

Criminal Legal News

PUBLISHED BY THE HUMAN RIGHTS DEFENSE CENTER

VOL. 8 No. 9
ISSN 2576-9987 (Print)
ISSN 2577-0004 (Online)

Dedicated to Protecting Human Rights

September 2025

SPECIAL DIGITAL CURRENCIES ISSUE: BITCOIN AND CBDCs

What Is Bitcoin? The Answer to Government Surveillance and Control Through Money

*An Essential Introduction, Glossary of Multidisciplinary
Terminology, and Colorful History*

by Richard Resch

"It is well enough that people of the nation do not understand our banking and monetary system, for if they did, I believe there would be a revolution before tomorrow morning." – Henry Ford

WHAT IS MONEY? EVERYONE NEEDS and wants it, but few can actually define it. At its core, money is a social construct, an abstract concept with tangible forms. Money is an agreement within a society about what constitutes a medium of exchange, a unit of account, and a store of value. Essentially, money represents a shared agreement on value and thereby facilitates economic interactions by providing a standardized way to measure worth, store wealth over time, and settle debts.

By engaging with the material in this article, you will be able to meaningfully answer that deceptively simple question about money as well as gain a clear understanding of Bitcoin – its revolutionary nature, its eventful history, its role as the future of global finance, and its ability to thwart mass surveillance and pervasive control by governments.

A Brief History of Money

Money facilitates trade by overcoming the limitations of barter, where goods and ser-

vices are directly exchanged. Without money, a farmer wanting to trade wheat for shoes would need to find a shoemaker who specifically wants wheat, and both would need to agree on the relative value of their goods. As societies grew more complex, the problem of the "coincidence of wants" – both parties wanting what the other party offered at the same time – as well as issues with portability and perishability made bartering impractical. Money solves bartering's limitations by providing a universally accepted intermediary, which allows for more efficient and complex economic interactions. Throughout history, societies have adopted various forms of money, each reflecting the technological and social structures of their time.

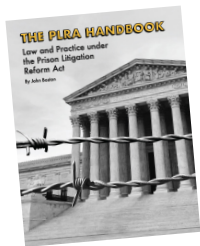
The earliest forms of money were often commodities with intrinsic value, such as livestock, grains, or tools. These "commodity monies" were useful in their own right, making them accepted within communities. As societies grew, more portable and durable items like shells (e.g., cowrie shells), beads, and precious metals (gold, silver, copper) emerged. These items were valued for their rarity, divisibility, and resistance to decay, making them superior forms of money. The use of standardized

weights of precious metals eventually led to the development of coinage, which further streamlined transactions by guaranteeing purity and weight.

The evolution continued with the advent of "representative money," where paper notes or other tokens represented a claim on a certain amount of a commodity, typically gold or silver, held in reserve. This "gold standard" or "silver standard" allowed for easier portability and larger transactions without physically moving heavy metals. Over time, as trust in institutions grew, money transitioned to "fiat currency" – money deriving its value based on government decree, not backed by a physical commodity but by the faith and credit of the issuing authority. This allows central banks greater flexibility in managing the money supply and influencing economic activity.

INSIDE

| | |
|---------------------------------|----|
| What Is Bitcoin? | 1 |
| From the Editor | 36 |
| Central Bank Digital Currencies | 39 |



The PLRA Handbook: Law and Practice under the Prison Litigation Reform Act

John Boston



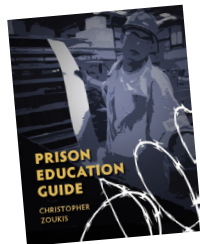
Prisoners \$84.95



Lawyers/Entities \$224.95

ISBN-13: 979-8-9854138-0-9 • Paperback, 576 pages

The PLRA Handbook: Law and Practice under the Prison Litigation Reform Act is the best and most thorough guide to the PLRA provides a roadmap to all the complexities and absurdities it raises to keep prisoners from getting rulings and relief on the merits of their cases. The goal of this book is to provide the knowledge prisoners' lawyers – and prisoners, if they don't have a lawyer – need to quickly understand the relevant law and effectively argue their claims.



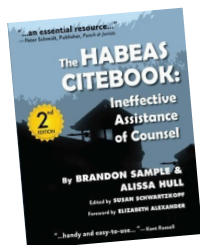
Prison Education Guide

\$24.95

Christopher Zoukis

ISBN: 978-0-9819385-3-0 • Paperback, 269 pages

Prison Education Guide is the most comprehensive guide to correspondence programs for prisoners available today. This exceptional book provides the reader with step by step instructions to find the right educational program, enroll in courses, and complete classes to meet their academic goals. This book is an invaluable reentry tool for prisoners who seek to further their education while incarcerated and to help them prepare for life and work following their release.



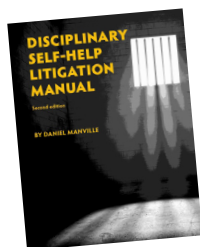
The Habeas Citebook: Ineffective Assistance of Counsel, Second Edition

\$49.95

Brandon Sample & Alissa Hull

ISBN: 978-0-9819385-4-7 • Paperback, 275 pages

The Habeas Citebook: Ineffective Assistance of Counsel is the first in a series of books by Prison Legal News Publishing designed to help pro-se prisoner litigants identify and raise viable claims for potential habeas corpus relief. This book is an invaluable resource that identifies hundreds of cases where the federal courts have granted habeas relief to prisoners whose attorneys provided ineffective assistance of counsel.



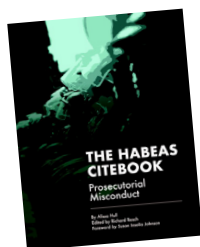
Disciplinary Self-Help Litigation Manual, Second Edition

\$49.95

Dan Manville

ISBN: 978-0-9819385-2-3 • Paperback, 355 pages

The Disciplinary Self-Help Litigation Manual, Second Edition, by Dan Manville, is the third in a series of books by Prison Legal News Publishing. It is designed to inform prisoners of their rights when faced with the consequences of a disciplinary hearing. This authoritative and comprehensive work educates prisoners about their rights throughout this process and helps guide them at all stages, from administrative hearing through litigation. The Manual is an invaluable how-to guide that offers step-by-step information for both state and federal prisoners, and includes a 50-state analysis of relevant case law and an extensive case law citation index.



The Habeas Citebook: Prosecutorial Misconduct

\$59.95

Alissa Hull

ISBN-13: 978-0-9819385-5-4 • Paperback, 300 pages

The Habeas Citebook: Prosecutorial Misconduct is the second in PLN Publishing's citebook series. It's designed to help pro se prisoner litigants identify and raise viable claims for potential habeas corpus relief based on prosecutorial misconduct in their cases. This invaluable title contains several hundred case citations from all 50 states and on the federal level, saving readers many hours of research in identifying winning arguments to successfully challenge their convictions.

- ☐ The PLRA Handbook
- ☐ Prison Education Guide
- ☐ The Habeas Citebook
- ☐ Disciplinary Self-Help Litigation Manual
- ☐ The Habeas Citebook: Prosecutorial Misconduct

Order by mail, phone, or online. Amount enclosed _____

By: ☐ check ☐ credit card ☐ money order

Name _____

DOC/BOP Number _____

Institution/Agency _____

Address _____

City _____ State _____ Zip _____



Human Rights Defense Center
Dedicated to Protecting Human Rights

PO Box 1151 • Lake Worth Beach, FL 33460 • Phone # 561-360-2523

WWW.PRISONLEGALNEWS.ORG • WWW.CRIMINALLEGALNEWS.ORG

Criminal Legal News

a publication of the

Human Rights Defense Center

www.humanrightsdefensecenter.org

EDITOR

Paul Wright

SENIOR MANAGING EDITOR

Richard Resch, JD

EDITORIAL ASSISTANT

Henry Lopez

CONTRIBUTING WRITERS

Anthony W. Accurso, Douglas Ankney,

Casey Bastian, Matthew Clarke,

Jeffrey Cohen, David Kim,

Jo Ellen Nott, David M. Reutter,

Sagi Schwartzberg, JD

Michael Dean Thompson,

Phillip Wasserman, JD

ADVERTISING COORDINATOR

Chris Bailey

HRDC LITIGATION PROJECT

Jonathan Picard - Litigation Director

CLN is a monthly publication.

A one year subscription is \$48 for prisoners and individuals, and \$96 for professionals and institutions. Subscriptions will be pro-rated at \$4 each; do not send less than \$24 at a time; pro-rated subscriptions are only available to prisoners. All foreign subscriptions are \$100 sent via airmail. CLN accepts credit card orders by phone. New subscribers please allow four to six weeks for the delivery of your first issue. Confirmation of receipt of donations cannot be made without an SASE. HRDC is a section 501 (c)(3) non-profit organization. Donations are tax deductible. Send contributions to:

Criminal Legal News

PO Box 1151

Lake Worth Beach, FL 33460

561-360-2523

info@criminallegalnews.org

www.criminallegalnews.org

CLN reports on state and federal appellate court decisions and news stories related to substantive criminal law, criminal procedure, official misconduct and constitutional rights within the criminal justice system, and the police state. CLN welcomes all news clippings, legal summaries, and leads on people to contact related to the foregoing issues.

Article submissions should be sent to - The Editor - at the above address. We cannot return submissions without an SASE. Check our website or send an SASE for writer guidelines.

Advertising offers are void where prohibited by law and constitutional detention facility rules.

What Is Bitcoin? (cont.)

In the modern era, physical currency has increasingly been supplemented and, in many cases, replaced by digital money. This includes funds held in bank accounts, credit and debit cards, and online payment systems. In this system, money is represented by digital entries rather than tangible objects. This digital transformation has dramatically accelerated transactions and global commerce. The latest iteration in this ongoing evolution of money is the emergence of the decentralized digital currency Bitcoin, which has redefined the very nature of money by operating outside traditional financial institutions and government control.

Beyond its economic functions, money has served as a tool for control, enabling those in power to shape societies through manipulation of supply, access, and surveillance. By debasing currencies to fund wars or imposing sanctions to enforce policies, authorities can erode individual wealth or restrict freedoms, as evidenced by historical coin clipping by Roman emperors or modern asset freezes during political unrest. In the digital age, this control greatly intensifies with traceable electronic transactions and programmable currencies like Central Bank Digital Currencies ("CBDCs"), which can dictate spending behaviors or exclude dissenters from economic participation. Bitcoin's decentralization is a direct assault on this paradigm, providing humanity with a form of money resistant to such centralized dominance. Ultimately, money is not merely a neutral medium of economic exchange but also an instrument of power, reflecting and perpetuating existing hierarchies.

What Is Bitcoin?

This section provides a concise, foundational primer on Bitcoin. Designed to furnish a clear, high-level understanding, think of it as your essential starting point for grasping the very basics of what Bitcoin is and why it is special. This article builds upon this foundational material, explaining the intricate details and broader concepts of what makes Bitcoin genuinely unique.

Bitcoin is a digital monetary system that operates without banks, governments, or any intermediaries. It is humanity's first successful implementation of a truly decentralized currency. It enables secure, direct financial transactions between any two individuals

anywhere in the world simply by using the internet, eliminating the need for costly and often restrictive intermediaries.

Unlike traditional financial systems where central authorities control money supply and transactions, Bitcoin runs on a global network of computers maintaining an immutable public ledger (the "blockchain") through mathematical consensus. The blockchain provides radical transparency. Every transaction is recorded publicly, verifiable by all, preventing fraud. This groundbreaking system replaces institutional trust with cryptographic proof, ensuring no single party can alter the rules, manipulate transactions, or inflate the supply. With a strict hard cap of just 21-million Bitcoins – a feature hard-coded into its protocol – Bitcoin successfully imposes absolute scarcity onto money for the first time in human history.

What makes Bitcoin revolutionary is its unique convergence of three transformative properties: (1) decentralized governance, making it resistant to censorship; (2) predictable scarcity, protecting against inflation; and (3) open access, enabling financial inclusion. The Bitcoin network achieves unprecedented security through a mechanism called "Proof-of-Work" mining, where participants compete to validate transactions and earn newly created Bitcoins – a process that renders attacks on the network prohibitively expensive while distributing power globally.

Beyond its technical innovations, Bitcoin represents a fundamental philosophical shift – money that cannot be confiscated, devalued, or restricted by any authority. It serves simultaneously as "digital gold" for the information age, a borderless payment system for the global economy, and financial infrastructure for the nearly 1.3 billion people globally who are unbanked. Bitcoin has demonstrated remarkable resilience through its numerous challenges during its relatively short existence. Each crisis has only validated its core value proposition: a global monetary system where rules cannot be changed by decree and no permission is needed to participate.

Bitcoin benefits humanity by providing something it has never experienced – a neutral, open, and decentralized monetary network that cannot be seized, censored, or debased and that operates beyond political control. In a world of increasing financial surveillance and currency debasement, Bitcoin is the most significant innovation in money since the creation of banking – and its story is just beginning.

Demystifying Bitcoin: A Glossary of Core Multidisciplinary Terminology

Bitcoin's creation required a unique synthesis of technical expertise and deep knowledge across a wide range of diverse and complex disciplines, a multidisciplinary marvel of engineering unparalleled in monetary history. The pseudonymous creator of Bitcoin, Satoshi Nakamoto, demonstrated polymathic mastery in computer science (especially distributed systems and network theory, including Byzantine Fault Tolerance), advanced cryptography (SHA-256, digital signatures, hash functions, and elements of information theory), monetary economics (with deep roots in Austrian economics), and game theory (specifically mechanism design and non-cooperative theory).

Satoshi successfully devised a system in which incentives are so perfectly aligned that all participants voluntarily choose to persistently defend the Bitcoin network in an inherently noncommunicative, trustless, and adversarial environment. The design requires rigorous mathematical precision for Proof-of-Work, intimate hardware awareness for energy-driven security, and a keen understanding of behavioral psychology to solve complex coordination problems where communication is not possible and trust is absent.

Beyond brilliant code, Bitcoin's engineering drew lessons from monetary collapses (Weimar Republic and Hungarian hyperinflation), failed digital cash experiments (DigiCash, B-Money, etc.), and cypherpunk ideals of adversarial resistance against government surveillance. This unprecedented convergence of so many disparate disciplines likely explains why no one invented it sooner – Bitcoin required a polymath with not just exceptional technical abilities but also a unified understanding of why trust-based systems in a persistent adversarial environment fail. Bitcoin's genius lies in how it transforms human nature (greed, skepticism, etc.) and physical laws (energy costs, cryptography, etc.) into an antifragile precision system in which each discipline's weaknesses are compensated for by another's strengths. Bitcoin is a da Vinci-like masterpiece that artfully synthesizes multiple seemingly unconnected fields, resulting in humanity's first self-sustaining system of decentralized digital money.

The Importance of This Glossary

For those unfamiliar with Bitcoin, the specialized terms and jargon – such as nodes, miners, and halving – often used in discussions may seem largely incomprehensible. However, acquiring a foundational understanding of this core multidisciplinary terminology is absolutely essential for understanding Bitcoin. Without a firm grasp of these fundamental concepts, Bitcoin's innovative design and underlying philosophy will remain unfathomable. Additionally, to truly grasp Bitcoin's cultural significance – from an obscure and audacious experiment by a tiny band of brilliant misfits on the internet to a global phenomenon eventually enthusiastically embraced by the most revered icons and institutions in traditional global finance – familiarity with its legendary characters and events, rich lore, and cypherpunk ethos is also needed.

This Glossary systematically explains essential Bitcoin terms and underlying concepts in clear, accessible language, serving as a valuable resource that brings together the disparate, multidisciplinary terms for understanding Bitcoin into one uniquely convenient and accessible location. By engaging with these definitions, you will not only know the specific meaning of these terms and concepts but also understand how they fit together, ultimately making clear why Bitcoin is fundamentally reshaping the global financial system as well as people's understanding of money as a lever of control.

21-Million-Coin Hard Cap (Absolute Scarcity): Bitcoin's finite supply is a core principle hardcoded directly into its fundamental rules. There will never be more than 21 million Bitcoins in existence. This absolute maximum limit is a transparent and unchangeable part of the Bitcoin protocol. New Bitcoins are introduced into circulation gradually, solely as "mining rewards" to "miners" who successfully add new "blocks" to the "blockchain." The rate at which these new Bitcoins are issued is precisely controlled and automatically halves approximately every four years (an event known as "halving") until the entire supply is issued around the year 2140.

This perfectly predictable and hard capped supply creates digital scarcity, similar to precious metals like gold but with even greater mathematical certainty. Unlike traditional fiat currencies, where central banks can print theoretically unlimited amounts of new money (often described as printing "to infinity," which can lead to inflation and a decrease in

purchasing power), Bitcoin's supply cannot be arbitrarily inflated. This mathematical certainty prevents sudden devaluations and firmly establishes Bitcoin as a store of value – an asset expected to hold or increase its value over time – serving as a hedge against inflationary monetary policies and a reliable way for individuals to preserve their wealth.

51% Attack: A 51% attack refers to a theoretical vulnerability in the Bitcoin network (and other cryptocurrencies that use a similar Proof-of-Work system). It describes a scenario where a single entity, or a coordinated group, manages to gain control of more than half of the network's total mining power. If this were to happen, this powerful entity could potentially manipulate how transactions are recorded on the "blockchain."

While theoretically possible, a 51% attack on the Bitcoin network is exceptionally difficult and prohibitively expensive to execute in practice. Bitcoin's network is vast and decentralized, with immense computational power ("hash rate") spread across thousands of "miners" globally. The financial resources required to acquire and maintain enough specialized mining hardware ("ASICs") and the electricity to power it, to consistently outpace the rest of the network, would be astronomically high – costing billions of dollars for even a short period. Moreover, successfully manipulating the network would likely cause a massive loss of trust in Bitcoin, crashing its value and making the attack economically irrational for the attacker because their own enormous investment would become worthless.

Antifragile: Antifragile describes systems that do not just resist shocks (resilient) or recover from them (robust) but actually get stronger and improve when exposed to volatility, randomness, chaos, and stressors. This is a perfect characterization of Bitcoin, especially in its early, precarious days when its continued existence was genuinely in doubt. When Bitcoin was first launched, it faced immense uncertainty: the pseudonymous creator Satoshi Nakamoto disappeared; it had no recognized economic value and was dismissed as a niche digital toy; and it suffered numerous attacks, hacks (most notably Mt. Gox), and government attempts at censorship and shutdown. Any one of these extinction-level events could have easily killed a fragile or even merely resilient system. However, each challenge Bitcoin faced – whether it was a bug that required a "fork," a major exchange hack that prompted users to prioritize self-custody,

or government attempts to regulate or ban it outright – led to greater decentralization, stronger security practices, improved code, and increased awareness and adoption. Bitcoin absorbed these potentially fatal blows, learned from them, and emerged more robust, accepted, and fundamentally stronger, proving that it is virtually indestructible and indeed antifragile.

Austrian Economics: Austrian economics is a school of thought that emphasizes individual choice, sound money, and distrust of central planning – principles that Bitcoin embodies perfectly. Austrian economists like Ludwig von Mises and Friedrich Hayek argued that money should be scarce, durable, and uncontrolled by governments to prevent inflation and economic chaos. Bitcoin mirrors this by being hard capped at 21 million Bitcoins, decentralized, and resistant to manipulation, which is a direct rejection of central banks' unlimited money-printing policies.

Bitcoin is Austrian economics in digital form – a money supply no politician can dilute, a system where users (not rulers) decide value, and a check against the boom-bust cycles caused by fiat currency experiments. It is why Bitcoiners often quote Hayek's famous

line: "I don't believe we shall ever have a good money again before we take the thing out of the hands of government, that is, we can't take them violently out of the hands of government, all we can do is by some sly roundabout way introduce something that they can't stop."

Bitcoin Core: Bitcoin Core is the original, open-source software client for the Bitcoin network, serving as its reference implementation. It enables users to run a "full node," which downloads and independently validates the entire history of Bitcoin transactions (the "blockchain") according to the network's "consensus rules."

Bitcoin Core Developers: Bitcoin Core developers are a decentralized group of volunteers and funded contributors who maintain and improve the open-source Bitcoin Core software, which is the reference implementation of the Bitcoin protocol. They are responsible for writing, reviewing, and testing code that ensures the security, stability, and functionality of the Bitcoin network, playing a crucial role in its ongoing evolution. Gavin Andresen, Hal Finney, Wladimir J. van der Laan, and Pieter Wuille were some of the legendary developers during the early and most chaotic days of Bitcoin.

Bitcoin Improvement Proposal ("BIP"): A BIP is a formal design document that describes a proposed change, feature, or new standard for the Bitcoin protocol or its ecosystem. Anyone can submit a BIP, but it must undergo a rigorous review and discussion process by the community. BIPs are crucial for Bitcoin's open-source development and its decentralized governance model. They provide a standardized way to propose, discuss, and document technical specifications, ensuring that significant changes to Bitcoin are transparently debated and reach a broad consensus among developers, "miners," and users before potential implementation.

Bitcoin Pizza Day (May 22, 2010): Bitcoin Pizza Day commemorates the first real-world transaction using Bitcoin, when programmer Laszlo Hanyecz paid 10,000 BTC for two pizzas. This is a seminal event in Bitcoin's adoption as a medium of exchange. It highlights Bitcoin's evolution from a conceptual digital asset to one with practical economic value. It is celebrated annually to reflect on Bitcoin's growth and the hindsight irony of those Bitcoins being worth well over \$1.2 billion at Bitcoin's all-time-high of nearly \$123,000 on July 14, 2025.

Special Offer for First Time Prison Legal News Subscribers

A 6-Month Subscription for \$5.00 (That's 75% off the cover!)

Are you reading someone else's PLN? You don't want to risk missing a single issue. For over 30 years, PLN has been bringing prisoners the information they need to stay informed.

This offer is only available to customers that have not previously subscribed to PLN. All sales are final. Orders placed for non-eligible prisoners will have a 2-month pro-rated period added to their PLN account. Your first issue will be mailed in 6-10 weeks via USPS. Renewal notices will be sent no later than 30 days prior to expiration at the current renewal rate (as of 1/1/2022 PLN's annual renewal rate is \$36.00, plus sales tax where applicable).

Act now as this offer is only valid through 12/31/2024

Name _____ Amount enclosed: \$ _____

DOC/BOP Number: _____ Facility: _____

Address: _____

City: _____ State: _____ Zip _____

**Human Rights Defense Center, PO Box 1151, Lake Worth Beach, FL 33460
561-360-2523 • WWW.PRISONLEGALNEWS.ORG • WWW.CRIMINALLEGALNEWS.ORG**



What Is Bitcoin? (cont.)

Bitcoin Whitepaper: The Bitcoin whitepaper, titled “Bitcoin: A Peer-to-Peer Electronic Cash System,” is the foundational document published by Satoshi Nakamoto on October 31, 2008, outlining the technical blueprint for a decentralized digital currency. It describes how Bitcoin solves the “double-spending problem” using a distributed ledger and Proof-of-Work consensus. This historic document laid the groundwork for the entire cryptocurrency ecosystem and remains essential reading for understanding Bitcoin’s core principles.

Block: A block is a data structure in the Bitcoin “blockchain” that contains a batch of verified information. Imagine a Bitcoin block as a digital page in a massive, public ledger. This page is where a batch of recently confirmed transactions (like payments or transfers) is permanently recorded. Each block also includes its own unique identifying code, a timestamp showing when it was created, and a special numerical proof generated by “miners.” Importantly, every new block contains a digital link to the one before it, forming a continuous and unbroken chain of pages – the blockchain. These blocks are competitively created by powerful computers (miners) approximately every 10 minutes, and once a transaction is included in a block, it becomes an unalterable record, ensuring the history of all Bitcoin activity is permanently secure and immutable.

Block Header: The block header is a tiny, fixed-size section of a Bitcoin “block” (just 80 bytes – smaller than a tweet!) that includes key metadata, or essential identifying information, about that block. Think of it like a block’s ID card or unique digital fingerprint. It contains details such as the version number; the “previous block hash” (a unique code that links it directly to the block that came before it, forming the “chain”); the “Merkle root” of transactions (a single, compressed summary of all the transactions inside that block); the timestamp (when the block was created); difficulty bits (a number indicating how hard it was to find this block); and the “nonce” (a random number that “miners” change over and over again to solve a puzzle). This compact header is the crucial input for the Proof-of-Work “hashing” process (the intense computational puzzle “miners” solve). When a miner finds a valid header, it proves they did the work. This structure also enables

efficient verification of the block’s integrity by anyone on the network. Because every single piece of information in the header is critical, even a tiny change to any element in it would completely invalidate the block, making it instantly recognizable as tampered with and ensuring the chain’s security.

Blockchain: The blockchain is Bitcoin’s public, distributed ledger. Imagine the blockchain as a gigantic, shared, and continuously growing digital ledger, like a never-ending financial history book that is stored on thousands of computers worldwide. Each “page” of this book is a “block,” which contains a confirmed batch of transactions. These pages are added one after another in perfect chronological order, forever. What makes it revolutionary is that it is “distributed”: instead of one bank or company keeping the master copy, everyone running Bitcoin software (called a “node”) has their own identical copy of the entire ledger. This means it operates entirely without a central authority; no single person, company, government, or even its creator controls it. Its entries are secured by powerful cryptography, making them virtually impossible to alter once recorded, and by “consensus mechanisms” (rules that all participants agree to follow, ensuring everyone’s copy of the ledger matches). This open, redundant, and self-enforcing system ensures complete transparency and unmatched security for all Bitcoin activity.

Block Reward: The block reward is like a prize or a bounty of brand-new Bitcoins that is given to the “miner” that successfully solves the complex computational puzzle and adds a new “block” of transactions to the “blockchain.” This reward is absolutely essential because it incentivizes miners to continue securing the network and is the primary way Bitcoin’s fixed supply is released into circulation. This reward is automatically cut in half approximately every four years (an event called “halving”), making Bitcoin increasingly scarce over time. This process will continue until around the year 2140, when the final Bitcoin will have been mined, and the total supply reaches its programmed hard cap of 21 million. After that, miners will be compensated solely by the transaction fees included in the blocks they verify, ensuring the network remains secure indefinitely.

Broadcasting: Broadcasting a transaction refers to the act of sending a signed transaction from your “wallet” to the decentralized network of Bitcoin “nodes.” Once your wallet

creates and digitally signs a transaction, it does not send it to a central server; instead, it “broadcasts” it to a few connected nodes, which then relay it to other nodes across the globe, effectively making the transaction known to the entire network so it can be verified and eventually included in a “block” by “miners.”

