the paper money business, I think the future of central banks and payment authorities is no longer in privacy provision, but in privacy regulation [Kahn 2017: 11].

That regulation is subject to constant negotiation and an observable erosion of citizen rights. In fact, in 2020, Kahn pushed his opinion even further away from a defense of privacy writing that an anonymous CBDC would pose "security risks" to users (Kahn and Rivadeneyra 2020: 3).

Even if citizens of democracies could convince their governments that digital cash should have the same privacy qualities as paper cash—which seems unlikely—could such a system be built? Technically, today, the answer is unclear.

For a digital currency to provide true freedom and privacy, it must be decentralized and not have "backdoors" that enable third-party control of transactions. The only proven mechanism to achieve this goal is decentralization of transaction processing, as found in bitcoin's proof-of-work model (Nakamoto 2008). But, as discussed later in this article, even bitcoin's model is only pseudonymous and has significant privacy issues. There is no way, at the moment, to make a decentralized currency that has both an auditable money supply and fully anonymous transactions. If priority is given to anonymity, the system could be undermined by an undetectable "inflation bug" where attackers could exploit flaws in the code to quietly create more money, wreaking havoc on the stability of the system.

A central bank could try the centralized route and issue digital cash that doesn't offer the confiscation resistance and censorship resistance of banknotes but provides strong privacy. This technology might look like Chaumian e-cash, which could theoretically allow an administrator to issue a digital currency made anonymous through blind signatures (Chaum 1982). But even if such a system could be built where transactor identities were hidden, administrators could still freeze or confiscate funds. And unlike banknotes, which can be collected in huge amounts, governments would likely not permit digital cash usage beyond a certain daily threshold. Today's stablecoins like Tether and USD Coin provide a useful comparison, as they are digital pseudonymous currencies operated by companies, pegged primarily to dollars. And yet, they still have blacklists and comply with government regulations.

According to the public money advocate Rohan Grey, as of October 2020, there is not "a single" technical paper or resource explaining how fully anonymous public money would work (Grey 2020). A 2019 Bank of Canada overview on privacy in CBDC technology concludes that "techniques to achieve cash-like privacy are immature . . . their risks include hidden vulnerabilities, a lack of scalability, and complicated operations" (Arora and Dharba 2020).

In sum, the age of central bank liabilities offering protection from surveillance and seizure is ending. It is unlikely that electoral democracies will soon learn how to build privacy-protecting CBDCs, and even more unlikely that they would have the motivation to provide them to the public. After all, many of the features that excite central bankers—the ability to micromanage the economy or to comply better with anti-money laundering laws—are incompatible with anonymous money. And for the billions of people living under dictatorships, there is simply no hope that the crucial privacy and savings benefits of cash will survive into the digital era.

Social Engineering through Monetary Control

In the early age of digital money, before smartphones, the machine learning and AI algorithms necessary to make sense of hundreds of millions of transactions did not exist. But today, governments and corporations can understand the language of global payments. Within moments of buying something online with a tap or

swipe, your identity is revealed to authorities and data markets that share and trade your personal information. The end of cash and the insta-analysis of financial transactions enable surveillance, state control, and, eventually, social engineering on a scale never thought possible.

In China, this is unfolding with alarming rapidity and existential social impact. Real-time linking of all payments to identities has allowed for the beginnings of a vast social credit system that—though more Kafkaesque than Orwellian and seemingly patchwork for the time being—lays the foundation for eventual financial omniscience (SupChina 2020). When the government can take financial privileges away for posting the wrong word on social media, saying the wrong thing in a call to parents, or sending the wrong photo to relatives, individuals self-censor and exercise extreme caution. In this way, control over money can create a social chilling effect.

Consider Andrew Liu's analysis of harsh Chinese mobile payment regulations: "While the Chinese government puts up an altruistic front of wanting to prevent criminal activity and improve mobile payment security, the People's Bank of China (PBOC) and Chinese Communist Party's true intentions . . . are far more pragmatic, and seek to help the Communist Party maintain full political, social, and economic power of the country" (Liu 2019: 96).

