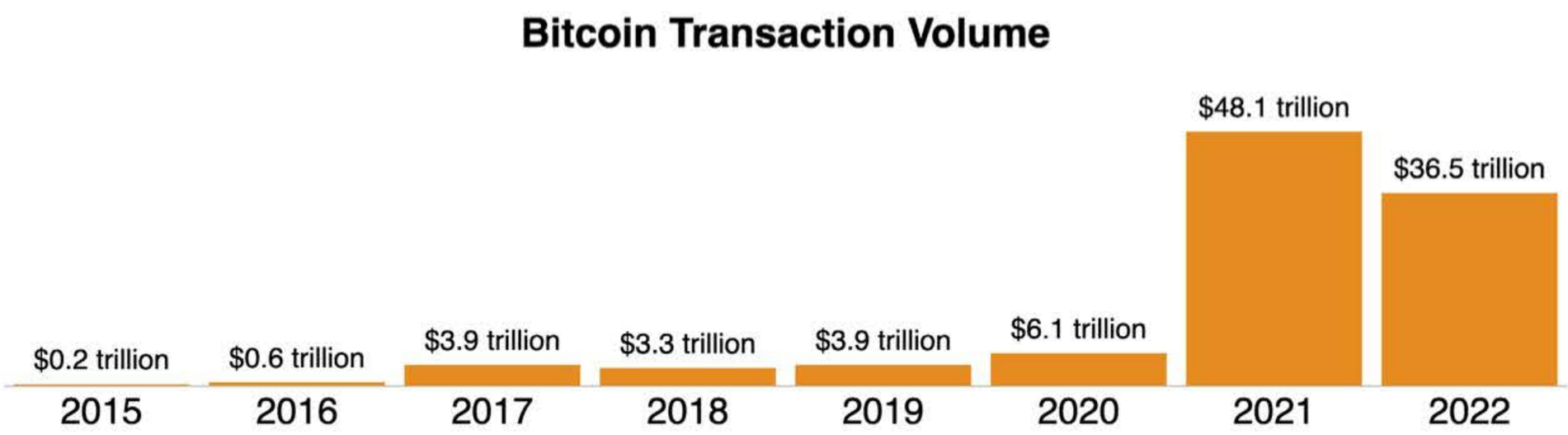
1. The value of Bitcoin

Satoshi Nakamoto summarized his reason for inventing Bitcoin in this way: “The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible. […] Bitcoin is a distributed system with no single point of failure. Users hold the crypto keys to their own money and transact directly with each other, with the help of the P2P network to check for double-spending.”[1]

Bitcoin (BTC) provides access to payments without relying on financial intermediaries. The benefits of transacting with Bitcoin include 24/7 availability, global electronic final settlement in less than one hour, open-source programmability and auditability, and cryptographic security. These benefits provide value to the public and have grown the transactional use of Bitcoin from zero in 2009 to $36.5 trillion worth of bitcoin transacted on its decentralized ledger in 2022.



In addition to its medium-of-exchange transactional users, Bitcoin has accrued a significant base of long-term investors. Investors value the Bitcoin network’s predictable issuance schedule[2]. The quantity of BTC units on the ledger can be independently verified using open-source node software[3].

Node software is like internet browser software, it enables a user to access the network. Unlike a web browser, a Bitcoin node downloads and verifies all the network’s data to independently re-calculate the ledger of all Bitcoin transactions and thus audit the supply of BTC. The majority of the BTC are held by long-term investors as a store-of-value often described as “digital gold”,