Byzantine Generals’ Problem: The Byzantine Generals’ Problem is a classic thought experiment illustrating the immense difficulty of achieving consensus among a group of independent actors when some of them might be unreliable, deceptive, or outright malicious, and communication channels themselves are untrustworthy.

To illustrate, imagine a group of generals, each leading a division, planning an attack on an enemy city. They must all agree on whether to attack or retreat, and vitally, they must attack simultaneously to succeed. A disorganized, partial attack would lead to catastrophic failure. However, they can only communicate via messengers, some of whom might be captured, deliver false messages, or simply fail to arrive. Adding to the dilemma, some of the generals themselves might be traitors who deliberately send conflicting information to sow confusion and prevent a coordinated decision. The problem is to find a strategy that guarantees all loyal generals will reach the same, correct decision despite these challenges, ensuring a unified outcome.

Bitcoin solves the Byzantine Generals’ Problem by replacing the need for perfect, trustworthy communication and perfectly loyal participants with Proof-of-Work and economic incentives. Instead of generals needing to trust messengers or each other’s loyalty, Bitcoin “miners” (the “generals”) expend significant computational resources to solve a cryptographic puzzle. The first to solve it broadcasts their solution and a new “block” of transactions.

This Proof-of-Work serves as an objective, verifiable “message” that is incredibly expensive to produce but cheap to verify. Other miners then build upon the longest valid chain because this is the most economically rational strategy (it is where the next “block reward” is most likely to be found). Any traitorous miner attempting to propose an invalid block or double-spend would waste their immense computational effort and lose potential rewards since honest participants would simply ignore their invalid work. Thus, Bitcoin aligns the self-interest of all rational miners with the

integrity and security of the shared ledger, effectively achieving consensus and coordinated action in a trustless environment.

This concept is central to understanding how Bitcoin maintains integrity without a trusted central party. Bitcoin was the first practical and widely successful implementation to solve the Byzantine Generals' Problem for a decentralized digital currency in a trustless environment. It bypassed the need for perfect, synchronous communication and explicit trust among all participants by introducing a probabilistic, economically incentivized "consensus mechanism" – Bitcoin's Proof-of-Work.

Cantillon Effect: The Cantillon Effect describes how the uneven expansion of the money supply in an economy leads to a redistribution of wealth. When new money is introduced into a centralized financial system (like through central bank quantitative easing or government spending), those who receive this new money first (typically large banks, financial institutions, and government contractors) benefit disproportionately. They can spend or invest this new money on goods, services, and assets at their original, lower prices before the increased money supply causes widespread inflation. By the time this new money trickles down to the broader population (wage earners and small businesses), prices for goods and services have already risen, effectively eroding their purchasing power. This creates a hidden, regressive tax on those furthest from the money creation process, exacerbating wealth inequality.

In sharp contrast, the Nakamoto Effect refers to the equitable distribution of newly created Bitcoins through the decentralized "mining" process. In Bitcoin's network, new Bitcoins are awarded to "miners" that solve complex mathematical problems to validate transactions and secure the "blockchain." This process is open to anyone with the necessary computational resources, ensuring that no centralized authority or privileged group exclusively benefits from new money issuance. Thus, the Nakamoto Effect can be conceptualized as Bitcoin's "reverse Cantillon Effect." Instead of centralizing the benefits of money creation at the top of a financial hierarchy, Bitcoin's design decentralizes the issuance process, distributing newly minted Bitcoins through a competitive, open, and transparent mechanism. This fundamental difference is a core reason why Bitcoiners view Bitcoin as a more equitable monetary system, one that counters the inflationary advantages

that early recipients of fiat money enjoy due to the Cantillon Effect.

Consensus Mechanisms: In a decentralized network like Bitcoin, where there is no central authority to validate transactions or maintain the ledger, "consensus mechanisms" are the set of rules and protocols that allow all independent participants ("nodes" and "miners") to collectively agree on the single, correct state of the "blockchain." Think of it like a large group of people needing to agree on the exact wording of a historical record, but without a leader or a shared meeting room. Everyone has their own copy, and these mechanisms provide the agreed-upon method for everyone to verify and update their copy so that they all match perfectly. They ensure that everyone has the same, verified copy of the transaction history and prevent fraudulent activities like the "double-spending problem." Bitcoin's specific consensus mechanism is called "Proof-of-Work."

Coinbase Transaction: The coinbase transaction is the first transaction in every Bitcoin "block," created by the "miner" to claim the "block reward" and any transaction fees. It includes a unique field for arbitrary data, often used for messages like the Genesis Block's headline reference. This transaction has no inputs and generates new Bitcoins, serving as the origin point for all Bitcoins in circulation. This is not to be confused with the company called "Coinbase," which is named after this type of transaction.

Custodial vs. Non-Custodial (Self-Custody): Custodial means a third party (like an exchange) holds your private keys and thus controls your Bitcoin on your behalf, similar to a bank holding your fiat currency. Non-custodial (or self-custody) means you hold and control your own private keys, giving you direct and exclusive control over your Bitcoin without needing to trust any intermediary. The Bitcoin philosophy strongly advocates for non-custodial ownership. In fact, Bitcoiners have a common saying regarding non-custodial ownership, "not your keys, not your coins," which means if you do not hold the private keys, you do not have true, undisputed ownership of your Bitcoin.

Cypherpunks: Cypherpunks refers to a group of activists, cryptographers, and technologists who emerged in the late 1980s and early 1990s. Their core belief was that strong cryptography – the science of secure communication – could be used to protect individual privacy and freedom in the digital

age from increasing government surveillance and corporate data collection. They famously summarized their philosophy with the motto "Cypherpunks write code," emphasizing that practical tools, not just political advocacy, were necessary to build a world where individuals could communicate and transact privately and securely without the need to trust intermediaries. They pioneered many privacy-enhancing technologies, like anonymous remailers and early forms of digital cash. The Bitcoin whitepaper was first shared publicly on the cypherpunk forum "Cryptography Mailing List" hosted by metzdowd.com.

Bitcoin is deeply rooted in the cypherpunk movement's ideals, where money is treated as speech and censoring it undermines freedom itself. Satoshi Nakamoto, Bitcoin's pseudonymous creator, was heavily influenced by and likely a part of this community, building upon decades of cypherpunk research into digital cash systems. Bitcoin embodies their vision of a decentralized, censorship-resistant form of money that operates without central banks or governments. Bitcoin's cryptographic security, pseudonymous nature, and permissionless transfers directly fulfill the

If You Write to *Criminal Legal News*

We receive numerous letters from prisoners every month. If you contact us, please note that we are unable to respond to the vast majority of letters we receive.

In almost all cases we cannot help find an attorney, intervene in criminal or civil cases, contact prison officials regarding grievances or disciplinary issues, etc. We cannot assist with wrongful convictions, and recommend contacting organizations that specialize in such cases, such as the Innocence Project (though we can help obtain compensation after a wrongful conviction has been reversed based on innocence claims).

Please do not send us documents that you need to have returned. Although we welcome copies of verdicts and settlements, do not send copies of complaints or lawsuits that have not yet resulted in a favorable outcome.

Also, if you contact us, please ensure letters are legible and to the point—we regularly receive 10- to 15-page letters, and do not have the staff time or resources to review lengthy correspondence. If we need more information, we will write back.

While we wish we could respond to everyone who contacts us, we are unable to do so; please do not be disappointed if you do not receive a reply.

What Is Bitcoin? (cont.)

cypherpunks' goal of empowering individuals with financial sovereignty and privacy in an increasingly digital and surveilled world.

Decentralization: Decentralization is a core principle of Bitcoin. It means the network operates entirely without a single controlling authority, central server, or governing body. Instead, power and control are distributed across thousands of independent computers (called "nodes") and "miners" located all over the world. Consequently, no one entity – whether an individual, corporation, or government – can unilaterally change Bitcoin's rules, censor transactions, or shut down the network.

This distributed structure is crucial for Bitcoin's resilience and trustworthiness. Because there is no central point of control, it inherently prevents censorship (no one can stop you from sending a transaction) and eliminates single points of failure (if one part of the network goes offline, countless others keep it running). It also makes the network incredibly resistant to manipulation because any attempts to cheat or change the rules would be rejected by the vast majority of par-

ticipants. Instead, Bitcoin relies on "consensus rules" – agreed-upon protocols enforced by all network participants – to maintain its integrity and secure its operation.

Difficulty Adjustment: Difficulty adjustment is Bitcoin's automatic system that fine-tunes the computational challenge for "mining" approximately every 2,016 "blocks" (which takes about two weeks). Its primary goal is to maintain an average 10-minute time for new blocks to be found, no matter how much computing power is active on the network. Think of it like a self-adjusting treadmill: if more runners ("miners") join and are suddenly running faster (more "hash power" or total computing power dedicated to mining), the treadmill automatically speeds up to keep the pace consistent. Conversely, if some runners leave or slow down (less hash power), the treadmill slows down to compensate. This mechanism ensures network stability, keeps Bitcoin's supply issuance perfectly predictable, and renders the network extremely resistant to attacks by continuously adjusting to keep mining competitive and costly.

Double-Spending Problem: The double-spending problem is the challenge of preventing the same digital asset from being spent more

than once, a key issue in electronic cash systems without a central authority. Bitcoin solves this through its "blockchain" and Proof-of-Work mechanism, where transactions are timestamped and confirmed by the network, making reversals or duplicates computationally infeasible. This innovation enables trustless, peer-to-peer transactions and is fundamental to Bitcoin's viability as money.

Fiat Currency (or Fiat Money): Fiat currency is the type of money used by most countries today, such as the U.S. dollar, euro, or Japanese yen. Unlike historical forms of money (like gold or silver coins), fiat money is not backed by any physical commodity. Instead, its value is derived from government decree (it is "legal tender") and the public's trust in that government and its central bank. Central banks have the authority to create ("print") theoretically unlimited amounts of new fiat currency, which they often do to manage the economy, stimulate growth, or fund government spending. While convenient for daily transactions, this ability to arbitrarily increase the money supply can lead to inflation and a gradual loss of purchasing power over time.

Fork (Hard Fork / Soft Fork): A fork in Bitcoin occurs when the "blockchain" diverges due

Special Offer for 1st Time Criminal Legal News Subscribers

A 6-Month Subscription for \$7.00 (That's 75% off the cover!)

Are you reading someone else's CLN? You don't want to risk missing a single issue.

For over 30 years, we have been bringing prisoners the information they need to stay informed.

This offer is only available to customers that have not previously subscribed to CLN. All sales are final. Orders placed for non-eligible prisoners will have a 2-month pro-rated period added to their CLN account. Your first issue will be mailed in 6-10 weeks via USPS. Renewal notices will be sent no later than 30 days prior to expiration at the current renewal rate (as of 1/1/2022 CLN's annual renewal rate is \$48.00, plus sales tax where applicable).

Act now as this offer is only valid through 12/31/2024



Name _____ Amount enclosed: \$ _____

DOC/BOP Number: _____ Facility: _____

Address: _____

City: _____ State: _____ Zip _____

**Human Rights Defense Center, PO Box 1151, Lake Worth Beach, FL 33460
561-360-2523 • WWW.PRISONLEGALNEWS.ORG • WWW.CRIMINALLEGALNEWS.ORG**

to changes in protocol rules. A hard fork creates an incompatible split requiring all “nodes” to upgrade (e.g., Bitcoin Cash from Bitcoin), while a soft fork is backward-compatible, allowing non-upgraded “nodes” to continue. Forks can resolve disputes or introduce improvements but risk community division. They highlight Bitcoin’s governance through consensus rather than central decree.

Game Theory: Bitcoin’s resilience and security are deeply rooted in game theory, the study of strategic interactions where participants (players) make decisions based on incentives and anticipated actions of others. Bitcoin’s design masterfully aligns the interests of all network participants – “miners,” “nodes,” developers, and users – through carefully crafted economic and cryptographic rules. Bitcoin’s game theory ensures that rational actors are rewarded for cooperation, while malicious or incompetent actors are punished by economic losses. This creates a self-sustaining system where (1) miners secure the network for profit, (2) users enforce rules by rejecting invalid transactions, and (3) holders preserve value by refusing to dilute supply.

Genesis Block (Block 0): The Genesis Block is the first “block” in the Bitcoin “blockchain,” mined by Satoshi Nakamoto on January 3, 2009, containing a message referencing a financial crisis headline to underscore Bitcoin’s purpose. It includes the initial “coinbase transaction” rewarding 50 BTC and serves as the unalterable foundation of the chain. This block symbolizes Bitcoin’s birth and its goal to create a system free from traditional banking failures.

Hal Finney: Hal Finney was a renowned computer scientist and cryptographer, recognized as one of the earliest and most crucial collaborators with Bitcoin’s creator, Satoshi Nakamoto. He made history by being the first person to receive a Bitcoin transaction directly from Satoshi himself, receiving 10 BTC on January 12, 2009. Finney actively engaged in early discussions, provided valuable feedback, and reported bugs in the nascent Bitcoin software, cementing his legacy as a true pioneer in the world of digital currency and a legendary figure within the Bitcoin community.

Halving: The halving is a programmed event every 210,000 “blocks” (about four years) that reduces the “mining block reward” by half, reducing Bitcoin’s supply issuance and enforcing scarcity. Past halvings (2012, 2016, 2020, 2024) have often correlated with

price increases due to reduced new supply. It transitions Bitcoin toward a fee-based model for “miners” and reinforces its deflationary economics.

Hash / Hashing (SHA-256): Hashing in Bitcoin uses the SHA-256 algorithm to convert data into a fixed 256-bit string (hash), which is unique and irreversible, serving as a digital fingerprint for security. No matter the input, this process always produces a fixed-length code, and even a tiny change to the original data creates a completely different fingerprint. This process is irreversible and foundational to Bitcoin’s security.

“Miners” use hashing to solve complex computational puzzles, repeatedly guessing until they find a hash that meets a specific target for a new “block” – this is their Proof-of-Work. Hashes also securely link blocks together in the “blockchain.” Because these digital fingerprints are unique and instantly change if data is tampered with, hashing ensures that all Bitcoin records are tamper-proof, resulting in undeniable integrity across the network.

Hash Rate: Hash rate is a measure of the total computational power per second that all the computers (“miners”) in the Bitcoin network are contributing to solve the complex mathematical puzzles required to verify transactions and add new “blocks” to the “blockchain.” A higher hash rate signifies a more robust and secure network because it becomes exponentially more difficult and expensive for any single entity to gain enough control to compromise the system.

Hyperinflation: Hyperinflation is an extremely rapid and out-of-control increase in the general price level of goods and services, often defined as a monthly inflation rate exceeding 50%. This phenomenon severely erodes the purchasing power of a currency, effectively making savings worthless overnight and leading to widespread economic instability and social unrest. It typically occurs when governments excessively print money to cover deficits without corresponding economic growth, leading to a loss of public trust in the currency. Bitcoin is the antidote to hyperinflation due to its precisely limited supply of 21 million Bitcoins, which cannot be arbitrarily increased by any central authority. Unlike fiat currencies, Bitcoin’s scarcity is mathematically enforced and predictable, positioning it as the “hard money” alternative that maintains its value even when national currencies collapse.

Immutability: Immutability refers to the inability to change or delete records once they have been added to the Bitcoin “blockchain.” Once a transaction is confirmed and included in a “block,” and subsequent blocks are added on top, it becomes virtually impossible to alter, reverse, or remove that record. This characteristic ensures the integrity and trustworthiness of Bitcoin’s historical ledger.

Inflation / Deflation: Inflation refers to a general and sustained increase in the prices of goods and services over time, which simultaneously causes a decrease in the purchasing power of money. For example, if a loaf of bread costs more next year than it does today, that is inflation – your money simply buys less. It is often caused by an increase in the money supply relative to the goods and services available. That is, when the government “prints” more of its fiat currency, there is no automatic corresponding increase in the goods and services available, so more money is now “chasing” the same amount of goods and services within the economy. Conversely, deflation is a general decrease in prices, meaning money’s purchasing power increases over time. While this might sound good, severe or prolonged deflation can lead to economic slowdowns as people delay spending, expecting prices to fall further.

Lightning Network: The Lightning Network is a layer-2 scaling solution built on Bitcoin for fast, low-cost micropayments via off-chain payment channels that settle on the main “blockchain” only when closed. It enables instant transactions with minimal fees, addressing Bitcoin’s on-chain limitations for everyday use. As an open protocol, it enhances Bitcoin’s usability without altering its core layer.

Imagine Bitcoin’s main blockchain as a busy highway that can get a bit congested and slow down for smaller, frequent payments. The Lightning Network is like building express lanes or private tunnels on top of that highway. It is a layer-2 scaling solution because it sits on top of the main Bitcoin network, not changing the highway itself but making it more efficient.

Here is how those tunnels work. You and another person can open an off-chain payment channel by putting some Bitcoin into it on the main blockchain. Once that channel is open, you can send instant, almost-free payments back and forth, as many times as you like, all inside that private tunnel, without touching the busy main highway. Only when you both decide to close the channel is the final net balance of all those payments recorded as a single transaction back on the main blockchain. This

What Is Bitcoin? (cont.)

means thousands of payments can happen instantly off-chain, but the main blockchain only records the final result, keeping it efficient and secure. This allows for millions of tiny, lightning-fast transactions, making Bitcoin practical for everyday use like buying a coffee, while still benefiting from the robust security of the core Bitcoin network.

Mempool (Memory Pool): The mempool is a temporary holding area on each “node” where unconfirmed transactions await inclusion in a “block” by “miners.” Transactions with higher fees are prioritized for faster confirmation during congestion. It reflects network activity and can influence fees, providing insight into pending demand.

Merkle Tree: Imagine a long list of transactions in a Bitcoin “block,” like entries on a giant spreadsheet. A Merkle Tree is an ingenious way Bitcoin organizes and summarizes all these transactions into a single, unique digital fingerprint called a “Merkle root.” It does this by repeatedly pairing and combining the unique digital codes (“hashes”) of individual transactions until only one code remains at the very top. This “fingerprint” is included in the block’s header, acting like a tamper-proof seal for all the transactions below it. This allows even a “light client” (like a simple wallet app on your phone) to quickly and securely verify that a specific transaction was indeed included in a block without having to download and check every single transaction ever made. It is like checking the table of contents to see if an article is in a book, rather than reading the entire book, which makes Bitcoin much more efficient and scalable.

Mining / Miners: Bitcoin mining is the competitive process by which new transactions

are verified, bundled into “blocks,” and added to the immutable public ledger known as the “blockchain.” This energy-intensive activity is performed by “miners,” which are specialized computers (called “ASICs” or Application-Specific Integrated Circuits) connected to the Bitcoin network. Miners repeatedly solve complex cryptographic puzzles (the Proof-of-Work) by guessing a “nonce” until they find a valid solution.

When a miner successfully finds the solution to the Proof-of-Work puzzle, it gets the exclusive right to add the next block of verified transactions to the blockchain. This act confirms recent transactions and secures the entire network’s history. As a reward for its significant computational effort and electricity consumption, the successful miner receives a “block reward” (newly issued Bitcoins) and any “transaction fees” attached to the transactions within that block.

Miners operate globally and compete fiercely, so with their combined computational power (“hash rate”), it is astronomically difficult and expensive for any single entity to gain enough control to manipulate the blockchain (a 51% attack). This distributed competition is fundamental to Bitcoin’s decentralization because it ensures that no single point of control can dictate the network’s rules or history. By enforcing Bitcoin’s protocol rules and predictable issuance schedule through their work, miners are the principal guardians of the network’s integrity and value.

Mining Node: A mining node is essentially a “full node” that also runs specialized mining software and hardware (“ASICs”) to participate in the Proof-of-Work competition to create new “blocks.” All mining nodes must be full nodes (or at least connect to one) so they can validate transactions and the current state of the “blockchain” before attempting to

build a new block. So, while “miner” refers to the hardware and the activity, a mining node is the full node component that facilitates this process.

Nakamoto Consensus: A specific type of “consensus mechanism” used by Bitcoin, named after its creator Satoshi Nakamoto. It is a set of rules that

combine Proof-of-Work and the longest chain rule to allow a decentralized network to agree on a single, shared history of transactions without a central authority. In this system, “miners” compete to solve a cryptographic puzzle, and the winning miner gets to add the next “block” of transactions to the “blockchain.” The network then collectively agrees to always build upon the longest chain of blocks, which is presumed to be the one with the most Proof-of-Work invested in it. This incentivizes honest participation and makes it computationally infeasible for a malicious actor to alter the blockchain’s history.

Nash Equilibrium: The Nash Equilibrium is a core concept in game theory and helps explain why the Bitcoin network is so stable and secure. It describes a stable state in a strategic interaction where no participant can improve their outcome by unilaterally changing their strategy, assuming all other participants maintain theirs. That is, it is a situation where everyone is doing the best they can, given what everyone else is doing, so no single player has an incentive to deviate. Bitcoin’s foundational design brilliantly leverages this principle by structuring incentives so that every participant, from powerful “miners” validating transactions to individual users, finds it in their self-interest to faithfully adhere to the network’s rules. For instance, miners are rewarded with new Bitcoin and transaction fees for honest work. Trying to cheat (like double-spending) would result in their work being rejected by the vast network of verifying “nodes,” leading to wasted effort and no reward.

For example, attempting a 51% attack would involve colossal energy and hardware costs, while the reward (“block reward” plus fees) is greater for honest mining. The punishment for miners trying to reverse transactions is that the network rejects their invalid “blocks,” wasting enormous amounts of resources. The result is that it is economically suicidal to attack Bitcoin – honesty pays better.

This ingenious alignment of individual self-interest with collective network security is why Bitcoin functions without a central authority. The system is precisely engineered such that cheating is economically irrational and self-defeating for any single actor, assuming the vast majority play by the rules. The stability and integrity of the Bitcoin network, therefore, arise not from trust in an institution but from a powerful Nash Equilibrium where the optimal strategy for all participants is to

John F. Mizner, Esq.

311 West Sixth Street
Erie, Pennsylvania 16507
(814) 454-3889
jfm@miznerfirm.com



Representing Pennsylvania Inmates

Medical mistakes
Inadequate care
Delay in treatment

act honestly. This fundamental game-theoretic equilibrium ensures Bitcoin's extraordinarily robust security and reliability, making it an unprecedented example of decentralized coordination.

Node (Full Node): A full node is essentially your own personal, independent copy of the entire Bitcoin "blockchain" and its rulebook, running on your computer. Instead of trusting someone else (like a bank or an exchange) to tell you whether a Bitcoin transaction is valid or if your balance is correct, your full node personally checks every single transaction and "block" against all of Bitcoin's rules from the very beginning. It constantly talks to other full nodes around the world, relaying valid information and rejecting anything that does not follow the rules. By running your own node, you become a fully independent participant in the Bitcoin network, acting as your own bank and auditor. This is key to Bitcoin's trustless nature because it means you do not have to rely on anyone else's verification; you can see and confirm the truth of the blockchain for yourself. This collective effort of many independent nodes is what truly secures and decentralizes Bitcoin.

Nonce: The nonce is a 32-bit arbitrary number in the "block header" that "miners" adjust during "hashing" to find a "hash" below the difficulty target. Think of the nonce as a special, changeable number that Bitcoin miners interact with to solve a very difficult digital puzzle. When a miner tries to create a new "block" of transactions, it combines all the block's information with this nonce and then runs it through a cryptographic process (hashing). The goal is to find a nonce that makes the final result (the hash) look a very specific way – like starting with a certain number of zeros. Miners do not know which number will work, so they just keep guessing different nonces through pure trial-and-error until they hit the right combination, which enables the Proof-of-Work process. Finding a valid nonce secures the block and chain.

Orange Pilled: Orange pill refers to someone who has undergone a profound shift in their understanding and belief system regarding money, economics, and traditional financial systems, resulting in a strong conviction in Bitcoin's superiority and importance with respect to its role in redefining economic systems and empowering individuals. It often leads to a desire to educate others about Bitcoin so that they too are orange pill.

Overton Window: The Overton Window describes the range of ideas that are considered politically and socially acceptable to the mainstream population at a given time. Ideas outside this "window" are deemed radical or unthinkable. Bitcoin was initially dismissed as a niche and even illicit digital currency but has steadily shifted the Overton Window. What was once considered a fringe concept for tech enthusiasts or criminals is now increasingly discussed by financial institutions, governments, and everyday investors. This shift is evidenced by the approval of spot Bitcoin Exchange-Traded Funds ("ETFs"), the establishment of the U.S. Strategic Bitcoin Reserve, the increasing institutional adoption by companies for their corporate treasury, and the growing political and everyday discourse around digital assets, moving Bitcoin from the "unthinkable" or "radical" categories towards "acceptable," "sensible," and even "popular" within the broader financial and political landscape.

Peer-to-Peer ("P2P") Network: Bitcoin's peer-to-peer network connects "nodes" directly without intermediaries, enabling decentralized propagation of transactions and "blocks." It relies on gossip protocols for data dissemination and resists censorship through redundancy. That is, each computer (node) in the Bitcoin network periodically and randomly shares any new information it has (like new transactions or blocks) with a few other computers it knows. Those computers then do the same, passing the information along to others they know. Because information is being shared and replicated by so many different, independent computers in a random, decentralized way, it becomes virtually impossible for any single entity to block or censor information. If one computer tries to stop a transaction from spreading, many others will simply bypass it and continue relaying the information. This creates multiple redundant paths for the data to travel, making the network highly resilient. This design fulfills the Bitcoin whitepaper's vision of electronic cash without trusted third parties.

Prisoner's Dilemma: The Prisoner's Dilemma is a fundamental concept in non-cooperative game theory that illustrates a paradox in decision-making: when two rational individuals act purely in their own self-interest, they can end up with a worse collective outcome than if they had cooperated. To visualize this, imagine two friends, Sam and Craig, arrested for a minor crime and held in separate cells

by the police. They are each offered the same deal: (1) If one confesses and the other stays silent, the confessor goes free while the silent friend gets three years, (2) If one stays silent and the other confesses, the silent one gets three years and the confessor goes free, (3) If both confess, they each receive two years, and finally, (4) If both remain silent, they both get only one year for the minor offense.

Since Sam and Craig cannot communicate, each faces a dilemma based solely on their individual rationality. Sam might reason, "If Craig stays silent, I should confess to go free, which is better than one year. If Craig confesses, I should still confess to get two years, which is better than three years." Craig would arrive at the same conclusion. No matter what the other does, confessing appears to be the best individual strategy. The paradox arises because if both follow this perfectly rational self-interest and confess, they each end up with two years, a worse outcome than the single year they would have received if they had both chosen to cooperate and stay silent. This classic scenario vividly highlights the inherent conflict between individual rationality and collective well-being.