Today, 90 percent of citizens in the most populous Chinese cities use WeChat and AliPay as their first choice for payments and already rely on QR codes and digital wallets for transactions (Tencent 2019). But a CBDC would allow the Chinese Communist Party (CCP) to take back some of the financial power that Ant Group and Tencent have accumulated through these products while giving the government greater and easier insight into citizens' daily micro-financial activity. As PBOC digital currency research head Mu Changchun said in October, "WeChat and AliPay are just wallets, while the DCEP is the money inside them" (Tang 2020).

DCEP, which stands for "digital currency and electronic payment," is the CCP's CBDC project, initiated in 2014 and launched in 2020, and is a digital liability of the PBOC. Though marketed as offering privacy for users, DCEP will offer the PBOC total surveillance capabilities, augmented by big data analysis and AI systems.

DCEP is being built primarily as a substitute for bank notes, and the PBOC doesn't plan to pay interest. As of now, citizens will purchase DCEP with their traditional digital RMB from commercial

banks, which are required to deposit one-for-one with the PBOC in a 100 percent reserve arrangement. The PBOC recently published a draft law that includes DCEP as part of the country's fiat currency and bans any other party from issuing RMB-backed digital tokens (Tang 2020).

In October 2020, distribution began with a government handout of 10 million RMB of DCEP to 50,000 winning residents in Shenzhen, around $30 per person (Manoylov 2020). Allocation was done by lottery, which some two million individuals signed up to enter. The winners could spend the DCEP at more than 3,000 cooperating merchants.

DCEP is already being piloted in several major regions in China, is scheduled to be used at the 2022 Olympic Games, and is a major fixture of CCP propaganda. According to a 145-page document released last summer by the Beijing municipal government, the overarching goal of Chinese products like DCEP is a "programmable society" (Graham 2020).

In a recent brief, the Australian Strategic Policy Institute made the following conclusion about DCEP:

> It has the potential to create the world's largest centralised repository of financial transactions data. . . . It would also create unprecedented opportunities for surveillance. . . . It is not far-fetched that the Chinese party-state will incentivise or even mandate that foreigners also use DC/EP for certain categories of cross-border RMB transactions as a condition of accessing the Chinese marketplace. . . . A successful DC/EP could greatly expand the party-state's ability to monitor and shape economic behavior well beyond the borders of the PRC [Hoffman et al. 2020: 3].

It is fair to question claims that most people across the world will one day use a Chinese digital currency, simply because only 2 percent of the world's foreign exchange transactions are done in yuan (Brown 2020), and less than 2 percent of the world's foreign exchange reserves are held in yuan (IMF 2020). But if these numbers begin to rise, perhaps on account of broader use of DCEP by citizens around the world through phone apps, then more attention should be paid—especially given the CCP's track record of mass financial transformation, where in just a matter of years, they leapfrogged

hundreds of millions of citizens from cash, past credit cards, and straight into mobile payments.

China's control and surveillance-based CBDC system is also an increasingly inspirational and attractive proposition for authoritarian governments from Cambodia to Cuba to Cameroon. Even if a few hundred million people in North America and Europe enjoy enough civil liberties and democratic rights to push back against a digital panopticon, more than 4 billion people lack those same rights and have no way to fight back.

Another point to consider is that in a fully implemented CBDC system, governments could financially exclude individuals or entire groups of people with the press of a button, leaving them with nothing. Governments like the CCP could target dissidents, sexual minorities, ethnic minorities, or religious minorities. If banknotes don't exist and access to government-issued digital cash is revoked, then they are truly helpless.

Freedom and Privacy through Technology

Given the global prevalence of authoritarianism and the eager nature of even democratic governments to erode privacy, public-driven policy reform is unlikely to protect the digital rights of everyone in the world. The alternative is to build monetary tools that cannot be abused by governments and that protect the financial freedom and privacy of individuals.

