THE CLUB FOR GROWTH FOUNDATION

Policy Report

NO. 7 | DECEMBER 2024

Blockchain and Digital Assets: *America Risks Missing the Open Internet Revolution*

BY PETER ST ONGE, PH.D.

EXECUTIVE SUMMARY

Blockchains and the digital assets they depend on represent the most transformational technology since the internet for our economy, our society, and our liberties. This unique, decentralized technology can fulfill the "Open Internet" promise of the original internet that instead collapsed into today's "Big Tech" oligopoly.

A digital-asset-enabled Open Internet carries transformational possibilities to grow our economy by trillions of dollars — indeed, on the order of the growth from the original internet boom. More importantly, the open internet is our best hope to protect our fundamental liberties to free speech, free association, and free exchange that are increasingly threatened by authoritarian governments and their enablers in Big Tech, Wall Street, and throughout our society.

Despite these transformational possibilities — indeed, because of them — blockchains and digital assets are opposed by a wide range of powerful and entrenched special interests. In contrast to the original internet, regulators are catering to these demands, moving to install a regulatory gauntlet that could kill off legitimate actors, driving the entire industry offshore and leaving Americans at the mercy of predators.

Instead, America's policymakers should take a page from the original internet and implement a regulatory "sandbox" that diligently punishes fraud and protects consumers, while giving good-faith actors room to grow and innovate here in America.

Blockchains and the digital assets they depend on represent the most transformational technology since the internet for our economy, our society, and our liberties. If America does not establish an environment where this technology can thrive, we risk losing a once-in-a-lifetime opportunity to safeguard our prosperity, our dominance in the world, and even our political rights as a free people.

Blockchains and digital assets are simple in concept: a blockchain is a list of data used like a database that is transparent, verifiable, immutable, and peer to peer. Digital assets are the essential cryptographically secured tokens that allow blockchains to interact with the real world. Those assets can represent any intangible thing — a data entry, an image, a unit of currency, even a contract or property title.

This simple architecture belies an incredible flexibility that makes blockchains and digital assets able to do everything that can be done by a traditional database, the key technology that underlies literally every computer system, network, and digital tool in use today. Yet blockchains can often do it orders of magnitude faster, cheaper, more securely, and in a completely uncensorable way that is decentralized and therefore routes around authoritarian governments, Big Tech, and corporate gatekeepers.

Blockchains' resistance to censorship and their marked transparency are highly likely to be revolutionary for protecting our freedoms that are increasingly under attack by politically powerful gatekeepers. Blockchains' speed and cost improvements may prove to be likely revolutionary for a wide range of industries. For example, complicated financial transactions or supply chain coordination that today takes days and costs hundreds of billions of dollars can be done by blockchains in a fraction of a second and at near-zero cost — indeed, some blockchains are literally free.[1]

Those cost and speed advantages come, fundamentally, from blockchains' and digital assets' ability to disintermediate exchange: to remove or automate the human element. Because blockchains can fine-tune coordination on a massive scale, they can reduce costs in any process that today pairs humans with a database — in today's complex economy, nearly every economically significant process.

"Blockchains' resistance to censorship and marked transparency are highly likely to be revolutionary for protecting our freedoms..."

To illustrate the magnitude involved, just one blockchain app, Bitcoin, showed that a substantial part of the entire global banking system — a $26 trillion industry[2] that dominates the skyline of every major city in the world — can be run on a couple of $200 pocket computers[3] talking to free software on your phone.

Blockchains can extend such spectacular cost reductions to a wide range of business functions. For example, a blockchain could be used to create a self-executing contract that automatically pays $100,000 from escrow whenever the temperature in Orlando falls below freezing. Such a contract could substantially replace crop insurance, essentially for free, compared to the roughly half of insurance premiums[4] today that are used up in overhead and processing costs. Such a model could be carried to any insurable event where some outside trusted