Bitcoin effectively solves or, more accurately, avoids the Prisoner's Dilemma by ingeniously redesigning the "game" itself, aligning individual self-interest with the collective good. Unlike the classic dilemma where a rational choice to betray leads to a suboptimal outcome for both parties, Bitcoin's Proof-of-Work mechanism, coupled with its reward structure, ensures that honest, cooperative participation is the dominant and most profitable strategy for all rational "miners." The economic cost of attempting to defraud the network (e.g., by double-spending or creating invalid "blocks") far outweighs any potential, fleeting gains because such actions would devalue the attacker's own Bitcoin holdings and mining investments. This economic disincentive, combined with transparent rules enforced by code, transforms a potential "betrayal" scenario into one where cooperation is the most beneficial path, resulting in network security without the need for traditional trust.

Bitcoin's avoidance of the Prisoner's Dilemma is further reinforced by the concept of a Schelling Point. A Schelling Point, or focal point, is a solution that people instinctively choose in the absence of communication but still needing to coordinate – like two strangers agreeing to meet at the only clock at a train station – because it seems natural, obvious, or special. With Bitcoin, the fixed

What Is Bitcoin? (cont.)

supply of 21 million Bitcoins acts as a powerful Schelling Point for its value. Despite there being no central authority dictating its worth, the universally known and verifiable scarcity of Bitcoin makes it a natural focal point for people to converge on as a store of value. Bitcoin's 21-million-coin hard cap is the ultimate Schelling Point – no one enforces it, yet everyone defends it because it is obvious, defying it is costly, and it is self-reinforcing.

Bitcoin's design turns selfish behavior into network security. Miners, users, and holders all profit most by playing fair because the system punishes cheaters and rewards cooperation. This ensures Bitcoin remains decentralized and trustless.

Private Key / Public Key / Bitcoin Address (Public Mailbox): At the heart of owning and using Bitcoin are three interconnected cryptographic elements: (1) a private key, (2) a public key, and (3) a Bitcoin address. They form a unique pair (or set) that allows you to securely control and participate in the Bitcoin network.

Your private key is a super-secret, unique alphanumeric code. It is the ultimate proof

of your ownership of Bitcoin. When you want to send Bitcoins, your "wallet" uses this private key to create a "digital signature" for the transaction. This "signature" proves that you, and only you, authorize the spending of those specific Bitcoins, without ever revealing the private key itself to the network. It is vital to keep your private key absolutely secret and secure. Losing it means permanent, irreversible loss of access to your associated Bitcoins.


Mathematically derived from your private key through a one-way cryptographic function, your public key is designed to be public. It is used by the Bitcoin network to verify the digital signature created by your private key, confirming that a transaction is legitimate and was authorized by the true owner of the funds. Importantly, because the function is one-way, it is virtually impossible to reverse-engineer your private key from your public key, ensuring your funds remain safe even though your public key is known.

A Bitcoin address is a shortened, user-friendly version of your public key (created by hashing the public key), e.g., 1A1zP1eW5QjhbPourZq2K8w2sXyQy42. This is the "address" you share with others when you want to receive Bitcoin. Think of it like a "public mailbox" or a bank account number that you

can give out freely. People can send funds to this address, but only the person holding the corresponding private key can "open the mailbox" and spend those funds.

This entire system operates on principles of asymmetric cryptography (also known as public-key cryptography). It is an extremely tamper-proof method that uses a pair of keys – one public, one private – for secure communication and authentication. In Bitcoin, it ensures that transactions are both secure (only the owner can spend) and verifiable (anyone can confirm they were sent by the legitimate owner), all while allowing for pseudonymous transfers where your real-world identity is not directly linked to your addresses unless you choose to reveal it.

Proof-of-Work ("PoW"): Proof-of-Work is Bitcoin's ingenious "consensus mechanism," which is the fundamental process that allows all the independent computers on the network to collectively agree on the single, accurate version of its transaction history without needing a central authority. It works by requiring Bitcoin "miners" to expend significant computational effort and real-world energy to solve an extremely difficult cryptographic puzzle. Imagine it as a massive, global digital



PRISONLEGALNEWS.org

Dedicated to Protecting Human Rights

>>FREE Data Search |

| Decisions | Investigations | Audits | Publications | Cases | Verdicts | Settlements |
|-----------|----------------|--------|--------------|-------|----------|-------------|
|-----------|----------------|--------|--------------|-------|----------|-------------|

If you need to know about prisons and jails or are litigating a detention facility case, you can't afford not to subscribe to our website!

Online subscribers get unlimited, 24-hour a day access to the website and its content!

Sign up for PLN's FREE listserv to receive prison and jail news and court rulings by e-mail.

- ▶ PLN's website offers all issues of PLN in both searchable database and PDF formats. Issues are indexed and posted as soon as they go to press.
- ▶ Publications section has numerous downloadable government reports, audits and investigations from around the country.
- ▶ Full text decisions of thousands of court cases, published and unpublished.
- ▶ All content is easy to print for downloading and mailing to prisoners.
- ▶ Most complete collection of prison and jail related verdicts and settlements anywhere.
- ▶ Order books, print subscriptions and make donations on line.

- ▶ Brief bank with a wide assortment of winning motions, briefs, complaints and settlements.
- ▶ Links to thousands of prison, jail, criminal justice and legal websites around the world.
- ▶ Thousands of articles and cases, all fully indexed by more than 500 subjects, searchable by case name, case year, state of origin, court, author, location, case outcome, PLN issue and key word search.
- ▶ Search free, pay only if you find it!
- ▶ The highest quality, most comprehensive prison litigation news and research site in the world.

Affordable rates to meet your budget
\$19.95 per month • \$149.95 per year

Subscribe to Prison Legal News Online! <http://www.prisonlegalnews.org>

lottery where miners are constantly guessing countless numbers until one of them finds the unique “winning ticket” (the “nonce”) that solves the puzzle for the next batch of transactions (a “block”).

This work proves miners invested substantial resources. By making it enormously expensive and time-consuming to create a valid block or to try to alter past transactions, PoW ties the network’s security directly to real-world economic costs. This makes it effectively impossible for malicious actors to cheat or reverse history, ensuring trustless agreement among all participants and forming the basis of Bitcoin’s decentralization and tamper-proof ledger.

Pseudonymity: Pseudonymity in Bitcoin means transactions are linked to “addresses” (strings of characters) rather than real identities, providing privacy unless external data correlates them. Users can generate new addresses per transaction to enhance anonymity. This feature protects against surveillance but is not absolutely anonymous.

Satoshi (Unit): A Satoshi is the smallest unit of Bitcoin, equal to 0.00000001 BTC (one hundred millionth), named after Bitcoin’s pseudonymous creator Satoshi Nakamoto. It allows for micro-transactions and divisibility as Bitcoin’s value rises. All amounts in the network are denominated in Satoshis internally.

Satoshi Nakamoto: Satoshi Nakamoto is the pseudonymous individual or group who invented Bitcoin, authoring its foundational whitepaper and releasing the initial software in 2009 before disappearing from public communication in 2011. Estimates indicate Satoshi mined around one million Bitcoins in the early days of Bitcoin’s existence, yet Satoshi’s vast holdings have remained entirely untouched to this day. Satoshi’s identity remains unknown, adding an air of mystique to Bitcoin.

Satoshi’s decision to walk away and remain anonymous is widely considered one of his most profound contributions to Bitcoin’s success and true decentralization. By ending his involvement and remaining unknown, Satoshi ensured that no single individual or entity could ever become a central authority figure or be pressured, targeted, or corrupted, thus allowing Bitcoin to truly flourish as a leaderless, community-driven project. This “gift” of anonymity solidified Bitcoin’s core principle of operating without a central trusted party, ensuring its long-term integrity and enabling Satoshi’s vision of decentralized

money to continue to influence the entire cryptocurrency space.

Seed Phrase: A seed phrase (also called a “recovery phrase” or “mnemonic phrase”) is a sequence of typically 12 or 24 common words (like “tree,” “river,” “house”). When you set up a Bitcoin “wallet” that gives you full control over your funds (a non-custodial wallet), it generates this unique phrase for you. It is essentially a human-readable “master key” that can unlock and restore your entire Bitcoin wallet, along with all the associated “private keys” and “addresses,” on any compatible hardware device or wallet software.

Think of your seed phrase as the ultimate backup and master password for all your Bitcoin. If your phone is lost, your computer crashes, or your hardware wallet malfunctions, your seed phrase is the only way to regain access to your Bitcoin. Since there is no bank or central authority to help you recover your password, you are solely responsible for keeping this phrase absolutely secret and safe. Anyone who gets hold of your seed phrase can instantly gain full control over your Bitcoin, highlighting its immense power and the critical importance of storing it securely, ideally offline and in multiple safe locations.

Self-Sovereignty: Self-Sovereignty refers to users taking self-custody of their Bitcoin by storing their “private keys” themselves (using hardware “wallets” or secure software wallets). This aligns with Bitcoin’s core philosophy of decentralization and financial sovereignty, empowering individuals to have full, uncensored control over their own money without relying on intermediaries. It means you are solely responsible for the security of your Bitcoin, but it also means no one can take your Bitcoin away from you without your consent or knowledge of your private key.

Transaction Fee: Transaction fees are small, voluntary payments you attach to your Bitcoin transaction, essentially like a tip or a bid to incentivize “miners” to include your transaction in the next “block” they add to the “blockchain.” Miners prioritize transactions that offer higher fees, especially during times when the network is busy (high congestion) and there is limited space in blocks. The fee is not based on the amount of Bitcoin you are sending but rather on the data size of your transaction and how quickly you want it processed. These fees will become the primary way miners are compensated after the halving events reduce the “block reward” to zero.

Trustless System: In game theory, the concept of a “trustless system” refers to a framework where participants do not need to rely on the good intentions, reputation, or direct oversight of other individual actors or a central authority to ensure a desired outcome. Instead, the system is designed with rules and incentives such that rational self-interest guides participants towards behavior that benefits the collective or at least prevents detrimental actions.

This is achieved through a carefully constructed set of rules that are transparent and verifiable (meaning they can be understood and their enforcement observed by all participants), combined with powerful economic or intrinsic incentives and disincentives. Rational actors who seek to maximize their own utility will choose to comply with these rules because the rewards for honest participation consistently outweigh any potential, usually short-lived, gains from defection, while the penalties for misbehavior are prohibitively high. The ideal outcome is a Nash Equilibrium, where no player can unilaterally improve their position by deviating from the established, cooperative strategy. By leveraging this predictability of rational self-interest, such systems can coordinate actions and maintain integrity without the need for traditional interpersonal or institutional trust, ensuring stable operation even in adversarial environments.

Bitcoin is the quintessential example of a trustless system. Its Proof-of-Work “consensus mechanism,” “block rewards,” and “difficulty adjustments” are meticulously designed game-theoretic mechanisms that solve the Byzantine Generals’ Problem in a decentralized and trustless environment. “Miners,” though anonymous and globally dispersed, are incentivized by the protocol to act honestly and validate transactions because this is the most economically rational choice. This eliminates the need for interpersonal trust, allowing the Bitcoin network to coordinate on a single, secure ledger, transforming the predictability of rational self-interest into a powerful force for system stability and integrity.

UTXO (Unspent Transaction Output): Unlike a bank account that tracks a single, running balance (like \$100 in your checking account), Bitcoin uses a different accounting model based on UTXOs, which are like individual digital cash notes or coins.

Imagine you have a “wallet” with bills of different denominations in it: a \$5 bill, a \$10 bill, and a \$1 bill. Each of these bills is like a

What Is Bitcoin? (cont.)

UTXO – it is an exact, specific amount of Bitcoin you received from a previous transaction that has not been spent yet. When you want to make a new transaction (for example, pay \$7), you do not just deduct it from a total balance. Instead, you select the specific “digital bills” (UTXOs) that add up to what you need. If you use your \$10 “bill” (“UTXO”) to pay \$7, that \$10 UTXO is completely “spent” or consumed, and two new UTXOs are created: one for \$7 (sent to the recipient) and one for \$3 (your “change” sent back to yourself).

The Bitcoin “blockchain” meticulously tracks all these individual digital “notes” or UTXOs to ensure that each one can only be spent once. It solves the “double-spending problem.” This model enhances privacy because your entire history is not tied to one account, and it makes the system very efficient compared to traditional account-based systems.

Wallet (Software / Hardware): A Bitcoin wallet is a specialized tool – either a software application (like an app on your phone or computer) or a physical device (like a small USB stick) – designed to help you manage your Bitcoin. Importantly, this is where a key concept comes in: a Bitcoin wallet never actually “contains” or “stores” any Bitcoin itself. Think of it like this: all Bitcoins always exist only as entries on the “blockchain.” They never leave the blockchain.

Instead of holding Bitcoin, your wallet’s true function is to securely manage your “private keys.” These are the secret, unique codes that prove your ownership of specific Bitcoins recorded on the blockchain and allow you to authorize their movement. Your wallet also helps you generate new Bitcoin addresses for receiving funds and creates the “digital signatures” necessary to send transactions. It gives you the control over your Bitcoin, not the storage of your Bitcoin. Understanding that your wallet is a key manager rather than a money holder is fundamental to Bitcoin security and the concept of “not your keys, not your coins.”

Wallets are either “software wallets” (“hot wallets”) or “hardware wallets” (“cold wallets”). Software wallets are convenient for frequent use as apps on your internet-connected devices. While easy to access, they carry a higher risk of being hacked if your phone or computer is compromised. Hardware wallets provide superior security because they store your private keys offline. This “cold storage” makes

them highly resistant to online threats like malware, making them the preferred choice for safeguarding larger amounts of Bitcoin.

The Birth of Bitcoin: An Idea Whose Time Has Come

Throughout history, groundbreaking inventions like the printing press and the internet have propelled humanity forward. We are currently on the verge of another, equally revolutionary advancement, but this time, it is how we think about and interact with money.

For centuries, we have relied on kings, governments, and banks to control our money by minting coins, printing bills, and managing ledgers with the assurance that our wealth remains secure and our transactions fair. But that trust has often been broken – currencies debased by emperors to fund wars, banks collapsing as a result of naked greed, and inflation eroding savings overnight. The 2008 global financial crisis exposed the flaws in the global financial system. A housing bubble fueled by reckless subprime lending and complex, opaque financial instruments burst, dragging down legendary institutions like Lehman Brothers and so-called “too big to fail” companies like AIG, which triggered billions in government bailouts for many of the same people and institutions largely responsible for the crisis, all while ordinary people lost homes, livelihoods, and savings.

Widespread distrust in banks and the failures of centralized financial institutions became palpable. Along with losing their homes and their savings, millions also lost their faith in the financial system. It was in this environment that a radical question was asked. What if money could exist independently of these institutions?

Amid this disillusionment and financial turmoil, Satoshi Nakamoto, the pseudonymous creator of Bitcoin, published the now-legendary nine-page whitepaper on October 31, 2008, titled “Bitcoin: A Peer-to-Peer Electronic Cash System.” It was posted to the Cryptography Mailing List on metzdowd.com and proposed a revolutionary alternative to traditional forms of money. The whitepaper described a chain of timestamped “blocks,” with each block having a unique digital fingerprint (called a “hash”) created from its contents to prevent any tampering, together forming what we now call the “blockchain.”

Satoshi, whose true identity remains unknown despite years of intense speculation, drew from decades of cryptographic research to propose a digital currency that

bypassed “trusted” intermediaries – no banks, no payment processors, no central authority, no intermediaries whatsoever. The vision was simple yet revolutionary: enable online payments directly between parties, solving the “double-spending problem” – where digital assets can be copied and spent twice – through a network of computers verifying transactions via “Proof-of-Work.”

Just a few months later, in January 2009, Satoshi “mined” the very first Bitcoin block, referred to as the “Genesis Block.” Leaving no doubt as to his motivation for gifting Bitcoin to the world, embedded in the Genesis Block’s data was an unmistakable message: “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.” The reference to the January 3, 2009, front-page headline of *The Times* newspaper (a London-based daily) served dual purposes – it provided a timestamp proving that no Bitcoins had been unfairly created or hoarded by Satoshi before the network went live (a practice with some cryptocurrencies called “premining,” where coins are created and held before public launch), while also providing a subtle critique of the flawed nature of centralized finance. The stage was set for a new era of money, one not reliant on trusting centralized institutions but on mathematical proof and an open, transparent network. The Bitcoin era had begun.

How Bitcoin Works: Putting the Pieces Together

Building on your understanding of Bitcoin terms and concepts from the Glossary, this section puts the pieces together by following the journey of a single Bitcoin transaction, while explaining how the key components interconnect to make the system work.

Bitcoin operates as a decentralized digital currency, functioning without a central authority like a bank or government. Its foundation is the blockchain, a public, shared ledger that records every transaction. Let us imagine you want to send 1 BTC to a friend. To do this, you use a digital “wallet” that holds your “private key” – a secret password that proves you own the Bitcoin at your specific “Bitcoin address.” When you initiate the transaction, your wallet uses your private key to digitally sign (create a unique, secure code proving it is really you validating) a message authorizing the transfer. This signed transaction, which says “send 1 BTC from my address to my friend’s address,” is then “broadcast” to the global network of computers.

This transaction now enters a pool of un-

confirmed transactions, waiting to be picked up by a miner. Miners, a specialized group of network participants, compete against each other using powerful computers to solve a complex mathematical puzzle – a process called Proof-of-Work. The goal is to be the first to find a solution, which earns them the right to create the next block. Our transaction is bundled with thousands of other pending transactions into this new block, which is then cryptographically sealed (locked using advanced mathematical techniques to ensure it cannot be altered without detection). This new block is added to the chain approximately every 10 minutes.

Once a miner finds the solution to the puzzle, they broadcast the new block – containing our transaction – to the entire Bitcoin network. This is the moment of confirmation. The thousands of independent computers known as “nodes” immediately receive this new block and individually verify its contents, making sure the transactions within it, including ours, are valid and follow all the network’s rules. Every node maintains a full and complete copy of the entire Bitcoin blockchain, so when a new block is added, they independently check it for validity. If the nodes agree

that the block is valid, they add it to their copy of the blockchain. If it is invalid, they simply reject it. This process is so resource-intensive that it becomes virtually impossible to alter our transaction once it is on the blockchain without re-doing all the work that followed it, making the ledger tamper-proof and immutable. This distributed verification eliminates the need for a trusted third party, shifting the burden of trust to the verifiable mechanics of the open-source protocol itself.

Now that the transaction is on the blockchain, your friend’s wallet – which is constantly monitoring the network – detects that their address has received 1 BTC. The journey is complete, and the Bitcoin is now securely theirs. For their hard work in securing our transaction and adding it to the blockchain, the successful miner receives the “block reward” (a predetermined number of newly minted Bitcoins) in addition to any “transaction fees” you paid. This incentive system is crucial to the network’s security because it aligns the interests of miners with the integrity of the network. It rewards honest behavior and makes any attempt to double-spend or create fraudulent transactions a financially ruinous course of action.

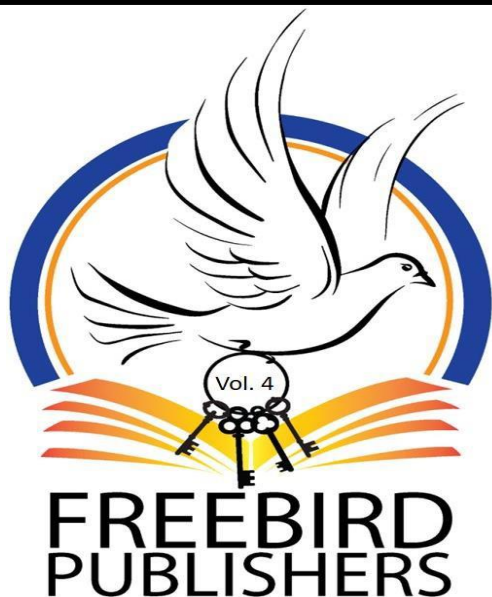
This entire process, from your initial send

request to your friend’s receipt of the Bitcoin, happens without needing a central bank, government, or any trusted third party to act as an intermediary.

Bitcoin’s Early Years: From Code to Currency (2009-2014)

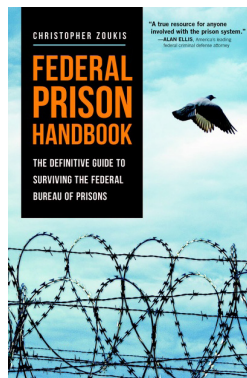
The story of Bitcoin truly begins on January 3, 2009, when its enigmatic creator, Satoshi Nakamoto, mined the Genesis Block. For nearly a year after its launch, Bitcoin existed as little more than an intriguing thought experiment circulating among members of the Cryptography Mailing List. The network was so small that Satoshi could mine blocks easily using just a basic CPU. There were no exchanges, no valuations in fiat currency, and no real-world use cases – just cryptographers passing the software among themselves.

The first recorded Bitcoin transaction occurred on January 12, 2009, when Satoshi sent 10 BTC to Hal Finney, a renowned cryptographer who had worked on Pretty Good Privacy (“PGP”) encryption. This exchange was not a commercial transaction but a crucial test, a validation that the peer-to-peer electronic cash system could indeed function as designed. Finney famously tweeted “Run-



All New Catalog Vol. 4. Our full color catalog has product listings of our prisoner publications: books, photo services, high quality gifts and holiday selections too! Catalog includes complete detailed ordering information, forms and more. All pages featured in detailed full color photographs on 5.5" x 8.5", 92 pages with full descriptions & prices. **\$5.00**

Freebird Publishers
221 Pearl St. Ste. 541 N. Dighton MA 02764



FEDERAL PRISON HANDBOOK

BY CHRISTOPHER ZOUKIS

THE DEFINITIVE GUIDE TO
SURVIVING THE FEDERAL
BUREAU OF PRISONS

Price: \$74.95 (shipping included)

This handbook teaches individuals facing incarceration, prisoners who are already inside, and their friends and family everything they need to know to protect themselves and their rights. The thorough information was compiled by someone who has first-hand experience with the federal prison system.

Name _____

DOC/BOP # _____

Institution/Agency _____

Address _____

City _____

State _____ Zip _____

Prison Legal News • PO Box 1151 • Lake Worth Beach, FL 33460
Tel. 561-360-2523 • www.prisonlegalnews.org

ning bitcoin,” a simple declaration that would become iconic in retrospect, signifying the network’s first steps into operational reality. In later interviews, Finney would recall those early days with amusement: “I was mining a block every once in a while ... the difficulty was so low you could find blocks with a CPU without even trying very hard.” Tragically, Finney would later be diagnosed with ALS, passing away in 2014 – but not before seeing his early belief in Bitcoin validated beyond anyone’s expectations.

The community grew slowly through 2009 on the newly created Bitcointalk forum, where Satoshi was an active participant. Discussions focused on technical improvements – such as fixing inflation bugs and optimizing the code – rather than speculation, because Bitcoin still had no widely agreed upon monetary value. However, a crucial step toward establishing its real-world value occurred on October 5, 2009, when Martti Malmi, a Finnish developer and early Bitcoin contributor, published the first-ever Bitcoin exchange rate against the U.S. dollar on his “New Liberty Standard” website, valuing 1 USD at 1,309.03 BTC (or \$0.00076 per Bitcoin), based on the electricity cost to mine it.

Everything changed on May 22, 2010, when Florida programmer Laszlo Hanyecz made history by offering 10,000 BTC to anyone who would deliver two pizzas to his Florida home. A British teenager accepted the offer, purchasing \$25 worth of Papa John’s pizzas using his credit card. This pizza delivery, now celebrated annually as Bitcoin Pizza Day, was the first documented real-world commercial transaction using Bitcoin and established Bitcoin’s first real-world valuation. It transformed Bitcoin from a theoretical digital curiosity into a medium of exchange with demonstrable economic value. It proved that Bitcoin could bridge the gap between the digital realm and everyday commerce. Notably, those two pizzas would be worth well over \$1.2 billion at Bitcoin’s all-time-high of over \$123,000 on July 14, 2025.

Just a few months later, on August 15, 2010, Bitcoin faced its first major existential threat when a critical bug, known as the “value overflow incident,” was discovered. This flaw allowed a malicious actor to attempt to create 184 billion Bitcoins out of thin air in a single transaction, violating Bitcoin’s “21-million-coin hard cap.” However, Satoshi

Nakamoto and other core developers quickly identified the exploit, coordinated a rapid patch, and executed a soft fork of the blockchain within hours. This swift, decentralized response prevented the catastrophic inflation of the supply and demonstrated the Bitcoin network’s unprecedented ability to self-correct and maintain its integrity even in the face of fundamental vulnerabilities.

As Bitcoin mining became more competitive and resource-intensive, the emergence of mining pools became essential to ensure that individual miners could still participate and contribute to the network’s security. In November 2010, Slush Pool (originally Bitcoin Pooled Mining Server) launched as the very first Bitcoin mining pool. This innovation allowed many individual miners to combine their computing power and share block rewards proportionally, democratizing access to mining and helping to further decentralize the network’s security as it grew.

Period of Extreme Turbulence

By 2011, Bitcoin began emerging from obscurity, though not always in ways its creator and early advocates might have hoped. The Silk Road marketplace (an underground online black market that operated on the dark web facilitating illicit trade) adopted Bitcoin as its primary currency, demonstrating its potential for censorship-resistant transactions while simultaneously linking it to criminality in the public consciousness. This duality of Bitcoin as both a tool for freedom and for crime would become a recurring theme. It was also around this time that Bitcoin’s open-source code inspired the first “altcoins” or alternative cryptocurrencies. Early examples like Namecoin (launched in April 2011, aiming for a decentralized domain name system) and Litecoin (launched in October 2011, often dubbed “digital silver” to Bitcoin’s “digital gold” with faster transaction times) showcased the permissionless innovation Bitcoin enabled, demonstrating that anyone could build on its underlying principles.

Meanwhile, the first Bitcoin exchanges began appearing. Mt. Gox, originally a Magic: The Gathering card trading site (hence its name, short for “Magic: The Gathering Online eXchange”), pivoted to become Bitcoin’s dominant centralized trading platform. Prices swung wildly from \$0.30 to \$32 and back to \$2 within months, as the market struggled to price this radically new asset class.

November 28, 2012, marked Bitcoin’s first halving, which automatically reduced the

block reward from 50 BTC to 25 BTC per block. This built-in scarcity mechanism, occurring every 210,000 blocks (approximately four years), was a key innovation that would gradually constrain Bitcoin’s supply.