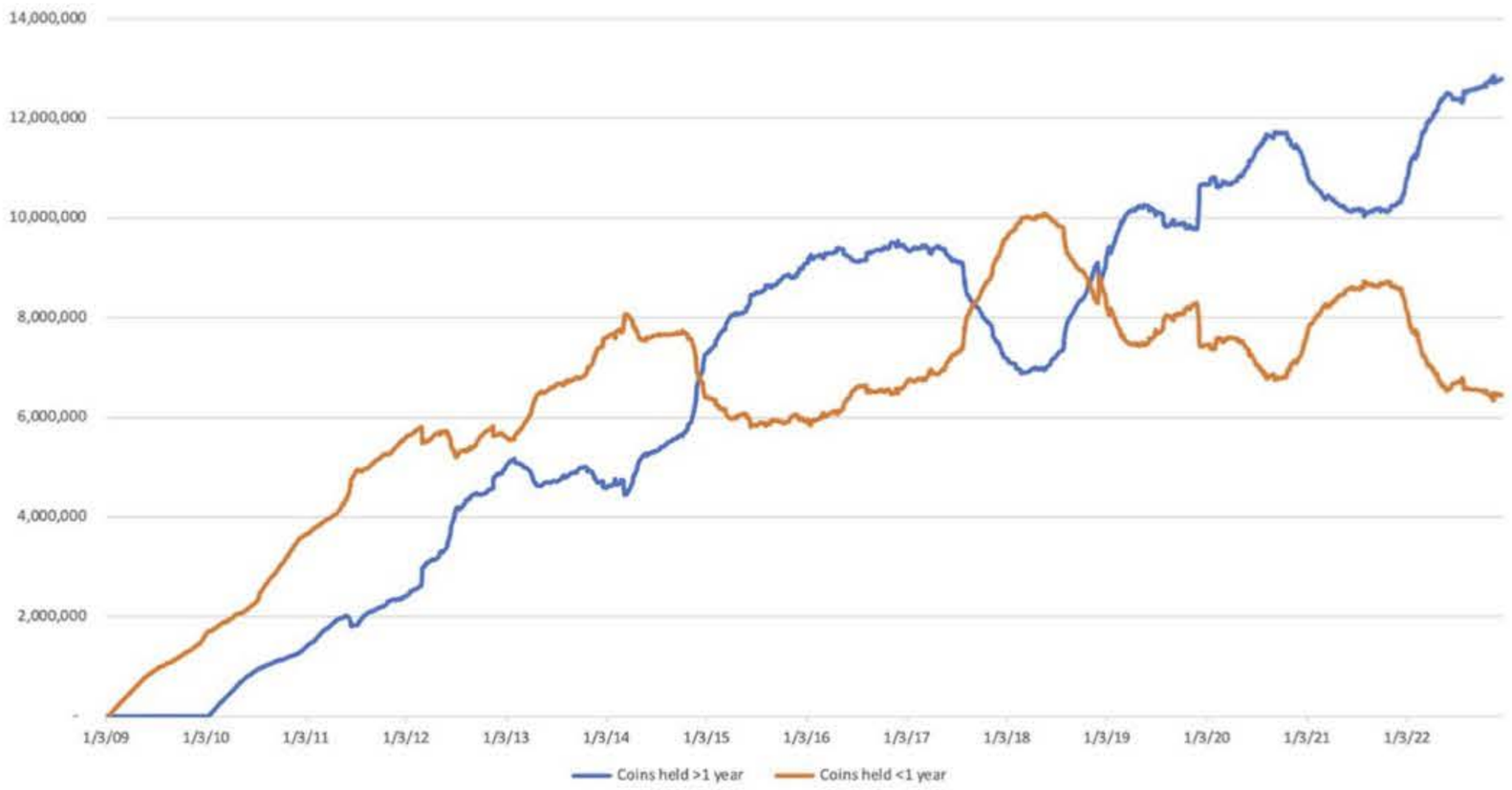
---

[1] Nakamoto, Satoshi. Bitcoin Open Source Implementation of P2P Currency. Satoshi Nakamoto Institute, 11 Feb. 2009, https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/1/.

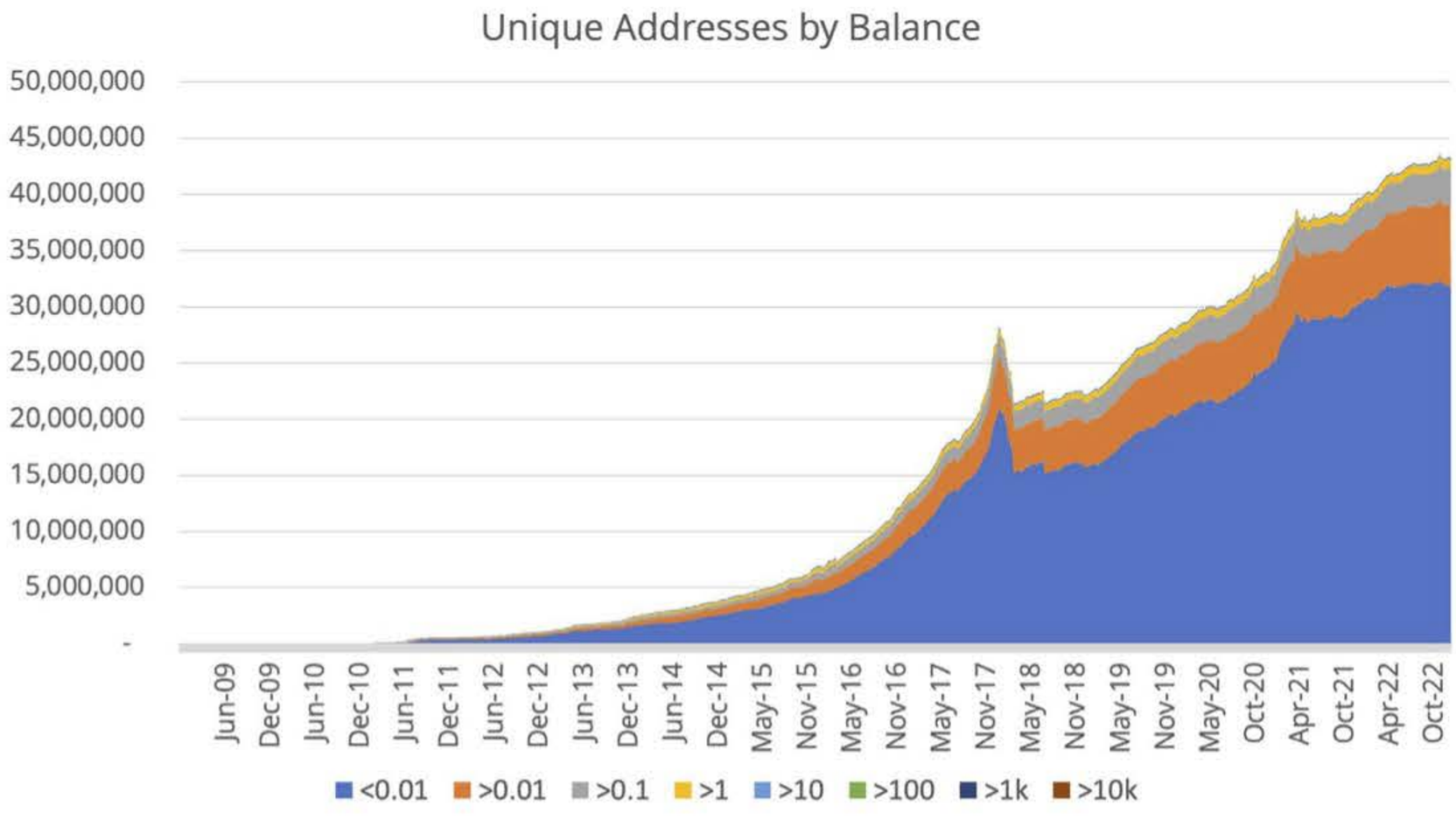
[2] Jones, Paul Tudor. “The Great Monetary Inflation.” Market Outlook – Macro Perspective, 10 May 2020, https://www.lopp.net/pdf/BVI-Macro-Outlook.pdf.

