THE DIGITAL CHAMBER

Blockchain and National Security

A Strategic Imperative

July

2025

Prepared by

The Digital Chamber and its membership

Acknowledgements

The Digital Chamber gratefully acknowledges the following contributors for sharing their insights and assisting in the preparation of this report on our behalf:

Kristopher Klaich
The Digital Chamber

Jean-Philippe Beaudet
The Digital Chamber

Dean Sovolos
B2C2

James Vivenzio
Perkins Coie

John O. Hurston
TRON Network

Maria-Kristina Hayden
OUTFOXM

William Kraus
Pierson Ferdinand LLP

Yevheniia Broshevan
Hacken

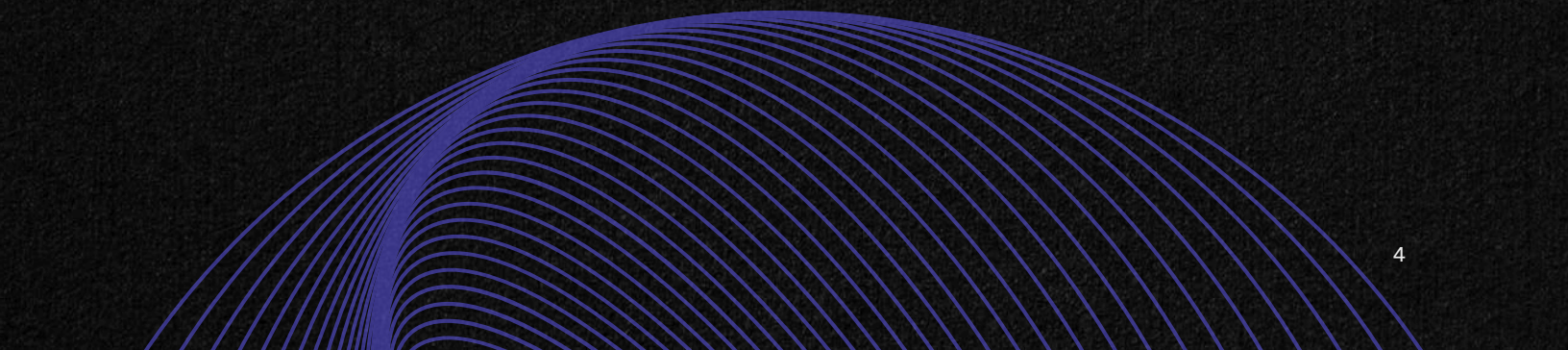
Blockchain and National Security: A Strategic Imperative

Executive Summary

As global national security threats continue to grow in scale and sophistication, the United States must invest in resilient, future-ready technologies to protect its critical infrastructure. Best known for its role in cryptocurrencies, blockchain can also protect data integrity, increase transparency, and reduce centralized vulnerabilities in computing networks underpinning our critical infrastructure.

Nations are racing to define the future of digital infrastructure and blockchain technology has emerged as a strategic vector in the competition for economic and geopolitical influence. U.S. adversaries—most notably China, Russia, North Korea and Iran—are advancing national blockchain strategies designed to reduce dependence on the U.S.-led financial system, negate the impact of U.S. sanctions, increase surveillance and control, and entrench their positions in emerging digital economies. These efforts are not speculative – rather, they are active, state-directed, and rapidly expanding. The power of blockchain's unique combination of attributes (decentralized, open, transparent, immutable, programmable, and secure) that can enable terrorism financing, sanctions evasion, money laundering, illicit financial activity on the dark web, strategic economic competition with adversaries also drives opportunities to enhance, protect, and support U.S. national security via improved economic resilience, cybersecurity, financial sovereignty, and strategic competitiveness.

Blockchain technology is emerging as a critical tool for national and economic resilience. Its decentralized architecture protects against financial censorship, empowering individuals and organizations to transact freely, even in hostile regulatory environments. Bitcoin, in particular, serves not only as a censorship-resistant store of value but also as a potential national security asset. A Strategic Bitcoin Reserve (SBR) and the introduction of Bitcoin-backed U.S. Treasury instruments ("BitBonds") could hedge against inflation, counter de-dollarization trends, and modernize sovereign finance. Meanwhile, stablecoins – over 99% of which are USD-pegged – are expanding the global reach of the U.S. dollar, reinforcing its dominance, facilitating humanitarian aid, and enabling traceable, programmable finance that aligns with U.S. foreign policy and intelligence operations.

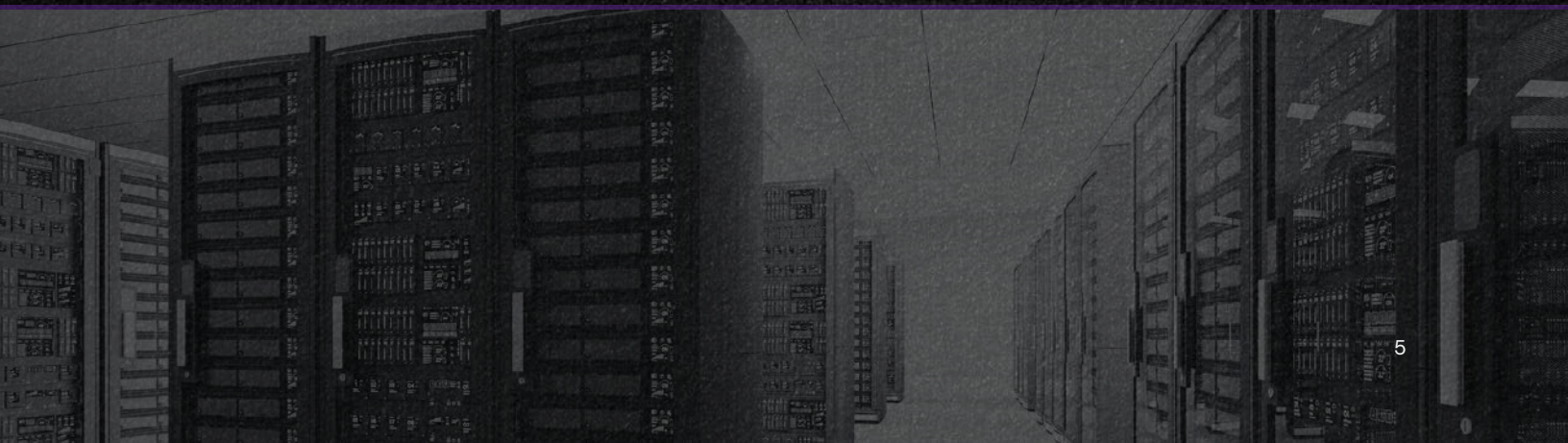


Blockchain also enhances cybersecurity and critical infrastructure protection. Its immutable, distributed ledger can detect tampering, log system actions in real time, and enable instant responses to anomalies – features crucial to securing defense systems, voting infrastructure, and supply chains. Smart contracts can automate incident response and ensure critical updates are implemented via multiparty verification. Community-driven audit ecosystems and bug bounty platforms have already prevented billions in potential losses.

These open, transparent security models are faster, more scalable, and more reliable than traditional siloed approaches. Decentralized communications networks like Helium and crowdsourced mapping tools like Hivemapper add layers of physical infrastructure resilience, enabling persistent operations even during crises or system failures.

Finally, decentralized finance (DeFi) reduces systemic financial risk by providing alternatives to legacy financial rails and with the ability to automate processes traditionally prone to human error and opacity. Smart contracts enable transparent risk management, prevent contagion, and democratize access to advanced financial tools. With smart regulation blockchain-based systems can deliver both freedom and security, advancing U.S. strategic interests while reinforcing economic sovereignty, technological leadership, and democratic values in an increasingly contested global environment.

If the United States does not act with urgency we risk ceding leadership in a foundational technology that will shape the rules of global commerce, economics, finance, media, privacy, and governance for decades to come. This report endeavors to comprehensively state the positive case for how blockchain protects and enhances U.S. national security and posits that it is integral to a comprehensive national strategy, especially vis-à-vis adversarial nations' activities.[1] The United States stands at a critical crossroads: embracing blockchain is not optional, but essential for maintaining global leadership. The nations that lead in blockchain development will set the rules for tomorrow's digital economy.



The Blockchain Imperative

Blockchain Adoption and the Risk to Financial Leadership

Right now the largest stablecoin issuer, largest digital asset custody firm, and three quarters of the largest crypto exchanges are domiciled outside the United States[2] — in addition to hundreds of other firms that chose not to launch in or fled the U.S. market entirely, perhaps best evinced by the U.S. being home to just 19% of the world's crypto developers in 2024, down from 38% in 2015.[3] The U.S. share of the pie has grown smaller, while the pie, representing the availability of blockchain developers, itself has grown massively at a 39% compound annual growth rate over the same period. If this trend continues, the U.S. risks ceding the home of the next generation of globally impactful and systemically important companies – like today's Google, Amazon, Apple, Tesla, and Facebook – to foreign competitors. As the President stated in his America First Investment Policy Executive Order in February,[4] and Secretary Bessent reiterated in April,[5] economic security is national security. Blockchain technology will underpin the next iteration of the internet – it is becoming the basis upon which value, communications, trade and data will be stored and transferred. We cannot risk fumbling this challenge.

U.S. Adversaries' Blockchain Strategies – Why We Must Compete Now

Blockchain is no longer a fringe innovation—it is a central pillar in the digital strategies of America's foremost adversaries. China, Russia, North Korea, and Iran are leveraging blockchain to reshape financial networks, evade sanctions, and challenge U.S. dominance in global markets. They are not merely experimenting, but rather executing top-down strategies to deploy blockchain tech at scale via state-controlled platforms, cross-border payment systems, and surveillance-driven digital currencies.

These efforts have profound implications: they threaten to fragment the international financial system, reduce the effectiveness of U.S. sanctions, empower authoritarian regimes to assert control over digital economies and civil liberties, and shape standards and infrastructure to their benefit.

China

Blockchain is a cornerstone of China's strategy to displace U.S. financial and technological leadership. Beijing considers blockchain core infrastructure and is pursuing a whole-of-nation effort—spanning domestic platforms, chip hardware dominance, and export-backed digital finance—to entrench its influence at home and abroad.

China has invested $54.5 billion in a National Blockchain Roadmap and created a "Blockchain Valley" in Shanghai, and its Blockchain-based Service Network ("BSN") launched in 2020 as a state-backed initiative to build the world's largest and most accessible blockchain infrastructure.[6] The BSN links 80+ Beijing government agencies to its central bank digital currency (CBDC), the digital yuan (e-CNY), and social credit systems,[7] embedding blockchain into China's surveillance and control architecture.

> China has invested $54.5 billion in a National Blockchain Roadmap and accounts for 90% of all blockchain patents globally.

This integrated access allows the Chinese Communist Party (CCP) to see into the finances, trade, and day-to-day activities of Chinese citizens. Globally, the BSN Spartan, China's internationally focused blockchain network, already operates hundreds of data centers spanning every continent except Antarctica, and it is being marketed globally as an affordable, easy-to-use, and technically advanced alternative to Western blockchain infrastructure—echoing the model used with Huawei in telecommunications and TikTok in social media: lure foreign developers, governments, and consumers with ease of access, low cost, and network effects, while embedding backdoor access and controls to assert strategic dominance and manipulate foreign societies and individuals. It provides China with the ability to monitor, manipulate, or restrict blockchain activity via backdoors and centralized governance tools, most importantly via digital identity, which would allow the CCP full control over a person's entire person, social interactions and economic transactions. EVERYTHING rolls up to identification infrastructure in China–this is the endgame goal that would empower the CCP in vast and nearly unimaginable ways, and we must not allow Chinese networks and standards to become the global standard. Alarmingly, some of the largest international blockchain companies have worked with Red Date, the Chinese tech firm developing, operating and maintaining the BSN.

Internationally, China is successfully exporting this model of centralized digital control.[8] BSN spans hundreds of data centers worldwide, offering low-cost rails that attract developers while embedding CCP governance controls. Marketed as a "SWIFT for CBDCs," referring to the Society for Worldwide Interbank Financial Transfers (SWIFT), the BSN courts BRICS and Belt-and-Road nations, creating dependencies that could displace Western financial infrastructure.[9] In April, China's Cross-border Interbank Payment System (CIPS) outpaced SWIFT in daily volume for the first time – an alarming sign of accelerating momentum.[10]

On the hardware front, Chinese firms dominate global bitcoin-mining rig production, gaining expertise repurposable for CBDC wallet chips and secure payment hardware. This pressure-tests existing U.S. export controls on advanced chips.
At the darker edge, Chinese criminal networks—often tied to state interests—exploit blockchain rails for pig-butchering scams and crypto laundering. These growing operations, exploiting over 300,000 trafficked workers, have funneled over $75B into Chinese criminal gangs' wallets while aiding cartels, North Korea, and organized crime.[11]

China accounts for over 90% of global blockchain patent applications. Unless Washington leads in building open blockchain standards, decentralized payment infrastructure, and tighter chip export controls, it risks ceding the world's digital settlement layer to Beijing — a shift that would reshape global finance and embolden other adversaries.

With Russia's support, Iran is developing a CBDC and testing tokenized oil trades outside the reach of FinCEN.

