Chinese Dominance in Bitcoin Mining Poses a National Security Threat

Executive Summary

Chinese dominance in Bitcoin Application-Specific Integrated Circuit (ASIC)[1] mining equipment manufacturing poses a significant threat to U.S. national security and critical infrastructure. As of 2025, more than 95% of Bitcoin ASIC mining equipment is manufactured by three Chinese companies, Bitmain, MicroBT, and Canaan. The resulting imbalance creates vulnerabilities, particularly as mining platforms are deeply integrated with U.S. energy grids.

Mining rigs consume vast amounts of power and possess energy optimization capabilities that could be exploited for remote disruption, grid synchronization attacks, or energy market manipulation. Additionally, Chinese manufacturers are actively evading U.S. tariffs and export controls by establishing US-based manufacturing facilities to circumvent tariffs and maintain market access.[2]

To counter these growing risks the US must engage in a coordinated federal policy response, involving national security assessments, enforcement of export controls, and congressional engagement is also crucial to ensure that the physical infrastructure powering U.S. digital assets is built by trusted allies.

[1] ASIC chips are designed for a particular purpose, in this context bitcoin mining. They are custom built to solve bitcoin's proof-of-work algorithm.

[2] Casey Hall and Li Gu, 'Dominant Chinese Makers of Bitcoin Mining Machines Set Up U.S. Production to Beat Tariffs,' Reuters, June 18, 2025, https://www.reuters.com/world/china/dominant-chinese-makers-bitcoin-mining-machines-set-up-us-production-beat-2025-06-18/.

Risks and Vulnerabilities of Chinese Dominance

The United States is a leader in cryptocurrency and digital assets innovation, but remains dependent on hardware produced in and heavily influenced by a geopolitical rival.

The imbalance introduces several layers of potential risk and vulnerability because:

- **Mining platforms are high-users of electricity, and are continuously integrated with electric grids around the country.** They are significant grid-connected infrastructure deployed in data-center-like facilities that run 24/7 and consume energy at levels comparable to small cities.
  - Mining platforms have access to real-time information, and the ability to affect usage rates at a significant scale. Industrial-scale miners often contract directly with utilities or operate in deregulated markets.
- **Modern mining platforms include unique and dynamic energy optimization capabilities.** They can ramp up or down energy usage in real-time based on grid needs. This capability can help stabilize electricity demand and prevent brownouts—if operated by trusted vendors; but could also do the opposite.

As a result, U.S. grid infrastructure faces potential vulnerabilities to:

- **Remote access or disruption**. Foreign-designed chips or firmware could potentially include backdoors that might allow adversarial control or surveillance of power usage.
- **Grid synchronization attacks**. If malicious firmware were activated, synchronized shutdowns or surges could potentially destabilize regional grid operations.
- **Energy market manipulation**. Coordinated behavior across foreign controlled machines could distort pricing or availability in energy markets.

The security of mining hardware is not an isolated IT issue; it is a grid infrastructure and a national security issue. Because digital assets are integrated into energy systems and payment rails, the hardware supporting them must be subject to the same scrutiny as any other critical electrical or financial infrastructure.[3]

China is Using Unfair Tactics to Dominate the U.S. Crypto Infrastructure

[3] "Examining Emerging Threats to Electric Energy Infrastructure," *House Committee on Energy and Commerce's Subcommittee on Oversight and Investigations*, July 18, 2023, https://d1dth6e84htgma.cloudfront.net/07_18_2023_Public_Memo_O_and_I_Hearing_Electric_Infrastructure_3fd9635180.pdf.

Chinese companies with deep financial backing and reported ties to the Chinese Communist Party (CCP), maintain their overwhelming market dominance (approximately 95% share) through predatory pricing practices that undercut competition and aggressive financial incentives to lure miners into long-term hardware commitments.[4]

While miners often choose Chinese hardware for cost reasons, this short-term economic incentive comes with long-term strategic risks. The United States has seen this playbook before: reliance on foreign vendors in sectors like telecommunications, semiconductors, unmanned aerial vehicles, and port equipment eroded national security and American innovation. Without action, the same vulnerabilities are being embedded into the backbone of the digital asset infrastructure; a sector crucial to America's leading role in tech innovation and global finance.[5]

Chinese Mining Equipment Manufacturers Are Evading U.S. Tariffs and Export Controls

The United States places stringent controls on advanced semiconductor technologies, including 2 nm, 3 nm, 4 nm, and 5 nm chips used in Bitcoin ASIC mining. These components have dual-use potential and strategic significance. Under the Export Administration Regulations (EAR) such high-performance chips require export licenses when destined for China or other controlled countries. Simultaneously, 25% Section 301 tariffs apply to electronics and computing equipment manufactured in China, covering a broad range of Bitcoin ASIC devices.

To circumvent these trade restrictions, Chinese mining equipment companies initially shifted production to final assembly subsidiaries in Southeast Asia, in particular Malaysia, Thailand, and Singapore. This tactic enabled their ASIC miners to be labeled as of non-Chinese origin and bypass certain tariffs and export controls.