[3] Rochard, Pierre. “Auditing Bitcoin Supply.” PierreRochard.com, 8 Oct. 2020, https://www.pierrerochard.com/auditing-bitcoin-supply/.

a hedge against fiscal and monetary risks[4] of proprietary centralized systems. Data from the blockchain indicates that the majority of BTC has been held as long-term savings, not as a short-term speculation.



Small and large balances of BTC are treated equally by the Bitcoin network. Wealth does not influence the Bitcoin protocol's operations, unlike the proprietary fiat system where wealth can waive fees, raise limits, and give access to exclusive perks[5]. Most of the Bitcoin addresses, analogous to accounts, hold less than 0.01 BTC (roughly $200 based on the current exchange rate).

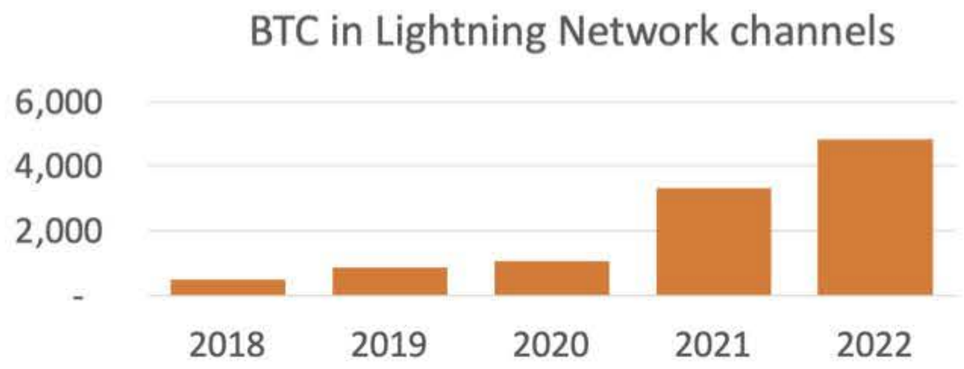


[4] Roy, Avik. "How Bitcoin Protects Americans from Inflation." Bitcoin Policy Institute, 26 Oct. 2021, https://www.btcpolicy.org/articles/how-bitcoin-protects-americans-from-inflation.

[5] Dimon, Jamie. "Chase Private Client Checking." Chase, https://www.chase.com/personal/checking/private-client.

Creating a Bitcoin address (a “wallet”) is just cryptographic math, and it's free and instant. Though it is still unfamiliar to most people, anyone can learn to use Bitcoin today. The option to use Bitcoin is available to everyone equally, the powerful and the marginalized, the banked and the unbanked. As a public network, Bitcoin is a beacon of global empowerment and financial inclusion[6].

To speed up small Bitcoin payments, open-source protocol developers invented an overlay network called Lightning[7]. This network routes payments through channels anchored in the Bitcoin blockchain. Lightning enables small transfers of BTC to be instant and almost free, while still benefiting from the Bitcoin protocol’s security and stability. The Lightning network’s openness and programmability has attracted successful fintech entrepreneurs like Jack Dorsey[8] and David Marcus[9] to build Lightning-integrated products. The quantity of BTC committed to the Lightning network has been increasing[10] over the past five years:



2. Realities of Bitcoin

No system can be or is perfect. While Bitcoin has fewer risks and harms than proprietary centralized fiat systems, it should be closely evaluated.