1 "Crypto Fee Comparison - What Is the Lowest Fee Cryptocurrency?" Medium, Nano, 11 Feb. 2021, blog.nano.org/cryptocurrency-fee-comparison-which-crypto-has-the-lowest-fees-4e9118590e1f. Accessed 5 Feb. 2023.
2 Financial Services Global Market Report 2022." Reportlinker.com, 2022, www.reportlinker.com/p06277918/Financial-Services-Global-Market-Report.html?utm_source=GNW. Accessed 14 Feb. 2023.
3 "How to Run a Bitcoin Full Node on a Raspberry Pi." Howchoo, 19 Oct. 2020, howchoo.com/bitcoin/run-bitcoin-full-node-raspberry-pi. Accessed 5 Feb. 2023; "What Is the Lightning Network in Bitcoin and How Does It Work?" Cointelegraph, 2023, decrypt.co/55510/how-to-run-a-bitcoin-node-on-a-raspberry-pi-2021.
4 Hopkins, Tony. "A Good vs. Bad Loss Ratio | Horton Group." Horton Group, 10 Feb. 2020, www.thehortongroup.com/resources/a-good-vs-bad-loss-ratio/. Accessed 5 Feb. 2023.

data source (called an "oracle") exists, from police reports of car accidents to coroner death certificates — rendering the trillion-dollar insurance industry near zero cost.

Blockchains are being widely researched and implemented across hundreds of applications in finance, healthcare, logistics, manufacturing, and national-security-related industries — 65 industries by one recent count, including many of the world's largest and most serious companies.[5] On top of these in-house efforts, blockchains attracted $25 billion in venture capital investment last year, up 713%[6] on the previous year, making blockchain one of the most in-demand technologies in venture capital. As a class, digital assets powered by blockchains have attracted over $1 trillion in investor capital for projects, including Ethereum and other token ecosystems, utility tokens, stablecoins, and Bitcoin.

Just as with the original internet, we can expect such dramatic cost reductions to discover literally trillions of dollars for new businesses, from near-zero-overhead banking and insurance to zero-cost supply chains, uncensorable social media, and decentralized versions of Uber, Airbnb, and other personal services.

One area of particular interest is tokenizing legal assets like contracts or loans, where a legal document can be converted into a token — akin to turning it into a locked PDF. That token can then be traded, for example, allowing fractional investment in a house or a fundraised startup. This allows liquid markets in valuable but illiquid assets like real estate or private companies that represent tens of trillions of dollars in value. Indeed, tokenization enables fully functional virtual companies ("decentralized autonomous organizations," or DAOs) that can operate at low cost, flexibly, and potentially more securely and with more protection against authoritarian governments.

Of course, just as the original internet took decades to invent Youtube, Twitter, Uber, or Airbnb, it will take time to realize the true potential of the blockchain-based open internet. We can only imagine how many trillions of dollars of economic value will be revealed by near-instant, near-costless, secure, and uncensorable exchanges. That is why it is critical to protect this technology lest it flee overseas from hostile regulators in the United States.

Blockchains and the digital assets they rely on ultimately fulfill the original promise of the internet — namely, a radical decentralization giving power and autonomy back to the people. Blockchains' peer-to-peer architecture offers the final word to secure our fundamental rights of free speech and free association in the digital internet, no matter how powerful the forces arrayed in opposition.

"Blockchains and the digital assets they rely on ultimately fulfill the original promise of the internet — a radical decentralization giving power and autonomy back to the people."

5 "Banking Is Only the Beginning: 65 Big Industries Blockchain Could Transform." CB Insights Research, CB Insights, 9 Mar. 2022, www.cbinsights.com/research/industries-disrupted-blockchain/. Accessed 5 Feb. 2023.
6 Ibid.

BLOCKCHAIN AND FREEDOM

Blockchain and digital assets' most important feature for protecting liberty is their decentralized architecture. A decentralized and easily anonymized blockchain has no "throat to choke": no physical address and no individual for a corporation or authoritarian government to threaten or arrest. Indeed, this is a key reason for Bitcoin's appeal: unlike gold, which turned out to be easy for FDR to seize,[7] Bitcoin cannot be killed by Wall Street or by government because there is no "throat to choke."

Beyond Bitcoin, thousands of entrepreneurs, researchers, and activists are researching and implementing blockchains to create decentralized and uncensorable versions of social media, fundraising platforms, financial exchanges, repositories of censored videos or documents, and messaging apps to protect free speech, free assembly, and the right to dissent in the face of authoritarian governments and their enablers in Big Tech.

This is an urgent need now that countries worldwide are using Big Tech[8] and the formal financial system to silence dissent and punish their enemies.[9] During the 2020 Canadian Trucker protests, the Canadian government, lacking legal means to crush the protests, turned to the financial system and commanded banks to cut off the protesters' access to funds.[10] Not only could the protestors not fundraise to replace their lost work, they could not even use their credit cards to buy lunch. Canadian Prime Minister Justin Trudeau even extended the political pressure to US-based companies such as donation platform GoFundMe, which obediently seized Canadian truckers' donations and cut off their access to the platform and any donated funds..[11]

"Blockchains reduce costs in any process that pairs humans and databases."