By early 2013, Bitcoin’s price surged past \$100, drawing mainstream media attention and Wall Street’s skepticism. The criticisms were harsh and often definitive. Economist Paul Krugman, in a December 2013 blog post for *The New York Times*, wrote a headline claiming “Bitcoin Is Evil,” while in 2011, *Forbes* ran an article titled “So, That’s The End Of Bitcoin Then.” Benjamin Wallace, writing for *Wired* in November 2011, published “The Rise and Fall of Bitcoin,” a lengthy piece effectively branding it a failure. Yet beneath the surface, adoption continued growing. The Bitcoin Foundation launched to advocate for the protocol, while major companies like WordPress began accepting Bitcoin payments.

Then came the crash. On April 10, 2013, Bitcoin’s price plummeted from \$266 to \$50 in hours after Mt. Gox froze withdrawals, citing “technical issues.” Mainstream commentators gleefully declared Bitcoin dead – again. Humorously, Bitcoin has been pronounced dead prematurely so many times by the mainstream media and prominent commentators that the website 99bitcoins began tracking Bitcoin obituaries in 2010 with the tally up to 477 by April 2024.

Following this dramatic volatility, the rising profile of Bitcoin also attracted increased attention from governments. On December 5, 2013, the People’s Bank of China issued a directive prohibiting Chinese financial institutions from handling Bitcoin transactions, viewing the cryptocurrency as a potential threat to financial stability and a vehicle for illicit activities. This significant regulatory move from one of the world’s largest economies sent shockwaves through the market, causing Bitcoin’s price to plummet by approximately 50%, from nearly \$1,200 down to around \$600 over the following weeks, highlighting the nascent market’s vulnerability to state intervention.

The Rise of HODL Culture

Amid the fallout from the China ban, the overall extreme market turbulence, and waning public confidence in Bitcoin, something remarkable was happening. Through the volatility and fear, Bitcoin’s underlying network kept operating flawlessly. Merchants continued accepting it. Developers kept improving the software. And a new battle-hardened Bitcoin culture emerged on forums, where

users encouraged each other to “HODL.” This now-iconic rallying cry originated on December 18, 2013, during the tumultuous period of the China ban price crash. A Bitcointalk forum user named “GameKyuubi” posted a famously unedited, whiskey-fueled rant titled “I AM HODLING,” accidentally misspelling “holding.” His passionate, albeit inebriated, plea for fellow Bitcoiners to resist selling their Bitcoin amid the chaos instantly resonated, turning a simple typo into an enduring meme and a fundamental philosophy for the community.

The HODL rallying cry was not merely an admonition for Bitcoiners not to sell their Bitcoin but also an affirmation of a deeper belief that despite the short-term uncertainty, the long-term vision and fundamental technology of Bitcoin were sound. This HODL culture fostered a sense of solidarity and resilience among early Bitcoiners, encouraging them to ignore the FUD (Fear, Uncertainty, and Doubt) and focus on the revolutionary potential of decentralized digital money. It became a badge of honor for those with “diamond hands” who weathered the storms, distinguishing them from “paper hands” who succumbed to panic selling. This collective us-versus-the-world mentality helped solidify Bitcoin’s community, enabling it to survive and eventually thrive through periods of extreme uncertainty, criticism, and multi-vector attacks.

Then came the final blow to the dominant exchange of the era. After suffering from a massive, multi-year hacking operation that had not been publicly disclosed, Mt. Gox eventually collapsed in February 2014, halting all withdrawals and filing for bankruptcy. At the time, it accounted for a staggering 70% to 80% of all Bitcoin transactions worldwide, and the Bitcoin price plummeted from about \$853 to about \$360 by April 2014. Its demise was catastrophic for the Bitcoin market and the broader cryptocurrency community, triggering a multi-year bear market, eroding the fragile public trust that had begun to emerge as news spread that approximately 850,000 Bitcoins were stolen due to the hacks, and it led to aggressive regulatory scrutiny worldwide.

Bitcoin’s first five years represent one of the most fascinating case studies in technological adoption and antifragility. What began as an obscure cryptographic experiment became, in rapid succession (1) a functioning digital currency, (2) a speculative asset, (3) a payment network, and (4) a new asset class of digital gold.

The early Bitcoin community – a motley crew of libertarians, anarcho-capitalists, cryptographers, and curious technologists – proved that decentralized money could work in practice, not just theory. They weathered existential crises, fixed critical bugs, and built the infrastructure that would support later growth on a global scale – all without central leadership after Satoshi’s disappearance in 2011. Most importantly, these formative years established Bitcoin’s core ethos in the real world: no central control, no bailouts, resistance to censorship, and permissionless innovation.

Bitcoin’s origin story reminds us that the most disruptive ideas often begin as obscure experiments, nurtured by relentless visionaries willing to challenge the status quo against all odds when no one else believed in them or their vision. The code may be mathematical, but Bitcoin’s history is profoundly human – an inspiring testament to how a small group of misfits, rebels, and troublemakers who see things differently can change things, can push the human race forward.

What Makes Bitcoin “Sound Money”

Bitcoin embodies the principles of sound money – a term describing a form of money that reliably maintains its value over a long period, without suffering from significant depreciation or being subject to arbitrary changes by a central authority. It functions as a resilient medium of exchange, unit of account, and store of value that inherently resists debasement and centralized control. For something to be considered truly sound money, it generally needs to possess several key characteristics:

- **Scarcity:** Its supply is genuinely limited and cannot be easily created or inflated.
- **Durability:** It does not easily wear out or degrade over time.
- **Divisibility:** It can be easily broken down into smaller units for various transaction sizes.
- **Portability:** It is easy to move or transfer, even across long distances.
- **Fungibility:** Any unit is interchangeable and has the same value as another unit (like any dollar bill is equal to any other).
- **Censorship Resistance:** No single entity can easily prevent or reverse transactions.

Unlike fiat currencies, which derive their value from government mandates and are prone to inflation through unlimited print-

ing, or CBDCs that enable unprecedented surveillance and control, Bitcoin’s design is based on these proven monetary ideals while utilizing modern cryptography. Its attributes directly address the flaws in traditional systems, providing absolute scarcity through its fixed supply, extreme durability by being digital, seamless portability across the internet, and inherent censorship resistance. Grouped thematically below, these features collectively demonstrate why Bitcoin is the hardest, most sound money humanity has ever experienced.

Core Monetary Properties

These attributes align Bitcoin with the essential qualities of sound money, emphasizing its role as a stable, practical asset superior to inflationary fiat.

Fixed Supply, Scarcity, and Deflationary:

What it means: Bitcoin is designed with an absolute, unchangeable maximum limit of 21 million Bitcoins that can ever exist. This is not a rule set by a government or a bank that can be changed on a whim. It is a fundamental part of Bitcoin’s underlying computer code. New Bitcoins are introduced into circulation through a process called mining. Just like gold miners find new gold, Bitcoin miners use powerful computers to solve complex puzzles, verifying transactions and adding them to Bitcoin’s public record (the blockchain).

Bitcoin is designed with a strict, immutable cap of 21 million Bitcoins that can ever be created. This is a limit hardcoded into its protocol in Satoshi’s 2008 whitepaper. This is not a flexible policy dictated by a central bank or government that can be altered through legislation or executive decision. Instead, it is enforced by the consensus rules of the Bitcoin software, which every participating computer – referred to as a “node” – in the network must adhere to for the network to function. If anyone tries to change this rule – for example, by proposing to increase the supply – the network would reject those changes unless a vast majority agrees, and even then, it could lead to a “fork,” creating a separate cryptocurrency while the original Bitcoin preserves its hard cap.

New Bitcoins enter circulation exclusively through mining, a competitive process where participants use specialized hardware to solve complex cryptographic puzzles – in essence, racing to find a valid “nonce,” a random number that meets the network’s difficulty target. This not only verifies and bundles user transactions

What Is Bitcoin? (cont.)

into blocks added to the blockchain – Bitcoin's tamper-proof, distributed ledger – but also secures the entire network against attacks. Successful miners are rewarded with newly created Bitcoins, plus any transaction fees from users.

Importantly, this issuance is not arbitrary or perpetual. It is governed by a predetermined, geometrically decreasing schedule. Every 210,000 blocks – approximately every four years based on the fact that blocks are produced about every 10 minutes – the block reward halves in an event called a “halving.” Bitcoin started in January 2009 with a block reward of 50 BTC. Halvings in 2012 (to 25 BTC), 2016 (12.5 BTC), 2020 (6.25 BTC), and most recently on April 19, 2024 (to 3.125 BTC), have progressively reduced the block reward in half and correspondingly decreased the inflation rate. The next halving is projected for around March or April 2028, reducing the block reward to 1.5625 BTC.

This pattern is programmed to continue through approximately 33 halvings until around 2140, when the reward becomes so minuscule (less than one Satoshi) that no new Bitcoins will be issued. At that point, miners will sustain the network solely through transaction fees. Additionally, real-world scarcity is amplified by “lost” Bitcoins – those inaccessible due to forgotten “private keys” or deceased owners – estimated at 3 to 4 million already, which effectively reduces the maximum circulating supply below 21 million and makes Bitcoin deflationary over time, i.e., the value of each unit rises as demand grows against a shrinking effective supply.

Bitcoin marks a historic breakthrough as the first form of money whose supply is completely inelastic to demand, with new coins minted at a predetermined, diminishing rate unaffected by market demand. No matter how intensely demand surges or prices skyrocket, Bitcoin's issuance schedule remains rigidly fixed, preventing any responsive increase to supply that would dilute its scarcity and value. With every other form of money or asset ever used by humanity, supply can be increased as demand and prices rise.

Why it is important: This hard limit on supply is arguably Bitcoin's most revolutionary feature and why many call it digital gold, though Bitcoin's inflation rate is currently lower than gold's and drops every four years because

Bitcoin's new supply issuance falls after every halving. It directly prevents the endless money printing that is common with traditional government-backed fiat currencies. When central banks print more and more money, it increases the total supply, which makes each existing unit of that currency worth less. This can lead to hyperinflation crises – where prices skyrocket and savings are wiped out almost overnight. Real-world examples include Zimbabwe in the 2000s and more recently in Venezuela. In stark contrast, Bitcoin's value cannot be diluted by an arbitrary increase in supply by a central authority.

Fungibility:

What it means: Every single Bitcoin (and even every Satoshi) is treated the same. There is no inherent difference between a Bitcoin that was just mined yesterday and one that has changed hands a hundred times. The Bitcoin network's software is designed to recognize all Bitcoins as equally valid and interchangeable units. It does not attach a unique serial number or ID to a specific Bitcoin that would make it different from any other. When you send one Bitcoin, you are not sending a specific physical item; you are updating a record on the shared ledger (the blockchain) to show that one Bitcoin has moved from one address to another.

Why it is important: Bitcoin's fungibility means that the network itself does not discriminate between units based on their past usage. This ensures that any Bitcoin you receive will be treated just like any other, supporting its viability as a reliable medium of exchange for everyone. You do not have to worry that the Bitcoin you are receiving might be “tainted” by previous transactions in the eyes of the network or other users, ensuring smooth and trustless economic activity. In contrast, CBDCs can tag and restrict “tainted” funds based on spending patterns or other arbitrary factors.

Divisibility and Portability:

What it means: Bitcoin is designed to be incredibly flexible in terms of how it can be valued and moved. First, its divisibility means you do not have to buy or send an entire Bitcoin. While one Bitcoin is worth over \$100,000, it can be broken down into incredibly tiny units. The smallest unit of a Bitcoin is called a Satoshi, and one Bitcoin is made up of 100 million Satoshis. This extreme divisibility means Bitcoin can be used for even very small payments, from buying a coffee to tipping an online content creator.

Also, its portability refers to how easily you can move your Bitcoin wealth around the world. Because Bitcoin is purely digital, it exists as data on the decentralized network, not as a physical object. This means you can transfer any amount of Bitcoin – from a few Satoshis to millions of dollars worth – to anyone, anywhere in the world, simply by using a smartphone or computer with an internet connection. Your wealth is not stored in a physical vault or tied to a specific country's banking system. You effectively “carry” your Bitcoin by remembering a simple phrase (your “seed phrase,” which generates your digital private keys) or by having a small, secure hardware device.

Why it is important: These two features are crucial for Bitcoin to function as a truly global and versatile form of money. Divisibility allows for micro-payments that are impractical with traditional banking systems, which often have minimum transaction sizes or fees that make very small payments uneconomical. It also ensures that even if Bitcoin's value continues to rise significantly, it can still be used for everyday transactions, not just large investments.

Portability enables seamless global transfers without the bulk and security risks of moving physical assets like gold across borders. It also bypasses the slow speeds, high fees, and bureaucratic hurdles of traditional bank wires or services like Western Union.

Durability and Uniformity:

What it means: As pure code, Bitcoin does not degrade, corrode, or vary in quality; all units are identical and eternally intact. Bitcoin possesses perfect uniformity. Every single Bitcoin is identical to every other Bitcoin. There are no “used” or “new” Bitcoins that are inherently different, no varying qualities like with some physical commodities (e.g., different grades of diamonds or purity of gold). One Bitcoin is always equal to any other Bitcoin.

Since Bitcoin is digital and verified by a global network, it is impossible to create fake Bitcoins. The system itself prevents the duplication or fraudulent creation of units. Additionally, the consistent quality of each unit ensures that there is no confusion or debate about its authenticity or inherent worth, contributing to its trustworthiness as a medium of exchange.

Why it is important: These attributes mean Bitcoin provides perpetual reliability that physical currencies cannot match. Paper

money requires constant replacement, costing governments money and creating environmental waste. Coins wear down over time. Bitcoin is immune to these physical vulnerabilities.

This durability stands in stark contrast to how a CBDC functions. While a CBDC is also digital, its existence and integrity depend entirely on a central bank's infrastructure. If that central system were to experience a major technical failure, be targeted by a cyberattack, or if its policies changed (e.g., an arbitrary decision to delete or alter digital records), the CBDC can be compromised. Being decentralized and digitally durable, Bitcoin is designed to outlast these kinds of central shutdowns or policy changes, providing a more resilient form of money that exists as long as the internet and its network of computers do.

Store of Value and Inflation Hedge:

What it means: A store of value is something that maintains its purchasing power over time, even across long periods. Gold has traditionally served this role for thousands of years because it is scarce, durable, and universally accepted. An "inflation hedge" is an asset that helps protect your wealth from the eroding effects of inflation, which is the decrease in the purchasing power of money (meaning your dollar buys less stuff tomorrow than it does today).

Bitcoin fits both these descriptions, even surpassing gold due to its absolute scarcity and independence from central control. Unlike fiat currencies whose supply can be increased by central banks at will, Bitcoin has a fixed, known supply cap of 21 million Bitcoins. This hard limit, combined with its predictable and diminishing issuance rate (due to halvings), means its supply cannot be arbitrarily inflated.

Why it is important: During periods of significant inflation, like the 2020–2022 inflation surge following massive government spending and central bank stimulus measures, the purchasing power of fiat currencies often diminishes rapidly. People's savings buy less and less, effectively draining their wealth over time.

In such scenarios, Bitcoin is increasingly acting as a decentralized safe haven for savings. Unlike fiat currencies or CBDCs, Bitcoin offers a mathematically enforced and transparent monetary policy that cannot be altered, providing a unique and compelling way to preserve purchasing power and serve as a hedge against economic instability.

Security and Resilience

Bitcoin's robust digital architecture ensures trust through technology, not institutions, making it far more secure than centralized systems.

Decentralization:

What it means: At its core, decentralization in Bitcoin refers to the way the entire system operates without relying on a single controlling entity, such as a bank, a company, or a government agency, to manage or oversee transactions and records. Instead, Bitcoin functions through a vast, distributed network of thousands of independent computers – referred to as nodes – spread across the globe, each running the same open-source software that anyone can freely download, review, and contribute to. These nodes work together in a peer-to-peer manner. It is similar to how file-sharing programs allow users to connect directly without a central server, forming a resilient network where the low barrier to entry means virtually anyone with a computer and internet can participate by running a node.

When someone wants to send Bitcoin, the transaction is broadcast to this network, and nodes verify it against a shared set of rules (like checking if the sender has enough funds and is not trying to spend the same coins twice – a problem known as double-spending, which Bitcoin solves without needing a trusted third party). Once validated, the transaction is bundled with others into a block and added to the blockchain – a public, chronological ledger that every node maintains a copy of, ensuring transparency where all transactions are visible but pseudonymous (not directly tied to real identities). This process is powered by miners, specialized computers that compete to solve complex mathematical puzzles to confirm blocks and earn new Bitcoins as a reward, ensuring the network remains secure and honest through collective effort rather than top-down authority. This mechanism is called Proof-of-Work and incentivizes honest behavior while making attacks prohibitively expensive.

Because no one party holds power or authority over the entire Bitcoin network, changes to the network require broad consensus among participants via a process known as "Nakamoto Consensus," where the longest valid blockchain (backed by the most computational work) is accepted as the truth, promoting democratic governance and resistance to tampering. Decentralization extends across layers: the network itself (geographi-

cally dispersed to avoid regional shutdowns), mining (distributed among participants to prevent dominance), and even development (open-source contributions from a global community). Overall, this structure achieves "Byzantine Fault Tolerance," meaning the network can function correctly even if some nodes are faulty or malicious.

Why it is important: Decentralization is the foundational pillar that sets Bitcoin apart from traditional financial systems. It fundamentally addresses the vulnerabilities inherent in centralized control by distributing power and responsibility across a global, voluntary network of participants that enhances overall

INMATE SHOPPER

DON'T WASTE YOUR MONEY! KNOW WHO YOU ARE DEALING WITH! BUSINESS DIRECTORY WITH RATINGS



AMERICA'S LARGEST PUBLICATION OF Inmate Resources & Services

1000+ LISTINGS: all businesses and services are reviewed regularly and rated by the publisher based on feedback from inmates. NEW Content every issue.

Pen Pal Resources
Photo Spread (Non Nude)
Catalogs to Order
Magazine Sellers
LGBTQ Section
Criminal Justice News

Sexy Photos Sellers
Social Media/Text/Phone
Major Sport Schedules
Articles, Tips & Facts
Always Up-to-Date
Softcover, 8x10 350 pgs.

NEW!! 2025-2026 INMATE SHOPPER

\$29.99 incl. s/h with tracking

PILLOW TALK ★ SOFT SHOTS

Non Nude Photo Books



FULL COLOR GLOSS PHOTOS

A Different Photo On Every Page

OVER \$100 WORTH OF SEXY PHOTOS IN 1 BOOK...

NON NUDE PRISON FRIENDLY

Each Book Softcover, 6x9", 150+ Gloss Color

PILLOW TALK or SOFT SHOT

\$33.99 EACH incl. s/h with tracking

Freebird Publishers

221 Pearl St., Ste. 541
North Dighton, MA 02764
www.FreebirdPublishers.com

What Is Bitcoin? (cont.)

resilience and user autonomy. By eliminating single points of failure – where a hack, policy change, or institutional collapse could cripple the entire system – it prevents scenarios like historical bank runs, such as the 2008 financial crisis when centralized banks faced mass withdrawals and required government bailouts, or the infamous 2014 Mt. Gox crypto exchange hack, where a single company's security flaws led to the loss of hundreds of thousands of Bitcoins because it acted as a centralized custodian.

In contrast, Bitcoin's decentralized design means that even if some nodes go offline (due to power outages, cyberattacks, or government restrictions in specific countries), the network as a whole continues to operate seamlessly, as other nodes pick up the slack – much like how the internet routes around damaged pathways to keep data flowing. This resistance to shut-downs or manipulations is particularly crucial in authoritarian regimes or during political unrest, where governments might attempt to censor financial flows, as seen in cases like

Nigeria's 2021 crypto ban attempts or China's repeated crackdowns on mining operations. Nevertheless, Bitcoin persists because no central switch exists to turn it off.

Unlike CBDCs – which amplify government oversight through a single, state-controlled ledger that can enable real-time monitoring, transaction blocking, or even programmable restrictions (like expiring funds or spending limits based on behavior) – Bitcoin's decentralization empowers individuals with true financial sovereignty, reducing the risk of arbitrary interference and fostering a system where trust is placed in verifiable code and collective verification rather than centralized authority. Additionally, this model promotes innovation and inclusivity because it lowers barriers for global participation without needing permission from gatekeepers, helping unbanked populations in developing regions access finance while encouraging a merit-based ecosystem where the best ideas rise through community consensus.

Bitcoin's decentralization ultimately creates a more equitable, tamper-resistant form of money that aligns with principles of liberty and self-reliance, making Bitcoin a

hedge against systemic risks in an increasingly interconnected and unpredictable world.

Proof-of-Work Security Model:

What it means: Proof-of-Work is the fundamental consensus mechanism that enables all independent computers (nodes and miners) in the Bitcoin network to collectively agree on a single, accurate, and unchangeable version of its transaction history, all without needing any central authority.

The process requires miners to expend significant computational effort and real-world electricity. They do this in order to solve an extremely challenging cryptographic puzzle. This puzzle involves taking new, unconfirmed transactions, combining them with data from the previous block's hash and a changing arbitrary number (nonce), and repeatedly processing this combined data through a one-way mathematical function (the SHA-256 algorithm). The objective is to find a specific output, or hash, that meets an exceptionally difficult condition, such as starting with a predetermined number of zeros. Discovering this solution is purely a trial-and-error process, as there is no shortcut

Prison Education Guide

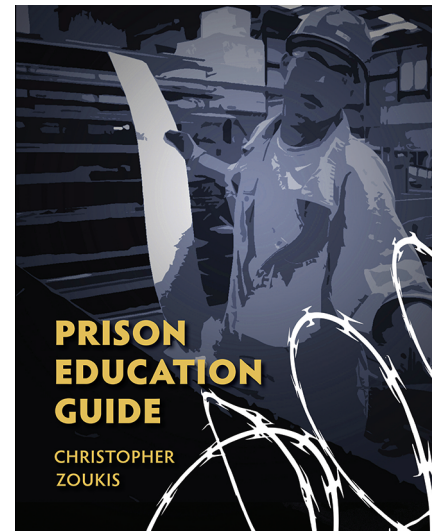
by Christopher Zoukis

This exceptional book is the most comprehensive guide to correspondence programs for prisoners available today. *Prison Education Guide* provides the reader with step-by-step instructions to find the right educational program, enroll in courses, and complete classes to meet their academic goals.

This guide is the latest and best resource on the market for the incarcerated nontraditional student. It includes a detailed analysis of the quality, cost, and course offerings of all correspondence programs available to prisoners.

"Education is always important but it is even more so for the more than two million Americans who live behind bars. When one's body is locked up, the freedom and development of one's mind becomes a powerful form of resistance and self-preservation. This book is an invaluable tool in the struggle for knowledge behind bars."

— CHRISTIAN PARENTI



Price: \$24.95
(shipping included)

280 pages

Order by mail, phone, or online.

Amount enclosed for PEG _____ By: ☐ check ☐ credit card ☐ money order

Name: _____ DOC/BOP Number: _____

Institution/Agency: _____

Address: _____

City: _____ State: _____ Zip: _____



Human Rights Defense Center
Dedicated to Protecting Human Rights

PO Box 1151 • Lake Worth Beach, FL 33460 • Phone # 561-360-2523
WWW.PRISONLEGALNEWS.ORG • WWW.CRIMINALLEGALNEWS.ORG

to determine the correct nonce. Once a miner finds the valid solution, it earns the right to add the next block of verified transactions to the blockchain. This substantial computational work is then easily verifiable by any other participant on the network.

Why it is important: Proof-of-Work ties Bitcoin's value to tangible resources. Because solving the cryptographic puzzle for a block demands so much computational effort, altering a past transaction on the blockchain becomes prohibitively expensive. A malicious actor would not only need to re-perform the Proof-of-Work for the target block but also for every single subsequent block that has been added to the chain. Because blocks are consistently added every 10 minutes, the cumulative computational cost required to rewrite history quickly becomes economically infeasible, effectively rendering the Bitcoin blockchain immutable and tamper-proof.

This energy-backed security model fundamentally differentiates Bitcoin from traditional fiat currencies or CBDCs. Fiat systems derive their value and security from government decree and public trust in the issuing authority. While they have their own sophisticated security measures against forgery and fraud, they are ultimately backed by debt and the promise of a central entity. Their supply can be expanded or contracted at will by central banks. Bitcoin, on the other hand, ties its security directly to a tangible, real-world cost – the energy expended by miners. This makes its integrity economically verifiable and provides a unique defense mechanism that CBDCs, as centrally issued digital fiat, fundamentally lack. It shifts the burden of trust from a central institution to the verifiable laws of physics and economics.

Security and Immutability:

What it means: At its core, Bitcoin's security and immutability are a product of its revolutionary design, combining several cryptographic and computational principles. When a transaction occurs on the Bitcoin network, it is first cryptographically signed by the sender using their private key. This digital signature serves as proof that the sender is the legitimate owner of the funds and has authorized the transaction, all without revealing their private key. The transaction data itself – which includes the sender's address, the recipient's address, and the amount of Bitcoin – is not encrypted. Instead, it is broadcast to the peer-to-peer network and added to the

public, transparent, and immutable blockchain ledger, where it can be viewed by anyone. Although the transaction is publicly visible and transparent on the blockchain, the sender's real-world identity remains hidden behind a pseudonym, as the private key is used solely to create a digital signature that authenticates the transfer, not to encrypt or privatize the transaction data.

These encrypted transactions are then bundled together into a block. Think of a block as a digital page in a very long, digital ledger. What makes this ledger unique is how these pages are connected. Each new block contains a cryptographic hash of the previous block. A hash is like a unique digital fingerprint of the data within the previous block. If even a single character in the preceding block were changed, its hash would completely change, breaking the chain. This creates an irreversible chain of blocks, thus the term "blockchain." Each block is inextricably linked to the one before it, all the way back to the very first block ever created – the Genesis Block.

The integrity of this chain is further reinforced by Proof-of-Work. This is the computational engine that secures the Bitcoin network. Miners (powerful computers connected to the network) compete to solve a complex mathematical puzzle. The first miner to solve the puzzle gets to add the next block of transactions to the blockchain and is rewarded with newly minted Bitcoins. The "work" in Proof-of-Work refers to the immense computational effort required to solve these puzzles. It is designed to be extremely difficult to solve but relatively easy for others to verify.

This process is intentionally resource-intensive, making it economically unrealistic for anyone to try to alter past transactions. To change a transaction in an old block, an attacker would not only need to re-do the Proof-of-Work for that block but also for every subsequent block in the chain, as each block's hash depends on the previous one. This would require an unfathomable amount of computing power, far exceeding anything a single entity could realistically possess.