Russia

Russia casts blockchain as both a sanctions-proof lifeline and a tool of asymmetric influence. After the U.S. froze $300 billion of its reserves in 2022, Russia moved quickly to legalize crypto mining, approve bitcoin payments for trade, advance efforts to tokenize energy exports, and develop a ruble-backed stablecoin.[12] This year, it launched the Exved network, an electronic transaction platform that allows firms to settle trade using USD stablecoins, rubles, and other currencies with fees of just 2–3% — significantly lower than traditional financial systems.[13] Russia's "Digital Financial Assets" regime also supports cross-border deals with Belarus and other partners.[14] Meanwhile, cheap energy in regions like Donbas and Abkhazia is used to convert stranded gas into "clean" bitcoin, helping fund covert influence operations and proxy wars beyond the reach of dollar-based oversight.[15]

Internationally, Russia pairs soft power with infrastructure: their Cryptoeconomics Association pushes blockchain standards across Africa while BRICS+ talks explore tokenized oil settlements that sidestep SWIFT.[16] Furthermore, Finance Minister Siluanov has floated the idea of creating a strategic bitcoin reserve.

Russia's most strategic partner in the digital asset realm may be Iran. Together they are developing CBDCs[17], a gold-backed stablecoin[18], and the 'CELLS' blockchain platform for identity-verified multi-currency trade.[19] Their 2025 treaty pledged to build a modern payment system independent of the West — a blueprint others from Caracas to Pyongyang could follow. As Russia and Iran tighten this loop, the United States must decide whether to continue to rely on traditional finance or compete with a parallel financial internet growing in the shadows.[20]

North Korea

North Korea has turned crypto theft into a key source of funding for its weapons program, bypassing sanctions through blockchain's liquidity, pseudonymity, and global reach. Between 2020 and May 2025, Lazarus Group and affiliated units stole an estimated $11.5 billion — including $1.34 billion in 2024 and $1.46 billion in a single February 2025 Bybit breach — targeting central banks, financial institutions, cryptocurrency exchanges, and individual users.[21] These attacks often route through Russian IP space, launching from border towns and masked by VPNs, with stolen assets laundered through mixers and Asia-Pacific exchanges.

Cyber theft now complements broader sanctions evasion efforts, helping sustain missile development despite tightened U.N. and U.S. restrictions. The U.S. Department of Defense's defend-forward cybersecurity teams disrupt some operations, but the gap between what North Korea steals and what the U.S. claws back remains in the billions of dollars. Closing that gap will require automated on-chain monitoring, real-time intel sharing, and diplomatic pressure on Moscow and Beijing — especially as others study North Korea's playbook for sanctions-resistant finance.

Iran

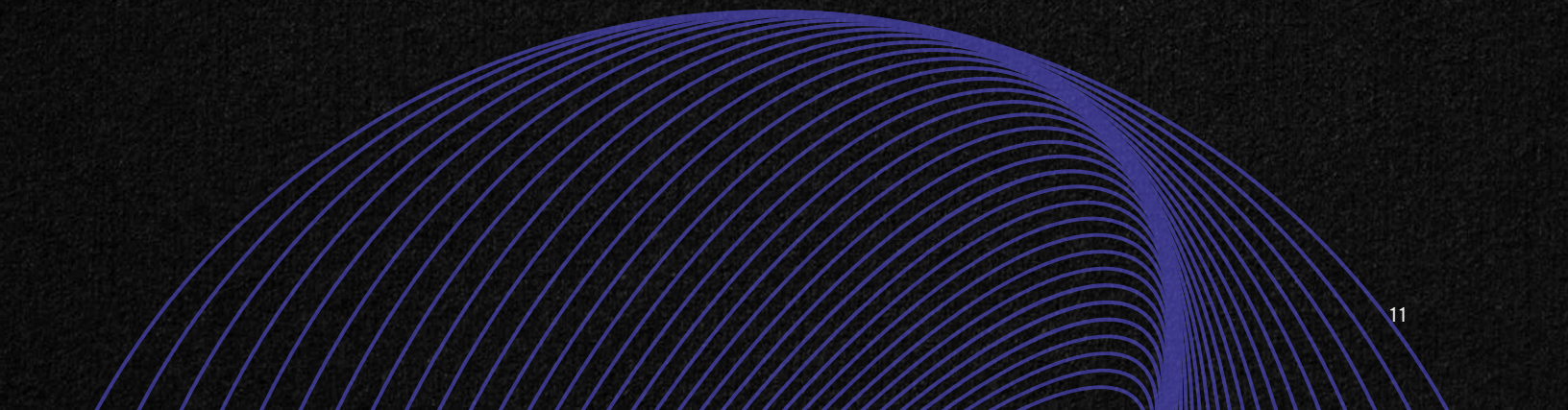
Iran uses blockchain as a pressure valve against sanctions and a tool to fund proxies beyond dollar oversight. Excluded from SWIFT since 2018 and blacklisted by the Financial Action Task Force (FATF) in 2020, Iran has used subsidized energy to produce bitcoin through state-backed mining, at one point contributing nearly 4% of global hash rate and generating over $1B in sanctions-resistant revenue.[22] With support from Russia, Iran is co-developing a wholesale e-rial — a digital version of its national currency — and is testing tokenized oil trades outside the reach of the dollar system.

Blockchain's successful application has also made Iranian cryptocurrency exchanges into essential infrastructure within the country, providing attractive targets for offensive cyber operations. These attacks can be standalone or – as in the June 19, 2025 attack on the Iranian Nobitex exchange, where approximately $90m was stolen and routed to addresses embedded with anti-regime messages. The June 19th attack has been attributed to Predatory Sparrow – an Israeli hacking group who timed the attack to coincide with Israeli air offensives during the "Twelve Day War," and who leaked the exchange's source code, infrastructure diagrams, and internal privacy R&D. Analytics firm TRM Labs discovered,

> A tiered wallet infrastructure and embedded API credentials for sanctioned platforms…enable seamless crypto–fiat movement within Iran's closed financial circuit. Embedded privacy tools…were engineered to defeat blockchain tracing, using stealth addresses, output splitting, and randomized endpoints. Internal documents confirmed this obfuscation was aimed at avoiding detection by FinCEN-compliant firms.[23]

While disclosure of Nobitex's architecture and code allows insight into how exchanges in sanctioned jurisdictions can evade Western financial controls, it also provided a blueprint for foreign actors seeking their own illicit access to Western finance.

Crypto flows from mining have funded wallets linked to Hezbollah, the Islamic Revolutionary Guard Corps, and regional militias, providing low-friction support for proxy warfare. The Treasury's Office of Foreign Asset Control's (OFAC) 2022 sanctions on nine exchange accounts tied to Hamas show how quickly energy converts to ordinance. Yet the same rails aid civil society: Faced with hyperinflation, banking repression, and pervasive censorship, many Iranians have turned to decentralized cryptocurrencies – especially stablecoins like USDT – as a store of value and means of transacting beyond the reach of both the regime and the international sanctions architecture. Peer-to-peer crypto markets flourish in Iranian cities, with Telegram and WhatsApp often serving as informal exchanges and price indicators.[24]



Blockchain & Crypto are Critical to U.S. National Security

Economic Resilience & Financial Sovereignty

Blockchain technology has the potential to significantly reduce undue financial censorship, as its decentralized design limits the ability of any single authority to block, alter, or control transactions. Financial censorship, also known as de-risking, occurs when individuals, organizations, or even entire countries or geographies are denied access to financial services or have their transactions blocked often due to political or ideological reasons, or sanctions and purported anti-money laundering (AML) concerns. When such objectives are not U.S. objectives, these controls are counter to U.S. interests.[25]

HOW BLOCKCHAIN PROTECTS AGAINST UNDUE CENSORSHIP

The irony of such activity's impact on the blockchain industry is that blockchain technology developed as a tool to counteract censorship and de-risking, offering a resilient alternative to traditional financial systems. Blockchain technology, at its core, is a distributed ledger maintained by a network of computers (nodes) rather than a single central authority. This decentralization is crucial in resisting censorship.[26] In fact, censorship resistance has been a fundamental feature of decentralized networks like Bitcoin.

In traditional banking, a government or financial institution can freeze accounts or block transactions with a simple directive. In contrast, on a public blockchain, no single party has the authority to prevent a transaction from being broadcast or validated — as long as the user has access to the internet and the necessary cryptographic keys. The protection against financial censorship provided by blockchain is rooted in several technical and structural features:

Decentralization: No single entity controls the network, making it extremely difficult for any government or organization to block transactions or freeze assets.

Immutability: Once a transaction is recorded on the blockchain it cannot be altered or deleted. This ensures a permanent, tamper-proof record of all transactions.

Global Accessibility and Transparency: All data and transactions are publicly available and accessible. Anyone with internet access can use blockchain networks regardless of location or local policies. This transparency makes attempts at censorship or data manipulation obvious.

Peer-to-Peer Transactions: Users can transact directly with one another, bypassing intermediaries that might otherwise be compelled to censor transactions.[27]

Blockchain technology has proven to be a valuable tool in the fight against financial censorship, providing a decentralized, transparent, and resilient means of transferring value across borders and around obstacles, including the disruption of traditional financial infrastructure in war-torn regions. In fact, Bitcoin's use in recent global events — including the so-called "Freedom Convoy" protests in Canada in early 2022[28] and for Afghan, Syrian, and Ukrainian humanitarian aid to assist refugees and others in dire need — demonstrates this in the real world.[29] Iranian citizens have also used blockchain tools to fund dissident journalism, support diaspora activism, and enable resistance to digital authoritarianism.[30] These practices echo similar movements in Venezuela and Russia, where blockchain's pseudonymous and censorship-resistant properties provide cover for activities that would otherwise be suppressed or criminalized. As the technology matures and adoption grows, blockchain is likely to play an increasingly important role in safeguarding financial freedom and supporting those at risk of censorship and de-risking.

Ultimately, however, adversarial regulatory environments can diminish users' ability to access these essential digital tools.[31] It is TDC's position that blockchain technology supports global economic freedom by empowering those who resist tyranny around the world.

Bitcoin's National Security Role

Bitcoin, the first cryptocurrency, is unique in its origin, decentralization, network security, and mass adoption, with several countries adding it to their balance sheets or mining it as a state-sanctioned activity. Given all of this, it can play an integral role in U.S. national security.

U.S. STRATEGIC BITCOIN RESERVE

The United States stands at a pivotal crossroads in global financial history. As authoritarian regimes seek to bypass the dollar-based system and deploy new forms of digital financial infrastructure, the U.S. must not remain a passive observer. Establishing a Strategic Bitcoin Reserve (SBR) is a forward-looking national security imperative—one that strengthens U.S. resilience, projects leadership, and cements U.S. influence over the future of global finance. Bitcoin, as a decentralized, censorship-resistant, and globally liquid asset, is uniquely suited for this role. Like gold, it cannot be inflated or manipulated by foreign governments. Unlike gold, it is natively digital and accessible across borders, offering a powerful hedge against financial instability or geopolitical disruption. An SBR would enable the U.S. to diversify its sovereign balance sheet, hedge against inflation and devaluation risks, and counter growing trends in global de-dollarization.

Our adversaries understand the power of financial infrastructure. China is exporting its digital yuan through the BSN, its digital Belt and Road initiative, while Russia and Iran are exploring crypto and commodity-based payment systems to evade sanctions. A U.S.-backed Bitcoin reserve sends a clear message: the United States will lead—not retreat—from the future of digital money.

Strategically, Bitcoin can serve as a contingency reserve in crisis scenarios, including cyberattacks on payment systems or major financial disruptions. It would also signal to allies and markets that the U.S. is prepared to lead in securing open, decentralized, and democratic alternatives to authoritarian-controlled currencies and financial surveillance networks.

Countries like El Salvador, Pakistan, and the UAE are already experimenting with sovereign Bitcoin strategies. The state of Texas just passed legislation to create a bitcoin reserve, building upon President Trump's March 6, 2025 Executive Order establishing the SBR, which recognized bitcoin as a digital strategic reserve asset—analogous to gold—and authorized the Departments of Treasury and Commerce to develop cost-neutral acquisition strategies.

BITBONDS: A STRATEGIC INNOVATION AMIDST GLOBAL BOND MARKET STRAIN

The United States faces a critical fiscal inflection point with approximately $9.3 trillion in federal debt maturing within the next 12 months. This unprecedented refinancing burden coincides with persistently elevated interest rates — currently hovering near 4.5% for 10-year Treasuries — substantially increasing the cost of servicing the national debt. These mounting interest obligations are not only a drag on the federal budget but also restrict the nation's capacity to invest in its national security, economic growth, and innovation. Meanwhile, the U.S. Treasury is facing waning foreign demand — particularly from key buyers like China — adding to refinancing uncertainty.[32] In this environment, market participants are increasingly demanding higher returns for perceived fiscal and inflationary risks. Bitcoin-backed U.S. Treasury Bonds, or BitBonds, could combat these macroeconomic headwinds, revitalize debt markets, attract global capital, and reduce federal borrowing costs.[33] BitBonds are designed to fulfill four key national objectives:

1. *Reduce debt servicing costs* by offering a novel, market-competitive instrument that could command lower interest rates due to its hybrid structure;

2. *Expand the SBR* without imposing additional tax burdens via bond proceeds rather than public revenues;

3. *Provide American savers with a secure, tax-advantaged vehicle* that combines the reliability of government bonds with the growth potential of bitcoin;

4. *Offer a pathway to long-term debt reduction* through bitcoin appreciation while avoiding politically contentious tax hikes or spending cuts.