The American government has identical tools to Canada, ostensibly to counter money-laundering and terrorism.[12] However, the US has much more ability to force foreign companies and governments to comply than Canada does. Indeed, the threats are already in process: Americans are already exposed to politically motivated financial persecution, from the IRS' targeting of conservatives[13] to recent cancellations of bank accounts[14] and credit cards[15] of high-profile conservatives. The shameful coordinated deplatforming of the free speech platform Parler in 2020 was a wakeup call that our liberties are not safe so long as Big Tech and authoritarian governments are united in centralizing the essential infrastructure of dissent.

By contrast, blockchain and digital assets allow dissidents and political opposition to compete on a level playing field with the regime champions in every aspect of building and running a movement, from communication and outreach to fundraising to content development and distribution. This can allow dissenters to communicate disfavored truths to enough voters to influence the political process.

7 "The Great Gold Robbery of 1933 | Thomas E. Woods, Jr." Mises Institute, 22 July 2008, mises.org/library/great-gold-robbery-1933. Accessed 5 Feb. 2023.
8 Mattox, Casey. "Here's What You Need to Know about the Twitter Files - Americans for Prosperity." Americans for Prosperity, 2 Feb. 2023, americansforprosperity.org/heres-what-you-need-to-know-about-the-twitter-files/. Accessed 5 Feb. 2023.
9 Michel, Norbert. "Newly Unsealed Documents Show Top FDIC Officials Running Operation Choke Point." Forbes, 15 Dec. 2020, www.forbes.com/sites/norbertmichel/2018/11/05/newly-unsealed-documents-show-top-fdic-officials-running-operation-choke-point/?sh=1d8544231191. Accessed 5 Feb. 2023.
10 Vanderford, Richard. "Canada's Banks Pressed into Effort to Quell Protests." WSJ, The Wall Street Journal, 18 Feb. 2022, www.wsj.com/articles/canadas-banks-pressed-into-effort-to-quell-protests-11645146830. Accessed 5 Feb. 2023.
11 Cerullo, Megan. "GoFundMe Investigated for Blocking Donations to Canadian Truckers." Cbsnews.com, CBS News, 10 Feb. 2022, www.cbsnews.com/news/gofundme-freedom-convoy-under-investigation-for-blocking-donations-canadian-truckers/. Accessed 5 Feb. 2023.
12 "FACT SHEET for Section 312 of the USA PATRIOT Act Final Regulation and Notice of Proposed Rulemaking | FinCEN.gov." Fincen.gov, 2023, www.fincen.gov/fact-sheet-section-312-usa-patriot-act-final-regulation-and-notice-proposed-rulemaking. Accessed 5 Feb. 2023.
13 Roff, Peter. "Last Chance for the Truth." US News & World Report, U.S. News & World Report, 2017, www.usnews.com/opinion/thomas-jefferson-street/articles/2017-11-22/dont-bury-the-truth-about-the-obama-irs-scanal. Accessed 5 Feb. 2023.
14 Choi, Joseph. "Florida Bank Says It Has Closed Trump's Accounts." The Hill, The Hill, 21 Jan. 2021, thehill.com/policy/finance/banking-financial-institutions/535282-florida-bank-says-it-has-closed-trumps-accounts/. Accessed 5 Feb. 2023.
15 Smith, Jennifer. "Chase Bank Backtracks after Telling General Flynn's Wife They're Cancelling Her Credit Card." Mail Online, Daily Mail, 31 Aug. 2021, www.dailymail.co.uk/news/article-9944457/Chase-tells-General-Flynns-wife-theyre-cancelling-card.html. Accessed 5 Feb. 2023.

For example, a dissident documentary maker or investigative reporter can use an uncensorable blockchain to preserve their content from censorship, but also to crowdfund, to sell subscriptions, to advertise to new donors, even to monetize their copyrights and intellectual property. This can all be done without being forced to promote regime-favored messaging even in the face of vigorous opposition from an authoritarian government. This is essential in the current American climate where we still have free speech in a legal sense, but in practice publishers and businesses often self-censor lest they be cut off by business partners or platforms and put the business at risk.