Why it is important: The groundbreaking significance of this security architecture lies in its ability to deliver irrefutable certainty to users. Once a transaction is confirmed and recorded on the blockchain (which typically involves its being included in several subsequent blocks, further cementing its position), it cannot be altered, deleted, or reversed. This is the essence of tamper-proof records.

Consider the pervasive problem of double-spending in digital systems. In traditional digital currencies, there is always the risk that a malicious actor could spend the same digital token twice, much like copying a digital file and sending it to two different people. Centralized systems combat this by maintaining a central ledger controlled by a single entity (like a bank), which verifies that a token is only spent once. However, this introduces a single point of failure and requires users to trust that central authority implicitly.

Bitcoin's design elegantly solves the double-spending problem without needing a trusted third party. The irreversible nature of its transactions means that once a Bitcoin is sent, it verifiably disappears from the sender's wallet and is recorded as belonging to the recipient. There is no way to "undo" that transfer or fraudulently spend the same Bitcoin again. This certainty is a radical departure from traditional digital finance, where chargebacks and reversals are common, often leading to disputes and financial losses.

This immutability also highlights a critical distinction from CBDCs. While CBDCs seek to digitize national currencies, they rely on centralized ledgers controlled by the central bank. This means that, in theory, the central bank (or the government behind it) can manipulate those records. They can freeze accounts, reverse transactions, or even censor certain types of payments. For users, this introduces a counterparty risk – the risk that a party in any financial transaction fails to satisfy its obligations – and a reliance on the benevolence of the central authority. In contrast, Bitcoin's decentralized and immutable blockchain ensures that no single entity, not even the network's creator or the most powerful governments, can unilaterally alter the historical record of transactions. This provides a level of financial sovereignty and censorship resistance that is unparalleled in traditional or proposed CBDC systems, providing users with a truly unassailable and verifiable history of their financial activities.

Auditable and Verifiable Supply:

What it means: The concept of an auditable and verifiable supply in Bitcoin refers to its unprecedented ability for anyone, anywhere in the world, to independently confirm the exact number of Bitcoins in existence and to trace every single transaction ever made. This is achieved through the open-source nature of the Bitcoin protocol and the distributed network of nodes.

What Is Bitcoin? (cont.)

A node is simply a computer running the Bitcoin software. When someone “runs a node,” they download a complete copy of the entire Bitcoin blockchain – the public ledger containing every Bitcoin transaction since its inception in 2009. This might sound like a lot of data (and it is, requiring hundreds of gigabytes) but it is vital for the network’s integrity. By having a full copy of the blockchain, each node can independently verify every rule of the Bitcoin protocol.

Because the entire transaction history is public and transparent on the blockchain, anyone running a node can literally audit the entire supply from the very first Bitcoin ever mined. There is never a need to request a report from a central authority; anyone can verify the numbers themselves.

Why it is important: This auditable and verifiable supply is essential because it fundamentally shifts the paradigm of trust in money. In traditional financial systems, we are forced to trust opaque central banks to manage the money supply. Central banks, like the Federal Reserve in the U.S., have the power to create new money at will, often through policies like quantitative easing (“QE”).

During QE, central banks essentially “print” new money (electronically) to buy government bonds or other assets. The stated goal is often to stimulate the economy, but a direct consequence is an increase in the money supply. The public often has to rely on the central bank’s own reports to understand the extent of this money creation. These reports, while publicly available, are typically so complex that the true impact on purchasing power or inflation is not immediately obvious or fully disclosed in an easily digestible manner for the average person. This lack of meaningful transparency and the inherent trust required can lead to concerns about hidden inflation, where the purchasing power of money erodes without clear public accountability.

Bitcoin’s “don’t trust, verify” ethos directly addresses the opacity surrounding centralized money. You do not need to trust Satoshi Nakamoto, the miners, or any other entity to ensure the 21-million hard cap is adhered to. You can download the software, run a node, and verify it yourself. This eliminates the need for faith in an intermediary and provides an unprecedented level of transparency and certainty with respect to monetary

policy. Bitcoin’s auditable and verifiable supply ensures that its monetary policy is fixed, transparent, and cannot be changed without the overwhelming consensus of the decentralized network of nodes.

Bitcoin’s open ledger fosters systemic trust, not through reliance on an authority, but through universal verifiability. Anyone can inspect the entire history of the network. This means there are no hidden manipulations. Thus, Bitcoin fundamentally empowers individuals to verify the system rather than being forced to blindly trust an opaque central authority.

User Empowerment

These features prioritize individual control, shielding users from the overreach common in traditional finance.

Self-Sovereignty, Seizure, and Censorship Resistance:

What it means: The concept of self-sovereignty in Bitcoin is fundamentally about returning complete control over one’s financial assets to the individual, rather than entrusting it to intermediaries like banks or governments. This is achieved through the mechanism of holding private keys.

Imagine your Bitcoin as a digital safe. To open that safe and access your funds, you need a unique, secret code – this is your private key. It is a long string of alphanumeric characters, often represented as a seed phrase (a list of 12 or 24 words in a specific order that can regenerate your private key) that can be used to mathematically derive your private key. If you possess this private key, you are the sole custodian of your Bitcoin. No one else has the ability to move, freeze, or access those funds without it. This is a radical departure from traditional banking, where the bank is the custodian of your money, and you merely have a claim against their ledger.

Why it is important: When you hold the private key, you can initiate permissionless transfers. This means you do not need anyone’s approval – not a bank’s, not a government’s, not a payment processor’s – to send your Bitcoin to anyone, anywhere in the world, at any time. The transaction simply needs to adhere to the rules of the Bitcoin protocol (like having enough funds and a valid signature from your private key), and the decentralized network of miners will process it. This permissionless nature directly enables “seizure resistance” and “censorship resistance.”

Seizure Resistance: One of Bitcoin’s most profound and empowering features is its inherent resistance to seizure, a principle that stems directly from its decentralized architecture and cryptographic design. Because no central authority holds your Bitcoin or controls access to it, no such entity can easily “seize” it through simple administrative actions. Unlike a traditional bank account, which can be frozen instantaneously by a court order, government directive, or even a bank’s internal policy (often without the account holder’s immediate knowledge or recourse), Bitcoin held securely with your private key remains outside the direct reach of these commands.

Your private key – a unique string of characters that proves ownership and allows you to sign transactions – is essentially the digital equivalent of a vault combination known only to you. It can be stored in various secure ways: on hardware wallets (physical devices resembling USB drives), paper backups, or even memorized as a seed phrase. When you hold your private key in a secure manner, then your Bitcoin effectively resides “off-grid” from traditional financial surveillance and control. For an authority to seize your Bitcoin, it would need to physically or coercively obtain this private key from you personally, which is far more challenging than issuing a remote freeze on centralized assets.

This seizure resistance is not merely theoretical – it is a lifesaving reality in crisis-stricken regions worldwide, where Bitcoin has enabled people to preserve and transport their life savings amid chaos, hyperinflation, or authoritarian crackdowns in ways impossible with traditional assets like cash, gold, or bank deposits. Consider the following examples.

- ♦ **Ukraine:** In the early days of the war in Ukraine in February 2022, as millions fled the war-torn country, many faced severe restrictions on withdrawing cash from ATMs (limited to about \$300 per day in some cases) or moving physical assets like gold, which could be detected at borders, stolen by looters, or were simply too cumbersome to carry during hurried escapes.

Compare those scenarios with stories that emerged of Ukrainians who memorized their Bitcoin seed phrases or stored them on inconspicuous USB drives, allowing them to cross borders with their entire wealth intact and inaccessible to thieves or government officials. For instance, a 20-year-old Ukrainian

refugee named Fadey P. fled to Poland with roughly \$2,000 in Bitcoin – nearly half of his life savings – on a USB drive, bypassing frozen banking systems and capital controls that trapped others' funds. Another Ukrainian, amid bank freezes and ATM overruns, escaped with his wealth secured in Bitcoin, later using it to rebuild his life and even support resistance efforts. These cases illustrate how Bitcoin's borderless, intangible nature allowed refugees to evade seizures that plagued those relying on physical gold (which Russian forces reportedly looted from homes and banks) or cash (subject to devaluation and confiscation at checkpoints). In critical moments, they were able to cross borders with nothing more than their memorized seed phrase. Once safely in another country, they could access their Bitcoin from any internet-connected device, converting it to local currency to cover essential needs and start a new life.

- **Venezuela:** Similar dynamics have played out in other global hotspots, solidifying Bitcoin's role as a hedge against economic tyranny. In Venezuela, where hyperinflation soared to over 1 million percent in 2018, citizens turned to Bitcoin to preserve value amid a collapsing bolivar currency and strict government controls that included freezing bank accounts and seizing assets from perceived opponents. Venezuelans used Bitcoin to convert their rapidly depreciating savings into a stable, unseizable form, sending remittances from abroad or trading locally to buy essentials and thereby evading the regime's financial surveillance that could block traditional transfers or confiscate funds outright.
- **Afghanistan:** Following the Taliban's takeover in 2021, the financial system in Afghanistan also collapsed, with banks closing and international aid frozen. Reports indicated that some Afghans who had adopted Bitcoin were able to access their funds, providing a vital means of survival and escape when traditional avenues failed.
- **Argentina:** In Argentina, facing repeated economic crises with inflation hitting 211% in 2023 and government-imposed capital controls that limited dollar access, many adopted Bitcoin to safeguard wealth from devaluation and potential seizures, using it for everyday transac-

tions and cross-border transfers that bypassed restrictive banking systems. These examples illustrate Bitcoin's seizure resistance. Bitcoin enables individuals to "be their own bank," resisting the asset grabs that have devastated generations reliant on centralized systems and physical assets for preservation of wealth.

- **United States:** For those skeptical that such seizures could ever occur in stable democracies like the U.S., history provides sobering, verifiable warnings that even advanced nations are not immune. In the midst of the Great Depression, on April 5, 1933, President Franklin D. Roosevelt issued Executive Order 6102, which criminalized private gold ownership overnight. It required Americans to surrender their gold coins, bullion, and certificates to the Federal Reserve in exchange for paper dollars at a fixed rate of \$20.67 per troy ounce. The government's stated goal was to expand the money supply and combat deflation, as the U.S. was then on a gold standard. By removing gold from private circulation, the government gained greater flexibility over monetary policy. Violators faced up to 10 years in prison and fines of \$10,000 (equivalent to about \$246,000 in 2025 dollars). The policy transferred immense wealth from citizens to the state, which it justified as an economic necessity.

Americans were forced to relinquish a significant portion of their wealth, at a price that would soon be devalued when the official price of gold was raised to \$35 per troy ounce shortly thereafter, effectively reducing their purchasing power. This historical event serves as a grim reminder that even in democracies, during times of perceived national emergency, governments can and have resorted (and will resort) to seizing private assets. Despite its historical role as a safe haven, gold proved susceptible to central control because its physical nature necessitates storage in ways that can be easily tracked and confiscated.

- **Cyprus:** In 2013, Cyprus' financial crisis led to an EU-brokered "bail-in" where uninsured bank deposits over €100,000 were seized – up to 47.5% in some cases – to recapitalize failing banks. The seizures affected thousands of savers who woke up to find significant portions of their life savings gone without warning or recourse. Wealthy depositors, including

many foreigners, lost billions, with the government closing the second-largest bank and imposing capital controls that froze access to funds for months. These events, from the U.S. gold confiscation to Cyprus' deposit raid, demonstrate how quickly supposedly "secure" assets in centralized systems can be appropriated under economic duress, justified as necessary for the "greater good."

Bitcoin is largely immune to this vulnerability. Without a central ledger to manipulate or accounts to freeze, it forces authorities to confront individuals directly for their private keys – an impractical and resource-intensive task for non-custodial holders. Importantly, those seeking to seize your Bitcoin would first need to know that you actually own it. But held as a seed phrase, it is merely a thought in your mind. Unlike cash or gold, which can be physically discovered during searches, a memorized seed phrase leaves no trace. It is pure thought, invisible at checkpoints, robberies, or interrogations. There is no document to confiscate, no device to hack, and no vault to raid – just undetectable knowledge locked in the mind.

This makes Bitcoin uniquely resistant to seizure in ways traditional assets cannot match. Bitcoin transcends the limitations of physical assets. It is globally transferable, divisible, and verifiable, all while remaining unseizable by third parties as long as you control your private keys. Thus, Bitcoin is humanity's preeminent bearer asset.

Censorship Resistance: Censorship resistance is not just a technical feature of Bitcoin. It is the foundational principle that transforms money from a tool of control into an instrument of individual financial freedom. It means that no single entity – whether a government, corporation, bank, or even a coalition of powerful actors – can arbitrarily prevent, block, or reverse a valid Bitcoin transaction. This stands in stark contrast to traditional financial systems, where intermediaries like banks, payment processors, or governments hold the power to freeze accounts, deny transactions, or seize funds at will.

If you attempt to send money through a bank or service like PayPal, it could be halted for reasons ranging from "suspicious activity" to compliance with sanctions, political directives, or even algorithmic errors. With Bitcoin, as long as your transaction adheres to the network's consensus rules – such as having sufficient funds and a valid signature – it will

be confirmed and stored immutably on the blockchain. There is no central “off switch,” no boardroom veto, and no governmental decree that can unilaterally stop it. Censorship resistance is not merely a convenience – it is survival for those in oppressive environments and insurance for everyone else.

Because financial access is increasingly weaponized, censorship resistance is necessary for preserving personal autonomy, privacy, and economic freedom. Traditional finance is built on trust in centralized institutions, but that trust is fragile and often abused. Governments and banks can – and do – use money as an instrument for social control, punishing dissent, enforcing policies, and protecting entrenched interests. This vulnerability manifests in several critical ways.

- **2022 Canadian Trucker Protests:** The “Freedom Convoy” emerged in January 2022 as truckers and supporters rallied against COVID-19 vaccine mandates for cross-border travel, paralyzing Ottawa for weeks and inspiring global solidarity actions. In a drastic response, Prime Minister Justin Trudeau invoked the Emergencies Act on February 14 – the first time since its 1988 inception – granting authorities unprecedented powers without parliamentary approval, including freezing bank accounts linked to protesters.

Over 200 accounts holding approximately \$7.8 million Canadian dollars were frozen, affecting not just active demonstrators but also donors who contributed as little as \$20 via platforms like GoFundMe and GiveSendGo, which were shut down under government pressure. This financial weaponization, later ruled unconstitutional by a federal court in January 2024 for violating rights to free expression and protection from unreasonable search, left individuals unable to access their own funds for essentials, demonstrating how centralized systems can swiftly crush dissent.

Organizers pivoted to Bitcoin, raising over 21 BTC through a decentralized campaign called “HonkHonkHODL.” Despite police attempts to blacklist 34 crypto wallets and seize some funds via compliant exchanges, self-custodied Bitcoin in private wallets proved unstop-

pable and unseizable. Authorities could recover only about 5.5 BTC because the network’s permissionless nature allowed donors worldwide to bypass controls entirely. This not only sustained the protests but proved to the world Bitcoin’s censorship resistance. No court order or decree could halt valid transactions, ultimately forcing the government to release accounts after just days of emergency measures.

- **WikiLeaks’ Survival via Bitcoin (2010):** In late 2010, WikiLeaks released thousands of classified U.S. diplomatic cables and war logs, exposing government secrets and sparking global outrage. In retaliation, under intense U.S. pressure, major financial giants – including Bank of America, Visa, MasterCard, PayPal, and Western Union – imposed an extralegal blockade starting December 7, freezing all donations and payments to the organization without formal charges or court orders. This “financial death penalty” crippled WikiLeaks, slashing revenues by 95% and depleting cash reserves from over €800,000 to near zero, threatening its very existence as traditional banking intermediaries bowed to political demands. Founder Julian Assange described it as a “war on journalism,” with the blockade persisting for years and costing millions in lost donations.

Desperate, WikiLeaks turned to Bitcoin in June 2011, publicly accepting donations via Bitcoin’s censorship-resistant network that no entity on Earth can unilaterally shut down. Thousands of Bitcoins flowed in, bypassing the blockade entirely through peer-to-peer transfers. This lifeline not only sustained operations but also yielded a staggering 50,000% return on early investments, as Assange later boasted. This episode vividly demonstrates how Bitcoin safeguards truth-tellers against coordinated financial strangulation, where traditional centralized financial institutions utterly fail.

- **Nigeria’s #EndSARS Protests (2020–2021):** Sparked by a viral video of police brutality in October 2020, the #EndSARS movement mobilized millions of Nigerian youth against the notorious Special Anti-Robbery Squad (“SARS”), which was accused of extortion, torture, and extrajudicial killings. Protests erupt-

ed in major cities like Lagos, drawing international attention and endorsements from prominent figures like Twitter CEO Jack Dorsey. The government responded with lethal force – soldiers killed at least 12 unarmed protesters at Lekki Toll Gate on October 20 – and financial repression, freezing bank accounts of key activists and blocking donation platforms like Flutterwave. A February 2021 central bank ban on crypto transactions was intended to choke off funding, labeling the movement a threat to stability.

In response to the Nigerian government’s move to sever traditional funding channels during the #EndSARS protests, the Feminist Coalition (“FemCo”), a group of young women, began to distribute donations via Bitcoin and other cryptocurrencies. FemCo successfully raised over \$150,000 in Bitcoin as part of a larger donation drive and provided aid transparently. The group’s disbursements included more than 40 million Naira (equivalent then to about \$96,000 USD) to support victims of police brutality and their families, medical supplies for injured protesters, legal fees for detainees, and mental health support. Bitcoin’s borderless, unstoppable transfers evaded the government repression, sustaining the resistance movement for months.

- **Hong Kong Pro-Democracy Protests (2019):** Triggered by a controversial extradition bill in June 2019 that threatened to erode Hong Kong’s autonomy by allowing transfers to mainland China, protests escalated into a massive pro-democracy uprising. Over two million people – nearly a third of the population – marched peacefully at its peak. Beijing-backed authorities cracked down harshly, arresting over 10,000 people, deploying tear gas, rubber bullets, and even live rounds, while surveilling bank transactions to identify and punish supporters. Traditional funding dried up as banks flagged “suspicious” donations.

Protesters and sympathizers responded by turning to Bitcoin to fund essentials anonymously. Bitcoin trading volumes surged amid the unrest, as residents sought financial escape from capital controls. This decentralized lifeline resisted Beijing’s grip, enabling sustained resistance for over a year despite escalating violence and a national security law in 2020 that criminalized dissent. Bitcoin’s

role during this episode demonstrates its indispensability for freedom fighters, providing untraceable, unseizable, and unstoppable support when traceable fiat flows result in arrest and persecution.

- ✦ **Iran and Russia Bypassing Sanctions (2023–2025):** Amid escalating U.S. sanctions crippling access to SWIFT and global trade, Iran and Russia turned to Bitcoin and crypto as lifelines, transacting billions despite the financial sanctions. Iran legalized crypto mining in 2019 and imports via digital assets in 2022, with citizens flocking to exchanges amid 40% inflation and currency devaluation.

Russia, post-2022 Ukraine invasion, faced the harshest sanctions in history. This prompted Russia to enact legislation in 2024 to integrate crypto into cross-border payments, bypassing the dollar-dominated global financial system. Crypto volumes spiked, with Russian entities like Garantex (a sanctioned exchange) facilitating billions in transactions, and overall flows from sanctioned jurisdictions reaching \$15.8 billion in 2024. Bitcoin's key role enabled imports of vital goods by evading Western financial blocks. For instance, Russia piloted crypto payments with allies like Iran for energy trades. Despite U.S. efforts to sanction wallets and exchanges, Bitcoin's decentralized network thwarted full enforcement, as peer-to-peer trades and non-KYC platforms proliferated. This surge in Bitcoin and crypto use sustained economies under siege and also proved Bitcoin's geopolitical invincibility, allowing nations and individuals to reclaim financial sovereignty against hegemonic controls.

- ✦ **United States – Operation Chokepoint 2.0:** Censorship resistance is also relevant and necessary even in highly developed democratic nations. In the U.S., Operation Chokepoint 2.0 exemplifies the insidious nature of financial censorship within traditional banking systems, where regulators under the Biden administration subtly but effectively pressured financial institutions through opaque guidance, indirect pressure, the suggestion of heightened oversight, and the weaponization of “reputational risk” to debank or unbank crypto-related companies solely because of their involvement in digital assets, without any evidence of wrongdoing or heightened risk.

These are not companies engaged in illicit activities but rather law-abiding enterprises whose sole “crime” is their involvement with cryptocurrencies. This systematic denial of essential banking services – from basic deposit accounts to credit lines – effectively cuts these companies off from the traditional financial system simply because of the nature of their business. Such actions, driven by political opposition rather than explicit legal prohibitions, represent a clear case of viewpoint or content-based debanking, which is the very definition of financial censorship. It illustrates how traditional finance, even in a supposed bastion of free markets, can be coerced into stifling innovation and limiting financial freedom for entire industries deemed disfavored by those in power. Bitcoin, by operating entirely outside this centralized and censorable framework, stands as the ultimate countermeasure, ensuring that legitimate economic activity cannot be shut down by arbitrary decrees or behind-the-scenes pressure campaigns.

This modern iteration of the original Operation Chokepoint, which targeted

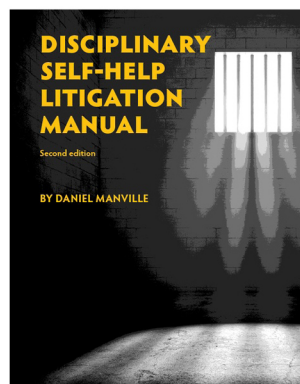
industries like payday lending, weaponized vague notions of reputational risk and supervisory guidance from agencies like the FDIC and Federal Reserve to coerce banks into terminating relationships with legitimate crypto firms, stifling innovation and excluding an entire sector from essential services such as payment processing and custodial accounts.

High-profile cases, including the denial of master accounts to banks like Custodia and widespread closures affecting over 30 tech and crypto founders, highlight how this debanking was not about compliance but viewpoint discrimination – punishing businesses that challenge centralized finance and promote decentralization, effectively censoring economic participation based on ideological grounds. Such actions underscore the vulnerability of traditional systems to political interference, where access to money can be revoked arbitrarily, reinforcing Bitcoin's primacy as a censorship-resistant alternative that operates beyond the reach of biased regulators and gatekeepers.

Disciplinary Self-Help Litigation Manual, Second Edition, by Dan Manville

By the co-author of the *Prisoners' Self-Help Litigation Manual*, this book provides detailed information about prisoners' rights in disciplinary hearings and how to enforce those rights in court.

Now available from Prison Legal News Publishing.
\$49.95, shipping included



Order by mail, phone or on-line.

By: ☐ check ☐ credit card ☐ money order

Name: _____

DOC/BOP Number: _____

Institution/Agency: _____

Address: _____

City: _____ State: _____ Zip: _____



Human Rights Defense Center
Dedicated to Protecting Human Rights

PO Box 1151 • Lake Worth Beach, FL 33460
Tel 561-360-2523 • www.prisonlegalnews.org

Operation Chokepoint 2.0 was financial suppression disguised as risk management. By weaponizing the banking system against lawful crypto businesses, regulators exposed the deep flaws in a financial infrastructure that can be manipulated to exclude dissenters and innovators at will. This campaign of debanking revealed a dangerous truth: even in advanced democracies, the tools of censorship are not confined to speech but extend to economic participation, where access to capital can be revoked without due process or recourse because there was no meaningful way for any individual firm or person targeted to appeal or challenge the debanking. In an era of increasing financial surveillance, exclusion, and control, Bitcoin stands as the only globally viable censorship resistant monetary network.

- **Trump family:** The Trump family's recent experience with debanking represents a high-profile example of financial censorship in the U.S. In a recent interview on CNBC's "Squawk Box" as well as at the Bitcoin Conference 2025, Donald Trump Jr. explained that his family ventured into Bitcoin and cryptocurrency out of sheer necessity following their debanking by traditional financial institutions in New York City, which he attributed to their political involvement after entering politics. He recounted how, prior to this, he could easily secure loans from any banker for real estate projects, but suddenly, calls went unanswered, financing dried up, and they were effectively excluded from the system, leading him and his brother Eric to realize that the traditional financial structure is an "undemocratized pyramid scheme" where access depends on favor rather than merit. This realization, compounded by what the family perceived as political persecution through subpoenas, drove them to fully embrace Bitcoin and other decentralized cryptocurrencies.

These examples of real-world financial censorship prove that Bitcoin's censorship resistance is not merely a theoretical benefit but a practical necessity for safeguarding economic freedom and free speech. The recurring pattern of financial censorship reveals one

undeniable truth: any system controlled by centralized authorities will inevitably be weaponized against dissenters and the unpopular. Whether under the guise of "national security," "reputational risk," or outright political retaliation, governments and financial institutions have repeatedly demonstrated their willingness to silence opposition by cutting off access to money, which is the lifeblood of modern existence. The Canadian Trucker Protests debacle, the WikiLeaks financial blockade, and the targeted debanking of crypto firms under Operation Chokepoint 2.0 all reveal the same chilling reality: when money is controlled by centralized power, it controls everything.

However, in every case, Bitcoin emerged as the ultimate countermeasure – a decentralized financial system impervious to authoritarian control. It cannot be frozen like a bank account, seized like property, or silenced like a dissident. It operates beyond the reach of politicians, regulators, and corporate gatekeepers, ensuring that no government or bank can unilaterally decide who participates in the economy. From Nigeria's #EndSARS protesters to Russian and Iranian sanctions circumvention, Bitcoin has repeatedly proven itself as the world's only bastion of financial sovereignty. Its decentralized architecture is not a flaw but its greatest strength – a safeguard against the inevitable corruption of centralized power. As the world accelerates inexorably toward digital authoritarianism, Bitcoin stands as the battle-tested apex censorship-resistant alternative.

Pseudonymity and Privacy:

What it means: When you engage in a Bitcoin transaction, your real name, address, or any directly identifiable information is not openly attached to that transaction. Instead, the system uses Bitcoin addresses. These addresses are unique, alphanumeric strings of characters – like 1BvBMSEYstWetqT-Fn5Au4m4GFg7xJaNVN2. They are what appear on the public ledger, recording the movement of Bitcoin from one address to another. While everyone can see that address A sent 2 BTC to address B on the public blockchain, they do not automatically know that address A belongs to "John Smith" or that address B is owned by "Jane Doe."

This creates a layer of separation between your real-world identity and your Bitcoin activity. This separation is key: your real identity remains hidden unless you voluntarily reveal it, for example, by publicly sharing your address on social media, linking it to a known

email during a purchase, or using an exchange that requires ID verification.