The perspective's ethos was perhaps best enunciated by Wei Dai, a cryptographer whose pioneering work was cited in the bitcoin white paper. In a prescient February 1995 email to the Cypherpunks mailing list, Dai said:

> There has never been a government that didn't sooner or later try to reduce the freedom of its subjects and gain more control over them, and there probably never will be one. Therefore, instead of trying to convince our current government not to try, we'll develop the technology . . . that will make it impossible for the government to succeed.
>
> Efforts to influence the government (e.g., lobbying and propaganda) are important only in so far as to delay its attempted crackdown long enough for the technology to mature and come into wide use.

> But even if you do not believe the above is true, think about it this way: If you have a certain amount of time to spend on advancing the cause of greater personal privacy (or freedom, or cryptoanarchy, or whatever), can you do it better by using the time to learn about cryptography and develop the tools to protect privacy, or by convincing your government not to invade your privacy? [Dai 1995]

It was easy for Dai to conclude, even in the mid-1990s, that it would be more effective to build authoritarian-resistant technology than to try and plead with governments that they should not invade individual privacy.

Over the past three decades, that strategy has been followed, and open source technology has forced public opinion and even government policy toward a more favorable view of citizens protecting their personal communications and information.

In the early 1990s, the U.S. government tried and failed to classify encryption technology as illegal. At that time, privacy activists like Adam Back printed encryption source code on T-shirts to protest the U.S. government's attempts to restrict the export of private email messaging tools. These shirts had, for example, code allowing one to encrypt a message on the front, and images of the U.S. Bill of Rights on the back, under a VOID stamp. Today, these shirts are no longer illegal to export from the United States or to show to foreigners, due to the government's changing the laws and conceding that it couldn't stop the code.

Today, communications encryption technology has become wildly popular, with open-source phone apps like Signal boasting tens of millions of daily active users and even closed-source chat applications that serve billions like WhatsApp and Facebook Messenger incorporating some level of encryption. Michael Hayden, who famously ran the National Security Administration at the time of the 9/11 attacks and the outbreak of the War on Terror, has even argued that "Americans are safer with end-to-end encryption," and that backdoors sought by the government undermine everyone's security (Hayden 2016).

Digital freedom and privacy tech have become so popular in part because many customers oppose third parties spying on or trying to sell their information. It has also spread because it is powered by open-source code that cannot be reliably stopped or easily regulated.

Personal communications remain at risk, with the governments of seven countries, including the U.S. Department of Justice (2020), recently threatening a crackdown on end-to-end encryption. But social sentiment on privacy is shifting toward mainstream acceptability. Even in authoritarian China, there is public surveillance fatigue, a fear of rising data collection (Feng 2020), and tens of millions of citizens who use VPN (virtual private network) technology to break the law and hide their internet browsing activity from authorities (Marvin 2018).

The past three decades demonstrate that even when there is no political will to enshrine digital freedom and privacy, computer scientists and cryptographers can defend it through open-source code.

Bitcoin: Open-Source Money

If all money is becoming digital, and if corporate money is going to be a tool of control and surveillance, and if most citizens across the world will not be able to convince or pressure their governments to develop and implement digital cash, then what can be done to protect financial freedom and privacy for all of humanity? Could someone do for money what the cryptographers of the 1990s did for personal communications?

Enter Satoshi Nakamoto and bitcoin, an open-source, peer-to-peer, decentralized electronic cash system. Nakamoto's (2008) creation offers three significant advantages versus CBDCs and convenient-yet-centralized fintech.

First, bitcoin is an international payment system that is not tied to any personal identification, cannot be stopped by authorities, and does not require trusted third parties. Today, with bitcoin, anyone can download software from the open internet and send any amount of money to anyone else within minutes, without asking permission from any government, without needing to provide personal information, and without the possibility of censorship. The transaction does not contain your phone number, email address, or any other identifying information. This is the revolution that Wei Dai and Adam Back pushed for in the 1990s: if citizens cannot convince governments to protect their financial rights, they must make technology that renders mass surveillance impossible.

Second, bitcoin's "be your own bank" feature makes it more difficult to seize. Users have the option of self-custody and can keep the

password to their funds written down or inscribed somewhere hidden, locked in a multiparty arrangement requiring the digital signatures of several individuals, or even memorized. When the U.S. government seized gold through executive order 6102, this effort was effective as authorities could simply go to banks custodying everyone's gold and capture it there. But it would be extraordinarily expensive and time consuming for a government to try and seize the bitcoin of all or even most of its citizens.