Beyond giving equal footing to dissident free speech, blockchains and digital assets do important work upstream, disrupting the very oligopolies that threaten the American people in the first place. By putting entrepreneurs and start-ups on a level playing field with industries ranging from Big Tech to Wall Street (for example, by allowing users to own their own accounts, profiles, data, and assets), blockchains and digital assets can dramatically reduce the network effect lock-in that concentrates industries in the hands of inevitably politicized big business. For example, the decentralized Nostr platform[16] is rapidly emerging as an uncensorable version of Twitter, gaining rapid market share as Americans come to understand the importance of not relying on a single sympathetic billionaire to protect our fundamental rights.

If individuals and small groups can raise funds, develop and market new products, and pay investors (all without intermediaries or even physical infrastructure) at far greater speed and far lower cost than legacy incumbents, even the most monopolistic industry becomes vulnerable to disruption by newcomers who can serve the customer better. In this sense, blockchain's decentralization and censorship-resistance represents a radical democratization of the very creative destruction that built and sustains our prosperity and our society.

"Blockchains' peer-to-peer architecture offers the final word to secure our fundamental rights of free speech and free association in the digital internet."

BLOCKCHAIN AND BANKING

Blockchain and digital assets can revolutionize the banking industry by providing faster, cheaper, more secure and transparent ways to process payments and manage assets while lowering the compliance costs and risks associated with error, abuse, rogue employees, and undetected risks.

While banks remain broadly wary of cryptocurrencies due to regulatory uncertainty,[17] they have actively explored the use of blockchains to improve the efficiency, speed, and security of financial transactions. Given the near-instant settlement, low costs, and inherently cross-border nature of blockchain ledgers, these can radically improve areas such as wire transfers, interbank clearing, overseas payments for trade or remittances, and currency exchange.

Moreover, smart contracts can be applied to existing financial relationships to allow nimble banks and financial organizations to monetize their existing customers, reach new users, and offer increasingly tailored products that can create more user value and carry higher profits margins. For example, by pairing secure digital identities to blockchain's inherent cost reduction, American banks could offer products and services to unbanked or underbanked people in underdeveloped countries. These long-abused customers might trust an American bank more than the shambolic local versions that can take days to process customer deposits[18] or that may simply run out of money.[19] Today, it is not economically viable for Citibank to offer services to a dusty village in rural El Salvador. With blockchain's dramatic improvements in cost and security, it would be.

The modern financial system is highly fragmented, partly due to existing regulations[20] and partly due to variation in systems or competencies between entities such as banks and payment processors. For example, a simple transaction like buying a coffee at Starbucks typically involves multiple processors — Mastercard, the customer's bank, and the merchant's bank. If a payment involves a foreign currency, crosses borders, or involves a large amount, it can involve progressively more organizations that often are not very well integrated — with human points of failure along each step. This not only slows transaction speed and raises costs, it also raises concerns about security, fraud detection, or access by illicit or sanctioned individuals, organizations, or even nations. By radically simplifying and raising the security of both identities and specific transactions, blockchains can render financial transactions tamper-proof, transparent, and verifiable to stakeholders, raising trust and lowering risk for both banks and for their users.

Banks are also at risk of fraud, error, and abuse by insiders. The American banking system is the largest and most developed in the world, yet it is still affected by error, misconduct, and systemic risks. These can range from seemingly pedestrian crimes like hiding potentially incriminating communications from law enforcement,[21] to more complex schemes, such as rigging the critical London Interbank Offered Rate (LIBOR) benchmark[22] or a group of rogue employees gambling hundreds of millions right under the nose of both internal auditors and the most competent regulators.[23]

"Increased transparency can streamline compliance and regulatory reporting in banking that already cost the industry more than $200 billion per year."

Blockchain-based digital assets can instead provide a transparent and tamper-proof record of all transactions for management, regulatory, or auditor scrutiny, helping to substantially reduce misconduct that can be very expensive, given the sums involved. Such increased transparency can streamline compliance and regulatory reporting in banking that already cost the industry more than $200 billion per year,[24] while repairing the faltering public trust in the financial and banking industries.[25]

In sum, blockchain and digital assets bring major opportunities for incumbent banks and financial firms financial firms, as well as new upstarts and fully decentralized financial platforms (DeFi). Just as nimble physical retailers used the challenge of ecommerce to thrive, nimble or well-run banks will successfully transform into a much larger and more successfully run industry that better serves customers. While firms that fail or try to fight blockchains may buy a few more years, they will ultimately end up as footnotes in history.