However, it is important to understand why this is referred to as "pseudonymity" rather than "anonymity." While your name is not directly on the ledger, there are ways that your real identity can be linked to your Bitcoin addresses. For example:

- **Exchange KYC/AML:** If you buy Bitcoin from a regulated exchange (like Coinbase, Binance, Kraken, etc.), you will almost certainly have to go through Know Your Customer ("KYC") and Anti-Money Laundering ("AML") checks. This involves providing your government ID, proof of address, and other personal information. The exchange then links your real identity to the Bitcoin addresses they use to send you your Bitcoin or receive Bitcoin from you.
- **On-chain analysis:** Sophisticated analytical tools and techniques can be used to "de-anonymize" Bitcoin transactions. This involves tracing the flow of funds, identifying common spending patterns, linking addresses that belong to the same entity, and correlating on-chain data with off-chain information (like public social media posts where someone mentions their Bitcoin address or leaked data). For instance, if an address consistently receives funds from an exchange you used or sends funds to a merchant where you provided personal details, your identity could potentially be inferred.
- **Voluntary revelation:** You might choose to reveal your Bitcoin address yourself, perhaps to receive payments for goods or services or to show your support for a cause. Once you do this, that address is no longer pseudonymous in relation to you.

Therefore, "pseudonymity" accurately describes the situation. You operate under a pseudonym (your address), but that pseudonym can potentially be linked back to your true identity through various means.

Why it is important: Pseudonymity in Bitcoin is crucial because it provides a level of privacy and protection against unwanted surveillance that does not exist in centralized financial systems. In traditional banking, every transaction is linked directly to your personal identity. Your bank account is tied to your name, address, Social Security number, and more. This means banks, governments, payment processors, and even hackers can track

your every financial move. For instance, when you use a credit card, details like what you bought, where, and when are recorded and often shared with third parties for purposes like targeted advertising or credit scoring.

Bitcoin takes the opposite approach by decoupling transactions from identities, acting as a firewall against such vulnerabilities. This privacy is not just a nice feature; it is essential in a world where financial data is increasingly weaponized. In places like Venezuela or Belarus, where governments monitor bank accounts to suppress opposition, Bitcoin allows people to receive donations or pay for necessities without revealing their identities, potentially avoiding arrest and persecution. Everyday users benefit too. Bitcoin enables people to avoid the constant data exploitation by big tech companies that track your spending to build alarmingly detailed profiles for ads.

This pseudonymity becomes even more vital when comparing Bitcoin to CBDCs, which are designed for efficiency but also with built-in tracking capabilities. In a CBDC world, every transaction can be monitored in real-time by authorities, enabling total surveillance – where your coffee purchase or

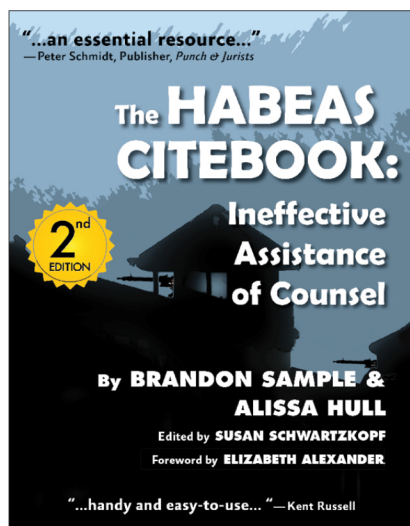
charitable donation is logged and analyzed for compliance, taxation, or even social scoring. Bitcoin prevents this by providing a decentralized alternative where no single entity controls the ledger, and privacy is preserved through pseudonymity. Ultimately, Bitcoin's pseudonymity enables users to control their own data, reducing risks of exploitation, censorship, and overreach, making Bitcoin not just a currency but a tool for personal sovereignty in an increasingly mass-surveilled digital age.

Permissionless and Globally Accessible:

What it means: "Permissionless" refers to the fundamental design of the Bitcoin network that allows anyone to join, use, or build upon it without needing approval from any central authority, such as a bank, corporation, or government. Unlike traditional financial systems where you need to provide personal identification, undergo background checks, or get explicit permission to open an account or make transactions, Bitcoin operates on a decentralized blockchain – a public, distributed ledger that records all transactions transparently and securely. To participate, all

you need is access to the internet and a basic digital wallet (which can be created for free via software on your phone or computer in minutes). This wallet generates a unique Bitcoin address (like a digital bank account number) that lets you send or receive Bitcoin instantly, without intermediaries verifying your identity or eligibility.

"Globally accessible" builds on this by emphasizing that Bitcoin transcends national borders and geographical limitations. The network is powered by thousands of computers (called nodes) spread across the world, ensuring that as long as you have an internet connection – whether through a smartphone in a remote village or a high-speed fiber optic line in a city – you can interact with it. This includes not just transacting (buying, selling, or transferring Bitcoin) but also innovating. Developers anywhere can write code to create new applications, tools, or even improvements to the Bitcoin protocol itself, all without seeking permission. For instance, someone in a developing country could build a Bitcoin-based payment app tailored to local needs, and it could integrate seamlessly with the global network. This openness stems from Bitcoin's



The Habeas Citebook (2nd edition)

by Brandon Sample and Alissa Hull

The second edition of *The Habeas Citebook* is now available! Published by Prison Legal News, it is designed to help pro-se prisoner litigants identify and raise viable claims for potential habeas corpus relief.

This book is an invaluable resource that identifies hundreds of cases where the federal courts have granted habeas relief to prisoners whose attorneys provided ineffective assistance of counsel. It will save litigants thousands of hours of research and it focuses on the winning cases criminal defendants need to successfully challenge their convictions.

Well organized into 52 concise chapters, this easy-to-use book puts the law at the reader's fingertips.

Price: \$49.95
(shipping included)
275 pages

Order by mail, phone, or online.

Amount enclosed for *Habeas Citebook* _____ By: ☐ check ☐ credit card ☐ money order

Name: _____ DOC/BOP Number: _____

Institution/Agency: _____

Address: _____

City: _____ State: _____ Zip: _____



Human Rights Defense Center
Dedicated to Protecting Human Rights

PO Box 1151 • Lake Worth Beach, FL 33460 • Phone # 561-360-2523
WWW.PRISONLEGALNEWS.ORG • WWW.CRIMINALLEGALNEWS.ORG

What Is Bitcoin? (cont.)

open-source nature, meaning its underlying code is publicly available for anyone to inspect, modify, or expand upon, encouraging a collaborative ecosystem.

In essence, permissionless and global accessibility democratize finance and technology, turning Bitcoin into a truly inclusive system where entry barriers are minimal, and participation is limited only by your access to basic technology, not by gatekeepers.

Why it is important: These features are crucial because they address deep-rooted inequalities in the global financial system by empowering individuals who are often excluded from traditional banking and enabling unrestricted innovation that drives progress.

Around the world, an estimated 1.3 billion adults remain “unbanked,” meaning they lack access to basic financial services like savings accounts, loans, or secure ways to send money. This is particularly acute in regions like Sub-Saharan Africa, where approximately 42% of adults are unbanked due to factors such as remote locations, lack of infrastructure, or stringent requirements from banks (e.g., needing proof of income or residency). Bitcoin changes this by allowing anyone with a smartphone and internet (which is increasingly common even in low-income areas via affordable data plans) to store value, make payments, or receive remittances from family abroad without high fees or delays. For example, a farmer in rural Kenya could receive payment for crops directly in Bitcoin from an international buyer, bypassing expensive wire transfers that might take days and cost 7-10% in fees through services like Western Union. This not only saves money but also provides a hedge against local currency inflation or instability – common in places like Venezuela or Zimbabwe, where hyperinflation has eroded savings in fiat money.

Additionally, this permissionless nature stands in stark opposition to CBDCs, which are digital versions of fiat money controlled by governments. While CBDCs promise efficiency, they can introduce restrictions, such as programmable money that expires after a certain time, spending limits based on user behavior, or built-in surveillance to track every transaction for tax or security purposes. Bitcoin stands as a direct counterpoint, encouraging “permissionless innovation” where solutions emerge organically from a global

community, driven by problem-solving rather than centralized directives. This resistance to top-down control ensures that the network and its applications can evolve freely, resulting in a truly open and dynamic financial future.

Path Dependence: The Reason a “New Bitcoin” Cannot Supplant the Original

In his thought-provoking essay, “The Number Zero and Bitcoin,” Robert Breedlove introduces the concept of path dependence to explain Bitcoin’s unique and unassailable position. He defines path dependence as “the sensitivity of an outcome to the order of events that led to it, implying that history has inertia.” He adds, “Path-dependence entails that the sequence of events matters as much as the events themselves ... you get a dramatically different result if you shower and then dry yourself off versus if you dry yourself off first and then shower.”

This irreversible sequencing is akin to the invention of zero itself. Once discovered in ancient India and integrated into global mathematics, zero became the irreplaceable foundation for all numerical systems, rendering any “new zero” inconceivable and obsolete from the start. Just as zero’s emergence did not merely create a new number but fundamentally changed our understanding of numbers and unlocked exponential advancements in calculation, science, and technology – transforming human civilization forever – the discovery of Bitcoin has irreversibly established absolute digital scarcity, making any subsequent attempt to “rediscover” it futile in a world in which it already exists.

Breedlove states that Bitcoin’s emergence into a world devoid of any comparable digital, decentralized money created a non-replicable historical sequence, thereby making “Bitcoin’s path-dependence ... a key factor protecting it from disruption.” That is, now that Bitcoin exists, it is not possible for any “New Bitcoin” to enter a world that does not already contain Bitcoin and its virtually insurmountable first-mover advantage coupled with inertia. He points out that “U.S. citizens saw path-dependent pushback firsthand when their government made a failed attempt to switch to the metric system back in the 1970s.”

Bitcoin Discovered in Nonreplicable True “State of Zero”

Path dependence here acts as an impregnable barrier for any would-be New Bitcoin. Unlike any attempt to launch a New Bitcoin in

today’s saturated market, Bitcoin emerged from a true “state of zero” in digital money, which can never be repeated because this “state of zero” will never exist again. Bitcoin’s unrepeatable genesis – a truly fair launch without premining or centralized control in a true “state of zero” – is a singular historical anomaly. This irreversible historical inertia of Bitcoin’s launch has resulted in organic, global adoption that no engineered “upgrade” can retroactively match.

Additionally, this inertia is amplified by powerful network effects, where Bitcoin’s value scales exponentially with its user base per Metcalfe’s Law, which posits that the value or utility of a network grows proportionally to the square of the number of its connected users or nodes, resulting in exponential benefits from network effects. For example, think of a social media platform: the more people who join, the more valuable it becomes because each new user can connect with everyone else, creating exponentially more interactions and benefits.

These network effects extend beyond mere size. Bitcoin’s decentralized hash power secures the ledger with unprecedented energy expenditure, making it the most tamper-proof asset in history, while its liquidity ensures seamless global exchange – qualities that compound over time, much like zero’s placeholder function enabled scalable numerals that revolutionized commerce and innovation.

A New Bitcoin would launch into a crowded landscape already dominated by Bitcoin. As the largest, most secure, and most liquid network, Bitcoin attracts more participants, creating a self-reinforcing cycle that deprives competitors of the impetus needed to achieve a critical mass of users. This dynamic mirrors the QWERTY keyboard layout phenomenon. Despite more efficient alternatives like Dvorak, path dependence and network effects have locked in QWERTY as the global standard, even though it was designed to slow typists down on old mechanical typewriters to prevent key jams.

The reason QWERTY cannot be replaced is not due to its technical superiority (it is demonstrably less efficient for modern typing) but because of the immense switching costs and network effects that have accumulated over a century. Millions of people have learned to type on QWERTY keyboards, building deep muscle memory and ingrained habits. Manufacturers produce billions of QWERTY keyboards, and software is universally designed for this layout. To switch

to a new, more efficient layout like Dvorak would require a massive, coordinated effort for everyone to relearn typing, for all keyboards to be redesigned, and for all software to adapt. The individual cost of relearning and the collective cost of coordinating such a global change are astronomically high, outweighing any potential efficiency gains.

Network Effects and Switching Costs Defend Bitcoin's Reign

Similarly, any New Bitcoin would struggle futilely to overcome Bitcoin's established user base, developer community, and the vast infrastructure built around it. The sheer weight of Bitcoin's existing network effects – the millions of users, thousands of businesses, robust security, and deep liquidity – means that even if a New Bitcoin offered technical improvements, the prohibitive cost and collective effort required to migrate trillions of dollars in value and millions of users would still render it effectively impossible to supplant the original. Unless a New Bitcoin were so vastly and indisputably superior to Bitcoin in genuinely meaningful ways, there is simply no reason for the world to abandon Bitcoin for something that is merely a minor or even

moderate improvement. The switching costs are simply too prohibitive.

The "invention of Bitcoin represents the discovery of absolute scarcity, or absolute irreproducibility, which occurred due to a particular sequence of idiosyncratic events that cannot be reproduced," Breedlove declares. Even if a New Bitcoin could mirror Bitcoin's scarcity, holders would inevitably gravitate towards the asset with the greatest liquidity, network security, and established network effects, ultimately leading them to "dump the 'New Bitcoin' for the original." The market has overwhelmingly validated this prediction: 44 separate hard forks have attempted to dethrone Bitcoin by promising superior scalability, privacy, or mining accessibility, but none has done so.

These New Bitcoins have featured various technical "improvements," but the market simply did not care. The vast majority of these New Bitcoins have failed to gain traction and are no longer operational due to low adoption and market irrelevance. Today, only four – Bitcoin Cash (BCH), Bitcoin SV (BSV), eCash (XEC), and Bitcoin Gold (BTG) – remain active, yet their market performance has delivered a brutal verdict. On August 1, 2025, while Bitcoin traded at approximately

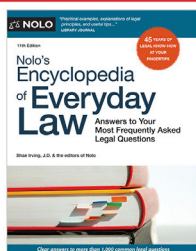
\$115,120, these surviving forks floundered far behind: BCH at \$607, BSV at \$26.55, BTG at \$0.54, and XEC at a mere \$0.00002187. Beyond their underwhelming valuations, these New Bitcoins remain mired in obscurity and irrelevance – outside of crypto circles, they are little more than footnotes in Bitcoin's history. This massive disparity underscores just how powerful network effects and switching costs are in defending Bitcoin's reign.

Bitcoin mirrors zero's singular discovery – both are foundational breakthroughs that, once integrated, defy replication due to their path-dependent origins and amplifying network effects. To supplant Bitcoin would require not just meaningful technical superiority but rewriting history itself – an impossibility that ensures its dominance as the apex predator of monetary systems, commanding the world to use it rather than an inferior imitation.

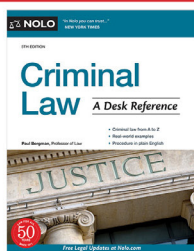
Bitcoin's Growth Spurt: Forks, Fights, and Financial Inroads (2015-2020)

The period from 2015 to 2020 marked Bitcoin's transition from a niche experiment to a globally recognized asset class. These

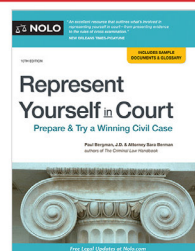
Great Self-Help Books



Encyclopedia of Everyday Law
\$34.99



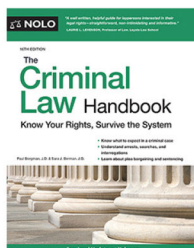
Criminal Law A Desk Reference
\$44.99



Represent Yourself in Court
\$39.99



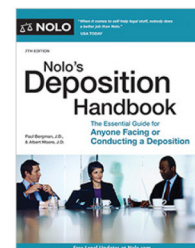
Win Your Personal Injury Claim
\$34.99



Criminal Law Handbook
\$49.99



Legal Research
\$49.99



Deposition Handbook
\$34.99

Order from Prison Legal News
Add \$6 shipping for orders under \$50

Prison Legal News

PO Box 1151

Lake Worth Beach, FL 33460

Phone: 561-360-2523

www.prisonlegalnews.org



NOLO YOUR LEGAL COMPANION

years were defined by scaling debates, regulatory battles, infrastructure growth, and the early seeds of institutional adoption. Despite intense volatility, skepticism, and criticism, Bitcoin's network and community proved yet again that both are antifragile. These years laid the groundwork for Bitcoin's eventual mainstream acceptance, though not without some bruising growing pains.

The Block Size War

By 2015, Bitcoin was recovering from the Mt. Gox collapse, with prices stabilizing around \$200 – \$300. However, a critical issue emerged – the network's capacity to handle growing transaction volumes. Bitcoin's 1 MB block size limit, designed to prevent spam and ensure decentralization, was becoming a bottleneck as adoption grew. Transactions could take longer to confirm, and fees started to rise, challenging Bitcoin's narrative as "peer-to-peer electronic cash." This sparked a heated and deeply ideological debate on scaling within the Bitcoin community known as the "Block Size War."

Two factions emerged: (1) "big blockers" – those favoring larger blocks to increase transaction throughput (supported by figures like Gavin Andresen and Mike Hearn) and (2) "small blockers" – those prioritizing decentralization and security, advocating for off-chain solutions like the Lightning Network (backed by developers like Gregory Maxwell and Luke Dashjr). The small blockers argued that a larger block size would lead to greater centralization because fewer entities would be able to run full nodes. Larger blocks would also compromise security and deviate from Bitcoin's core principles of decentralization. The debate became heated on Bitcoin talk and Reddit, exposing ideological fault lines between pragmatists and purists.

On July 9, 2016, Bitcoin underwent its second halving that reduced the block reward for miners from 25 BTC to 12.5 BTC. This further reinforced Bitcoin's scarcity model, making it even more appealing as a digital gold and a hedge against inflation. While the immediate price impact was not always dramatic, the halving events consistently precede significant bull markets in the subsequent years, demonstrating their long-term influence on Bitcoin's supply dynamics.

The ideological schism between big blockers and small blockers culminated in a

contentious "hard fork" on August 1, 2017. Dissatisfied with the pace and direction of Bitcoin's scaling solutions, a group of developers and miners created Bitcoin Cash. This new cryptocurrency essentially copied Bitcoin's entire transaction history up to that point but implemented an increased block size (initially 8MB and later more). Anyone holding Bitcoin at the time of the fork automatically received an equal amount of Bitcoin Cash. The emergence of Bitcoin Cash highlighted the decentralized nature of open-source projects, where fundamental disagreements can lead to entirely new chains, and underscored the power of consensus (or lack thereof) in a decentralized network. The fork also created a new dynamic where "fork coins" became a common occurrence in the cryptocurrency landscape.

On August 24, 2017, Bitcoin activated Segregated Witness ("SegWit") through a "soft fork." SegWit was a backward-compatible upgrade that separated transaction signatures (the "witness" data) from the transaction data, effectively increasing the transaction capacity of each block without increasing the physical block size. This was a monumental technical achievement, demonstrating the community's ability to upgrade the protocol in a backward-compatible manner.

Following the contentious split, the proponents of Bitcoin Cash sought to fulfill their vision of its becoming the dominant global digital currency by prioritizing larger block sizes. However, despite its technical modifications designed for faster, cheaper transactions, Bitcoin Cash's fortunes diverged dramatically from Bitcoin's. While Bitcoin Cash initially saw a surge in value and support from a segment of the community, it ultimately failed to rival Bitcoin's dominance. Its price, hash rate, and overall adoption have remained a tiny fraction of Bitcoin's. This outcome serves as solid evidence of path dependency and network effects defending the primacy of Bitcoin. The Bitcoin Cash fork demonstrates that while code can be copied and allegedly improved upon, the decentralized, organic network that has formed around Bitcoin is incredibly resilient and impossible to replicate, cementing Bitcoin's position as the undisputed leader.

The ICO Boom and Emergence of Institutional Interest

Despite the internal community strife, Bitcoin's public profile soared in 2017, culminating in an unprecedented bull run. From under \$1,000 at the start of the year, Bitcoin's

price surged to nearly \$20,000 by December, attracting global media attention and a new wave of retail investors. This parabolic rise firmly established Bitcoin in the public consciousness as a speculative asset with immense potential, leading to what many now refer to as the "ICO boom" (initial coin offering) as countless new cryptocurrencies emerged with little more than a whitepaper and a promise, hoping to emulate Bitcoin's success.

However, the ICO boom was short-lived. Many projects were revealed to be scams or simply unsustainable, and the market entered a prolonged "crypto winter" in 2018. Bitcoin's price plummeted, along with the vast majority of altcoins, leading to widespread investor losses and renewed skepticism from traditional finance and regulators. This period intensified calls for clearer regulatory frameworks, as governments grappled with how to classify and oversee this burgeoning digital asset class.

Nevertheless, despite the bear market, the period from 2018 to 2020 marked a significant shift in how traditional institutions viewed Bitcoin. While previously dismissed as a niche technology for libertarians and illicit activities, its resilience, increasing liquidity, and growing technological maturity began to attract serious attention. For example, Bakkt, a regulated digital asset platform and custody service launched by Intercontinental Exchange, the parent company of the New York Stock Exchange, began offering physically-settled Bitcoin futures in September 2019. This was a crucial step towards providing institutional-grade infrastructure for Bitcoin, signaling a growing acceptance by traditional finance.

Towards the end of 2020, publicly traded companies began to allocate portions of their treasury reserves to Bitcoin. MicroStrategy (now known as "Strategy"), led by CEO Michael Saylor, famously announced on August 11, 2020, that it had purchased 21,454 BTC for an aggregate purchase price of \$250 million, making it the first publicly-traded company in the U.S. to adopt Bitcoin as a primary treasury reserve asset. In doing so, it characterized Bitcoin as a superior inflation hedge and store of value compared to traditional fiat currencies. This marked a turning point, signaling to other corporate treasuries that Bitcoin is a legitimate asset for balance sheet management.

The period closed with Bitcoin's third halving on May 11, 2020. With the block reward further reduced from 12.5 BTC to

6.25 BTC, the event once again underscored Bitcoin's programmatic scarcity as global economies grappled with the early stages of the COVID-19 pandemic and unprecedented monetary easing by central banks. In this environment, Bitcoin's narrative as a scarce, decentralized, and censorship-resistant digital gold gained significant traction. Both retail and institutional investors began to view Bitcoin as a hedge against economic uncertainty and inflation, accelerating its adoption and cementing its role as a recognized macroeconomic asset.

From 2015 to 2020, Bitcoin proved its resilience and adaptability. It successfully navigated vicious ideological battles, survived major network forks, and began to shed its niche reputation, attracting the attention of the general public as well as institutional investors. This era laid the groundwork for Bitcoin's continued expansion into the public consciousness and mainstream financial world. Each challenge faced by Bitcoin – scaling disputes, dramatic crashes, and regulatory crackdowns – actually strengthened its network and solidified its value proposition. Once again, Bitcoin proved to be the preeminent antifragile monetary system.

Central Bank Digital Currencies: The Antithesis of Bitcoin

In an era where governments and central banks are racing to digitize their fiat currencies, a civilizational battle for the future of money and freedom is unfolding – one that pits individual liberty against centralized control, financial privacy against pervasive surveillance, and self-sovereignty against state-imposed restrictions. At the heart of this struggle lies Bitcoin, the decentralized digital currency that stands as a defiant counterpoint to CBDCs. While Bitcoin empowers individuals with unprecedented control over their wealth, CBDCs threaten to entrench power in the hands of institutions, enabling governments to monitor, regulate, and even dictate the financial lives of their citizens. Bitcoin is not just a technological innovation but a critical bulwark against the encroaching dangers of state-controlled digital money.

Bitcoin emerged as a radical but necessary response to the failures of centralized financial systems. Its design is rooted in principles of decentralization, transparency, and immutability. Operating on a peer-to-peer network secured by cryptographic proofs, Bitcoin eliminates

the need for so-called trusted intermediaries like banks or governments. Its fixed supply of 21-million Bitcoins, enforced by code rather than human discretion, ensures that no authority can inflate its value away. Transactions are recorded on a public ledger visible to all yet pseudonymous, preserving user privacy unless explicitly linked to real-world identities. This architecture reflects a philosophy of trust in mathematics over trust in institutions.

In contrast, CBDCs are digital versions of fiat currencies issued and controlled by central banks. Unlike Bitcoin, CBDCs are inherently centralized, with their issuance, circulation, and oversight subject to the whims of monetary authorities. While proponents argue that CBDCs offer efficiency, financial inclusion, and modernized payment systems, their structure and design reveal a darker ambition: unprecedented surveillance and control over money and its users.

With CBDCs, every transaction occurs within a permissioned system, validated and recorded by the central bank or its designated intermediaries. This centralized ledger creates a comprehensive, real-time map of every financial interaction. The potential for pervasive, real-time state-sanctioned financial

PLN & CLN Subscription Bundles STAY INFORMED AND SAVE MONEY

Pricing Effective as of 6/30/2023

☐ 1 Year PLN & CLN Subscription Bundle

Prisoners/Individuals - \$74.00 (\$10.00 Savings), Professionals/Entities - \$170.00 (\$22.00 Savings)

☐ 2 Year PLN & CLN Subscription Bundle

Prisoners/Individuals - \$148.00 (\$20.00 Savings), Professionals/Entities - \$338.00 (\$46.00 Savings)

☐ 3 Year PLN & CLN Subscription Bundle

Prisoners/Individuals - \$222.00 (\$30.00 Savings), Professionals/Entities - \$508.00 (\$68.00 Savings)

☐ 4 Year PLN & CLN Subscription Bundle

Prisoners/Individuals - \$296.00 (\$40.00 Savings), Professionals/Entities - \$676.00 (\$92.00 Savings)



Name: _____ Amount enclosed: _____

DOC/BOP Number: _____ Facility: _____

Address: _____

City: _____ State: _____ Zip: _____



Human Rights Defense Center
Dedicated to Protecting Human Rights

PO Box 1151 • Lake Worth Beach, FL 33460 • Phone # 561-360-2523

WWW.PRISONLEGALNEWS.ORG • WWW.CRIMINALLEGALNEWS.ORG

surveillance is not a dystopian fantasy; it is an inherent design feature of the technology. The Bank for International Settlements, a key driver of CBDC research, explicitly highlights “programmability” and “identity-linked” accounts as core attributes enabling “more targeted and timely” policy interventions. The loss of financial privacy with CBDCs is not a side effect – it is a core feature.

This programmability opens a Pandora’s box of potential abuses. Imagine the potential abuses: money that expires to force spending during recessions (“use-it-or-lose-it” stimulus); money restricted to specific vendors or product categories (approved “healthy” food only); money that cannot be used for donations to disfavored groups or purchases in certain geographic regions; or money that can be “turned off” for individuals deemed politically problematic or simply out of favor. The technical capacity for such granular, behavioral control is actively being researched and developed under the banner of CBDCs. Once in place, the temptation for governments to leverage this tool for social engineering, political compliance, or enhanced punitive measures will be immense and, as history and human nature have repeatedly proven, irresistible.