Software Limitations

The public can independently verify Bitcoin transactions and audit the Bitcoin ledger to ensure compliance with the Bitcoin protocol rules by using node software. This software connects with the Bitcoin p2p network to download the blockchain data from peers, independently verify each accounting entry, and reproduce the entire Bitcoin ledger. The user’s wallet can query this ledger to summarize balances and transactions. Anyone with a high-speed internet connection and a contemporary computing device can use node software.

---

[6] Hernández, Carlos. “Bitcoin Has Saved My Family.” The New York Times, The New York Times, 23 Feb. 2019, https://www.nytimes.com/2019/02/23/opinion/sunday/venezuela-bitcoin-inflation-cryptocurrencies.html.

[7] “What Is the Lightning Network?” River Learn - Bitcoin Technology, River Financial, https://river.com/learn/what-is-the-lightning-network/.

[8] Namcios. “Jack Dorsey's Cash App Integrates Bitcoin's Lightning Network.” Nasdaq, 7 Feb. 2022, https://www.nasdaq.com/articles/jack-dorseys-cash-app-integrates-bitcoins-lightning-network.

[9] Betz, Brandy. Libra Creator David Marcus Begins New Lightning Network Venture, Lightspark. CoinDesk, 12 May 2022, https://www.coindesk.com/business/2022/05/12/libra-creator-david-marcus-begins-new-lightning-network-venture-lightspark/.

[10] “Bitcoin: Lightning Network Capacity.” Glassnode Studio - On-Chain Market Intelligence, https://studio.glassnode.com/metrics?a=BTC&category=&m=lightning.NetworkCapacitySum.

The primary source of risks for users of Bitcoin is potential flaws in their node software that mis-apply the protocol rules. The first major incident was in 2010 when an inflation bug in the software enabled anyone to create an infinite amount of bitcoin[11]. This bug was solved by users of node software as they rolled the blockchain back to the last known valid block.

The second and most recent major incident was in 2013[12], when a flawed new version of the node software caused the block size limit to accidentally be increased. To resolve this bug the node operators changed their software back to the previous version. Those are the only two times Bitcoin has a significant consensus-level risk materialize, and in both cases Bitcoin the issue was promptly solved by the users of the software. There have been many minor flaws discovered and resolved of Bitcoin's history. Satoshi Nakamoto's now-famous white paper itself has many known problems that have been discovered[13] and resolved in the 14 years since its publication.

Custody Experiences

With freedom comes responsibility. There are cases of Bitcoin users losing their private keys[14] or getting their wallet hacked[15]. In response to these risks and harms, secure products and best practices have emerged.

Users are encouraged to keep only small amounts of BTC on mobile and desktop software wallets[16]. Keys that control large amounts of BTC should be held in specialized devices known as hardware wallets. The latest generation of devices from leading manufacturers like Coinkite, Ledger, and Trezor have not had a successful private key extraction by security researchers - meaning no one has been able to hack into a wallet and access a user's funds. While critical vulnerabilities may emerge in the future, hardware wallets are currently considered to be secure if properly setup by the user[17].

---

[11] "CVE-2010-5139 Detail." NIST, 6 Aug. 2012, https://nvd.nist.gov/vuln/detail/CVE-2010-5139.

[12] Narayanan, Arvind. "Analyzing the 2013 Bitcoin Fork: Centralized Decision-Making Saved the Day." Freedom to Tinker, 27 Mar. 2019, https://freedom-to-tinker.com/2015/07/28/analyzing-the-2013-bitcoin-fork-centralized-decision-making-saved-the-day/.

[13] Harding, David. "Bitcoin Paper Errata and Details." Gist GitHub, 6 Aug. 2018, https://gist.github.com/harding/dabea3d83c695e6b937bf090eddf2bb3.

[14] Hamilton, Isobel Asher. "The Quest to Find $181 Million in Bitcoin Buried in a Dump." Business Insider, Business Insider, 24 July 2022, https://www.businessinsider.com/james-howells-threw-away-bitcoin-dump-masterplan-get-back-2022-7.

[15] "Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency." The United States Department of Justice, 8 Feb. 2022, https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.

[16] Lopp, Jameson. "Recommended Bitcoin Wallets." Lopp.net, https://www.lopp.net/bitcoin-information/recommended-wallets.html.

[17] Stevens, Robert. "How Do Hardware Wallets Keep Crypto Safe?" CoinDesk, CoinDesk, 22 Nov. 2022, https://www.coindesk.com/learn/how-do-hardware-wallets-keep-crypto-safe/.

To further reduce risk and harms from holding private key material, users are encouraged to use Bitcoin's multi-signature ("multisig") functionality[18]. This functionality can be thought of as a form of two-factor authentication; it removes any single point of failure by requiring a quorum of signers from a set of private keys, for example 2-of-3 or 3-of-5. Decentralization and redundancy of cryptographic key material in different geographic locations with the multisig feature creates unique value for users, unavailable with physical and financial assets.