16 Bent, Marty. "Issue #1310: The Potential Power of Nostr." TFTC, TFTC, 31 Jan. 2023, tftc.io/martys-bent/issue-1310-the-potential-power-of-nostr/. Accessed 5 Feb. 2023
17 Sun, Mengqi. "Regulatory Uncertainty Is a Barrier for Wider Bitcoin Adoption." WSJ, The Wall Street Journal, 6 Apr. 2022, www.wsj.com/articles/regulatory-uncertainty-is-a-barrier-for-wider-bitcoin-adoption-11649289387. Accessed 5 Feb. 2023.

18 "El Salvador's Law: A Meaningful Test for Bitcoin." www.pwc.com/gx/en/financial-services/pdf/el-salvadors-law-a-meaningful-test-for-bitcoin.pdf.
19 He, Laura. "Small Banks in China Are Running into Trouble. Savers Could Lose Everything." CNN, CNN, 24 June 2022, www.cnn.com/2022/06/23/economy/china-bank-runs-protests-intl-mic-hnk/index.html. Accessed 5 Feb. 2023.
20 "FDIC: Important Banking Laws." Fdic.gov, 2023, www.fdic.gov/resources/regulations/important-banking-laws/index.html. Accessed 5 Feb. 2023.
21 Natarajan, Sridhar, et al. "Wall Street Hit with $2 Billion of Fines in WhatsApp Probe (1)." @BLaw, 27 Sept. 2022, news.bloomberglaw.com/white-collar-and-criminallaw/wall-street-whatsapp-probe-poised-to-result-in-historic-fine. Accessed 5 Feb. 2023.
22 Browning, Jonathan. "How Much Did Libor-Rigging Cost? U.S. FDIC Finally Has an Answer." Bloomberg.com, Bloomberg, 18 Mar. 2021, bloomberg.com/news/articles/2022-09-27/wall-street-whatsapp-probe-poised-to-result-in-historic-fine?embedded-checkout=true. Accessed 5 Feb. 2023.
23 Narioka, Kosaku. "Japan's Mitsubishi Says Rogue Oil Trader Lost $320 Million." WSJ, The Wall Street Journal, 20 Sept. 2019, www.wsj.com/articles/japans-mitsubishi-says-rogue-oil-trader-lost-320-million-11568977505. Accessed 5 Feb. 2023.
24 "The High Costs and Low Returns of AML Compliance | FTI Consulting." Fticonsulting.com, 2022, www.fticonsulting.com/insights/fti-journal/high-costs-low-returns-aml-compliance-banks-better-way. Accessed 5 Feb. 2023.
25 "Trust in Institutions and the Political Process." The Institute of Politics at Harvard University, 2023, iop.harvard.edu/trust-institutions-and-political-process. Accessed 5 Feb. 2023.

BLOCKCHAIN AND NATIONAL SECURITY

While a recent Accenture report estimated that 61% of defense companies are working with blockchain solutions to improve their supply chains[26] and the Department of Defense (DoD) is estimated to lose hundreds of billions of dollars due to waste,[27] defense needs that can be addressed by blockchains run much deeper than efficiency.

In November 2022, Ars Technica reported that German researchers bought a US military biometric database for $68 on eBay. This database contained names, nationalities, photographs, fingerprints, and iris scans of 2,632 people, including US military members, who had been scanned by American forces in Afghanistan.[28]

Information security is among the most important elements of defense: controlling and monitoring who has access to what information, when or for how long, and for what purpose or under what authority. Classified documents can be easily and customizably tokenized on an immutable, tamper-proof, and — going by Bitcoin's own security — impossible-to-hack distributed ledger. The blockchain can automatically track who accesses what information, and under whose authority or instruction. Using smart contracts, access to information can be customized by specific individuals, including limited-time access or partial access — in contrast to the dangerous all-or-nothing nature of a traditional database like the one bought on eBay.

Smart contracts are particularly important when sensitive information needs to be shared among a large base of users, such as in coalition operations, military provisioning, or R&D and military production. With blockchains, a private contractor or coalition member can have access limited to what they need to know, with details progressively and customizably parceled out on a need-to-know basis. Combining such tokenization with secure blockchain-based digital IDs completes the circle, allowing a two-way blinder on information according to operational needs. Secure digital identities raise operational security against threats like spoofing, phishing, and social hacks that are widely effective in corporate espionage, for example.