The differences between Bitcoin and CBDCs are stark. Bitcoin is a system of rules without rulers, designed to resist interference. On the other hand, CBDCs are tools of rulers, built to enforce compliance. Bitcoin’s decentralized network of global miners ensures no single entity can alter its protocol without broad consensus. CBDCs, however, are subject to the policies of central banks and governments, which can change rules at will. These differences are not merely technical but philosophical: Bitcoin champions individual agency, while CBDCs prioritize institutional dominance.

Bitcoin’s greatest feature lies in its ability to grant individuals true financial freedom. By operating outside the control of any single government, corporation, or entity, Bitcoin allows users to transact without permission, store wealth without fear of seizure, and preserve privacy in an increasingly surveilled world. For dissidents in authoritarian regimes, Bitcoin has proven invaluable. In places like Venezuela, where hyperinflation has rendered fiat currency worthless, or in Belarus, where protesters faced frozen bank accounts, Bitcoin has enabled individuals to bypass state-controlled financial systems weaponized to

crush dissent. Its borderless nature means that a refugee fleeing persecution can carry their wealth in a memorized seed phrase, immune to confiscation at checkpoints.

CBDCs invert this framework. Far from empowering individuals, they hand governments a surveillance apparatus of unparalleled scope. Because CBDCs are digital and centralized, every transaction can be traced to an individual’s identity, creating a permanent record of their financial behavior. Such capabilities are not unique to authoritarian regimes. In democratic societies, CBDCs can enable governments to enforce policies like negative interest rates, compelling spending by penalizing saving, or to restrict purchases deemed undesirable – whether that is ammunition, political donations, or even certain types of food.

Bitcoin is far more than merely a monetary system. It is a choice; it is an act of resistance. For those who choose to take the “orange pill,” it offers individuals the ability to opt out of centralized financial systems. As the world marches inexorably towards digitized mass surveillance and comprehensive control, Bitcoin is the most effective technological countermeasure for preserving financial freedom and personal liberty.

Bitcoin’s Maturation: From Thought Experiment to Global Integration (2021–2025)

The years from 2021 to 2025 represented Bitcoin’s maturation from a disruptive idea squarely outside the Overton Window to a crucial element of global finance. The period was marked by explosive bull markets, devastating crashes, groundbreaking innovations, and pivotal regulatory milestones. Amid macroeconomic turbulence – including pandemics, inflation, and geopolitical tensions – Bitcoin experienced institutional adoption, nation-state level experiments, and technological upgrades. The period tested Bitcoin’s resilience, with price swings from under \$16,000 to over \$123,000, while reinforcing its narrative as digital gold. Despite scandals and skepticism, Bitcoin’s network grew stronger, attracting billions in institutional capital and laying the foundation for widespread integration into traditional financial systems across the globe.

The year 2021 began with Bitcoin riding the momentum from 2020’s halving. This surge was fundamentally driven by growing institutional interest, as the narrative of Bitcoin as digital gold gained significant traction amid global economic uncertainties

and aggressive monetary policies. Leading the way were publicly traded companies like MicroStrategy (now known as “Strategy”), under the leadership of Michael Saylor, who continued to make large Bitcoin purchases, effectively converting their corporate treasuries into Bitcoin. This pioneering strategy set a precedent, prompting other corporations to consider similar allocations. The most high-profile corporate adoption came from Tesla, led by CEO Elon Musk, which announced a \$1.5 billion Bitcoin purchase in February 2021 and briefly accepted Bitcoin for vehicle payments. While Tesla later paused Bitcoin payments citing environmental concerns, the initial endorsement brought immense global attention and validated Bitcoin’s potential as a transactional currency. Additionally, Coinbase’s direct listing on the NASDAQ stock exchange in April 2021 further legitimized the cryptocurrency industry.

Beyond corporate treasuries, the financial industry began to integrate Bitcoin. In February 2021, the Purpose Bitcoin ETF in Canada was launched. It was the first physically-backed Bitcoin ETF in North America, offering traditional investors a regulated and accessible way to gain exposure without direct custody. This milestone signaled Bitcoin’s integration into traditional finance.

An even more historic moment came in June when El Salvador, led by President Nayib Bukele, announced Bitcoin as legal tender, implementing it in September alongside a national wallet and mining initiatives powered by geothermal energy. This made El Salvador the first sovereign nation to adopt Bitcoin officially, holding thousands of Bitcoins on its balance sheet and reporting unrealized profits of approximately \$443 million as of July 2025. Bukele’s bold move inspired other countries, like the Central African Republic in 2022, and established Bitcoin’s potential as a tool for financial inclusion in emerging economies. El Salvador’s adoption of Bitcoin was highly controversial and met with unsurprising criticism from entrenched international financial bodies like the International Monetary Fund. Nevertheless, it marked a seminal moment in Bitcoin history by demonstrating its potential as a tool for national economic strategy.

It was not all positive news in 2021. In May, China’s full ban on cryptocurrency mining caused a 50% drop in Bitcoin’s hash rate as miners fled to friendlier jurisdictions like the U.S. and Kazakhstan. Despite this major setback, the Bitcoin network recovered swiftly and once more proved its decentralized antifragility.

THE PLRA HANDBOOK

Law and Practice under the Prison Litigation Reform Act

By John Boston

Edited by Richard Resch

The PLRA Handbook is the best and most thorough guide to the PLRA in existence and provides an invaluable roadmap to all the complexities and absurdities it raises to keep prisoners from getting rulings and relief on the merits of their cases. The goal of this book is to provide the knowledge prisoners' lawyers – and prisoners, if they don't have a lawyer – need to quickly understand the relevant law and effectively argue their claims.

Anyone involved in federal court prison and jail litigation needs *the PLRA Handbook* – lawyers, judges, court staff, academics, and especially, pro se litigants.

Although *the PLRA Handbook* is intended primarily for litigators contending with the barriers the PLRA throws up to obtaining justice for prisoners, it'll be of interest and informative for anyone wishing to learn how the PLRA has been applied by the courts and how it has impacted the administration of justice for prisoners. It is based primarily on an exhaustive review of PLRA case law and contains extensive citations.

John Boston is best known to prisoners around the country as the author, with Daniel E. Manville, of the *Prisoners' Self-Help Litigation Manual* – commonly known as the “bible” for jailhouse lawyers and lawyers who litigate prison and jail cases. He is widely regarded as the foremost authority on the PLRA in the nation.

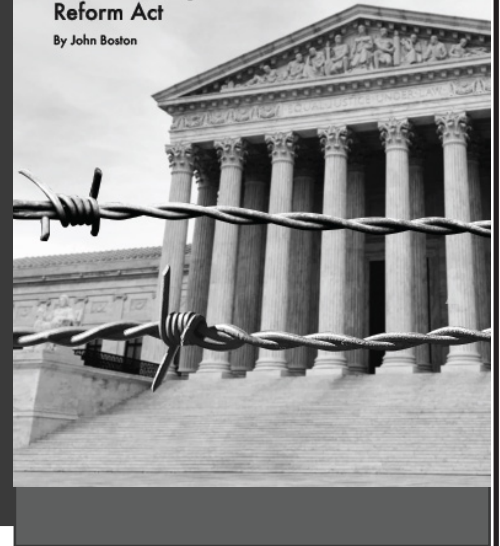
“If prisoners will review *The PLRA Handbook* prior to filing their lawsuits, it is likely that numerous cases that are routinely dismissed will survive dismissal for failure to exhaust.”

— Daniel E. Manville, Director, Civil Rights Clinic

THE PLRA HANDBOOK

Law and Practice under
the Prison Litigation
Reform Act

By John Boston



THE PLRA HANDBOOK

Paperback, 576 pages

Prisoners: \$84.95

Professionals: \$224.95

(includes shipping)

Order by mail, phone, or online. Amount enclosed _____

By: ☐ check ☐ credit card ☐ money order

Name _____

DOC/BOP Number _____

Institution/Agency _____

Address _____

City _____ State _____ Zip _____



Human Rights Defense Center
Dedicated to Protecting Human Rights

PO Box 1151 • Lake Worth Beach, FL 33460
Tel 561-360-2523 • www.prisonlegalnews.org

The Crypto Winter and Regulatory Crackdown

The euphoric highs of 2021 gave way to a challenging “crypto winter” in 2022 and early 2023. Bitcoin and the broader crypto market experienced a significant price correction triggered by a confluence of factors, including macro-economic headwinds, rising interest rates, and a series of high-profile collapses within the crypto industry. The contagion began in May 2022 with the collapse of Terra’s algorithmic stablecoin UST and its LUNA token, wiping out \$40 billion and exposing leveraged excesses. This triggered a domino effect: hedge fund Three Arrows Capital liquidated in June, crypto lender Celsius filed for bankruptcy in July after freezing withdrawals, and another prominent crypto lender, BlockFi, followed suit.

However, the year’s low point came in November with the implosion of FTX, the second-largest crypto exchange, amid revelations of rampant fraud and misuse of customer funds by founder Sam Bankman-Fried (“SBF”). FTX’s bankruptcy exposed \$8 billion in missing assets, leading to SBF’s arrest and eventual 25-year prison sentence in 2024 after a high-profile trial. These events shook confidence in the crypto market.

In the wake of these market upheavals, regulatory scrutiny intensified globally. Governments and financial watchdogs, particularly in the U.S., increased their efforts to establish clear frameworks for digital assets. The U.S. Securities and Exchange Commission (“SEC”), under Chair Gary Gensler, took an increasingly aggressive stance, though not always tethered to the law, asserting that many cryptocurrencies were unregistered securities and initiating numerous enforcement actions against crypto firms, which many critics and even courts characterized as an inappropriate strategy of “regulation by enforcement.” Once more, despite the market turmoil and regulatory hostility, the Bitcoin network itself continued to operate flawlessly, processing transactions and securing its ledger without interruption, reinforcing its fundamental resilience and decentralization.

The ETF Tsunami and the Fourth Halving

The year 2024 emerged as another landmark year for Bitcoin, largely dominated by two

significant events: the approval of spot Bitcoin ETFs in the U.S. and the fourth Bitcoin halving.

After years of rejections and legal challenges, the SEC finally approved several spot Bitcoin ETFs on January 10, 2024. This decision opened the floodgates for traditional investors, allowing them to gain direct exposure to Bitcoin through regulated and familiar investment vehicles offered by major asset managers like BlackRock (the world’s largest asset manager with AUM of about \$11.5 trillion in 2024), Fidelity, and Franklin Templeton. The launch of these ETFs triggered an unprecedented influx of institutional capital into the Bitcoin market, pushing its price to new all-time highs and signaling a profound shift in how Wall Street viewed Bitcoin. In fact, the demand for Bitcoin exposure was so great that BlackRock’s Bitcoin ETF reached \$50 billion AUM in an astounding 227 trading days, shattering the previous ETF record of 1,323 trading days.

Adding to the bullish momentum, the fourth Bitcoin halving occurred on April 20, 2024 UTC (April 19, 2024 EDT). This automatically reduced the block reward for miners from 6.25 BTC to 3.125 BTC. The supply shock further reinforced Bitcoin’s inherent scarcity, reducing its issuance rate at a time of surging demand. Historically, halvings have been catalysts for significant price appreciation in the subsequent months, and the 2024 halving continued this trend, contributing to the renewed enthusiasm and price surges observed throughout the year. The halving also intensified the focus on mining efficiency and the adoption of renewable energy sources within the mining industry as miners adapted to the reduced rewards.

In a historic move on March 6, 2025, President Donald Trump signed Executive Order 14233, establishing the U.S. Strategic Bitcoin Reserve – the first national stockpile of Bitcoin funded initially by seized cryptocurrencies from law enforcement actions, with provisions for future acquisitions to build a digital asset portfolio similar to the nation’s gold reserves. This initiative, complemented by the BITCOIN Act introduced shortly after to ensure transparent management and a goal for holdings of 1 million Bitcoins over five years, mandates that Bitcoin be held as a long-term reserve asset rather than sold, enhancing economic sovereignty and integrating cryptocurrency into federal fiscal strategy. It marked a philosophical shift, positioning the

U.S. as the pioneer in treating Bitcoin as digital gold on a sovereign scale, hedging against inflation, encouraging innovation in financial technology, and declaring global leadership in the cryptocurrency industry amid rising geopolitical competition.

For its part, Congress passed the Guiding and Establishing National Innovation for U.S. Stablecoins (“GENIUS”) Act with bipartisan support in both chambers in July 2025. Signed into law by President Trump on July 18, 2025, this landmark bill was the first major federal, crypto-specific legislation in U.S. history. The GENIUS Act regulates stablecoins – digital assets pegged to the value of a national currency, like the U.S. dollar. Its main goal is to protect consumers and ensure financial stability by requiring stablecoins to be fully backed by reserves and providing clear rules for their issuance and oversight.

From Mockery to Mainstream

Not long ago, the luminaries of traditional finance derided Bitcoin as basically worthless at best and an outright fraud at worst. As recently as 2022, Warren Buffett declared, “I wouldn’t pay \$25 for all the Bitcoin in the world because it wouldn’t do anything,” while his Berkshire Hathaway partner Charlie Munger branded it “rat poison squared” in 2018, decrying it as a tool for “kidnappers and extortionists.” The scorn was not limited to legendary investors. In 2017, Jamie Dimon, the CEO of JPMorgan Chase, the largest bank in the U.S., famously declared that “Bitcoin is a fraud.” Paul Krugman, winner of the 2008 Nobel Prize in Economics, branded it as a currency for criminals with no “meaningful economic role” in 2018. And Nouriel Roubini – the economist nicknamed “Dr. Doom” for predicting the 2008 financial crisis – called Bitcoin “the mother of all scams.” Unbothered by the vitriol, Bitcoin continued performing flawlessly – “tick tock, next block.”

Remarkably, by 2025, a seismic shift in attitude had occurred with the financial elite enthusiastically embracing Bitcoin. Federal Reserve Chair Jerome Powell likened Bitcoin to gold, stating in 2024 that it is “like gold, only it’s virtual, it’s digital.” BlackRock CEO Larry Fink, once a skeptic, now hails Bitcoin as “an asset class that protects you,” characterizing it as “digital gold” in 2024. Billionaire investor Stanley Druckenmiller – a macro-investing icon best known for a massive and successful bet against the British pound in 1992 that forced its devaluation – went

from Bitcoin skeptic to advocate, declaring, "I own Bitcoin because I believe it's a store of value ... if the gold bet works, the Bitcoin bet will probably work better." And in a stunning turn of events, even traditional finance guru Ray Dalio – founder of Bridgewater Associates, the world's largest hedge fund, and world-renowned expert in macro investing – currently advises investors to allocate up to 15% of their portfolios to Bitcoin or gold as a hedge against inflation. Bitcoin has not just survived – it has thrived, becoming a fixture in institutional portfolios, corporate treasuries, and mainstream markets, making true believers out of the very establishment figures who recently scorned it.

Bitcoin was born as a cypherpunk rebellion against flawed centralized financial systems. In a twist of profound irony, those same institutions are now forced to acknowledge and engage with the rebellious technology that sought to render them obsolete. However, Bitcoin will not – and cannot – be controlled by them. Its incorruptible decentralization ensures it operates both as a seamless layer within the legacy system and as a sovereign monetary network in parallel to it. In the end, the establishment has bent to the will of Bitcoin. It has been forced to accept the inescapable truth: you do not change Bitcoin – Bitcoin changes you.

The recent years of Bitcoin – from 2021 to mid-2025 – represented a period of momentous transformation. It has rapidly matured from a fringe speculative asset associated with a rogue's gallery of scoundrels and scammers into a lauded and integrated component of the global financial system. Despite market volatility and ongoing regulatory debates, Bitcoin's intrinsic antifragility, its unwavering decentralization, and its programmed scarcity continue to win over a diverse range of devotees. This era has undeniably laid the foundation for Bitcoin's continued expansion, marking its transition from a disruptive innovation to a permanent fixture in the world of finance. As astonishing as Bitcoin's journey has been, many believe its best days are yet to come.

Conclusion

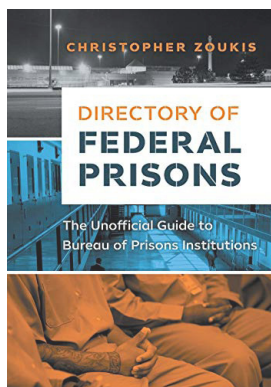
Misinformation and disinformation about Bitcoin still run rampant. Many continue to dismiss it as a Ponzi scheme, others fear its volatility, and many more simply do not know how it works or its magnitude beyond simply a monetary system. Bitcoin does not

care. Having grown from an obscure cypherpunk experiment on a niche corner of the internet into a multi-trillion-dollar global asset class without asking for permission, Bitcoin has proven itself to be antifragile and inevitable.

Bitcoin allows us to imagine a world where money cannot be weaponized. Where privacy is a human right, not a luxury. Where inflation is optional, not imposed. Where financial access is attainable for all, not the few. Where freedom is a birthright, not a privilege. Bitcoin is far more than a once-in-a-generation technology. It is the digital age's declaration of independence.

Bitcoin is a radically liberating idea, and "Nothing in the world is so powerful as an idea whose time has come." 🦋

Sources: Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." 2008; Ammous, Saifedean. "The Bitcoin Standard: The Decentralized Alternative to Central Banking." 2018; Popper, Nathaniel. "Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money." 2015; Breedlove, Robert. "The Number Zero and Bitcoin." 2020; Hayek, F.A. "Denationalisation of Money: The Argument Refined." 1976; Hughes, Eric. "A Cypherpunk's Manifesto." 1993; May, Timothy C. "The Crypto Anarchist Manifesto." 1992; Aczel, Amir D. "Finding Zero: A Mathematician's Odyssey to Uncover the Origins of Numbers." 2015; Bhatia, Nik. "Layered Money: From Gold and Dollars to Bitcoin and Central Bank Digital Currencies." 2021; Farrington, Allen and Meyers, Sacha. "Bitcoin is Venice: Essays on the Past and Future of Capitalism." 2022; Ammous, Saifedean. "The Fiat Standard: The Debt Slavery Alternative to Human Civilization." 2021; Antonopoulos, Andreas M. "Mastering Bitcoin: Programming the Open Blockchain." 2017; Taleb, Nassim Nicholas. "Antifragile: Things That Gain from Disorder." 2012; Poon, Joseph and Dryja, Thaddeus. "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments." 2016; Mezrich, Ben. "Bitcoin Billionaires: A True Story of Genius, Betrayal, and Redemption." 2019; Bank for International Settlements; International Monetary Fund; The Economist; World Economic Forum; Cato Institute; Mises Institute; Council on Foreign Relations; Brookings Institution; New York Times; Wall Street Journal; Forbes; CoinDesk; Bitcoin Magazine; PwC; Oanda; Chicago Booth Review; Yale Law School; NBER; European Central Bank; Atlantic Council; American Economic Association; Center for Global Development; Federal Reserve Bank of St. Louis; Reserve Bank of Australia; OAPEN Library; arXiv; Journal of Financial Innovation; Quarterly Journal of Economics; Investopedia; Medium; Substack; Bitcointalk Forum; Cryptography Mailing List; Electronic Frontier Foundation; White House; U.S. Securities and Exchange Commission; Coin Center; Blockchain Association; NASDAQ.



DIRECTORY OF FEDERAL PRISONS

The Unofficial Guide to Bureau of Prisons Institutions

BY CHRISTOPHER ZOUKIS

The Directory of Federal Prisons is the most comprehensive guidebook to Federal Bureau of Prisons facilities on the market. Not simply a directory of information about each facility, this book delves into the shadowy world of American federal prisoners and their experiences at each prison, whether governmental or private. What sets the Directory of Federal Prisons apart from other prison guidebooks is the first-hand validation of information.

Price: \$99.95 (shipping included)

Name _____ DOC/BOP # _____

Institution/Agency _____

Address _____

City _____ State _____ Zip _____

Prison Legal News • PO Box 1151, Lake Worth Beach, FL 33460
Tel. 561-360-2523 • www.prisonlegalnews.org

From the Editor

by Richard Resch

WELCOME TO THIS MONTH'S ISSUE OF *Criminal Legal News* ("CLN"). As you can see, it's devoted to the revolutionary and controversial topic of digital currencies, spotlighting the two most important participants in the enduring clash between individual liberties and state control. In this issue, we take a deep dive into Bitcoin – the groundbreaking decentralized digital monetary network that is appropriately characterized as "freedom money" – and Central Bank Digital Currencies ("CBDCs") – the government-controlled digital form of fiat money that effortlessly enables mass surveillance, programmable restrictions, and unparalleled control. Whether you're skeptical of these evidence-based assessments or already convinced, this issue of *CLN* is your vital resource for understanding these two starkly different digital currencies and the stakes involved. Our meticulously researched articles will challenge your assumptions, provide fresh insights, and entertain you along the way.

"Crypto Week" Showdown in Congress Over CBDCs

The timeliness of this issue is underscored by the dramatic events that unfolded in Washington, D.C., during "Crypto Week" from July 14 to 18 in the United States House of Representatives. What was intended as a bipartisan celebration for passing a trio of digital asset

bills nearly imploded entirely due to a dramatic intra-party showdown among Republicans. At the core of the conflict was intense pushback from a faction of lawmakers who believed the legislation, specifically the GENIUS Act, did not provide strong enough guarantees against the establishment of a CBDC. This group, driven by deep-seated concerns about government overreach, feared that "loopholes" in the stablecoin framework could be exploited to create a "layered" CBDC system that would inevitably lead to mass surveillance and the erosion of financial privacy – precisely the concerns this issue of *CLN* explores.

This tense political standoff, which required direct intervention from President Trump to resolve, vividly illustrates that the debate over digital currencies is no longer a fringe conversation; it is at the center of the legislative battle for the future of finance. The holdouts eventually relented after receiving guarantees that no bill would inadvertently authorize a CBDC in any form – direct, indirect, or layered through stablecoin frameworks. But as with liberty itself, the price of remaining CBDC-free is eternal vigilance. The pro-CBDC forces will inevitably try again and again to implement their vision of a controlled, centralized digital monetary system. The lessons of this legislative showdown are a grim reminder that the war will never truly be over. It is precisely because this fight for financial freedom remains ongoing that we have dedicated this entire issue to providing you with the critical context and in-depth information needed to stay informed and engaged in this struggle for our future.

Our Perspective on Digital Currencies

In line with *CLN*'s mission of championing individual liberties and privacy, we proudly acknowledge our pro-Bitcoin and anti-CBDC perspective. Yet rest assured, all content in this issue remains painstakingly researched, rigorously factual, and unassailably accurate.

Our deep dive into Bitcoin is not just a technical exploration. It is also a journey into the philosophical ideals that underpin and drive it. As our Bitcoin article declares: "Bitcoin allows us to imagine a world where money cannot be weaponized. Where privacy is a human right, not a luxury. Where inflation is optional, not imposed. Where financial access is attain-

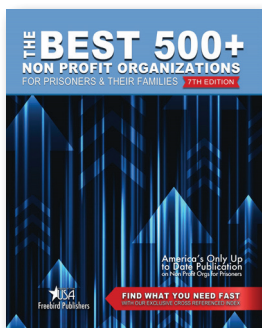
able for all, not the few. Where freedom is a birthright, not a privilege. Bitcoin is far more than a once-in-a-generation technology. It is the digital age's declaration of independence."

Conversely, our opposition to CBDCs is based on a foundational understanding of what they represent: a government-controlled digital form of fiat money that enables mass surveillance, programmable restrictions, and unparalleled control over citizens. While proponents tout them as a more efficient way to manage money, we recognize them for what they are – a new, powerful, and deeply alarming tool of state power. Unlike Bitcoin, which is permissionless and censorship-resistant, a CBDC gives central authorities the ability to monitor every transaction, restrict disfavored purchases, and even seize funds with the push of a button. It is a precision instrument that turns money itself into a lever of control, fundamentally undermining the principles of privacy and individual liberty.

Our Approach to Explaining Bitcoin

In our experience, most of the material available on Bitcoin falls into one of a few traps: (1) it is either too technical for the average reader, (2) too superficial to be useful, or (3) it suffers from a narrow, "tunnel vision" perspective. This last pitfall is especially common, with much of the content either focusing exclusively on financial speculation, getting lost in technical minutiae, or dwelling solely on philosophical ideals without grounding them in a complete picture. The goal with our article is to avoid these traps by offering a holistic and accessible exploration of Bitcoin that imparts a clear and comprehensive understanding.

We have structured our Bitcoin article as a cohesive journey, combining the foundational knowledge you need with the historical and philosophical context that gives it meaning. To start, we provide a primer on the multidisciplinary concepts that underpin Bitcoin's brilliant design, from Austrian economics to game theory, offering accessible explanations of the terms and ideas that can often intimidate newcomers. We then take you through the journey of a Bitcoin transaction – a vital, step-by-step narrative missing from most other educational material – that reveals how the network operates in practice. This is followed by a comprehensive discussion of how



The Best 500+ Non-Profit Organizations for Prisoners & Their Families (7th edition)

Only \$19.99

Order from: Prison Legal News, POB 1151
Lake Worth Beach, FL 33460
561-360-2523

Add \$6 shipping for all book orders under \$50.

Bitcoin is “sound money” – demonstrating how it satisfies and exceeds all the historical criteria for a scarce, censorship-resistant currency. To contextualize Bitcoin’s durability, we also provide a fascinating narrative on path dependence and network effects, explaining why no “New Bitcoin” can ever supplant the original. Finally, we anchor these concepts in a recounting of Bitcoin’s rich and colorful history, from its cypherpunk beginnings to its evolution into a global phenomenon.

We believe that this uniquely holistic and unified approach sets our content apart from all other Bitcoin teaching materials. By integrating these elements, our intent is to leave you not just informed but truly knowledgeable about what Bitcoin is, why it works, and why it matters.

Bitcoin Is the Best Performing Asset in Recorded History

While our Bitcoin article focuses on its profound implications for individual liberties and its role as an effective countermeasure to a surveillance state, it’s worth taking a moment to address another aspect that cannot be ignored and likely attracts more people to Bitcoin than any other – its mindboggling financial performance. If the promise of “freedom money” doesn’t immediately resonate and convince you of the superiority and necessity of Bitcoin, then this will: Bitcoin is the single best-performing asset in all of recorded financial history, over any comparable 15-year period of its existence.