The proposed design directs 90% of bond proceeds toward conventional government financing and 10% toward the purchase of bitcoin, preserving the safety and liquidity of traditional Treasuries while providing strategic upside exposure. BitBonds would also send a global signal that the U.S. is prepared to lead in digital asset strategy and financial innovation—at a time when economic hegemony is increasingly contested.

BitBonds could combat macroeconomic headwinds, revitalize debt markets, attract global capital, and reduce federal borrowing costs.

Under historical median performance scenarios, the government's share of bitcoin appreciation could be sufficient to meaningfully offset, or even eliminate, the long-term debt burden.[34] The enormous and unprecedented demand for bitcoin exchange traded products — which have grown faster than any in history (and five times faster than gold reached the $70B threshold) — suggests that there would be demand for such a product.[35] It is important to recognize that the U.S. dollar need not lose its status as the world's reserve currency for significant consequences to arise. Even a gradual, sustained reduction in demand for U.S. Treasuries by foreign sovereigns could trigger substantial inflationary pressures at home, with far-reaching impacts on the economy.

ENERGY AND BITCOIN MINING

Technological development is inextricably tied to the availability of abundant energy and bitcoin mining is fundamentally changing the way we define energy's value, use, and distribution. Bitcoin mining incentivizes expansion of the grid with green energy, stabilizes volatile demand and is a source of innovation in cooling, chip manufacturing and compute efficiency. Because energy is the costliest component in bitcoin mining the industry is driving innovations in energy use, immersion cooling, chip design, and waste heat recovery—innovations accessible to the broader energy and tech sectors. Mining can stabilize grids by providing a consistent and reliable demand vector, in effect commoditizing electricity on a global scale and monetizing previously stranded or wasted energy at the source – energy that would otherwise never be brought to market, be it flared gas in west Texas or hydro-electric during flood season in Eastern Africa.

Bitcoin mining incentivizes the buildout of green energy infrastructure by providing a reliable, consistent demand for energy, consuming excess power when green energy providers would otherwise be forced to PAY consumers to take their energy. Additionally, miners provide a flexible demand element, allowing stressed grids the ability to respond to extreme cold or heat conditions near-instantaneously by curbing their energy consumption.

Perhaps most important is the Bitcoin/AI nexus. The central input to both the Bitcoin network and AI is energy and China is generating power faster than the U.S. while competing ferociously on innovation. Bitcoin allows American companies to harvest underused power, monetize it, acquire financing with it, and build the infrastructure needed for AI – Riot Platforms is doing this right now in Texas. Bitcoin mining is a bootstrapping mechanism – we can use what we have to build what we need, and win this modern day space race for both Bitcoin and AI.

BITCOIN AND NATIONAL SECURITY RISKS

The Bitcoin network also presents distinct national security risks for the U.S., particularly through vulnerabilities in its mining infrastructure. Bitcoin mining rigs — critical to the network's operation — are produced almost entirely by Chinese firms, with one company controlling 90% of the market, creating a dangerous single point of failure. This supply chain dependency exposes U.S. miners to potential supply chain attacks or hidden backdoors in rig firmware, which could be exploited by adversaries. Compounding the risk, a significant portion of Bitcoin's computing power is concentrated in Chinese-operated mining pools. These factors give the CCP the capability to disrupt U.S. miners and potentially overwhelm the U.S. power grid or interfere with strategic transactions, including those involving any future U.S. Bitcoin reserve, through cyber or supply chain operations.

There are signs of positive change: at least two U.S.-operating companies — Auradine and Bitdeer — are designing and manufacturing chips and mining rigs outside of China to diversify the supply chain and harden the hardware ecosystem against external manipulation. This manifested in May 2024, when President Biden issued an executive order requiring MineOne Partners (a China-affiliated miner) to divest land and equipment located within a mile of the Francis E. Warren Air Force Base in Wyoming. The Committee on Foreign Investment in the United States (CFIUS) flagged this acquisition — done without prior approval — as a national security risk, citing the proximity to a nuclear missile base.[36]

Financial Stability & Dollar Dominance

HOW STABLECOINS CAN REINFORCE THE DOLLAR'S ROLE AS THE WORLD RESERVE CURRENCY

Stablecoins are becoming a powerful digital extension of the U.S. dollar, reinforcing its status as the world's reserve currency. Stablecoins expand the dollar's reach across borders, bolster demand for U.S. Treasuries, and offer stability in both advanced and emerging markets. Over 99% of stablecoins are pegged to the dollar,[37] facilitating over $27.6 trillion of transactions in 2024 and surpassing the combined transaction volumes of Visa and Mastercard that same year.[38] Their utility in digital finance underscores the dollar's enduring role in a rapidly evolving monetary landscape. Accordingly, the stablecoin market has served as a digital extension of the U.S. dollar as a payment tool and store of value, reflecting the stability, utility, and familiarity of the world's most used fiat currency. With the combined dollar stablecoin market cap at more than $240 billion,[39] stablecoin issuers have emerged as one of the largest global holders of U.S. Treasuries,[40] and Citigroup projects the market to potentially balloon to $3.7 trillion by 2030.[41]

Such market share dominance reflects a broad-based trust in the U.S. dollar as a stabilizing force, bolstered by network effects that further entrench its central role in both digital and conventional financial systems, regular audits, and transparent reserve disclosures.[42] The powerful value proposition that extending dollar stablecoins to emerging digital rails portends is not lost on China, whose state-affiliated think tanks have begun exploring how to combat this development[43]. The borderless nature of stablecoins further promotes USD primacy. Given their digital nature and low usage barriers, these assets can transcend geographical and institutional limitations, allowing the U.S. dollar to be transacted internationally and stored seamlessly on blockchain networks. This ensures the role of the dollar in international markets remains robust and allows it to grow into nascent international markets — all that is required to access stablecoins is an internet connection and something to trade for them.

In emerging markets characterized by financial instability and inefficient local financial institutions, stablecoins often provide a reliable alternative and protective mechanism for businesses and individuals who contend with high remittance or currency conversion fees, currency volatility, and mismanaged monetary policy. Increased stablecoin penetration in foreign markets may even enhance U.S. tariffs under the right conditions.[44] As an international aid tool, the deployment of USD-linked stablecoins — such as the Office of the United Nations High Commissioner for Refugees (UNHCR)'s distribution of stablecoin to crisis-affected populations in Ukraine — illustrates their utility in delivering rapid, low-cost financial support during emergencies.[45]

They also allow distribution of funds for government operations or civil affairs projects in a demonstrably transparent fashion, helping to win hearts and minds for disaster relief, mission support, or "milk runs" — deliveries of supplies or cash to U.S. military bases, embassies, or partner entities in foreign nations. These types of operations, which sometimes involve significant risk to U.S. citizens to physically deliver cash in war zones, can now be executed remotely and instantly, risk-free. Similarly, U.S. intelligence and law enforcement agencies are exploring how they can utilize the ability to transfer value instantly in an obfuscated manner to deliver funding to U.S. partners abroad surreptitiously.

To maintain reasonable restrictions on OFAC-sanctioned entities, smart contract-based stablecoins can advance national security priorities by allowing ubiquitous technical surveillance and by being frozen (and unfrozen) by issuers in response to law enforcement requests or other legal processes. This capability has been used for several years to combat money laundering, nuclear proliferation, and terrorist financing, with the largest stablecoin issuer reportedly blocking over 2,000 wallets — including 960 in coordination with U.S. agencies — freezing more than $2.5 billion in illicit activity.[46]

Better payments systems encourage the use of formal markets and discourage the use of black and grey markets. This results in extending USD into markets where dollars are not normally utilized. This projects the U.S. government's tool of economic warfare or statecraft even further; however, criminal enterprises continue innovating to thwart this reach.[47]

Stablecoins are rapidly expanding the global reach of the USD, facilitating over $27.6T in transactions in '24. With >99% market share and volumes projected to grow exponentially, stablecoins are becoming a powerful tool of U.S. economic statecraft, humanitarian aid, and national security.

THE ROLE OF DEFI IN REDUCING SYSTEMIC RISKS IN FINANCIAL MARKETS

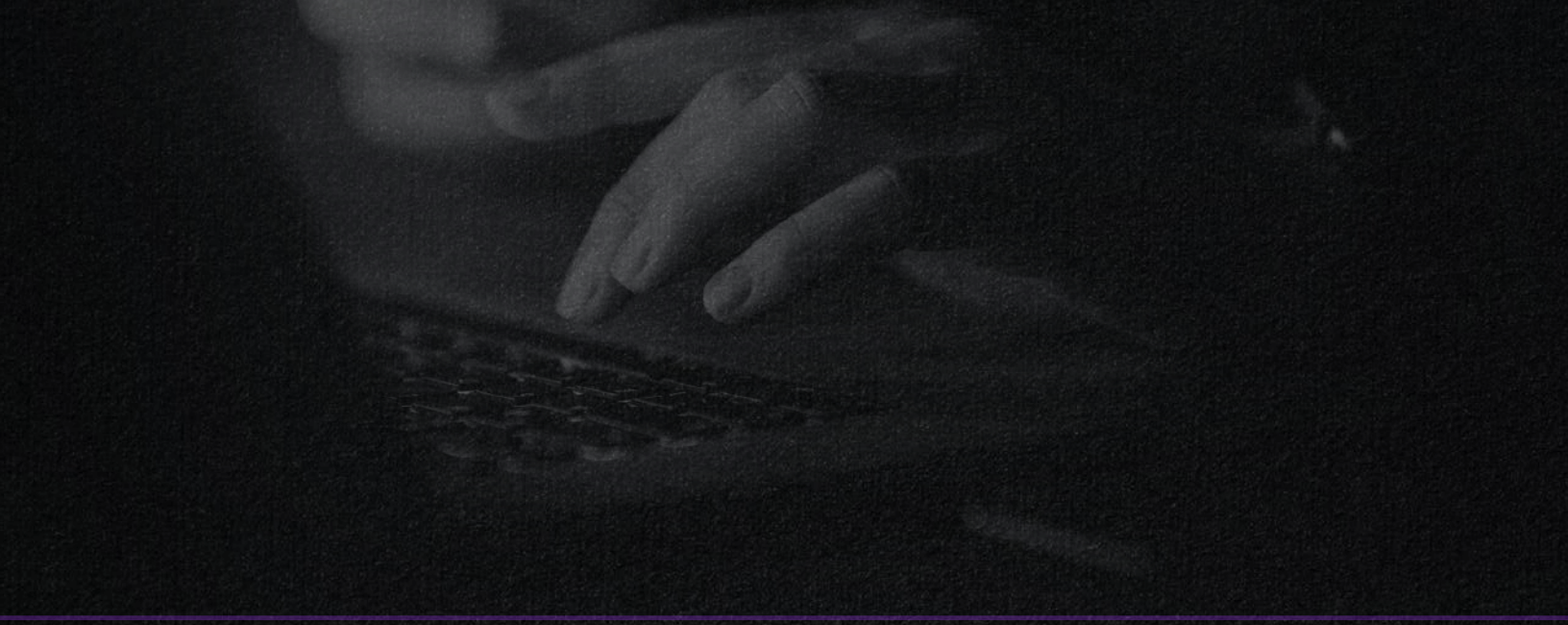
Decentralized Finance (DeFi) offers innovative tools for mitigating systemic risks in financial markets through automation and decentralization. Its ultimate effectiveness, however, depends on key factors: consumer confidence, the resilience of underlying protocols, the sophistication of risk management practices, and the evolution of regulatory frameworks. As DeFi matures it has the potential to complement traditional financial systems by providing alternative mechanisms for risk mitigation and market stability.

At the heart of DeFi are smart contracts — self-executing code that enforces the terms of agreements without human intervention. This automation reduces operational risks associated with manual processes and human error. Smart contracts can also embed risk management functions, such as automatic collateral liquidations, margin calls, and circuit breakers, that help contain contagion and prevent liquidity runs during periods of market stress.

Traditional financial systems often rely on centralized entities, which can become single points of failure and are subject to heightened regulatory scrutiny, such as designation as systemically important financial institutions by the Federal Reserve. In contrast, DeFi protocols are typically distributed across networks of nodes, making them more resilient to targeted attacks, operational disruptions, and cascading failures that can arise from the collapse of a major financial institution.

A defining feature of DeFi is the elimination of centralized intermediaries that can obscure transparency and increase risk. By leveraging open-source protocols and public blockchains, DeFi platforms provide fully auditable, transparent transaction records. This transparency reduces information asymmetry and enables the public, market participants, and regulators to monitor systemic exposures and identify emerging risks. The open nature of DeFi protocols further allows for real-time risk assessments, helping to prevent the accumulation of hidden vulnerabilities that have historically contributed to systemic crises in traditional finance.

DeFi's accessibility—open to anyone with an internet connection—promotes broader participation in financial markets. This inclusivity fosters greater market depth, breadth, and liquidity, creating buffers against systemic shocks and reducing the risk of de-banking for political or other arbitrary reasons. Moreover, DeFi enables the creation of novel financial instruments and risk-sharing mechanisms, supporting more balanced and diversified portfolios and lowering concentration risks. Despite the volatile reputation of cryptocurrency and the numerous internal and external "black swan" events that have challenged the crypto markets in recent years, DeFi protocols have demonstrated impressive resilience and continued to function under extreme stress.