It's worth pausing to note that current smart contract security is not yet to the Bitcoin level of quality that top secret documents would need. This is due to the greater "attack surface" in programmable contracts, and poorly designed tokens that continue to be hacked.[29] This is precisely key takeaway of this paper: **innovation must continue**. After all, the US military will never have the best programmers and counter-hackers in the world. But Silicon Valley and the US tech industry absolutely do have the best programmers in the world, and thousands are already working on secure blockchains because of their importance in civilian applications. It is imperative to continue letting this innovation progress, precisely so that our military can benefit along with our wider financial, healthcare, and manufacturing sectors. If not, we can be sure other countries' militaries will.

"Blockchains' transparency and immutability can dramatically ease the challenge of finding and tracking illicit money."

26 "Banking Is Only the Beginning: 65 Big Industries Blockchain Could Transform." CB Insights Research, CB Insights, 9 Mar. 2022, www.cbinsights.com/research/industries-disrupted-blockchain/. Accessed 5 Feb. 2023.
27 "Pentagon Buries Evidence of $125 Billion in Bureaucratic Waste." Washington Post, The Washington Post, 5 Dec. 2016, www.washingtonpost.com/investigations/pentagon-buries-evidence-of-125-billion-in-bureaucratic-waste/2016/12/05/e0668c76-9af6-11e6-a0ed-ab0774c1eaa5_story.html. Accessed 5 Feb. 2023.
28 Belanger, Ashley. "Military Device with Biometric Database of 2K People Sold on EBay for $68." Ars Technica, Ars Technica, 27 Dec. 2022, arstechnica.com/tech-policy/2022/12/military-device-with-biometric-database-of-2k-people-sold-on-ebay-for-68/. Accessed 5 Feb. 2023.
29 "Crypto Hacks & Historical Cryptocurrency Exploits." Milk Road, 2022, milkroad.com/hacks. Accessed 5 Feb. 2023.

A second important application of blockchain and digital assets to national security involves their use in fighting money laundering and terrorism. Blockchain's transparency and immutability can dramatically ease the challenge of finding and tracking illicit money, whether it be drug cartels laundering proceeds via shell companies or terrorists fundraising or exploiting seemingly legitimate fronts. Even foreign propaganda campaigns, such as Russian or Chinese funding of media or networks of "bots" targeting the American public, can be identified, traced to associated organizations, and rolled up using blockchain data as "cookie crumbs" showing the connections.

Digital assets also provide important improvements to our ability to monitor international movements of goods and services. This can help enforce sanctions and punish cheating, topical at the moment with billions in Russian fossil fuels being smuggled on an industrial scale through China, then resold into world markets, including the European Union.[30] This problem is long-standing in trade and sanctions where, for example, Chinese goods are fraudulently mislabeled as "Made in the USA,"[31] while Chinese nuclear-weapons supercomputers freely use advanced American microchips in violation of strict sanctions.[32]

BLOCKCHAINS AFTER FTX

Like the original internet, blockchain technology has endured a steady stream of attacks from politicians and regulators. Senator Elizabeth Warren decried that crypto puts the financial system in the hands of "shadowy super coders,"[33] while SEC Chair Gary Gensler has promised to crack down on the lawless "Wild West"[34] of crypto. These attacks have intensified since the collapse of the FTX Ponzi scheme, which authoritarians have tried to use to attack the entire technology underpinning the open internet.

The truth is the FTX disaster was caused not by blockchains and digital assets but by old-fashioned fraud, enabled by inept and even venal regulation.

In 2009, Bernie Madoff's $65 billion penny stock empire collapsed in the biggest Ponzi scheme in American history, losing $20 billion[35] in investor money. Yet even though Madoff dealt in stocks and billed himself as an equity investor, there were no efforts to ban the joint stock corporation.

FTX, similarly, was a run-of-the-mill centralized financial operator that did not use blockchains, did not research them, and had no sway or relationship with blockchain technology. It is true that FTX used part of its stolen money to speculate in cryptocurrencies, just as it used stolen funds to speculate in Bahamian real estate and corporate equities.[36] Additionally, FTX surely rode the crypto-hype just as Bernie Madoff rode the "irrational exuberance" in stocks that so