In addition, hardware wallets can be backed-up on metal as 12 to 24 words, called a "seed plate". This enables private keys to be resilient to fire and flood[19]. Alternatively, these 12 to 24 seed words can be memorized.

The dematerialization of value as private keys is new and unfamiliar to the public, creating risks of harm, but education and new products are bridging the gap to enable the public to secure their Bitcoin. Third-party custody adds risks of harm to the public, as evidenced by the failures of FTX, Celsius, Voyager, and BlockFi[20]. Federal policymakers and researchers should identify ways to encourage the public to self-custody their Bitcoin and avoid trusting third parties.

Illicit Activity

Almost all Bitcoin transaction volume reflects lawful usage by the public. In 2022, only an estimated 0.24% of transaction volume was associated with illicit usage[21] whereas the UN estimates that traditional fiat money laundering is 2.7% of global GDP[22]. To improve their investigative capabilities, law enforcement and prosecutorial agencies can familiarize themselves with Bitcoin through education[23] and usage. The Justice Department has a proven track-record of effectively combating illicit use of Bitcoin[24].

Fiat-crypto exchanges have had guidance on their Bank Secrecy Act AML/KYC obligations since FinCen issued an administrative ruling in 2014[25] to define "virtual currency". Generally, criminals want to convert crypto-currencies to fiat and their activity at regulated exchanges can contribute evidence for prosecution. An industry has emerged to assist law enforcement in

---

[18] "Operational Security Guide." Unchained Capital, Unchained Capital, May 2020, https://unchained.com/wp-content/uploads/2022/01/Unchained-Operational-Security-Guide.pdf.

[19] Lopp, Jameson. "Metal Bitcoin Seed Storage Stress Test." Cypherpunk Cogitations, Lopp.net, 24 Jan. 2020, https://blog.lopp.net/metal-bitcoin-seed-storage-stress-test/.

[20] Olinga, Luc. "FTX, BlockFi, Voyager, Celsius: Awful Year for Crypto Investors." TheStreet, 29 Nov. 2022, https://www.thestreet.com/investing/cryptocurrency/ftx-blockfi-voyager-celsius-awful-year-for-crypto-investors.

[21] The 2023 Crypto Crime Report. Chainalysis, Feb. 2022, https://go.chainalysis.com/2023-crypto-crime-report.html.

[22] "Tax Abuse, Money Laundering and Corruption Plague Global Finance." United Nations, United Nations, https://www.un.org/development/desa/en/news/financing/facti-interim-report.html.

[23] Bhasker, Sanjeev, et al. "Carpe Crypto: Prosecuting Cases Involving Digital Assets and Blockchain Technology." DOJ Journal of Federal Law and Practice, Dec. 2022, pp. 105–116.

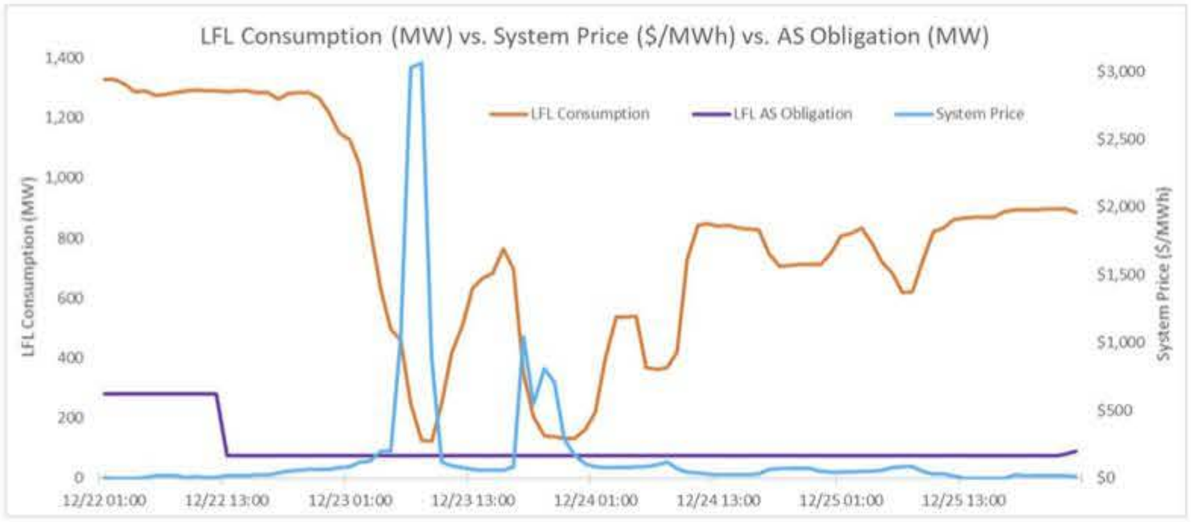
[24] Mallin, Alexander. "DOJ Seizes Millions in Ransom Paid by Colonial Pipeline." ABC News, ABC News Network, 7 June 2021, https://abcnews.go.com/Politics/doj-seizes-millions-ransom-paid-colonial-pipeline/story?id=78135821.