CYBERSECURITY & CRITICAL INFRASTRUCTURE RESILIENCE

BLOCKCHAIN CAN SECURE CRITICAL INFRASTRUCTURE AND MITIGATE HUMAN ERRORS

Critical infrastructure underpins the economic stability, public safety, and national defense of the U.S. and our allies globally. A single successful cyber attack can disrupt essential services, cost billions, and create cascading effects across sectors. The U.S. faces a dynamic threat environment characterized by state-sponsored cyberattacks, sabotage of physical infrastructure, and digital espionage. Traditional cybersecurity systems are increasingly challenged by coordinated attacks that target vulnerabilities across energy, transportation, water, healthcare, communications, and financial sectors. While much attention is aptly focused on defending against malicious cyber threats, it is equally important to recognize the significant risks posed by inadvertent human errors. These include misconfigurations of systems, accidental deletion or exposure of sensitive data, the granting of improper access permissions, and inadequate testing of software or system updates before deployment which can compromise critical infrastructure.

These types of errors are particularly dangerous because they often go undetected until substantial damage has occurred. In complex, high-stakes environments such as those involving national defense, energy grids, or financial systems, even a minor lapse in testing or configuration can evolve into a major security incident. Addressing these vulnerabilities requires not only rigorous operational protocols and training, but also the integration of technologies like blockchain that inherently promote transparency, traceability, and accountability in system operations. Current centralized and siloed systems are highly vulnerable to breaches, data manipulation, and service interruption. Without adopting new paradigms in security architecture, the nation risks falling behind in both defense capability and technological leadership.

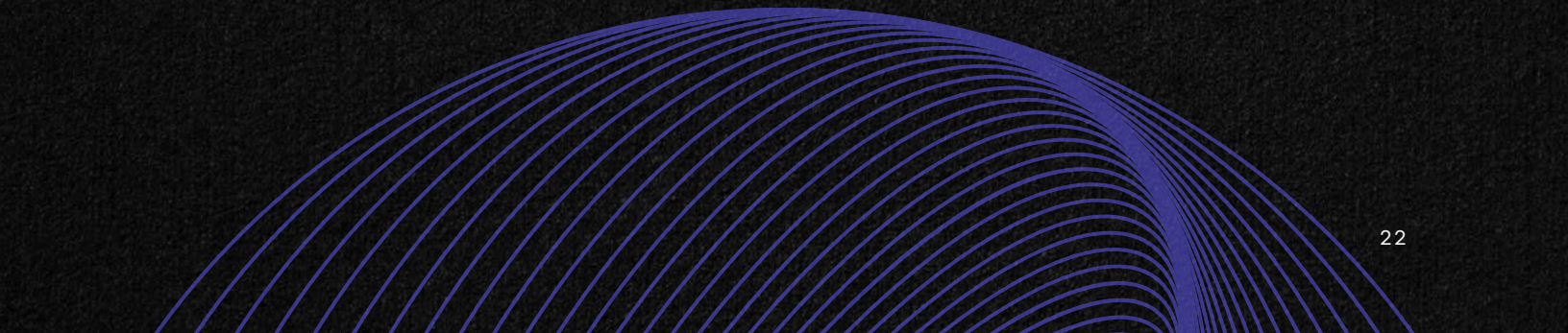
One of the most underutilized strengths of blockchain-based ecosystems is their community-driven security culture. Unlike traditional IT infrastructure, which are managed by siloed administrators and often rely on closed-source logic that limits external validation, decentralized systems are inherently open to broad, continuous peer review by global cybersecurity researchers, security auditors, and white-hat communities. This shift in paradigm introduces two critical strategic advantages:

1. **Security Through Transparency:** In decentralized environments, codebases and system behaviors are often open-source and publicly accessible. This enables crowdsourced audits, real-time bug bounty programs, and continuous vulnerability research, increasing the probability of identifying and mitigating zero-day threats before exploitation.

2. **Incident Containment via Built-In Flexibility:** While not all security incidents are fully preventable, the presence of on-chain upgradeability, circuit breakers, and modular protocol design allows projects to execute incident response measures in real time — reducing systemic risk and contagion.

Blockchain security auditors like Hacken have observed that robust audit ecosystems — enabled through both independent reviews and community bounties — serve as the first line of defense in blockchain national resilience. Crowdsourced security platforms such as HackenProof, which mobilize thousands of vetted researchers through incentivized programs, have become central hubs for global peer review—accelerating vulnerability discovery and supporting operational security at scale. Complementing this, runtime observability solutions like Extractor, which monitor smart contract behavior and flag suspicious on-chain activity, add a critical layer of continuous detection to the security stack.

Over the past five years, the global security community working through bug bounty platforms has helped prevent exploits valued at over $100 billion—clearly demonstrating the effectiveness of this model in protecting digital assets. We advocate for a broader adoption of these audit-centric practices across critical blockchain infrastructure and encourage regulators to incorporate such models into national cyber readiness strategies.



Further, blockchain's immutable and transparent ledger not only deters malicious tampering but also strengthens system integrity by making all actions traceable, verifiable, and resistant to accidental or unauthorized changes. It provides real-time assurance that every action is recorded, enabling easier auditing and correction of inadvertent errors without compromising the system's overall integrity. This built-in accountability reduces the risk of data loss, misconfiguration, or unauthorized changes caused by oversight or miscommunication.

Through its distributed, immutable, and secure architecture, blockchain offers capabilities well-suited to today's cybersecurity challenges. Balcony Labs, for example, is applying distributed ledger technology to improve cybersecurity in municipal real estate systems while monitoring foreign ownership of land and critical infrastructure — already helping identify several properties that violate parameters set by CFIUS.[48] Other firms, like Constellation Network, are working with the DoD to securely, effectively, and efficiently transfer confidential data and enable interoperability between legacy system data and cloud infrastructure and secure, tamper-proof communications.[49] While not a standalone solution, blockchain should be viewed as a foundational technology within the broader digital security framework.

BLOCKCHAIN AS A NATIONAL SECURITY ASSET AND RELATED USE CASES

The ability to transfer value instantly and transparently has value to the U.S. government and defense apparatus. According to one special operations forces member, "The cryptocurrency ecosystem does offer utility for special operations as a complimentary tool for tactical concepts and as a component to financial intelligence assessments. Beyond financial settlements, blockchains offer the ability to build private and secure applications to deliver valuable non-standard communication or data management tools for military operations."[50] Blockchain's unique technical features offer robust support for critical infrastructure protection, including:

1. Tamper-Proof Auditing and Data Integrity

Immutable, time-stamped records ensure transparent tracking of system activity and allow rapid forensic analysis. This is vital for sectors like energy grids, air traffic control, and water management, where even brief interruptions can be catastrophic. These records, furthermore, would update in real-time across the entire network.

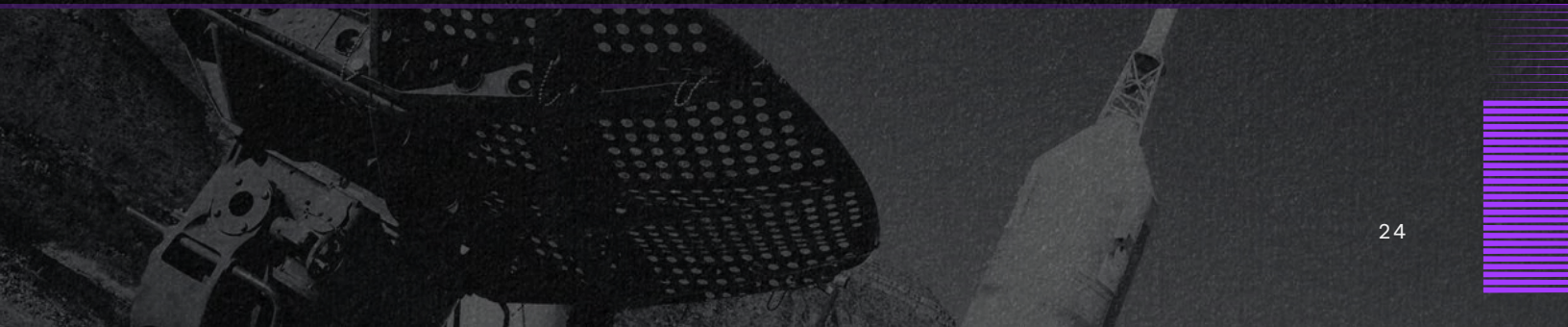
By layering a lightweight, permissioned blockchain beneath existing logging pipelines, every event generated by a SCADA node or application server is immediately hashed, time-stamped, and appended to an append-only ledger that is replicated across all mission partners (operator, regulator, independent auditor). Any subsequent attempt to delete or rewrite a log entry breaks the cryptographic chain, making tampering instantly visible and providing a court-admissible chain of custody. Smart-contract "watchdogs" can also correlate suspicious patterns – e.g., a relay trip plus an unrecognized firmware push – and trigger real-time alerts before service is disrupted.

2. Decentralized System Resilience

Distributing control across a network of nodes minimizes single points of failure, reducing the likelihood and impact of system-wide outages or breaches caused by targeted attacks. If any single node is compromised via attack, outage, or environmental disruption—others maintain uptime. Decentralization aligns with western democratic values and is the antidote to centralized control of systems which enables, facilitates, and exacerbates repressive social and regressive economic policy.

This is essential for ensuring continuity in government, defense, and critical private-sector operations, and is a bulwark against Chinese efforts to disrupt communications and critical infrastructure networks in a severely budget-constrained environment. As one example, a decentralized physical infrastructure (DePIN) protocol like decentralized mapping project Hivemapper can allow defense or law enforcement to incentivize mapping of real-time, on-the-ground conditions prior to a planned operation — something that cannot be done as inexpensively or efficiently using satellites or commercial mapping applications. Similarly, in the event of a large-scale disruption of communications networks, the Helium network is a decentralized, persistent, and scalable fallback data network that cannot be disrupted, having recently hit an all-time high of 1.1 million daily active users.[51]

Decentralization aligns with western democratic values and is the antidote to centralized control of systems which enables, facilitates, and exacerbates repressive social and regressive economic policy.



3. Secure Digital Identity and Access Management

Blockchain enhances identity verification for individuals, devices, and systems, enabling precise access control and accountability—critical in safeguarding sensitive government networks, infrastructure networks, and voting systems. The integrity of the voting system election results are critical to our nation's functioning and security. Protocols like Voatz allow for secure voting with verifiable, incorruptible results, rejecting manipulation and fraud while also providing the basis for trust in the system and outcome–one person, one vote, without ineligible participation and protected from cyber attacks on voting systems and machines. The cryptographic technique called 'zero-knowledge proofs' allows for verification of data without revealing the actual data itself – think verifying THAT person has voted, but not for WHOM they voted; or verifying that one's age is greater than 21 but not what the actual age is, nor providing access to any other additional personal information contained on an ID like address or name. Personal data can be owned and controlled by the individual rather than the corporation they are patronizing. Beyond security and control, implementation of digital IDs could unlock economic benefits of up to 13% for advanced economies.[52]

One blockchain-based project combines data from internet-of-things networks to provide a secure, decentralized, and tamper-proof system for real-time data verification and sharing for first responders, tied to real-world infrastructure networks that creates a layered, holistic security strategy that can, for example, prevent or mitigate school shootings or other catastrophic public safety events.[53]

4. Automated Resilience via Smart Contracts

Smart contracts can trigger predefined responses to cybersecurity events, such as a failover activation in response to a system failure or protocol enforcement, streamlining crisis response and maintaining operational continuity. Smart contracts also give critical systems the ability to react as fast as they detect. Running on a permissioned, government-operated blockchain, these self-executing rules could continuously monitor trusted data feeds whether they come from measurements from the grid, endpoint-detection sensors inside a defense network, or chemical gauges at a water-treatment plant. When a predefined threshold is crossed, the contract triggers an authorised response and records every step on the same immutable ledger. For example, a sudden frequency dip can automatically dispatch battery storage and release micro-payments to independent generators, stabilising the grid before a cascading blackout begins. In cyberspace, confirmation of malware on a mission-critical controller can rotate the device's keys, fence it off from the wider network, and alert the Cybersecurity and Infrastructure Security Agency (CISA) – all within seconds, no phone-tree required.

