The Washington Post *Democracy Dies in Darkness*

Cryptocurrency could help governments and businesses spy on us

The popularity of digital currencies like bitcoin could erode the last vestiges of financial privacy online

By Eswar Prasad

Eswar Prasad is a professor at Cornell University, a senior fellow at the Brookings Institution and author of, "The Future of Money: How the Digital Revolution Is Transforming Currencies and Finance."

Today at 6:00 a.m. EDT

Listen to article 6 min

Bitcoin, the original cryptocurrency, was designed to enable transactions using only digital identities and without the intervention of a trusted third party, like a bank. This seemed a godsend to those concerned about the rapid erosion of privacy in our increasingly digital age — and those looking for covert ways to exchange money. Bitcoin's introduction in early 2009, when the global financial crisis had decimated trust in governments and banks, was perfectly timed with a growing aversion to these big institutions.

It turns out that the cryptocurrency does not, in fact, guarantee anonymity. Users' digital identities can, with some effort, be connected to their real identities. Moreover, in an ultimate irony, the revolution that bitcoin started might end up destroying whatever vestiges of privacy are left in modern financial markets. As the technology goes mainstream, it threatens to give big corporations and government a better view into our financial lives and greater control over how we spend our money.

Bitcoin's reputation as a tool for shady dealings is perhaps overstated. While it has played a role in allowing hackers to obtain payoff money for ransomware attacks, this requires a level of technical sophistication beyond that of most garden-variety criminals. Bitcoin's use in transactions that once fueled the "dark Web," where unsavory and illicit commerce is conducted, has fallen sharply. The Russian government can scarcely count on bitcoin to evade the sanctions levied for its war in Ukraine — after all, payments for international transactions still need to be settled in real money such as dollars or euros.

Still, the ability to conduct secure, somewhat private financial transactions helps explain cryptocurrency's growing appeal. That's largely thanks to its groundbreaking blockchain technology. A blockchain is, in effect, a digital ledger of transactions or ownership records. The bitcoin blockchain contains a publicly visible record of all transactions ever undertaken using this cryptocurrency: the dates and amounts, as well as the digital — but not real-life — identities of the transacting parties.

These electronic ledgers are maintained on a large number of computers around the world and synchronized in real time, making them tamper-proof and secure. Any attempt to meddle with a ledger on one or even a few computers would quickly be detected and rejected by the rest of the network. This technology could soon be adapted for a broad range of more conventional uses, including buying a house and maintaining digital registries of public records. The blockchain enables such transactions to be executed securely without the involvement of intermediaries such as settlement lawyers or bankers.

As a result, a lot of large corporations are trying to cash in — some of which have dubious records when it comes to protecting personal information. Meta, formerly Facebook, had plans to issue its own cryptocurrency, ostensibly to make the world a better place by giving everyone easy access to a low-cost payment system. Under pressure from government regulators suspicious of its intentions, though, Meta was forced to shut down the project. Meanwhile Amazon and PayPal are reportedly considering developing cryptocurrencies. (Amazon founder Jeff Bezos owns The Washington Post.) Imagine these companies, which already pervade our lives, now having a window into all aspects of our social and commercial existence.

As various forms of crypto enter the mainstream, governments are taking notice. President Biden's recent executive order on digital assets attempts to rein in the Wild West aspects of this technology by bringing it under regulatory oversight.

Offshoots of bitcoin's technology are also setting the stage for central banks to issue their own digital currencies. The central banks of China, Japan and Sweden are already experimenting with this. The U.S. Federal Reserve has been slower but is now considering options for a digital dollar. That would provide a free, convenient digital payment system for the masses, even those without a bank account or a credit card. Tax-dodging and counterfeiting would become harder, and the use of currency for money laundering, terrorism financing and other nefarious activities would be curtailed.

But these advantages have strings attached. Electronic transactions leave a digital trail that cannot easily be erased. Using cryptographic tools, the identities of transacting parties using electronic money can be masked, but a central bank would always have the option of unraveling those identities if it suspected that its money was being used for illicit purposes. Even with privacy protections in place, transactions using a central bank's digital currency would ultimately be auditable and traceable.

And deeper changes could be afoot in the nature of money. Electronic currency offers possibilities that cash cannot. For instance, in an economic crisis, a government could dole out digital money with expiration dates, ensuring it is spent rather than saved and thereby stimulating the economy. This could make economic policy more effective — but it would take some key decisions out of the hands of households in favor of government-directed outcomes.

It is now technologically feasible for a central bank to offer digital currency accounts similar to bank accounts that would pay no interest and charge no

fees, but would give everyone in an economy easy access to a digital payment system. The downside is that this could give central banks and, ultimately, governments more visibility into our financial transactions.

These risks could be mitigated through careful design. For instance, the Federal Reserve could manage the payment infrastructure for its digital currency while leaving it to banks and other private companies to provide payment services to customers and businesses. This could preserve some confidentiality in transactions, with the central bank getting access to the identities of transacting parties only when it suspects foul play. But it is not difficult to imagine governments and central banks playing far more direct and intrusive roles in managing payments, allocating credit and engineering specific outcomes.

That's not all. Digital "smart money" that replaces cash could become an instrument of government control, with authoritarian regimes using it as a surveillance tool and even ostensibly benevolent governments conceivably employing it to promote social objectives: preventing its use to purchase ammunition, abortion services or pornography, for instance. This prospect might seem dystopian — except it has become clear that, even in an open democracy such as the United States, with many guardrails against corporate and government overreach, long-standing norms on privacy and confidentiality are surprisingly fragile. There are few regulations governing the collection and use of our data that Meta hoovers up from its Facebook, Instagram and WhatsApp platforms, for instance (just try restricting WhatsApp from gaining access to the full set of contacts on your phone).

Bitcoin's blockchain technology will help in creating better digital payment systems, automating a broad range of transactions and democratizing finance. But in an ironic twist, the true (and potentially dark) legacy of bitcoin might be the erosion of confidentiality, the broader prevalence of government-managed payment systems, and a greater intrusion of big business and government in financial systems — and in the functioning of society.