Third, bitcoin provides a level of financial freedom beyond even the capabilities of banknotes: protection against inflation. There were private digital currencies before bitcoin, most famously David Chaum's DigiCash. However, a fundamental problem of DigiCash and other similar experiments was that they were tied to the existing banking system. Their tokens were digital representations of dollars and euros and were, in one way or another, controllable by the issuers of dollars or euros. In contrast, bitcoin is an entirely parallel economic system.

The following text is embedded in the very first entry in bitcoin's blockchain ledger: *Times 03/Jan/2009 Chancellor on brink of second bailout for banks*. The text references a report from the British newspaper *The Times* on how the government rescued banks by printing more money. In contrast, Nakamoto created a monetary system that could not be arbitrarily inflated, instituting a decentralized, algorithmic issuance schedule that will eventually end with a final circulation of just under 21 million bitcoin. With this, Nakamoto was the first to invent decentralized digital scarcity. Like gold, bitcoin is scarce, and its issuance is based not on the whims of bureaucrats but on a decentralized global competition. But unlike gold, bitcoins are digital and can be sent across the world in minutes and can be effectively hidden from seizure.

Neither governments nor billionaires can change the rules of the bitcoin network or prevent individuals from making transactions. This set of properties has given bitcoin tremendous monetary value. Today, each bitcoin is worth more than $50,000, and the network has a global market capitalization of more than $1 trillion.

An increasing percentage of Wall Street and Silicon Valley insiders are starting to buy bitcoin directly or through financial vehicles. For example, Paul Tudor Jones, one of the world's most prominent investors, announced a large bitcoin position in June 2020; two months later, Michael Saylor, the CEO of the publicly traded MicroStrategy,

swapped more than $450 million of cash on his company's balance sheet for bitcoin; and one month later, fintech giant Square announced an acquisition of $50 million of bitcoin and has launched an effort to support bitcoin software development. Most recently, Tesla bought $1.5 billion of bitcoin. The trends point to a future where large corporations and even governments add bitcoin positions to their balance sheets to hedge against instability and inflation.

If economic elites and governments invest in bitcoin—even if merely because of self-interest—it inhibits their ability to stop it. This could potentially drive them to want to accumulate more bitcoin, as opposed to shutting it down. The first governments to join the fray might be rogue states that may resort to bitcoin as a plan-B reserve asset if they are locked out of the Western financial system, are sanctioned, or can't easily acquire dollars or euros. In a world where there may be no government incentive or ability to make digital cash, bitcoin could harness greed and self-interest to help it survive.

Bitcoin and Financial Privacy

As of 2020, bitcoin faces several challenges in its quest to become digital cash, including privacy, small transaction usability, and merchant adoption. On a technical front, bitcoin has a long way to go to provide privacy for its users. Given its open ledger model, today it can be trivial to track transactions on its blockchain ledger. While it is true that governments or corporations have to deanonymize users first and pair their personal information to addresses to make sense of what's happening on the blockchain, the reality is that, at the moment, most users buy bitcoin from exchanges like Coinbase, where they must provide their personal information. This means Coinbase knows everything about them so that when they withdraw their funds to a private address, Coinbase knows who owns those coins. Coinbase could then be subject to regulatory pressure (perhaps a call from the NSA or FBI) or hacking (if criminals steal internal information, they might launch ransomware attacks against individuals who have withdrawn large amounts of bitcoin).

On the bright side, a growing number of smartphone applications and techniques are improving transaction privacy by enabling users to collaboratively spend their coins and move funds or make payments in an extremely difficult way for authorities to follow. There are also nascent technologies like the Lightning Network and statechains that

help by moving bitcoin transactions off the surveillable ledger onto a second layer. So, while today chain surveillance is a clear and present danger to bitcoin users, the currency's programmability points in the direction of more privacy. An upcoming bitcoin network upgrade called Taproot will provide significant privacy upgrades by enabling systems that make it harder to differentiate transactions and that push more transactional data off the ledger.