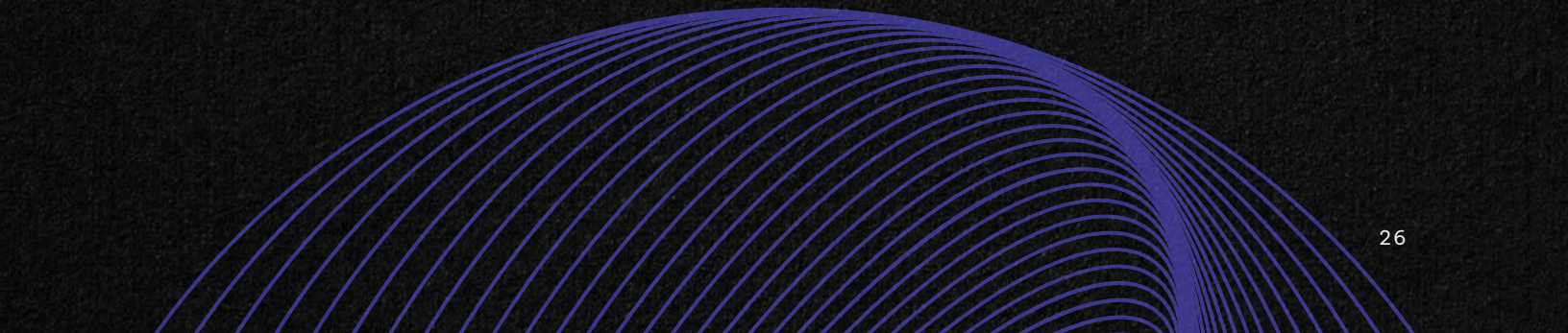
This complements other aspects of the technology, and can integrate promisingly with AI agents and protocols. The result is a shift from manual playbooks to machine-speed resilience – delivering faster incident containment, lower operational overhead, and a hard-to-contest deterrent against adversaries who count on slow reaction times in U.S. critical infrastructure.

5. Supply Chain Verification

The U.S. federal and defense supply chains span thousands of suppliers, multiple classification levels, and billions of line-item transactions – a surface rich for counterfeits, diversion, and audit failure. A permissioned, zero-trust blockchain collapses that sprawl into a single, tamper-proof timeline. Every hand-off – from semiconductor wafers to finished weapons – writes an immutable hash to the ledger, often pushed automatically by Internet of Things tech or smart-label Radio Frequency Identification tags. Because no single actor can edit the record, allies, auditors, and combatant commands share the same real-time view of provenance and custody.

At the tactical level, that transparency deters diversion: each crate of rifles arrives with a verifiable, unbroken chain of custody, making it far harder for corrupt brokers or hostile third-parties to siphon hardware into black markets. Inside the industrial base, smart contracts can automatically block payment if a vendor's cyber-hygiene score or export-control status lapses, eliminating paper compliance checks and counterfeit parts before they reach the line. That same data feed could power predictive-maintenance models, letting depot crews, automated AI agents, or smart contracts order certified spares the moment a component nears end-of-life – maximizing asset uptime while trimming inventory and emergency-lift costs.

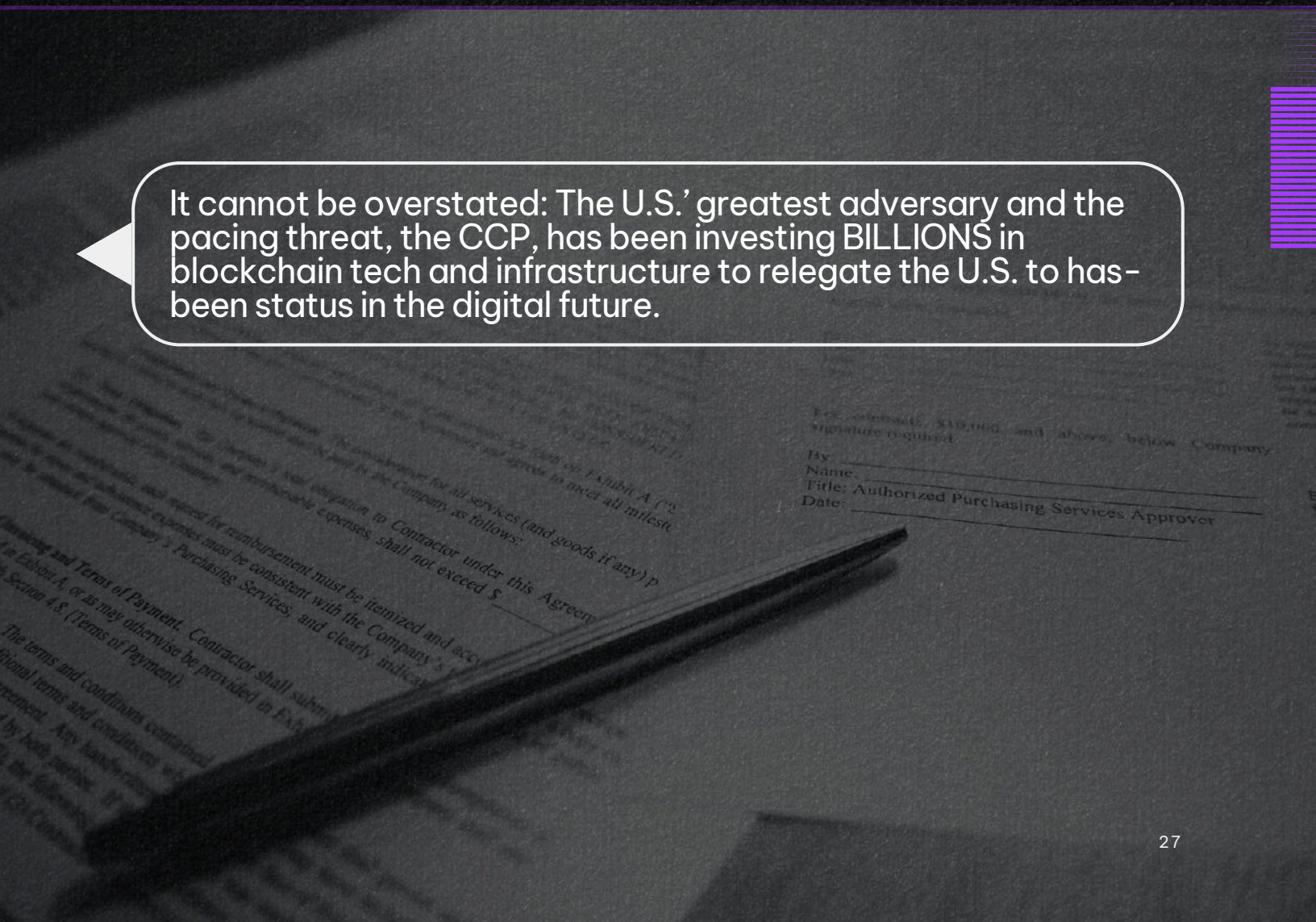
At enterprise scale, every fuel draw, spare-part purchase, or depot transfer can be time-stamped and cryptographically signed, giving the Pentagon an auditable ledger that cannot be massaged before fiscal year-end. Automated verification slashes reconciliation time and chips away at the multi-trillion-dollar "unaccounted for" gap that has plagued successive DoD audits. In short, blockchain replaces opaque paper trails with deterministic, machine-speed logistics, fortifying both battlefield readiness and public accountability.



6. Smart Contracts and Consensus: a safety net for critical updates

Consider a hypothetical faulty software update that is distributed as part of a routine content push. Such an update could cause widespread system crashes resulting in boot failures across critical infrastructure, including airlines, hospitals, and financial institutions.

Blockchain based solutions could help prevent the incident through the implementation of smart contracts for certain deployment conditions and a decentralized approach to the critical updates validation before rollout. Smart contracts could enforce automated pre-deployment checks, such as verifying that all new classes, functions and parameters are explicitly handled by the code interpreter, ensuring that memory safety tests are passed, blocking deployment rollout if any critical tests are missing or if they fail. A blockchain-based system could require multi-party consensus before pushing sensitive updates. Each party would digitally sign off on the update, and the blockchain would record this transparently. This would reduce the risk of oversight or rushed approvals, especially for high-risk component releases.



Principles & Policy Recommendations for U.S. Leadership in Blockchain that Protect National Security and Enhance Strategic Competition

To maintain technological leadership, safeguard national security, and counter adversarial models like China's BSN, the U.S. should employ a principled approach to blockchain policy providing the foundation for a strategic, secure, and innovation-driven blockchain national framework.

Leadership & Technological Sovereignty

Establish technological sovereignty and lead development of critical blockchain infrastructure while incentivizing investment and educational programs via grants, subsidies, and public-private partnerships.

To maintain a strategic edge in the digital era the U.S. must proactively invest in blockchain technologies that enhance cybersecurity, financial resilience, and defense capabilities. As adversaries leverage blockchain to evade sanctions, fund asymmetric warfare, and build sovereign alternatives to the global financial system, it is imperative that the U.S. not only respond with defensive measures, but that we lead in shaping and deploying the technology itself. It cannot be overstated: The U.S.' greatest adversary and the pacing threat, the CCP, has been investing BILLIONS in blockchain tech and infrastructure to relegate the U.S. to has-been status in the digital future.

Establish a Blockchain and Digital Asset Solarium Commission.

To unify U.S. efforts in blockchain governance, innovation, and national security, Congress should establish a bipartisan Blockchain and Digital Asset Solarium Commission, modeled after the successful post-World War II Project Solarium to counter Soviet expansion and the more recent Cyberspace Solarium Commission of 2020. A blockchain-focused commission would bring together government, academia, and the private sector to develop consensus among senior officials on a cogent, holistic approach to ensure U.S. national security and global leadership, as TDC advocated in 2023.[54]

Expand Federal Funding & Incentives to Establish National Blockchain R&D Centers & PPP Innovation Labs. The federal government should significantly expand funding, grants, and incentives to establish National Blockchain Research and Development Centers and Public-Private Partnership (PPP) Innovation Labs dedicated to decentralized technologies. Modeled on successful initiatives like DARPA, the DHS Science and Technology Directorate's Silicon Valley Innovation Program Blockchain Portfolio, and other national laboratories, these centers should focus on the secure design, testing, and deployment of blockchain systems critical to national security and economic resilience and oster collaboration among federal agencies, academia, and the private sector, to drive innovation while supporting education, workforce development, and skills training to cultivate blockchain expertise across government and industry. Incentives should include grants, subsidies, and tax credits to accelerate private-sector investment in blockchain infrastructure and workforce development. U.S. Special Operations Forces (USSOF) should leverage the 2023 NDAA, SEC: 5913 "National Research and Development Strategy for Distributed Ledger Technology" to request additional resources for advancing education and experimentation with digital assets in U.S. special operations units. USSOF, in conjunction with academic and private partnerships, should conduct surveys to help illuminate the level of adoption and literacy for digital assets which will drive training requirements and experimentation.

Secure Open and Free Blockchain Standards

Lead development of open and interoperable standards to embed privacy, civil liberties, resilience and redundancy as default design principals for digital infrastructure. Blockchain technology offers transformative potential to strengthen national security, protect critical infrastructure, and enhance operational integrity across defense and emergency systems. We can better safeguard the nation against evolving threats and reflect democratic principles embedding decentralization, transparency, and resilience at the core of our digital infrastructure. Otherwise, in the absence of U.S. leadership, China will fill this vacuum with its own centralized, exploitative standards being deployed on the BSN.

Mandate privacy-preserving design in digital ID systems and privacy protocols. Enshrine in law the right to publish and innovate with open-source code, rejecting efforts to criminalize the development of decentralized protocols. A decentralized, secure, and voluntary digital identity framework allows secure logins for government portals, voting systems, and financial services in addition to empowering digital wallets–this is a direct counterposition to China's centralized, manipulable authoritarian digital ID architecture.

Re-Introduce the Securing Open Source Software Act in the 119th Congress. Introduced by Representative Mark Green (R-TN-7) in the House and Senator Gary Peters (D-MI) in the Senate during the 117th Congress, this legislation directs CISA to coordinate security efforts for open-source software, develop a risk-assessment framework for high-value assets using open-source code, and support both federal and private-sector efforts to strengthen supply chain security relating to open-source components. This focus on open-source security is essential, as the majority of blockchain code is, itself, open-source.[55]

Establish U.S.-led international standards for secure and responsible blockchain use. Participate in and lead in new and ongoing International Standards Organization (ISO), World Economic Forum (WEF), Organization for Economic Development (OECD), Financial Action Task Force (FATF) and World Wide Web Consortium (W3C) blockchain standardization processes to promote open and interoperable standards to ensure compatibility across public sector and allied nation states, combating China's attempt to implement its own. Work with allies to create a democratic blockchain coalition deploying open-source, decentralized alternatives to BSN and sharing blockchain tools and best practices for use in elections, disaster response, trade, and other applications. Develop smart contract audit, secure development incident response and risk scoring standards to identify and mitigate risks.

Pass the Deploying American Blockchains Act of 2025.

The *Deploying American Blockchains Act* establishes a National Blockchain Deployment Advisory Committee appointed by the Secretary of Commerce, whose goal is "to examine and to provide recommendations on issues and risks relating to the deployment, use, application, and competitiveness of blockchain technology or other distributed ledger technology, applications built on blockchain technology or other distributed ledger technology, tokens, and tokenization, including the issues of decentralized identity, cybersecurity, key storage and security systems, artificial intelligence, fraud reduction, regulatory compliance, e-commerce, health care applications, and supply chain resiliency."[56] Specifically, TDC encourages the following applications, below:

- The Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response should incorporate blockchain-based smart coordination to withstand cyberattacks or local failures and promote grid security.[57]
- The Federal Emergency Management Agency should implement decentralized logistics tracking for medical and food aid in emergencies.[58]
- The Department of Defense should utilize permissioned blockchains to enable secure, real-time data exchange between allies without reliance on a centralized system vulnerable to attack.[59]
- The Department of Defense should implement blockchain to verify the provenance and authenticity of components in sensitive defense technologies, reducing the risk of sabotage or counterfeit infiltration.[60]
- The Department of Defense and State Department should deploy blockchain solutions to ensure transparency and accountability in foreign assistance, weapons transfers, and logistical operations, which are often targeted by adversaries for corruption or disruption.[61]

Improve Economic Competitiveness

Use blockchain policy to enhance U.S. innovation leadership and financial power via expansion of dollar usage, digital asset markets and energy innovation.