[25] "Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System." FinCEN.gov, Financial Crimes Enforcement Network, 27 Oct. 2014, https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R012.pdf.

countering illicit financial activity using digital assets, for example Coinbase, Ciphertrace, and Chainalysis have received government contracts[26].

Energy Facts

Electricity is a dynamic market with volatile supply and demand. On the supply side, volatility is driven by natural gas prices and the intermittency of wind and solar power generation. On the demand side, consumption of electricity is highly seasonal with wide daily oscillations. Bitcoin mining's electricity consumption is highly interruptible, it can quickly and granularly shed load to stabilize the electricity grid and decrease price volatility[27]. Bitcoin contributes to grid resilience and energy security. Texas' ERCOT grid operator illustrated this inverse relationship between electricity prices and Bitcoin mining electricity consumption during the December 2022 Texas freeze[28]:



Computing cryptographic hashes ("Bitcoin mining") does not directly emit any EPA criteria air pollutants or greenhouse gases (GHG). From a Scope 1 emissions[29] perspective, Bitcoin mining is fully electrified and zero-emissions. Indirectly, Bitcoin mining may reduce electricity grids' greenhouse gas emissions by replacing natural gas and coal peaking power plants[30]. Peaker plants only turn on for short periods of time when there is temporarily high demand, their use is avoided when Bitcoin miners temporarily curtail power usage. This enables the grid to have more zero-carbon electricity producers.

---

[26] Ehrenhofer, Justin. "Coinbase, Ice and Bitcoin Blockchain Surveillance - Bitcoin Magazine ..." Bitcoin Magazine, 14 July 2022, https://bitcoinmagazine.com/business/coinbase-ice-and-bitcoin-blockchain-surveillance.

[27] Mellerud, Jaran, and Anders Helseth. "How Bitcoin Mining Can Transform the Energy Industry." Arcane Research, 1 Sept. 2022, https://arcane.no/research/how-bitcoin-mining-can-transform-the-energy-industry-new-report.

[28] Woodfin, Dan. "December 2022 Cold Weather Operations: Preliminary Observations." ERCOT Public. ERCOT Public, 24 Jan. 2023.

[29] "Scope 1 and Scope 2 Inventory Guidance." EPA Center for Corporate Climate Leadership, Environmental Protection Agency, https://www.epa.gov/climateleadership/scope-1-and-scope-2-inventory-guidance.

[30] Ibañez, Juan & Freier, Alexander. (2023). Can Bitcoin Stop Climate Change? Proof of Work, Energy Consumption and Carbon Footprint (SoK).

Bitcoin mining's unique controllable load profile was recognized as a benefit to the ERCOT grid by the Texas Work Group on Blockchain Matters Report[31]. Electricity and water consumption, noise pollution, and electronic waste from Bitcoin mining can all be reduced using innovative immersion cooling technology[32].

Benefits of Consensus

The central benefit of Bitcoin's use of proof-of-work ("mining") is the network's decentralized consensus on the order of transactions that are recorded on the ledger. Satoshi Nakamoto's breakthrough was a solution to the "double-spending" problem that did not rely on trusting a third-party[33]. The central benefit of Bitcoin's use of proof-of-work is freedom and inclusion for users[34]: anyone can run a Bitcoin node at a very low cost to verify the miners' work, anyone can earn the block reward by mining[35], and anyone can use the ledger by paying a transaction fee.

Bitcoin miners generate cryptographic hashes using SHA-256. Bitcoin nodes require the miners to provide a hash with a minimum number of leading zeros, called the difficulty. Since each hash is random, miners must generate many hashes to probabilistically find one with enough leading zeros. The difficulty is updated every 2,016 blocks to average a winning hash, and thus a block, every 10 minutes.

Proof-of-stake relies on signatures from a set of token-holders, or "stakers." Unlike proof-of-work hashes, proof-of-stake signatures are not probabilistically anchored in time. Blockchains that use proof-of-stake are therefore more vulnerable to ledger re-writes that compromise their transaction settlement finality, and therefore, the overall integrity of the ledger[36]. Computer science researchers refer to this flaw in proof-of-stake as the "nothing at stake" or "costless simulation" problem[37] and it increases the risk of fraud on the network. A potential solution to this security vulnerability would be to checkpoint proof-of-stake blockchains in

---

[31] Texas Work Group on Blockchain Matters. "Texas Work Group on Blockchain Matters Report: TX BCWG." Texas Work Group on Blockchain Matters Report | TX BCWG, 15 Nov. 2022, https://portal.bcwg.texas.gov/General-Documents/Texas-Work-Group-on-Blockchain-Matters-Report/wbtp-2m5k.

[32] Economics of Immersion Cooling for Bitcoin Miners. Braiins, 9 May 2022, https://braiins.com/blog/economics-immersion-cooling-bitcoin-miners.

[33] Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." To, 31 Oct. 2008, https://nakamotoinstitute.org/bitcoin/.