There are, of course, other cryptocurrencies that market themselves as privacy protecting. They are important to track in as much as they experiment with privacy features that aren't stable enough to be introduced into bitcoin. Monero and ZCash are two examples. There are also ways to build private transactions using Ethereum. These alternatives, however, in the long term, lack bitcoin's decentralized scarcity value proposition and are vulnerable to the following:

- Creator or majority-owner abuse or conflict;
- Undetectable inflation bugs causing instability;
- Scaling issues;
- Small crackable anonymity sets;
- Or some combination of the foregoing.

Any major problems cause the price of the system's token to drop on the open market, which disincentivizes mining, which reduces network security, causing a further drop in price. So, while these alternative cryptocurrencies are useful to observe from a scientific perspective, they project to eventually dwindle to zero in bitcoin or dollar terms, making them weak financial tools for future generations.

Bitcoin and Small Transactions

In recent years, bitcoin could be used like banknotes for small purchases, as the transaction fee was only on the order of a few cents or dollars. However, fees have at times eclipsed $15 in recent months and should continue to rise significantly with increased global network usage. In the far future, users will pay a premium to make bitcoin transactions and will only likely use it as a settlement layer or when they need to cash out savings or take advantage of bitcoin's borderless, confiscation-resistant, censorship-resistant properties.

If bitcoin is to replicate the social function of cash over the long term, tiny amounts must be spendable. This is where second-layer scaling technology could provide a solution. Just as promises to pay gold in the form of banknotes historically triggered the growth of

commerce, and just as promises to pay banknotes in the form of credit cards later triggered the growth of even more commerce, a similar evolutionary phenomenon could be possible with bitcoin.

In addition to improving privacy, the Lightning network provides instant and cheaper payments, without users needing to trust intermediaries. Lightning fees are based on the amount sent, making it favorable for small transactions. Statechains like the Mercury network could also increase the amount of bitcoin activity without increasing the amount of network-level bitcoin transactions. Both ideas allow users to batch many payments into a single entry, avoiding transaction fees. For now, these solutions are early in development and lack sufficient usability and stability. But every few months, they are improved by a growing ecosystem of open-source developers and corporate competition.

These types of technological solutions to scaling bitcoin are vastly preferable to scaling bitcoin through third parties. For example, if 10,000 users buy bitcoin on Coinbase, they aren't making 10,000 transactions: Coinbase marks these purchases on its internal ledger, and only occasionally buys bitcoin in batches to add to its reserve. But in this case, the users don't actually control their bitcoin. They are trusting Coinbase, which knows everything about them, and bitcoin used in this way, while perhaps an effective savings asset, is simply an expansion on the current system of corporate money and not a digital replacement for cash.

Bitcoin and Merchant Adoption

A significant challenge for increased bitcoin adoption is the increasing number of restrictions on exchanges and users. If one is to use bitcoin like cash, then one should be able to buy something or withdraw bitcoin from an exchange without divulging personal information.

Mixing and second-layer privacy technology covered above may help users retain privacy after withdrawing bitcoin from custodians. But if merchants are forced by "know your customer" laws to identify customers who wish to pay in bitcoin, then any technological privacy benefits could be nullified. These rules, designed by FATF, FinCEN, and others, will provide major challenges for the growth of the bitcoin ecosystem. However, it's again important to give global consideration to bitcoin, which may not see adoption as a means of payment first in advanced economies where there is already so much fintech competition. Much of bitcoin's growing user base is elsewhere.

An increasing number of users are navigating trade channels between, for example, Nigeria and China, or sending remittances home to countries like the Philippines from thousands of miles away, or are living inside sanctioned countries like Iran and Venezuela. Merchants in certain regions will accept bitcoin to varying degrees and will be subject to, or will choose to enforce, different kinds of KYC (know your customer).

Conclusion

In "Cypherpunk's Manifesto," privacy activist Eric Hughes (1993) wrote: "We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence." The world seems destined to track toward the extinction of banknotes and an endgame of trackable and seizable CBDC and commercial money. In the post-cash world, there simply may not be very much financial freedom and privacy. In this context, bitcoin is worthy of continued study and exploration by monetary economists and human rights activists alike.