Pass stablecoin, market structure and other essential legislation as soon as possible.
A clear regulatory framework will encourage compliant U.S. dollar–denominated stablecoins for global trade and remittances and encourage the best and brightest minds to repatriate or start up in the U.S. Once these bills become law, Congress should focus on other high-payoff topics like tokenization of real-world assets via pilot projects around tokenized Treasuries, real estate, and securities, or in sandbox environments as Commissioner Peirce has called for.[62]

Establish a U.S. Strategic Bitcoin Reserve.
Congress should pass the BITCOIN Act (S.954) and the Reserve and Stockpile Act (H.R.2112) to leverage Bitcoin as an alternative asset, strengthen the federal balance sheet, and protect and shape our financial future by giving the force and effect of law to the Executive Order issued on March 6, 2025 entitled "Establishment of the Strategic Bitcoin Reserve and United States Digital Asset Stockpile." In an era of rapid digital transformation, the U.S. cannot afford to sit on the sidelines. A Bitcoin reserve could be a tool of resilience, deterrence, and global leadership.

Introduce "BitBonds."
Bitcoin-backed U.S. Treasuries can revitalize debt markets, attract global capital, and reduce federal borrowing costs. As Treasuries demand wane BitBonds offer the U.S. a rare opportunity: to simultaneously reduce borrowing costs, modernize sovereign finance, and cement its leadership in the digital financial era.

Secure Critical Digital Asset Supply Chains Through Strategic Subsidies.
To support the Administration's vision of making the U.S. the global capital of bitcoin and digital assets—and to protect the emerging Bitcoin Strategic Reserve—the U.S. must act urgently to secure its critical digital asset supply chains. The U.S. should provide targeted subsidies and incentives to accelerate the design and manufacture of bitcoin mining rigs and chips onshore. This will ensure American miners have reliable, secure equipment, and reduce dependence on foreign adversaries.

Combat Illicit Finance

Modernize regulatory standards, leverage public-private partnerships, and improve offensive and defensive cyber capabilities to prevent illicit activities and terrorism financing.

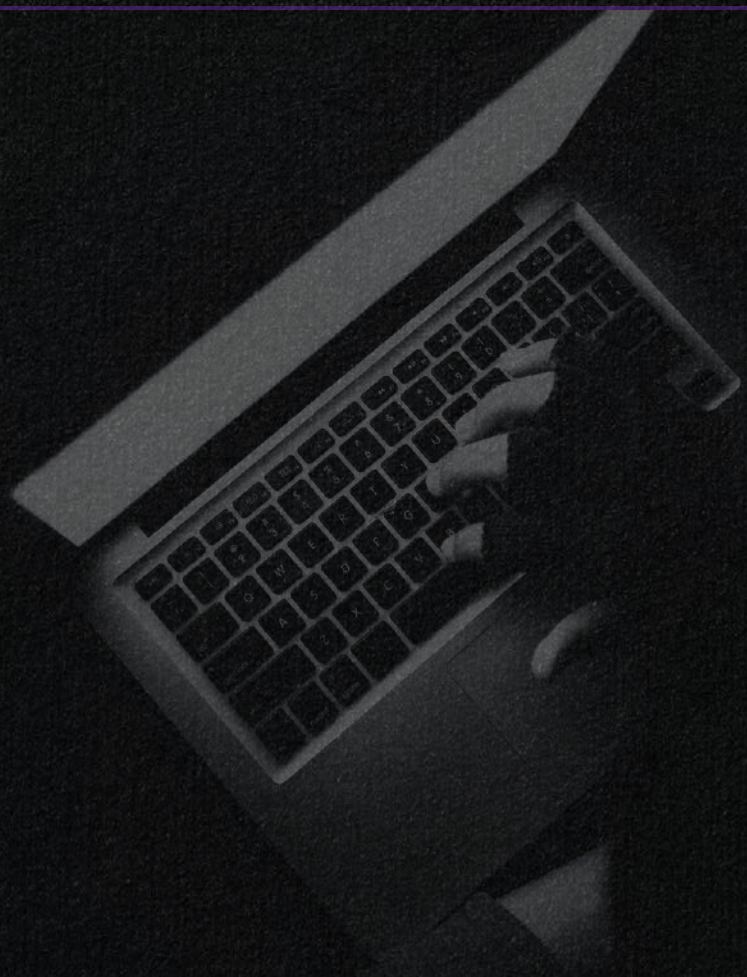
Combating sanctions evasion, terror financing, money laundering and other illicit state and individual activity requires a comprehensive approach because infinite value can move on-chain at the speed of light and nefarious actors continue to proliferate and innovate. The U.S. must integrate blockchain into cyber defense and national security operations. The DoD and USSOF should coordinate with allies and across U.S. government departments to develop a pilot program that places cryptocurrency in the hands of SOF operators and tactical teams to help develop new operational concepts, like using blockchain to authenticate drones, satellites, or secure command and control systems. Public-private partnerships – especially with blockchain analytics firms – are essential to detecting illicit flows, flagging high-risk wallets, and supporting real-time threat monitoring across decentralized networks. And it is working – TRM Labs' 2025 Crypto Crime Report shows that crypto-related crime is on a clear downward trend with illicit transaction volume dropping ~24% in 2024 to roughly $45 billion—just 0.4% of total crypto activity, down by half from the prior year. Major crime categories, including hacks, sanctions evasion, and scams, all saw significant declines with hack proceeds down 50% and scam payments falling 40%. This reflects a maturing crypto ecosystem and more effective enforcement actions globally.[63]

Defensively, blockchain can secure critical systems through immutable logs and authentication of drones, satellites, and communications. Offensively, the U.S. should explore neo-privateering, deputizing white hat hackers to recover stolen funds and neutralize malicious actors while aligning with constitutional principles and international norms.

Regulators must modernize financial rules for the digital asset economy. A unified, risk-based AML/know-your-customer (KYC) framework should clarify responsibilities across custodians, exchanges, and developers without stifling innovation or compromising privacy. Special attention should be paid to mixers, tumblers, and decentralized protocols, where traceability and compliance tools should be encouraged.

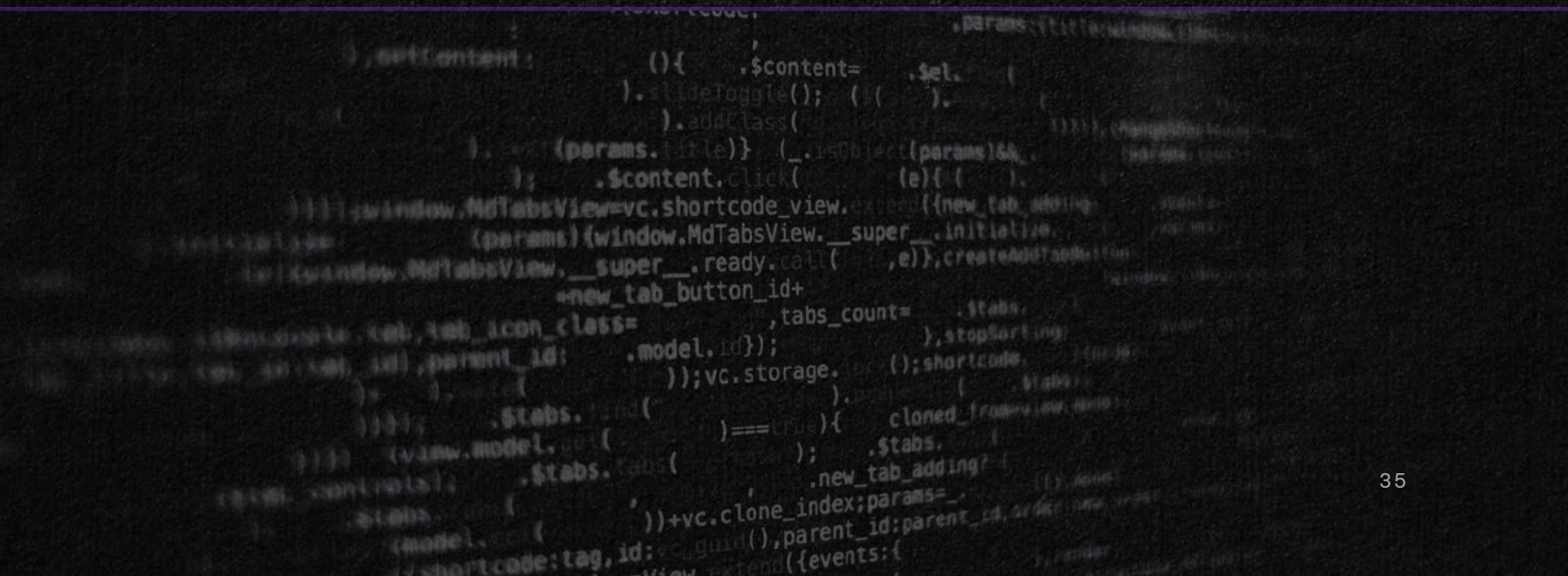
Codify and Legalize Privateering.
Deputizing, enabling and incentivizing white hat hackers to exploit smart contract vulnerabilities to track, freeze, and repossess stolen funds for a bounty via a neo-privateer program would empower the private sector to hack the hackers, protect consumers and support national security. This could be a low- or no-cost, effective component of a broader strategy that leverages American ingenuity and technical prowess while keeping pace with the scope and speed that digital rails necessitate. As more value is stored and transferred on blockchain networks the incentive for bad actors to abscond with digital assets will grow apace - and this solution scales along with it as the incentives for success grows.

Expand and Leverage Public Private Partnerships and Industry Watchdogs.
The speed at which value can move on-chain requires novel and robust relationships between government and industry via constructs like the T3 (Tether, TRM Labs and TRON, a leading layer one blockchain) Financial Crimes Unit (FCU), Illicit Virtual Asset Notification (IVAN), the Security Alliance (SEAL), the Crypto Information Sharing and Analysis Center (ISAC), and FBI - Operation Level Up (the FBI's proactive approach to identify and notify victims of cryptocurrency investment fraud and prevent further financial loss).



Real-time data sharing is vital to stifling illicit on-chain activity. Integrating robust compliance, audit, and transaction monitoring tools like those offered by Solidus Labs can significantly bolster security. The T3 FCU swiftly identifies on-chain transfers of USDT associated with illicit activity, isolates those funds, and partners with global law enforcement agencies to implement remedies. In less than a year, the T3 FCU successfully identified and froze over $200 million in funds linked to illicit activity on-chain, including commandeering funds associated with money laundering and hacks conducted by the Lazarus Group. Similarly, the Crypto ISAC — as a member-driven industry alliance — is well suited to provide the self-regulatory component that U.S. agencies can immediately leverage to protect consumers. Atomic real-time payment transactions increase the need to reduce false positives in risk detection and to improve and implement instant detection tools to halt fraudulent transactions before they are executed. Tools like Extractor by Hacken — an advanced on-chain monitoring platform — enable real-time detection of anomalous smart contract behavior, address activity, and cross-chain flows, providing actionable intelligence to exchanges, law enforcement, and intelligence agencies. Creative private partnerships with academia, such as the University of Wyoming's collaboration with Balcony Labs, are developing blockchain-based systems to securely monitor foreign ownership of sensitive U.S. land and critical infrastructure while protecting American landowners' privacy.[64]

Binance, the largest global exchange by volume and user base, has overhauled and enhanced its public-private collaboration and user protections. In 2024 alone, these efforts prevented over $4.2 billion in potential losses, safeguarded 2.8 million users, and enabled the recovery of $88 million in stolen assets, while Binance assisted authorities in dismantling international criminal networks.[65] The U.S. government must continue to engage large industry players, building on the successful examples of the T3 FCU and Binance's security and partnership initiatives to prevent abuse and fraud in cryptocurrency markets.



Modernize Financial Regulations for the Digital Asset Economy and reform the BSA.
The U.S. should harmonize AML/KYC standards across the digital asset ecosystem to balance security with financial privacy, ensuring that AML/KYC regulations are risk-based, innovation-friendly, and responsive to the unique characteristics of digital assets. Current oversight is fragmented between agencies (e.g., FinCEN, SEC, CFTC, IRS, DOJ), relies on legal frameworks that were drafted in the 1970s, and creates regulatory arbitrage opportunities that bad actors exploit while simultaneously creating uncertainty for innovators. A unified, risk-based approach to AML/KYC would provide clarity for compliant businesses, enable stronger enforcement, and reinforce U.S. leadership in international financial integrity efforts.

Applying traditional KYC requirements indiscriminately–especially to decentralized protocols, non-custodial wallets, or open-source developers–risks stifling innovation, abusing privacy, and misapplying rules to entities that lack the ability to comply. Instead, U.S. policy should encourage risk-based and layered AML standards like stricter obligations for custodians and fiat on/off ramps, flexible guidance for decentralized systems and non-custodial actors such as wallets and developers, and support for privacy-preserving compliance technologies such as decentralized identity. This tailored approach would uphold national security and provide protection for consumers without undermining innovation or competitiveness.