30 "China Reselling Europe Russian LNG." China-US Focus, 2022, www.chinausfocus.com/finance-economy/china-reselling-europe-russian-lng. Accessed 5 Feb. 2023.
31 "Federal Trade Commission Finalizes Action against 'Made in USA' Offender Who Ripped 'Made in China' Tags out of Apparel, Replacing Them with 'Made in USA' Tags." Federal Trade Commission, 28 July 2022, www.ftc.gov/news-events/news/press-releases/2022/07/federal-trade-commission-finalizes-action-against-made-usa-offender-who-ripped-made-china-tags-out. Accessed 5 Feb. 2023.
32 Lin, Liza, and Dan Strumpf. "China's Top Nuclear-Weapons Lab Used American Computer Chips Decades after Ban." WSJ, The Wall Street Journal, 29 Jan. 2023, www.wsj.com/articles/chinas-top-nuclear-weapons-lab-used-american-computer-chips-decades-after-ban-11674990320. Accessed 5 Feb. 2023.
33 Gottsegen, Will. "Senator Warren: Crypto Puts Financial System in the Hands of 'Shadowy Super-Coders.'" Decrypt, Decrypt, 27 July 2021, decrypt.co/76997/elizabeth-warren-crypto-big-banks-shadowy-super-coders. Accessed 5 Feb. 2023.
34 U.S. Securities and Exchange Commission, "Testimony Before the United States House of Representatives Committee on Financial Services," October 5, 2021, https://www.sec.gov/news/testimony/gensler-2021-10-05 (accessed March 15, 2022).
35 Langer, Emily. "Bernard Madoff, Mastermind of Vast Wall Street Ponzi Scheme, Dies at 82." Washington Post, The Washington Post, 14 Apr. 2021, www.washingtonpost.com/local/obituaries/bernie-madoff-dead/2021/04/14/f8e33fa8-c5da-11df-94e1-c5afa35a9e59_story.html. Accessed 5 Feb. 2023.
36 Sigalos, MacKenzie, and Rohan Goswami. "FTX Spent $256 Million on Bahamas Real Estate — Now the Island's Government Wants It Back." CNBC, CNBC, 13 Dec. 2022, www.cnbc.com/2022/12/12/ftx-sam-bankman-fried-snapped-up-256-million-in-bahamas-real-estate.html. Accessed 5 Feb. 2023.

disturbed Federal Reserve chair Alan Greenspan.[37] Yet Madoff's scheme led to no effort to ban stocks or even exuberance, irrational or otherwise.

In reality, research says Bitcoin has between 6 and 15 times[38] less illicit use than cash, arguably because underlying blockchain technology featuring immutability and transparency is far less suited to illicit use than a traditional closed, hidden, eminently falsifiable database one can smuggle on a key-fob and rewrite on a whim.

That is not to say there should be no response to the FTX collapse. On the contrary, our current regulatory mess was largely responsible for FTX. Ever since the emergence of Bitcoin 14 years ago, American regulators have failed either to issue clear guidance[39] or to communicate an explicit all-clear.[40] This has left legitimate actors afraid to enter the sector, lest they incur regulatory ire or even criminal penalties. Just as Prohibition empowered the mafia, regulatory grey areas chase out good actors and leave the field to progressively bad actors. Regulators bear direct responsibility for every illicit actor who fills in where regulated entities are afraid to serve the customer.

In the case of FTX, it's even worse. It turns out the company had used its stolen billions to cultivate shockingly warm relationships, including personal meetings,[41] with the White House, DNC, SEC, CFTC, and even the Federal Reserve. FTX was even openly lobbying for preferential rules[42] — lobbying almost certainly greased by FTX founder Sam Bankman-Fried's enormous political contributions, second only to those by George Soros,[43] which extended to one in three members of Congress.[44]

In short, our current regulatory approach to the digital assets industry is broken. Innovation is killed off by legal uncertainty, while bad actors are left to fill the void.

What is the solution? To take the same approach we did with the original internet: Communicate that the industry will be allowed to innovate, to discover those transformational services and products that will build our economy, and to protect our rights and our national security for decades to come while at the same time assiduously investigating and prosecuting as fraud genuine cases where investors or users were lied to. This hands-off "regulatory sandbox" approach, advocated by SEC commissioner Hester Pierce,[45] is particularly important because blockchain, like the original internet, touches so many industries that it necessarily crosses a multitude of regulators, politicians, and threatened lobbyists at both the federal and state levels.[46] These regulators can amount to a regulatory gauntlet all but guaranteed to kill off good-faith actors and leave the industry to predators.