However, in 2025, these companies moved another step further by establishing U.S.-based production facilities. This most recent maneuver enables their ASIC miners to be designated U.S.-origin, further evading trade barriers and regulatory oversight. Leading industry sources now confirm that firms such as Bitmain and MicroBT are assembling mining hardware in the United States as their primary tariff-mitigation strategy.

Enforcement actions have intensified in parallel. In late 2024, U.S. Customs and Border Protection (CBP) significantly escalated seizures of Bitcoin miners upon the discovery of restricted AI chips from Sophgo. In January 2025, Sophgo– a Bitmain subsidiary– was officially blacklisted by the U.S. government due to national security concerns and links to

[4] Eliza Gkritsi, "Bitmain Discounts Bitcoin Mining Machines in an Already Depressed Market," *Coindesk*, May 11, 2023, https://www.coindesk.com/business/2022/09/21/bitmain-discounts-bitcoin-mining-machines-in-an-already-depressed-market.
[5] "Across U.S., Chinese Bitcoin Mines Draw National Security Scrutiny," *The New York Times*, October 13, 2023, https://www.nytimes.com/2023/10/13/us/bitcoin-mines-china-united-states.html.

Huawei. CBP also considered whether the seized miners could function as unauthorized communications devices, even when they possess no radio frequency capabilities.[6,7]

This evolving pattern of evasion of U.S. trade and export control policies creates enforcement blind spots by allowing advanced chips with potential dual-use applications to enter the U.S. for use in critical mining infrastructure without the proper licensing, scrutiny, or classification. The resulting regulatory gap poses serious and significant challenges to U.S. supply chain integrity and national security, especially as ASIC mining hardware becomes increasingly embedded in the nation's energy grids and digital financial systems.

Recommended Actions

1. **Initiate a Coordinated Federal Policy Response**

The U.S. has coordinated several policy reforms in critical sectors such as telecommunications (Huawei), port infrastructure (ZPMC), and semiconductors. That same strategic approach can now be extended to bitcoin and digital asset infrastructure through executive orders or other means. Including:

- ❖ **National Security Assessment.** Direct sector risk management agencies (e.g. DOE, CISA, DHS) to formally assess crypto mining infrastructure as a national security concern and include findings in the annual and biennial risk reports to Congress for the 2025−2026 cycles

- ❖ **White House Crypto Council Workstream.** The Council should prioritize crypto infrastructure, similar to the manner in which it has emphasized infrastructure security for AI.[8]

- ❖ **Priority for Investigation.** Include crypto mining infrastructure as part of the Commerce Department's 2025/2026 technology priorities for investigation.

- ❖ **Congressional ASIC Engagement.** Include trusted vendor language for ASIC security in Administration requests to Congress.

This framework would ensure that the physical infrastructure powering blockchain ecosystems is built by trusted allies and not geopolitical rivals. Having a national strategy and drawing a clear line between trusted and untrusted vendors is essential to

---

[6] Daniel Kuhn, "US Customs and Border Patrol expands Bitcoin mining machine seizures to MicroBT and Canaan units: Blockspace," *The Block*, February 13, 2025, https://www.theblock.co/post/340756/border-patrol-expands-bitcoin-mining-machine-seizures-to-microbt-and-canaan-units-blockspace.

[7] A.J. Vicens and Raphael Satter, "US authorities begin releasing some seized cryptocurrency miners, industry executives say," *Reuters*, March 5, 2023, https://www.reuters.com/technology/us-authorities-begin-releasing-some-seized-cryptocurrency-miners-industry-2025-03-05/.

[8] America's AI Action Plan, Pilar II. Pages 17-22 https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.

safeguarding U.S. financial security and long-term competitiveness in the digital economy.

2. **Congressional Action**

Congress has a role to play in addressing these concerns and stimulating the growth of U.S.-based solutions:

- ❖ Incorporate policy language in major legislation (e.g., NDAA, appropriations, energy security bills) encouraging procurement from trusted vendors for ASIC mining equipment.
- ❖ Demand agency briefings on national security risks of PRC-controlled crypto infrastructure.
- ❖ Use oversight authority to press the Administration for a public position and risk assessment.
- ❖ Insert language into NDAA, appropriations, or digital asset legislation mandating a public report on the role of foreign hardware and actors in the U.S. digital asset infrastructure and grid systems.

The Time to Act Is Now

Blockchain validation is rapidly emerging as a foundational pillar of global digital infrastructure.The hardware that secures digital ledgers, verifies transactions, and maintains trust in decentralized systems must be demonstrably secure and trusted–rather than manufactured by geopolitical competitors known for unfair market practices and strategic leverage.

The federal government must take decisive steps to reduce strategic dependence on Chinese suppliers, particularly in sectors that form the backbone of our economy and national security. Congress and the Administration can ensure the United States leads not only in digital asset adoption but in the underlying infrastructure that protects and sustains it.

Whether it’s drones that patrol our skies, cranes that move goods through our ports, or the chips that secure our cryptocurrencies, the principle remains the same: America must operate with trusted hardware that reflects its values and protects its sovereignty.