Bitcoin's unique combination of open source programmability, permissionlessness, scarcity, censorship resistance, seizure resistance, and decentralization makes it a promising foundation for digital cash, especially for the billions of people unable to lobby their governments to uphold digital freedom and privacy, who may have no other option.

Bitcoin is already helping individuals in nearly every country on earth replicate the savings aspect of physical cash. Whether it can just as effectively replicate the private payments aspect may be something that only follows later, as adoption and awareness spread.

References

Alloway, T., and Weisenthal, J. (2020) "Benoît Coeuré on Central Bank Digital Currencies." Bloomberg's *Odd Lots Podcast* (October 21).

Arora, R., and Dharba, R. (2020) "Privacy in CBDC Technology." Staff Analytical Note 2020–9 (June), Bank of Canada. Available at www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/ Bank of Canada.

Auer, R., et al. (2020) "Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies." Bank for International Settlements (August 24).

Bank for International Settlements (2020) "Central Bank Digital Currencies: Foundational Principles and Core Features." Available at www.bis.org/publ/othp33.pdf.

Board of Governors of the Federal Reserve System (2019) "The 2019 Federal Reserve Payments Study." Available at www.federalreserve.gov/paymentsystems/2019-December-The-Federal-Reserve-Payments-Study.htm.

_____ (2020) "Agencies Invite Comment on Proposed Rule under Bank Secrecy Act" (October 23). Available at www.federalreserve.gov/newsevents/pressreleases/bcreg20201023a.htm.

Brainard, L. (2020) "An Update on Digital Currencies." Speech at the Federal Reserve Board and Federal Reserve Bank of San Francisco's Innovation Office (August 13).

Brito, J., and Valkenburgh, P. (2020) "Comments to the Board of Governors of the Federal Reserve System and the Financial Crimes Enforcement Network on Changes to Threshold for 'Travel Rule' Obligations." CoinCenter (October 29).

Brown, T. (2020) "China's Digital Currency Ambitions Are on Display in 1 Billion Yuan Roll Out." *Barron's* (October 15).

Bureau of Labor Statistics (2020) "CPI Inflation Calculator."

Carter, N. (2020) "The Crypto-Dollar Surge and the American Opportunity." CoinDesk (September 3). (Note: Carter provided author with updated number on October 30.)

Chaum, D. (1982) "Blind Signatures for Untraceable Payments." University of California, Santa Barbara.

Dai, W. (1995) "Law vs Technology." Cypherpunks Mailing List (February 10). Available at https://cypherpunks.venona.com/date/1995/02/msg00508.html.

European Central Bank (2019) "Exploring Anonymity in Central Bank Digital Currencies." *In Focus* 4 (December).

Federal Deposit Insurance Corporation (1978) "Right to Financial Privacy Act."

Feng, E. (2020) "In China: A New Call to Protect Data Privacy." NPR (January 5).

Financial Crimes Enforcement Network (2020) "Inflation Adjustment of Civil Monetary Penalties." *Federal Register* (February 19).

FinCEN Files Reporting Team (2020) "HSBC Moved Ponzi Scheme Millions Despite Warning." *BBC News* (September 20).