37 "Irrational Exuberance." Princeton.edu, Princeton University Press, 2016, press.princeton.edu/books/paperback/9780691173122/irrational-exuberance. Accessed 5 Feb. 2023
38 Lennon, Hailey. "The False Narrative of Bitcoin's Role in Illicit Activity." Forbes, 13 Dec. 2021, www.forbes.com/sites/haileylennon/2021/01/19/the-false-narrative-of-bitcoins-role-in-illicit-activity/?sh=329b371c3432. Accessed 5 Feb. 2023.
39 Bovaird, Charles. "Regulatory Uncertainty Greatest Problem for Blockchain Entrepreneurs, Says Producer." Forbes, 30 July 2020, www.forbes.com/sites/cbovaird/2020/07/31/regulatory-uncertainty-greatest-problem-for-blockchain-entrepreneurs-says-producer/?sh=36a89e8481f7. Accessed 5 Feb. 2023.
40 St Onge, Peter. "Biden Sics Bureaucrats on Cryptocurrencies." The Heritage Foundation, 2019, www.heritage.org/technology/commentary/biden-sics-bureaucrats-cryptocurrencies. Accessed 5 Feb. 2023.
41 Hawley, J. (2023, February 5). Following FTX Collapse, Hawley Demands Correspondence Between Regulators, DNC and Biden White House. [Press release]. Retrieved from https://www.hawley.senate.gov/following-ftx-collapse-hawley-demands-correspondence-between-regulators-dnc-and-biden-white-house
42 "FTX.US Bills Lobbied." OpenSecrets, 2022, www.opensecrets.org/federal-lobbying/clients/bills?cycle=2022&id=D000073694. Accessed 5 Feb. 2023.
43 Mollman, Steve. "Oops. Sam Bankman-Fried's Implosion Took down Democrats' Second-Biggest Donor with It as the Party Gears up to Regulate Crypto." Fortune, Fortune, 10 Nov. 2022, fortune.com/2022/11/10/sam-bankman-fried-ftx-joe-biden-democratic-party-second-biggest-donor/. Accessed 5 Feb. 2023.
44 Hamilton, Jesse, et al. "Congress' FTX Problem: 1 in 3 Members Got Cash from Crypto Exchange's Bosses." CoinDesk, 17 Jan. 2023, www.coindesk.com/policy/2023/01/17/congress-ftx-problem-1-in-3-members-got-cash-from-crypto-exchanges-bosses/. Accessed 5 Feb. 2023.
45 Schonberger, Jennifer. "Crypto Regulation Is Coming, Just Not This Year: SEC's Peirce," Yahoo! Finance, February 3, 2022, https://finance.yahoo.com/news/crypto-regulation-coming-just-not-this-year-se-cs-pierce-172824069.html (accessed February 4, 2022)
46 St Onge, Peter. "Biden Sics Bureaucrats on Cryptocurrencies." The Heritage Foundation, 2019, www.heritage.org/technology/commentary/biden-sics-bureaucrats-cryptocurrencies. Accessed 5 Feb. 2023.

CONCLUSION

Blockchains and the digital assets they depend on represent the most transformational technology since the internet for our economy, our society, and our liberties. Today, America stands at a crossroads. On the one hand, there is an increasingly dark and stunted future where we fall behind other countries and leave Americans and their fundamental liberties wide open to predators and authoritarian governments. Alternatively, we can embrace a renaissance for liberty and openness that fulfills the promise of the original internet — indeed, the original promise of our constitutional republic and the respect for the individual that has characterized this nation since 1776.

The potential of blockchains to disrupt our political oligarchy and the entrenched trillion-dollar industries they serve means we must expect even greater resistance from powerful special interests and politically sophisticated incumbents, including Wall Street and Big Tech, who will seek to strangle the decentralized internet in the crib, walling off their power from a technology that empowers the individual, the entrepreneur, and the disruptor.

Opponents will paint the decentralized internet as an existential risk, as a plaything of hackers and fraudsters, just as they tried with the original internet 30 years ago. We must fight these efforts if Americans, and the world, are to enjoy the liberty and prosperity the internet originally promised but failed to deliver. We must insist that, just as with the original internet, politicians and their pet regulators do not choke liberty in the crib, but rather embrace one of the most transformative and pro-freedom technologies ever invented.

What we stand to gain are ironclad protections for free speech, free association, and free inquiry, trillions of dollars in wealth and rising prosperity, and the maintenance of America's central position in the world. Otherwise, we will face a continuing erosion of our rights, our prosperity, and our ability to protect and project our power as a nation. The stakes could scarcely be greater.

THE CLUB FOR GROWTH FOUNDATION

CLUB FOR GROWTH FOUNDATION | 2001 L ST. NW, SUITE 600, WASHINGTON, DC 20036 | WWW.CLUBFORGROWHTFOUNDATION.ORG