Establish An Effective AML Framework for DeFi.
To mitigate money laundering risks and protect the digital asset ecosystem the U.S. should establish a clear, AML framework for DeFi participants, including cryptocurrency exchanges, mixers, tumblers, and protocols with identifiable developers, operators, or decentralized autonomous organizations (DAOs). Effective AML frameworks require clear governance structures and accountability mechanisms. Where DeFi protocols are governed by identifiable developers, operators, or DAOs they should be subject to AML obligations commensurate with their level of control. International cooperation is also vital given the borderless nature of DeFi. Harmonization of AML standards and information-sharing among jurisdictions will help close regulatory gaps and prevent regulatory arbitrage. While fully decentralized mixers and tumblers may lack traditional onboarding processes, developers and operators can be encouraged or required to implement technical solutions that enhance traceability or limit access to sanctioned individuals. Finally, blocking protocols are a critical component of a comprehensive AML framework for DeFi participants to comply with sanctions and prevent illicit transactions.

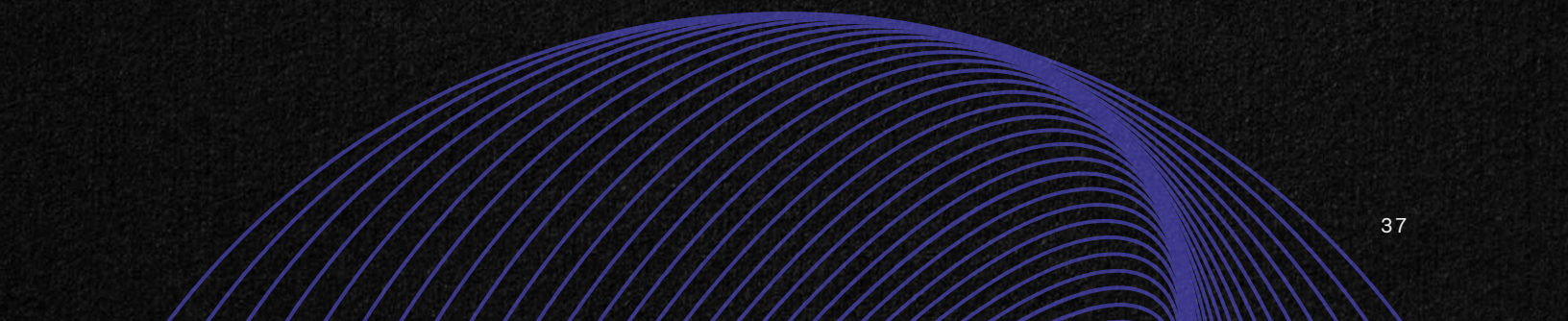
Conclusion

These principles are based on core American principles that form the foundation for many of the freedoms and privileges that Americans enjoy and that repressed populations yearn for. These should guide the formation of policy, law and regulation.

Blockchain is a present-tense strategic asset already shaping global power dynamics. The U.S. must lead in this new terrain or our adversaries will write the new rules of financial infrastructure, digital identity, and information security. Authoritarian states are weaponizing blockchain to bypass U.S. sanctions, finance proxy warfare, surveil populations, and export centralized digital systems. These are not theoretical threats. They are active, coordinated strategies that exploit the openness and fragmentation of Western digital governance.

At the same time, blockchain remains an underleveraged tool of American strength. Its attributes – decentralization, immutability, programmability, transparency – map closely to national security needs in an era of cyber threats, dollar devaluation risks, and asymmetric warfare. The report outlines concrete avenues for leveraging blockchain to bolster U.S. resilience: deploying Bitcoin-backed sovereign debt instruments (BitBonds) to modernize federal finance and reduce debt servicing costs; securing digital infrastructure and supply chains through smart contracts and tamper-proof audit trails; countering financial censorship and de-risking through stablecoins and decentralized finance; and restoring communications and mapping capacity in crisis zones through DePIN. These are forward-compatible solutions for a rapidly changing strategic landscape.

Critically, the U.S. must treat blockchain as dual-use infrastructure: simultaneously financial and military, civil and intelligence-enabling. That demands a shift in posture—from reactive regulatory skirmishes to proactive strategic engagement. A new Blockchain and Digital Asset Solarium Commission, targeted federal incentives for hardware, mining, and cybersecurity innovation, expansion of public-private partnerships for real-time threat detection, and legislation to legalize open-source development and codify privacy-preserving identity tools are urgent needs but not exhaustive.



America's adversaries understand the stakes. China's BSN, Russia's cross-border stablecoin trade networks, and North Korea's billion-dollar cyber raids are serious threats to the international financial systems that the U.S. and Western allies have cultivated for decades. The U.S. must respond by asserting a positive, democratic vision for blockchain development that reinforces both liberty and sovereignty. The path forward is not without risk, but inaction carries far greater cost. If the United States fails to lead, it will find itself operating in a digital world architected by others – one where control is centralized, surveillance is total, and American influence is diminished. Blockchain must be treated not as a curiosity, but as a foundational pillar of 21st-century national security. The time to act is now.

Appendix 1

Government Derisking / Sanctions Impacts on Platform Viability

Blockchain technology alone is not enough to prevent derisking — government and traditional banking rules can undo some of the inherent anti-censorship aspects of the technology. For example, cryptocurrency exchanges that have substantial business in the U.S. are required to be registered with FinCEN and are therefore subject to supervision and examination as money services businesses.[66] Through these requirements, a certain level of censorship can be achieved. Another example is OFAC sanctions rules, which stipulate that OFAC compliance obligations are the same regardless of whether a transaction is denominated in digital currency or traditional fiat currency.[67]

Two recent reports examined the effects of OFAC sanctions on blockchain networks, both concluding that censorship occurred. The first was a report by the Federal Reserve Bank of New York, examining how OFAC sanctions negatively impacted the autonomy and profitability of the cryptocurrency mixer Tornado Cash (part of the Ethereum blockchain network).[68]

A second analysis, conducted by several university professors and researchers, looked at the impact of OFAC sanctions on permissionless blockchains and found that 46% of Ethereum blocks were made by censoring actors complying with OFAC sanctions — indicating a significant impact on the neutrality of public blockchains.[69] This second analysis also found that censorship prolongs the time until a transaction is confirmed. Increased transaction confirmation latency not only compromises the integrity and trustworthiness of the blockchain but also opens avenues for various security vulnerabilities, including double-spending and network congestion.[70] Thus, censorship degrades the security of existing blockchains and the quality of service for users.[71]

Thus, while blockchain offers significant protection against financial censorship, it is not a panacea. Governments can still target individuals by imposing restrictions, monitoring transactions, restricting internet access, criminalizing the use of cryptocurrencies, or monitoring blockchain addresses. Public blockchains are also transparent, meaning that while transactions cannot be blocked, they can be traced, potentially exposing users to surveillance or retaliation.

Appendix 2

Blockchain Security

Not all blockchains offer the same level of security. The number and geographical distribution of nodes and whether running on decentralized infrastructure versus centralized cloud providers affect resilience to outages and attacks. More redundant networks with multiple independent nodes and overlapping infrastructure are better equipped to continue operating when parts of the system fail or are compromised.

Consensus mechanisms also matter; Proof of Work and Proof of Stake (PoS) present security tradeoffs, with PoS often relying on economic penalties (slashing) and validator incentives to deter bad behavior. A blockchain's market capitalization and token value further contribute to its security, as higher-value networks are more expensive to attack, increasing the economic deterrent to adversarial action. Throughput and latency also play a role: high performance networks are better equipped to withstand denial-of-service events and transaction surges, especially when coupled with redundant pathways for transaction processing and data validation.

The Lindey effect also applies here: blockchains that have persisted over time without major security failures signal greater long-term viability, as survival itself becomes evidence of resilience. Systems that have endured through market cycles, technological shifts, and adversarial conditions are statistically more likely to continue doing so in the future.

Finally, the security of the codebase itself, including audit history, bug bounty programs, and governance processes for upgrades - can significantly impact a chain's long-term integrity and responsiveness to emerging threats. In short, redundancy - in both infrastructure and system design - is a foundational component of blockchain security, enhancing fault tolerance, continuity, and trust.

Footnotes

[1] The industry's pace of development is frenetic and many early stage ventures launch in stealth; we recognize that other use cases, risks, opportunities, companies, tools or techniques may exist. We welcome input on such developments: policy@digitalchamber.org

[2] Campbell, A. [CampbellJAustin]. (2025, February 21). That Colossal Wreck [Post]. X. https://x.com/campbelljaustin/status/1830960930874749765?s=43

[3] Electric Capital Partners, LLC, Developer Report: Analysis of Open-Source Crypto Developers (Dec. 12, 2024), Crypto Developer Report. (2024). In 2024 Crypto Developer Report. Electric Capital.

[4] The White House, Executive Order No. 14105: America First Investment Policy (Feb. 21, 2025).

[5] U.S. Dep't of the Treasury, Transcript of U.S. Treasury Secretary Scott Bessent Interview with Tucker Carlson on President Donald Trump's Tariff Plan and Its Impact on the Middle Class (Press Release No. SB-0073) (Apr. 7, 2025), https://home.treasury.gov/news/press-releases/SB0073.

[6] Dashveenjit Kaur, China Unveils $54.5B National Blockchain Roadmap (Editorial), The Block (Jan. 9, 2025), https://blockchaintechnology-news.com/news/china-unveils-54-5b-national-blockchain-roadmap/; See also, Li Qian, Blockchain Valley Unveiled in Jing'an District, SHINE News (Oct. 25, 2024), https://www.shine.cn/news/metro/2410257011/

[7] Bitcoin.com News, People's Bank of China Highlights Digital Yuan and Blockchain in 2025 Strategy, Bitcoin.com News (Jan. 12, 2025), https://news.bitcoin.com/peoples-bank-of-china-highlights-digital-yuan-and-blockchain-in-2025-strategy/

[8] Valentin Weber, Data-Centric Authoritarianism: How China's Development of Frontier Technologies Could Globalize Repression, Nat'l Endowment for Democracy (Feb. 28, 2023), https://www.ned.org/data-centric-authoritarianism-how-chinas-development-of-frontier-technologies-could-globalize-repression-2/

[9] BRICS is an intergovernmental organization comprising ten countries – Brazil, Russia, India, China, South Africa, Egypt, Ethiopia, Indonesia, Iran and the United Arab Emirates. Re: BRI, see: Ximmei Shen, China's State-Backed Blockchain Project Aims to Be 'SWIFT' for Stablecoins and Central Bank Digital Currencies, S. China Morning Post (Apr. 6, 2023), https://www.scmp.com/tech/tech-trends/article/3207599/chinas-state-backed-blockchain-project-aims-be-swift-stablecoins-and-central-bank-digital-currencies

[10] VanEck, Our Portfolio Managers Weigh Impact of Trump's Tariffs, VanEck Insights (Apr. 8, 2025), https://www.vaneck.com/us/en/blogs/investment-outlook/our-portfolio-managers-weigh-impact-of-trumps-tariffs

[11] Zeke Faux, New Study Estimates as Much as $75 Billion in Global Victims' Losses to Pig-Butchering Scam, TIME (Feb. 29, 2024), https://time.com/6836703/pig-butchering-scam-victim-loss-money-study-crypto/. For $100,000 figure, see: U.S. Inst. of Peace, Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security (May 2024), https://www.usip.org/sites/default/files/2024-05/ssg_transnational-crime-southeast-asia.pdf

[12] Aidan Connor & David Wessel, What Is the Status of Russia's Frozen Sovereign Assets?, Brookings Inst. (Apr. 16, 2025), https://www.brookings.edu/articles/what-is-the-status-of-russias-frozen-sovereign-assets/

[13] 2-3% in blockchain-based systems vs. 6-7% in legacy systems.