[34] Huberman, Gur and Leshno, Jacob and Moallemi, Ciamac C., Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System (September 30, 2020). Columbia Business School Research Paper No. 17-92, Available at SSRN: https://ssrn.com/abstract=3025604 or http://dx.doi.org/10.2139/ssrn.3025604

[35] Prat, Julien and Walter, Benjamin, An Equilibrium Model of the Market for Bitcoin Mining (February 05, 2018). CESifo Working Paper Series No. 6865, Available at SSRN: https://ssrn.com/abstract=3143410 or http://dx.doi.org/10.2139/ssrn.3143410

[36] Tas, E. N., Tse, D., Yu, F., & Kannan, S. (2022). Babylon: Reusing Bitcoin Mining to Enhance Proof-of-Stake Security. doi:10.48550/ARXIV.2201.07946

[37] Poelstra, A. (2016, May 25). A Treatise on Altcoins. WP Software. Retrieved September 9, 2022, from https://download.wpsoftware.net/bitcoin/alts.pdf.

Bitcoin's proof-of-work history using Taproot, a recent upgrade to Bitcoin's smart contract scripting language[38].

Bitcoin's use of a proof-of-work system in combination with a difficulty adjustment is at the cutting edge of computer science and software engineering. Bitcoin empowers the public to earn, save, and spend their money freely in a peer-to-peer process, without relying on trusted third-party intermediaries.

3. Federal research opportunities in Bitcoin

Federal research in semiconductor efficiency[39], immersion cooling technologies, and renewable electricity production[40] would increase the competitiveness of Bitcoin mining in the United States. Increasing domestic production of Bitcoin hashrate is in the national security interest of the United States as it reduces hard currency revenues to adversaries[41].

Regulators can help protect consumers from fraud by educating the public about how to securely use Bitcoin node software, hardware wallets, and multisig. Regulators should re-use and elaborate on common phrases that have emerged over the past decade relating to safe Bitcoin use such as "not your keys, not your bitcoin" and "don't trust, verify". In particular, regulators should be cautious not to conflate Bitcoin with knockoff "altcoins" or allegedly unregistered securities in "digital assets".

To effectively improve Bitcoin usability for underserved communities, Federal research opportunities should be directed towards open-source Bitcoin projects with the guidance of organizations like Bitcoin Design[42] and Summer of Bitcoin[43].

4. Federal research priorities for Bitcoin

Federal research opportunities should be introduced to:

---

[38] Azouvi, S., & Vukolić, M. (2022, August 10). *Pikachu: Securing proof-of-stake blockchains from long-range attacks by checkpointing into Bitcoin proof-of-work using Taproot*. arXiv.org. Retrieved September 9, 2022, from https://arxiv.org/abs/2208.05408.

[39] "Efficiency of Bitcoin Mining Hardware." IEA, https://www.iea.org/data-and-statistics/charts/efficiency-of-bitcoin-mining-hardware.

[40] Sigalos, MacKenzie. "Tesla, Block and Blockstream Team up to Mine Bitcoin off Solar Power in Texas." CNBC, CNBC, 8 Apr. 2022, https://www.cnbc.com/2022/04/08/tesla-block-blockstream-to-mine-bitcoin-off-solar-power-in-texas.html.

[41] Orcutt, Mike. "North Korea Appears to Have Expanded Its Crypto-Mining Operation." MIT Technology Review, 22 Mar. 2022, https://www.technologyreview.com/2020/02/11/844871/north-korea-cryptocurrency-mining-monero/.

[42] "Open-Source Design for Bitcoin Products." Bitcoin Design, July 2020, https://bitcoin.design/.

[43] "Summer of Bitcoin." Summer of Bitcoin, Oct. 2021, https://www.summerofbitcoin.org/.

- Verify estimates that Bitcoin's indirect emissions of 62 MtCO2e per year are orders of magnitude less than tourism's indirect emissions of 4,500 MtCO2e per year[44].
- Build on existing research to quantify reduced GHG emissions from Bitcoin miners replacing peaker plants[45].
- Compare the low cost of Bitcoin's open-source Lightning network[46] protocol versus the high cost of closed proprietary fiat card fees[47]. Lowering the cost of payments and removing the Visa/Mastercard duopoly as gatekeepers of commerce would advance U.S. competitiveness and leadership in the world.
- Study the potential effect of a de minimis tax exemption[48] on consumer choice for the 19% of Americans who are unbanked or underbanked[49]. Putting Bitcoin and the Lightning network on a level playing field with traditional payment incumbents that are not subject to capital gains tax could help the U.S. catch up to countries that already have a tax exemption for Bitcoin[50].
- Assess how accumulating BTC in a Bitcoin Strategic Reserve can strengthen the US Dollar, increase Federal resilience, reduce Bitcoin's price volatility, and diversify the nation's gold reserves. The U.S. Federal government is already a leading holder[51] of Bitcoin due to past seizures of the asset, but auctions of seized Bitcoin would cede this leading position.
- Evaluate the national security interest in out-competing adversaries with Bitcoin mining[52]. China, North Korea, Iran, Russia, and Venezuela are all mining Bitcoin, the more market share of hashrate the United States can take, the less profitable it is for others to mine. Domestic Bitcoin mining helps advance U.S. competitiveness and leadership in the world.
- Examine the risks and harms of growing authoritarian CBDC networks[53]. CBDCs may enable human rights abuses by authoritarian regimes and undermine economic

---

[44] "Comparisons of Greenhouse Gas Emissions." Cambridge Centre for Alternative Finance, https://ccaf.io/cbeci/ghg/comparisons.