Giancarlo, C., and Gorfine, D. (2019) "We Sent a Man to the Moon. We Can Send the Dollar to Cyberspace." *Wall Street Journal* (October 15).
Graham, M. (2020) "Last Week the Beijing Municipal Government Released a 145 Page Document Outlining Its Vision for Utilizing Blockchain to Create a 'Programmable Government.'" We Read the Doc So You Don't Have to. Here's What's Important. THREAD" Twitter (July 22).
Grey, R. (2020) "There Isn't One Single One, Unfortunately. But at This Stage That Isn't the Issue as Much as Political Will." Twitter (October 9).
Gringoli, V., et al. (2020) "The Covid-19 Tipping Point for Digital Payments." Bain & Company (April 29).
Hayashi, Y. (2020) "Fed Takes Cautious Approach to Possibly Issuing Digital Currency." *Wall Street Journal* (October 19).
Hayden, M. (2016) "Michael Hayden: America Is Safer With End-To-End Encryption." WBUR (March 1).
Hoffman, S., et al. (2020) "The Flipside of China's Central Bank Digital Currency." ASPI International Cyperpolicy Center.
Hughes, E. (1993) "A Cypherpunk's Manifesto." Available at https://nakamotoinstitute.org/static/docs/cypherpunk-manifesto.txt.
Human Rights Foundation (2020) "Political Regime Map."
H. R. 4173 (2010) "Dodd-Frank Wall Street Reform and Consumer Protection Act." Commodity Futures Trading Commission (January 5).
International Monetary Fund (2020) "Currency Composition of Official Foreign Exchange Reserves."
Kahn, C. M. (2017) "The Threat of Privacy." Keynote Address at Financial Market Infrastructure Conference II: New Thinking in a New Era, De Nederlandsche Bank, Amsterdam (June 7–8).
Kahn, C. M.; McAndrews, J.; and Roberds, W. (2005) "Money is Privacy." Available at SSRN: https://ssrn.com/abstract=714265.
Kahn, C. M., and Rivadeneyra, F. (2020) "Security and Convenience of a Central Bank Digital Currency." Bank of Canada (October 5). Available at www.bankofcanada.ca/wp-content/uploads/2020/10/san2020-21.pdf.
Koning, J.P. (2020) "Central Banks are Privacy Providers of Last Resort." CoinDesk (July 30).
Kumar, R., and O'Brien, S. (2019) "2019 Findings from the Diary of Consumer Payment Choice." Cash Product Office.

Lagarde, C., and Panetta, F. (2020) "Report on A Digital Euro" European Central Bank." Frankfurt: European Central Bank.
Liu, A. (2019) "An Analysis of the PBOC's New Mobile Payment Regulation." *Cato Journal* 39 (1): 87–98.
Manoylov, M. K. (2020) "Chinese City to Host Digital Currency Lottery as Part of DCEP Trial." *The Block* (October 9).
Marvin, R. (2018) "Breaking Down VPN Usage around the World." *PCMag* (September 21).
Mester, L. J. (2020) "Payments and the Pandemic." Keynote Address, 20th Anniversary Chicago Payments Symposium, Federal Reserve Bank of Chicago (September 23).
Nakamoto, S. (2008) "Bitcoin: A Peer-to-Peer Electronic Cash System."
Narula, N. (2020) "Digital Currency Initiative and Federal Reserve Bank of Boston Announce CBDC Design Collaboration." *Medium* (August 14).
Noonan, L.; Tilford, C.; Milne, R.; Mount, I.; and Wise, P. (2018) "Who Went to Jail for Their Role in the Financial Crisis?" *Financial Times* (September 20).
Rauchs, M. (2020) "What CBDC Is (Not) About: Part I." *Mrauchs.com* (October 6).
Rutkowski, M., et al. (2020) "Responding to Crisis with Digital Payments for Social Protection." Washington: World Bank (March 31).
Scott, B. (2020) "The Landscape of Money: Visualizing Crypto Invasions, Stablecoins & CBDCs Amidst the War on Cash." *YouTube* (August 18).
Sindreu, J. (2020) "Central Banks Haven't Made a Convincing Case for Digital Currencies." *Wall Street Journal* (October 12).
SupChina (2020) "In Beijing, Social Monitoring and Control Turns Kafkaesque." *SupChina* (March 23).
S. 3571 (2020) "To Require Member Banks to Maintain Pass-Through Digital Dollar Wallets for Certain Persons, and for Other Purposes." *Govinfo* (March 23).
Tang, F. (2020) "China Moves to Legalize Digital Yuan and Ban Competitors with New Draft Law." *South China Morning Post* (October 27).
Tencent (2019) "2019 Annual Report."
U.S. Department of Justice (2020) "International Statement: End-To-End Encryption and Public Safety" (October 11).
White, L. H. (2020) "Should the U.S. Government Create a Token-Based Digital Dollar?" *Alt-M* (June 19).