[114] Maria Kolobova, Поддали монет: Россия и Белоруссия провели первые сделки в ЦФА [Russia and Belarus Conduct First Deals in Digital Financial Assets], Izvestia (n.d.), https://iz.ru/1875813/maria-kolobova/poddat-token-rossiia-i-belarus-proveli-pervye-sdelki-v-tsfa

[15] Mark Townsend, Russia Skirts Sanctions Using Bitcoin, Glob. Fin. Mag. (Feb. 3, 2025), https://gfmag.com/economics-policy-regulation/russia-skirts-sanctions-bitcoin-cryptocurrency/
Neil Barnett, The Other Bitcoin Boom: Crypto Mining in Russia's Shadow Territories (Commentary), Royal United Serv. Inst. (Dec. 12, 2024), https://www.rusi.org/explore-our-research/publications/commentary/other-bitcoin-boom-crypto-mining-russias-shadow-territories
Reuters, Russia Is Using Bitcoin in Foreign Trade, Finance Minister Says (Dec. 5, 2024), https://www.reuters.com/markets/currencies/russia-is-using-bitcoin-foreign-trade-finance-minister-says-2024-12-05/

[16] American Blockchain Initiative, Russian Cryptoeconomics Association (RCA) Expands to Africa: A Strategic Tool in Russia's 'Cold War' Against the West, Am. Blockchain Initiative Blog (Jan. 31, 2023), https://www.americanblockchaininitiative.org/blog/russian-cryptoeconomics-association-rca-expands-to-africa-a-strategic-tool-in-russias-cold-war-against-the-west

[17] Ledger Insights, Iran Confirms Working with Russia on CBDC, Tokenized Assets for Payments, Ledger Insights (May 3, 2024), https://www.ledgerinsights.com/iran-confirms-working-with-russia-on-cbdc-tokenized-assets-for-payments/

[18] David Carlisle, Crypto Regulatory Affairs: Iran and Russia Exploring Cross-Border Stablecoin Settlements, Elliptic Blog (Jan. 23, 2025), https://www.elliptic.co/blog/analysis/crypto-regulatory-affairs-iran-and-russia-exploring-cross-border-stablecoin-settlements

[19] Lubomir Tassev, Iran and Russia Talk Crypto Cooperation, Unveil Tool Streamlining Trade in National Currencies, Bitcoin.com News (June 12, 2023), https://news.bitcoin.com/iran-and-russia-talk-crypto-cooperation-unveil-tool-streamlining-trade-in-national-currencies/

[20] Reuters, Key Provisions of Russia–Iran Strategic Cooperation Treaty (Jan. 17, 2025), https://www.reuters.com/world/key-provisions-russia-iran-strategic-cooperation-treaty-2025-01-17/
American Blockchain Initiative, The Expanding Role of Blockchain in Russian Defense, Am. Blockchain Initiative Blog (Sept. 6, 2023), https://www.americanblockchaininitiative.org/blog/the-rising-role-of-blockchain-in-russian-defense

[21] Chainalysis Team, $2.2 Billion Stolen From Crypto Platforms in 2024, but Hacked Volumes Stagnate Toward Year-End as DPRK Slows Activity Post-July, Chainalysis Blog (Dec. 19, 2024), https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/

[22] Reuters. (2021, May 21). Iran uses crypto mining to lessen impact of sanctions, study finds. Reuters. https://www.reuters.com/technology/iran-uses-crypto-mining-lessen-impact-sanctions-study-finds-2021-05-21/

[23] Ari Redbord, Global Head of Policy and Government Affairs at TRM Labs, LinkedIn Post. https://shorturl.at/etv3t

[24] Crystal Intelligence. (2025, March 5). Beyond the headlines of Iran's crypto usage. Crystal Intelligence Investigations. https://crystalintelligence.com/investigations/beyond-the-headlines-of-irans-crypto-usage/

[25] De-risking is defined by the Treasury Department as the practice of financial institutions terminating or restricting business relationships indiscriminately with broad categories of clients rather than analyzing and managing client risks in a targeted manner. U.S. Department of the Treasury, AMLA, The Department of the Treasury's De-risking Strategy, April 2023, p. 1.

[26] See: Appendix 2, for discussion of variations in decentralization and how this impacts different blockchain networks.

[27] See: Kansky, A. CCN, What is Censorship Resistance: Can Bitcoin Be Censored (Sept. 24, 2024).

[28] CBC, Digital Currency Donations for Freedom Convoy Evading Seizure by Authorities (Mar. 21, 2022).

[29] Nellin-Zitter J., Business Insider, Impoverished Afghan Women are Receiving Emergency Aid in Crypto as the Taliban Limits Cash Withdrawals and Millions Go Hungry (Jan. 22, 2022).

[30] Siripurapu, A., & Berman, N. (2024, January 17). The Crypto Question: Bitcoin, Digital Dollars, and the Future of Money. Council on Foreign Relations. https://www.cfr.org/backgrounder/crypto-question-bitcoin-digital-dollars-and-future-money

[31] See: Appendix 2

[32] China's holdings stand at $757B, the lowest since 2009. https://www.ft.com/content/9b91b88e-cff0-4c70-8b49-5e7edc6b9f23?

[33] Andrew Hohns & Matthew Pines, Bitcoin-Enhanced Treasury Bonds: An Idea Whose Time Has Come, Bitcoin Policy Inst. (Mar. 31, 2025), https://www.btcpolicy.org/articles/bitcoin-enhanced-treasury-bonds-an-idea-whose-time-has-come

[34] Hohns & Pines, Bitcoin-Enhanced Treasury Bonds.

[35] Okwatch, L. (2025, June 10). BlackRock's IBIT becomes the fastest ETF in history to surpass $70 billion AUM. Crypto News. https://crypto.news/blackrock-spot-bitcoin-etf-ibit-hits-70b-fastest-2025/

[36] U.S. Department of the Treasury. (2024, May 13). Statement on the President's decision prohibiting the acquisition by MineOne Cloud Computing Investment I L.P. of real estate, and the operation of a cryptocurrency mining facility, in close proximity to Francis E. Warren Air Force Base. U.S. Department of the Treasury. https://home.treasury.gov/news/press-releases/j2335

[37] Jack Spira & David Wessel, What Are Stablecoins, and How Are They Regulated?, Brookings Inst. (June 6, 2025; updated June 18, 2025), https://www.brookings.edu/articles/what-are-stablecoins-and-how-are-they-regulated/

[38] Illya Otychenko, Stablecoin Landscape: What 2024 Reveals About 2025?, CEX.IO Blog (Jan. 31, 2025), https://blog.cex.io/ecosystem/stablecoin-landscape-34864

[39] Ian Allison, Stablecoins Will Expand Beyond Crypto Trading, Become Part of Mainstream Economy, Citi Predicts, CoinDesk (May 12, 2025), https://www.coindesk.com/business/2025/05/12/stablecoins-will-expand-beyond-crypto-trading-become-part-of-mainstream-economy-citi-predicts

[40] Douglas Kurdziel, Ricardo Correia, Thomas Olsen, Mike Baxter & Philipp Grimming, From Niche to Utility: Stablecoins Move toward the Financial Mainstream, Bain & Co. Brief (Apr. 29, 2025), https://www.bain.com/insights/from-niche-to-utility-stablecoins-move-toward-the-financial-mainstream/

[41] Citi Glob. Perspectives & Sols., Digital Dollars: Banks and Public Sector Drive Blockchain Adoption (Citi GPS Report, Apr. 23, 2025), https://www.citigroup.com/csc/citigpa/storage/public/GPS_Report_Blockchain_Digital_Dollar.pdf

[42] TDC explored these impacts in a 2025 report: The Digital Chamber, How Stablecoins Are Extending U.S. Dollar Dominance: A Policymaker's Guide to Action (Policy Report), https://digitalchamber.org/stablecoinreport/

[43] Ledger Insights, Chinese Think Tank Mulls US Dollar Stablecoin Response, Ledger Insights (Mar. 20, 2025), https://www.ledgerinsights.com/chinese-think-tank-mulls-us-dollar-stablecoin-response/

[44] This phenomenon is explored in an upcoming paper by TDC, and rests largely on removing target nations' monetary policy responses to a US tariff regime. Where USD-linked stablecoins serve the populations of target nations, those states will be unable to devalue their local currency to increase export viability, as local citizens will shift funds out of local currencies to USD-backed stablecoins as a store of value—and one that can be used as a payments tool, given the local acceptance of stablecoins.

[45] UNHCR, UNHCR Launches Pilot Cash-Based Intervention Using Blockchain Technology for Humanitarian Payments to People Displaced and Impacted by the War in Ukraine (Dec. 15, 2022), https://www.unhcr.org/ua/en/news/unhcr-launches-pilot-cash-based-intervention-using-blockchain-technology-humanitarian-payments

[46] Tether, Tether Recognized for Assisting the United States Secret Service in $23M Freeze Related to Transfers on Sanctioned Exchange, Garantex (Press Release, Mar. 7, 2025), https://tether.to/news/tether-recognized-for-assisting-the-united-states-secret-service-in-23m-freeze-related-to-transfers-on-sanctioned-exchange-garantex/

[47] It is important to note that major illicit actors like Huione Group, the Cambodian conglomerate that runs a Telegram-based market place enabling all varieties of illicit trade, have issued their own (unregulated, of course) stablecoin (Huione USD or USDH) that is uncensorable (along with a crypto exchange and blockchain). This makes it all the more important for sanctions that limit its ability to interact with traditional and regulated financial entities and rails, as U.S. Treasury's FinCEN has proposed. This is no small concern — Elliptic estimates that Huione Group entities received $98B in digital assets for illicit activity like pig butchering, money laundering and other scams while enabling $27B on its platform, the largest ever illicit online marketplace. Following the takedown of Huione Group, however, Huione's biggest competitor, "Tudou Guarantee," has seen users more than double — and cryptocurrency inflows are now approximately equal to those seen for Huione Group prior to its shutdown, displaying illicit actors' robustness in the face of enforcement. It is also important to note that though Huione Guarantee, the crypto darknet marketplace, was shutdown in May 2025, the same volume of activity simply migrated to other darknets, some of which Huione Group also controls.

[48] Univ. of Wyo., UW to Aid Efforts to Prevent 'Bad Actors' from Acquiring Sensitive U.S. Real Estate and Infrastructure (Oct. 10, 2024), https://www.uwyo.edu/news/2024/10/uw-to-aid-efforts-to-prevent-bad-actors-from-acquiring-sensitive-us-real-estate-and-infrastructure.html

[49] PR Newswire, Constellation Network Achieves Scalability, Security, and Defense Approval in Executing US Air Force Phase II Blockchain Contract (Apr. 19, 2023), https://www.prnewswire.com/news-releases/constellation-network-achieves-scalability-security-and-defense-approval-in-executing-us-air-force-phase-ii-blockchain-contract-301821462.html

[50] M. S. Rowen, Special Operations and Cryptocurrency: Concepts to Harness Innovation for National Security (master's thesis, Naval Postgraduate School 2022).

[51] SolanaNews.sol (@solananew), "Breaking: Solana DePIN Helium Hits All-time High — 1.1m Daily Users" (X post, Sept. 14, 2023), https://x.com/solananew/status/1702408562233665793?s=43

[52] Olivia White et al., Digital Identification: A Key to Inclusive Growth (In Brief), McKinsey Glob. Inst. (Apr. 2019), https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-In-brief.pdf

[53] Project ASAP, Blog, https://projectasap.io/blog/

[54] Digital Chamber, Chamber Calls on Congress to Form a Digital Asset & Blockchain Technology Solarium Commission (June 19, 2023), https://digitalchamber.org/chamber-calls-on-congress-to-form-a-digital-asset-blockchain-technology-solarium-commission/

[55] For House bill text, see: Text - H.R.3286 - 118th Congress (2023–2024): Securing Open Source Software Act of 2023. (2023, July 27). https://www.congress.gov/bill/118th-congress/house-bill/3286/text; for Senate bill text, see: S.917 - 118th Congress (2023–2024): Securing Open Source Software Act of 2023. (2023, May 16). https://www.congress.gov/bill/118th-congress/senate-bill/917

[56] Text - S.1492 - 119th Congress (2025–2026): Deploying American Blockchains Act of 2025. (2025, April 30). https://www.congress.gov/bill/119th-congress/senate-bill/1492/text

[57] To promote resiliency, CESER should also be considered an essential service, and budget reductions should not impact the agency, where possible.

[58] Jameel Ahmad, Muhammad Rizwan, Syed Farooq Ali, Usman Inayat, Hafiz Abdul Muqeet, Muhammad Imran, Tabbi Awotwe, Cybersecurity in smart microgrids using blockchain-federated learning and quantum-safe approaches: A comprehensive review, Applied Energy, Volume 393, 2025, 126118, ISSN 0306-2619, https://doi.org/10.1016/j.apenergy.2025.126118.

[59] Chow, Harry, Leveraging Blockchain for Military Automation and Cybersecurity (February 17, 2025). Available at SSRN: https://ssrn.com/abstract=5182637 or http://dx.doi.org/10.2139/ssrn.5182637

[60] See: Deloitte US, Using blockchain to drive supply chain transparency: Use cases and future outlook on blockchain in supply chain management, June 2024. https://www2.deloitte.com/us/en/; Also: Fleet Readiness Center Southwest. (2018, September 24). FRCSW and NAVAIR exploring blockchain technology. Naval Air Systems Command. https://frcsw.navair.navy.mil

[61] Successful examples include the World Food Programme's Building Blocks program. Information can be found at: WFP Innovation Hub. https://innovation.wfp.org/project/building-blocks

[62] U.S. Securities and Exchange Commission. (2024, May 29). Comment on Digital Securities Sandbox Joint Bank of England and Financial Conduct Authority consultation paper [Statement by Commissioner Hester M. Peirce]. https://www.sec.gov/newsroom/speeches-statements/peirce-boe-fca-comment-05302024

[63] TRM Labs, Crypto Crime Report 2025. https://cdn.prod.website-files.com/6082dc5b670652507b3587b4/6823baf9045160ea474b3f7a_TRM_2025%20Crypto%20Crime%20Report.pdf

[66] 31 C.F.R. 1010.100(ff).

[67] OFAC, Questions on Virtual Currency, #560 (Mar. 19, 2018).

[68] Federal Reserve Bank of New York, Staff Report No. 1112, Regulating Decentralized Systems: Evidence from Sanctioned Tornado Cash (Aug. 2024).

[69] Wahrstätter A., et al., BlockChain Censorship, In Proceedings of the ACM Web Conference 2024, May 13–17.

[70] Id., p. 1639

[71] Id.