[45] How Bitcoin Mining Can Support the Energy Transition. Wood Mackenzie, 7 Apr. 2021, https://www.woodmac.com/news/opinion/how-bitcoin-mining-can-support-the-energy-transition/.

[46] Ogawa, Yuya. Lightning Network's Advantages as Payment Technology. Bitcoin Magazine, 8 Aug. 2022, https://bitcoinmagazine.com/technical/lightning-network-payment-technology-advantages.

[47] Durbin, Marshall Introduce Bipartisan Credit Card Competition Act: U.S. Senator Dick Durbin of Illinois. 28 July 2022, https://www.durbin.senate.gov/newsroom/press-releases/durbin-marshall-introduce-bipartisan-credit-card-competition-act.

[48] Brito, Jerry. "Congress Takes a Step toward a De Minimis Capital Gains Exemption for Everyday Cryptocurrency Transactions." Coin Center, 26 July 2022, https://www.coincenter.org/congress-takes-a-step-toward-a-de-minimis-capital-gains-exemption-for-everyday-cryptocurrency-transactions/.

[49] "Economic Well-Being of U.S. Households in 2021." Board of Governors of the Federal Reserve System, May 2022, https://www.federalreserve.gov/publications/files/2021-report-economic-well-being-us-households-202205.pdf.

[50] "Crypto Tax Free Countries 2023." Koinly, 3 Jan. 2023, https://koinly.io/blog/crypto-tax-free-countries/.

[51] "Bitcointreasuries.net." BitcoinTreasuries.NET, https://bitcointreasuries.net/.

[52] Lowery, Jason. Softwar: A Novel Theory on Power Projection and the National Strategic Significance of Bitcoin. Massachusetts Institute of Technology, 2023.

[53] Kimani, Michael. "China Leads Africa's Digital Currency Race." CoinDesk, 14 Sept. 2021, https://www.coindesk.com/policy/2021/02/03/china-leads-africas-digital-currency-race/.

growth[54]. The introduction of this foreign technology in the United States could enable adversaries to fully control and surveil domestic economic activity, directly undermining U.S. leadership and competitiveness.

- Identify and responsibly disclose vulnerabilities, as well as suggest usability improvements, in the MuSig family of cryptographic protocols[55] to increase security for Bitcoin users.

Federal R&D for software and hardware development should be focused on open-source contributions to existing projects, rather than creating duplicative new projects. Furthermore, research should be oriented towards solving real Bitcoin user problems. These problems can be identified in existing UX research[56], through new research initiatives, with first-hand experience using Bitcoin in various contexts, and by working directly with Bitcoin stakeholders.

5. Bitcoin education in the United States

Regardless of warnings from skeptical adults, children of all ages are going to experiment with Bitcoin because the technology is freely available. To protect children from risks and harms of Bitcoin, educational curriculums at all age levels should be updated to include how to use Bitcoin and Lightning wallets securely and responsibly. In higher education, Texas A&M University has introduced a Bitcoin Protocol course[57] for computer science students to familiarize themselves with the technical underpinnings of Bitcoin. Workforce training at technical colleges should include opportunities to learn how to repair Bitcoin mining rigs. The unfamiliarity of Bitcoin indicates that a significant national competitive advantage can be developed through education.

Conclusion

Bitcoin's freedom and inclusion benefits have resulted in significant adoption by the public over the past decade. The Bitcoin community[58] and industry have developed educational material and products to successfully mitigate the risks and harms of Bitcoin. The National Digital Assets Research and Development Agenda should build on this track-record to help advance U.S. competitiveness and leadership in the world.

---

[54] Smolenski, Natalie. "Why the U.S. Should Reject Central Bank Digital Currencies." Bitcoin Policy Institute, 27 Sept. 2022, https://www.btcpolicy.org/articles/why-the-u-s-should-reject-central-bank-digital-currencies.

[55] "Musig." Bitcoin Optech, https://bitcoinops.org/en/topics/musig/.

[56] Estevão, Patrícia. "Bitcoin UX Research." Patrícia Estevão, 15 Aug. 2021, https://patestevao.com/work/bitcoin-ux-research/.

[57] Henton, Lesley. "New Class Explores Technical and Economic Foundations of Bitcoin." Texas A&M Today, 3 Feb. 2023, https://today.tamu.edu/2023/01/20/new-class-explores-technical-and-economic-foundations-of-bitcoin/.

[58] Rizzo, Pete. "Why Bitcoin Maximalism Is Critical." Bitcoin Magazine, 12 July 2022, https://bitcoinmagazine.com/culture/why-bitcoin-maximalism-is-critical.