To characterize an asset as “the best-performing in recorded history” is a singularly bold claim, but in the case of Bitcoin, it’s one that is empirically verifiable and factually accurate. Since its earliest trading days, Bitcoin’s Compound Annual Growth Rate (“CAGR”) has been over 136%, a figure that completely obliterates every major asset class in history. While the S&P 500 – the benchmark for stock market performance – has delivered an impressive long-term CAGR of approximately 10-14%, and tech stocks in the NASDAQ-100 have seen returns in the 20-30% range, these figures are utterly dwarfed by Bitcoin’s performance. When compared to traditional safe-haven assets like gold (1-7% CAGR) or real estate, the performance gap widens to an almost unimaginable degree. These figures demonstrate that Bitcoin is literally in a league of its own.

This outperformance isn’t limited to asset classes; astonishingly, it extends to individual assets as well. While legendary high-growth stocks like Apple or NVIDIA

have delivered phenomenal long-term returns in the high double digits, none has sustained a CAGR even remotely close to Bitcoin’s over any 15-year timeframe. Even renowned historical speculative bubbles like the 17th century Dutch Tulip Mania, which saw explosive short-term gains, ultimately failed to provide the long-term, sustained returns that Bitcoin has delivered. This fact is crucial because it thoroughly debunks the common mainstream narrative that Bitcoin is merely a fleeting bubble. Unlike historical anomalies, Bitcoin’s long-term track record proves it’s a new asset class with a unique and durable market value.

The Power of Absolute Scarcity

Bitcoin’s staggering returns, however, are not a fluke but the direct result of an economic reality that applies to no other asset or currency in history. Every asset and currency in human history, from fiat currencies printed “to infinity” by central banks to gold mined from the earth, shares one fundamental trait: its supply can be increased to meet increased demand. While assets like real estate or commodities face high production costs, a soaring market price will always, eventually, spur new supply – whether through new mines, land development, or oil wells. For instance, if gold’s price surges, it triggers costlier mining operations, tempering the price with fresh supply (though some quibble that unique assets like the Mona Lisa are fixed, their non-monetary nature makes this a pedantic distraction).

Bitcoin stands alone as the solitary exception to this economic truth. Its supply isn’t just resistant to increase; it’s mathematically and programmatically fixed at 21 million coins, a cap no amount of demand, price spikes, or political edict can alter (despite nitpicking about theoretical hard forks, which would create a new, separate asset, not alter Bitcoin’s 21-million-coin fixed supply). This absolute, verifiable scarcity – unmatched by any other currency or asset to have ever existed, even those with capped supplies like certain altcoins (a cavil dismissed by Bitcoin’s pioneering dominance) – makes it the first and only asset in history with a supply completely inelastic to skyrocketing demand and price, cementing its revolutionary uniqueness.

Bitcoin Is the Answer to Inflation

While Bitcoin’s fixed supply may sound abstract, we can easily understand its impact by discussing the concept of inflation. Inflation is what happens when prices for things go up because there’s more money available but

not more goods and services to buy. This describes the situation when a government prints more fiat money. The additional money in circulation is now “chasing” the same total amount of goods and services because they don’t correspondingly increase simply because the government turned on the money printer, so prices must go up. The more money the government prints, the greater the imbalance between the money supply and available goods and services, so prices for everything begin to spiral out of control. Sound familiar?

For example, imagine a small, isolated town with only one toy store. Everyone loves a special robot toy it sells. There are only 100 of these robots, but a new factory opens up nearby and suddenly everyone has more money at their disposal to spend. Before, a robot cost \$20, and only a few people could afford one. Now that everyone has more money, they all rush to the toy store. Since there are still only 100 robots, the store owner realizes he can charge more because people are willing and able to pay more. The price of the robot might jump to \$40 or even \$60, even though the robot itself hasn’t changed. This is inflation in a nutshell: more money chasing the same limited number of goods and services, which drives up prices.

What if the toy store owner could never

Are Phone Companies Taking Money from You and Your Loved ones?

HRDC and PLN are gathering information about the business practices of telephone companies that connect prisoners with their friends and family members on the outside.

Does the phone company at a jail or prison at which you have been incarcerated overcharge by disconnecting calls? Do they charge excessive fees to fund accounts? Do they take money left over in the account if it is not used within a certain period of time?

We want details on the ways in which prison and jail phone companies take money from customers. Please contact us, or have the person whose money was taken contact us, by email or postal mail:

HRDCLEGAL@HUMANRIGHTSDEFENSECENTER.ORG



Human Rights Defense Center
Attn: Legal Team
PO Box 1151
Lake Worth Beach, Florida 33460

restock more robots, no matter how much money people had or how high the price went? If the price of a robot hit a million dollars, there would still only be 100 robots in the world. This is exactly how Bitcoin works. It's like a limited-edition collector's item where no new ones can ever be created regardless of the increase in demand or price. This makes Bitcoin truly special and unique because its supply can't be increased to meet demand.

Because Bitcoin's supply is fixed, it's immune to the kind of inflation that affects fiat currencies. When governments print more money, your savings don't buy as much as they previously did. This is why people, companies, banks, hedge funds, institutions, sovereign wealth funds, and even nation-states are starting to view Bitcoin as a reliable asset in which to store value and protect wealth. They believe that because there will never be more than 21 million Bitcoins, it will hold its value over time, unlike fiat money that can be printed endlessly. They are starting to see it as a form of "digital

gold" – a safe place for their wealth that can't be devalued by an increase in supply – but even better than the original.

"It might make sense just to get some in case it catches on"

Bitcoin's extraordinary financial track record, despite its well-documented volatility, isn't a fluke. It is the market itself recognizing and rewarding the very attributes that comprise its philosophical core. Bitcoin's immutable 21-million-coin hard cap guarantees absolute monetary scarcity for the first time in human history, protecting it from the inflation and debasement that plague fiat currencies. Its decentralized, permissionless nature ensures it is resistant to confiscation and censorship, making it the ultimate tool for financial sovereignty. The market is not simply betting on a digital currency; it is valuing these fundamental properties of "freedom money" and its ability to serve as the most pristine store of value the world has ever seen.

The pseudonymous creator of Bitcoin, Satoshi Nakamoto, famously wrote in January 2009, "It might make sense just to get some in case it catches on." In retrospect, that was the financial understatement of all time. The return on Bitcoin purchased when it first had a recorded exchange rate in October 2009 – albeit an informal one based on the electricity cost of mining Bitcoin – would have increased by approximately 14,922,941,900% or 149,229,420-fold. This means a purchase of a dollar's worth of Bitcoin then would be worth about \$161,010,690 at its all-time-high of roughly \$123,000 on July 14, 2025. Although a repeat of that type of gain is exceedingly unlikely, it's still good advice today.

Conclusion

We stand at a pivotal fork in monetary history, where the choice between Bitcoin's decentralization and CBDCs' centralized control will determine whether money serves as a means of individual freedom or an instrument of state surveillance. The recent congressional showdown proves this battle is no longer theoretical. It's happening now, and the stakes couldn't be higher. We are witnessing the rise of two fundamentally opposing visions: one where every transaction is a vote for privacy and self-determination and another where every transaction becomes a data point for government monitoring and control. The revolution in money is not coming – it's here. Which vision of the future do you choose? 🖱️

CLASS ACTION LAWSUIT CHALLENGING THE HIGH PRICES OF PHONE CALLS WITH INCARCERATED PEOPLE

Several family members of incarcerated individuals have filed an important class action lawsuit in Maryland. The lawsuit alleges that three large corporations – GTL, Securus, and 3CI – have overcharged thousands of families for making phone calls to incarcerated loved ones. Specifically, the lawsuit alleges that the three companies secretly fixed the prices of those phone calls and, as a result, charged family members a whopping \$14.99 or \$9.99 per call. The lawsuit seeks to recover money for those who overpaid for phone calls with incarcerated loved ones.

If you paid \$14.99 or \$9.99 for a phone call with an incarcerated individual, you may be eligible to participate in this ongoing lawsuit.

Notably, you would not have to pay any money or expenses to participate in this important lawsuit. The law firms litigating this case—including the Human Rights Defense Center—will only be compensated if the case is successful and that compensation will come solely from monies obtained from the defendants.

If you are interested in joining or learning more about this case, please contact the Human Rights Defense Center at (561)-360-2523 or info@humanrightsdefensecenter.org.

ADVERTISING MATERIAL

Central Bank Digital Currencies: Trojan Horses Delivering Mass Surveillance Under the Guise of Monetary Innovation

by David Kim

"He who controls the food supply controls the people; he who controls the energy can control whole continents; he who controls money can control the world." – Widely Attributed to Henry Kissinger

Introduction to Central Bank Digital Currencies

Central banks around the world have long issued money in physical form, but the rise of digital technologies has spurred them to explore new frontiers, such as a Central Bank Digital Currency ("CBDC"), a digital version of a nation's fiat money issued and backed directly by the central bank. Proponents herald CBDCs as the next evolution of money, a digital counterpart to physical cash, promising a more efficient financial landscape: reduced transaction fees, streamlined e-commerce and international transfers, and greater financial inclusion for the unbanked. They envision a "digital banknote" for an increasingly digital world, fostering innovation and modernizing payment systems. Yet these promises conceal a sinister reality. CBDCs are not a mere upgrade to our financial infrastructure – they represent a seismic transformation of money itself, centralizing unprecedented power in the hands of governments and threatening financial privacy and individual liberty on an unimaginable scale.

Imagine an ordinary citizen, Jane, buying coffee with a CBDC. Unlike cash, which leaves no trace, her transaction is recorded on a centralized ledger, linked to her identity, location, and spending habits. Over time, this digital trail reveals her political affiliations, medical needs, or even her support for controversial causes – data that could be accessed by governments or shared with third parties. This is not speculation but a plausible outcome of CBDC architecture, which, by design, enables pervasive surveillance. Supporters tout "managed anonymity," claiming small transactions might retain some privacy while larger ones are traceable. But this is a hollow compromise. The Electronic Frontier Foundation and the American Civil Liberties Union emphasize that financial records are deeply personal, revealing sensitive details about one's life. Anonymity in transactions is vital for free speech, especially for dissenters or marginalized groups whose purchases –

books, donations, or protest materials – could expose them to retaliation. The centralized infrastructure of CBDCs, whether built on blockchain-like ledgers or programmable money, ensures that personal data is always accessible, often with a mere court order or, in some regimes, without any oversight. Once this surveillance apparatus is in place, its expansion becomes inevitable, especially during crises or political unrest.

History warns us of such dangers. In the 20th century, governments used financial controls to suppress dissent, from freezing dissidents' bank accounts to monitoring transactions under programs like the United States' post-9/11 surveillance initiatives. CBDCs amplify this threat exponentially, creating a digital panopticon where every transaction – down to a vending machine purchase – can be tracked in real time, linked to identities, and analyzed for behavioral patterns. Unlike cash, which offers anonymity, CBDCs generate a permanent digital footprint, encompassing transaction histories, demographics, and even predictive profiles of individual behavior. This data can be weaponized far beyond payment processing, enabling governments to target specific groups, silence unpopular voices, or exacerbate inequalities by prioritizing access for compliant citizens. In authoritarian states, CBDCs could become tools of social control, programming money to restrict purchases or penalize dissent – scenarios hinted at by critics in discussions around China's digital yuan trials, with concerns that transactions could potentially be tied to social credit systems.

The global push for CBDCs intensifies this threat. China has advanced its digital yuan through extensive pilots, aiming to challenge the U.S. dollar's dominance while tightening domestic control. The European Union and Hong Kong are testing or implementing CBDCs, while the Eastern Caribbean is planning a relaunch of its DCash CBDC after suspension. In the U.S., the Federal Reserve's Project Hamilton, conducted with MIT, signals exploratory steps, though it claims no final decision without congressional approval. These developments are not just technical but geopolitical, as nations race to secure financial influence in a digital age. Yet the cost is clear: CBDCs risk entrenching a global surveillance

economy where power concentrates in the hands of a few, eroding the freedoms of many.

What will it mean to live in a world where every transaction is watched, every choice recorded, and every dissent traceable? The shift to CBDCs is not merely a digitization of money – it is a gateway to authoritarian overreach, threatening the very foundation of individual and societal freedom. As this infrastructure takes root, the window to resist narrows. The stakes demand scrutiny, not complacency, lest we surrender our autonomy to a future of unyielding control.

Unprecedented Surveillance and the Erosion of Privacy

The most immediate and chilling threat posed by CBDCs is the inherent and pervasive surveillance they enable. In today's financial landscape, privacy is already fragile, compromised by laws like the Bank Secrecy Act, which mandates reporting of suspicious activities without notifying individuals. A CBDC would amplify this fragility, allowing real-time, centralized monitoring of all transactions. Federal Reserve Chair Jerome Powell has acknowledged that a U.S. CBDC would require identity verification, potentially linking transactions to digital IDs and creating comprehensive government records. Internationally, officials like Agustín Carstens of the Bank for International Settlements have described CBDCs as enabling "absolute control." In the U.K., proposals for a digital pound suggest transactions would be traceable under anti-money laundering regulations, far less private than cash. Such visibility could expose everyone's everyday activities – purchases of books, donations to causes, or medical expenses – to unwarranted scrutiny, chilling free expression and association.

The risks extend beyond mere monitoring to the perils of data leakage and abuse. Centralized CBDC systems, by consolidating vast amounts of sensitive financial information, become attractive targets for cyberattacks, potentially leading to widespread identity theft and financial fraud. Even when data is legally obtained, the risk of abuse remains significant. Such data could be used for purposes entirely different from its original collection, leading to invasive marketing, discrimination, or ma-

nipulation of consumer behavior, especially in jurisdictions where the rule of law is weak. The sheer scale of existing financial surveillance provides a stark warning: in the U.S. alone, financial institutions were required to file approximately 3.2 million reports on suspicious customer activity to the government in 2022. A CBDC would dramatically expand this already sweeping surveillance state.

The implications for fundamental rights are clear. The Fourth Amendment of the U.S. Constitution has struggled to adapt to the digital age. While it protects information kept physically, it often provides less protection for data stored online. Additionally, law enforcement in the U.S. often does not need a warrant to access financial information held by commercial financial institutions. A CBDC would eliminate the last remaining buffer of protection that private financial institutions might offer by centralizing this sensitive information directly with the government. This effectively codifies and exacerbates the erosion of financial privacy rights, transforming every financial transaction from a private exchange into a government-monitored activity.

Programmable Money and Censorship

Beyond even unprecedented persistent mass surveillance, CBDCs introduce an alarming new dimension of control: programmable money. This means the issuing central bank or government can embed specific conditions directly into the digital currency, dictating precisely how, when, or even if it can be spent. This capability represents a radical departure from the fundamental, fungible nature of traditional cash, transforming money from a neutral medium of exchange into a direct instrument of social engineering and control. Consequently, experts warn that CBDCs could pave the way for “digital authoritarianism,” where governments use them for political discipline.

The negative consequences for individual autonomy cannot be overstated. As International Monetary Fund Deputy Managing Director Bo Li openly stated, “By programming a CBDC, money can be precisely targeted for what people can own and what [people can do].” This is not a theoretical concern. Such programmability could manifest as prohibitions on purchasing certain goods, such as alcohol on a weekday or strict limits on the quantity of items one is allowed

to buy. The potential limits and controls that could be programmed into a CBDC is limited only by one’s imagination. Ominously, this power could extend to preventing donations to specific disfavored organizations or unpopular causes. This mechanism allows the government to enforce social norms and political agendas through economic coercion, effectively dictating individual choices.

The potential for financial censorship and exclusion is a profound threat. With a CBDC, the government gains an unprecedented ability to freeze or seize assets with only a few keystrokes, enabling instant and crippling economic sanctions against dissidents or anyone deemed an enemy of the regime.

Furthermore, CBDCs can empower policymakers to impose negative interest rates, causing individuals to lose money (purchasing power) simply by holding it. While proponents argue this could spur spending and stimulate the economy, it fundamentally undermines money’s role as a reliable store of value and forces economic behavior. This direct manipulation of individual financial decisions represents a significant shift in the relationship between citizens and the government.

The very concept of programmable money fundamentally politicizes the monetary system. Traditional monetary policy typically operates at a macroeconomic level, influencing broad economic conditions through interest rates and money supply. In contrast, programmable money enables micro-level control, dictating individual spending choices and even prohibiting transactions based on government-defined criteria. This transforms money from a neutral medium of financial exchange into a direct tool for social engineering and political enforcement. Federal Reserve Governor Michelle Bowman cautioned against this, stating, “There is also a risk that this type of control could lead to the politicization of the payments system and at its heart, how money is used.”

The erosion of economic self-determination is a direct consequence. The ability to program money means individuals lose the fundamental right to decide how to earn, save, and spend their own resources. If funds can be made to expire or be restricted to certain purchases, economic choices are no longer truly free. This is a direct assault on the principle of economic self-determination, a cornerstone of individual liberty. The very idea of “permissionless” transactions, central to both physical cash and true cryptocurrencies, is obliterated. This is not merely an inconve-

nience. It is a fundamental philosophical shift, moving society closer to a command economy at the individual level, where the government, not the individual, wields ultimate power over one’s financial life.

What Are CBDCs

The emergence of digital currencies presents a fascinating paradox. There is the rise of decentralized cryptocurrencies, born from a cypherpunk ethos of individual liberty and resistance to surveillance and control. In stark contrast, a more insidious form of digital money is also taking shape – CBDCs. While often presented as a natural evolution of our financial system, a deeper examination reveals CBDCs to be instruments fraught with peril, threatening the very foundations of privacy, economic freedom, and the delicate balance of power between the individual and the government.

At their core, CBDCs are the digital equivalent of a nation’s fiat currency – that is, dollars, euros, or yuan – but issued and overseen directly by the central bank rather than commercial banks or private entities. This means they hold the same legal status as physical cash or bank deposits, backed by the government’s authority and designed for everyday transactions, from buying groceries to settling debts. Unlike the coins in your pocket, however, CBDCs exist solely in electronic form, stored in digital “wallets” and transferred via secure networks. CBDCs can be retail-oriented, accessible to the public for daily use, or wholesale, limited to financial institutions for large-scale settlements. Either way, the central bank maintains ultimate control over issuance, circulation, and even destruction, ensuring stability in value tied directly to the national currency. In addition, the central bank has direct oversight of or at least an unfettered view of every transaction.

This centralized control is where CBDCs diverge sharply from true cryptocurrencies like Bitcoin. Bitcoin, and many other cryptocurrencies such as Ethereum and Cardano, are built on decentralized, permissionless blockchain networks. “Permissionless” means anyone can participate without needing authorization from a central authority. That is, there are no gatekeepers. “Decentralized” means there is no single point of control; the network is maintained by a distributed ledger, verified by a multitude of participants spanning the globe, making it incredibly resilient to censorship and manipulation. Transactions are typically pseudonymous, offering a significant degree of privacy, and the supply of

the currency is often governed by pre-defined cryptographic rules, not the arbitrary whims of a central bank or government that needs to continuously print more money to fund its reckless spending, thereby devaluing the currency, fueling inflation, and eroding the savings of ordinary people.

Conversely, CBDCs are fundamentally permissioned and centralized. The central bank dictates who can access the system, who can transact, and under what conditions. This is a crucial difference often obscured by proponents who attempt to conflate the two by highlighting the “digital” aspect of both. The digital nature is merely superficial; the underlying architecture and control mechanisms are diametrically opposed. Where cryptocurrencies champion individual sovereignty, CBDCs represent the ultimate expression of government financial control.

The Hidden Ambitions of CBDC Motivations

Governments and international financial institutions often present a seemingly benign array of motivations for pursuing CBDCs. They speak of enhancing “financial inclusion,” bringing banking services to the unbanked. They champion “efficiency” in payment systems, promising faster, cheaper transactions. We hear rhetoric about fostering “innovation” and combating “illicit finance” by providing a transparent and traceable alternative to cash.

These purported motivations have superficial appeal, and that is what makes them so effective and dangerous. However, upon critical examination, those hopeful motivations espoused by proponents of CBDCs give way to reveal darker ambitions. “Financial inclusion,” when coupled with a CBDC, could easily morph into a system where access to money is conditional, where certain transactions are disallowed, or where dissenters find their financial lives restricted. The promise of “efficiency” risks paving the way for a surveillance dragnet, where every purchase, every payment, every financial interaction leaves an indelible, transparent, and immutable trail accessible to the government. This is not efficiency; it is an infrastructure for pervasive mass surveillance and control.

The argument for combating “illicit finance” is particularly specious, often serving as a convenient justification for expanding government surveillance under the guise of public safety. While no serious person advocates for crime, the concept of illicit finance is remarkably elastic, often expanding to encompass

activities deemed undesirable by the government, rather than genuinely criminal. With a CBDC, every transaction becomes a data point, every financial decision a piece of information for analysis. Imagine a world where your purchase of a book deemed subversive, or a donation to a politically unpopular cause, is instantly flagged and analyzed by government algorithms. This is not about stopping illicit global money flows; it is about establishing a financial panopticon.

A financial panopticon is a fitting analogy when discussing CBDCs. A panopticon is a type of prison design conceived of by the eighteenth-century English philosopher Jeremy Bentham. It is characterized by large, round rooms with the walls lined with prisoners’ cells and a watchtower in the center. By design, prisoners never know whether the watchmen in the tower are watching them, but the watchmen can observe any prisoner at any time. Bentham hoped that the panopticon could achieve in society that which had never been achieved – control of the mind instead of the body. He theorized that prisoners, constantly aware of surveillance but never certain when they were specifically being watched, would self-regulate their behavior to avoid potential discovery and punishment. Fittingly, the word “panopticon” is derived from two Greek words that together mean “all-seeing.”

The Death of Financial Privacy: Building the Panopticon

In an era where digital footprints already map our lives with unsettling precision and ubiquity, CBDCs represent a dramatic escalation in the government’s mass surveillance capabilities. Governments tout these digital forms of fiat money as efficient, inclusive alternatives to cash, but their architecture inherently enables unprecedented tracking. CBDCs digitize every exchange, recording it in a centralized ledger controlled by authorities and thereby turning every purchase into a permanent dossier for scrutiny.

For centuries, cash has served as the bedrock of financial privacy. Cash makes anonymous transactions possible. This anonymity is not merely a convenience. It is a vital safeguard for dissent, for vulnerable populations, and for the fundamental right to conduct one’s life free from persistent governmental scrutiny. Cash enables people to engage in commerce, support causes, and just go about daily life without every transaction being known and permanently recorded by the government. Unfortunately, with the inexorable march to-

wards a cashless society, the introduction of a CBDC presents a unique and unprecedented opportunity for governments to eliminate this last vestige of financial anonymity.

Granular Surveillance Capabilities: The All-Seeing Eye

At the heart of CBDCs lies their capacity for granular, real-time monitoring, far surpassing current banking systems. Unlike physical cash or even existing digital payment systems that operate through commercial banks, every CBDC transaction – down to the amount, timestamp, location, and parties involved – becomes instantly accessible to central banks. For instance, the Bank for International Settlements has explored designs where CBDC systems record unique identifiers for each digital coin, linking them back to users during withdrawals or transfers.

This is not speculative. China’s digital yuan, or e-CNY, already demonstrates such tracking in practice, with tiered accounts requiring phone numbers for basic access and escalating to full identity verification for larger holdings. This results in a continuous stream of permanently recorded data that paints a vivid picture of an individual’s economic behavior, from routine groceries and sundries to one’s most intimate proclivities and pastimes.

The implications are staggering. Every CBDC transaction – the amount, the exact time, the location of both parties, and the identities of the counterparties – is immediately accessible to the central authority. Imagine buying a book on a politically sensitive topic, donating to a controversial charity, or purchasing goods from a business critical of government policy. With a CBDC, these seemingly innocuous actions become data points in an aggregated digital dossier, a comprehensive record of an individual’s entire economic life – and by extension, social and political life. This is not merely about tracking large illicit transactions. It is about developing a meticulously detailed mosaic of every citizen’s daily habits, preferences, and associations. It is the height of naiveté to believe that people will not be punished and rewarded accordingly.

But it gets much worse. CBDCs integrate seamlessly with other government databases, amplifying their reach. Tax authorities, social security systems, law enforcement, and nascent social credit-esque systems (remember the emergence of the functional equivalent of digital health passports rolled out by several states during COVID-19, ostensibly for travel and entrance to certain places?) can cross-link

financial data, creating a holistic, 360-degree surveillance view of citizens. In such a system, financial transactions are no longer private exchanges. They become public declarations, fully visible to the government with absolute precision. This level of aggregation creates a digital footprint so comprehensive and granular that it could be used to infer political affiliations, health conditions, social connections, and even future intentions.

Erosion of Anonymity

Physical money allows exchanges without a trace – no digital breadcrumb leading back to real-world identities. CBDCs strike at the core of such transactional anonymity. They embed identity linkage as a foundational element. This stands in sharp opposition to the early promise of cryptocurrencies like Bitcoin, which offer pseudonymous transactions where users operate via public addresses rather than names, preserving a veil of anonymity. Bitcoin's decentralized ledger does not require central verification of identities, allowing transfers without revealing personal details. However, CBDCs are fundamentally antithetical to this principle. Their core design feature is identity linkage.

The central bank, by definition, must know who is holding and transacting its digital currency. This means that unlike the privacy afforded by a cash transaction, where identities are rarely exchanged unless legally required, every CBDC transaction is irrevocably tied to a verified identity. There is no equivalent of cash-like privacy in this digital realm. The concept of an “anonymous” digital transaction, as it exists with physical currency, simply ceases to exist. This shift is not a minor technical detail. Rather, it is a paradigm-shattering change in the fundamental nature of money and its relationship to individual freedom.

The risks are compounded by the potential for persistent digital identity wallets. These wallets, which hold an individual's CBDC, are tied to national digital identity schemes, consolidating a vast array of personal information. Such a system creates a single point of failure, a honeypot of sensitive data that, if compromised, could lead to catastrophic identity theft or targeted harassment. Moreover, the very existence of such a comprehensive digital identity, linked to one's financial existence, makes it far easier for authorities to monitor, restrict, or even freeze an individual's access to

funds based on subjective criteria or shifting political winds.

Chilling Effects

When individuals know they are under constant surveillance, their behavior inevitably changes. This phenomenon is known as the “chilling effect,” and it poses one of the most pernicious dangers of CBDCs. There is immediate and subtle self-censorship of free expression and behavior that inevitably permeates daily life. People who are aware of constant monitoring self-censor their spending, avoiding donations to controversial causes or purchases of sensitive items like books on dissent or other ideas disfavored by those currently in power. The Cato Institute warns that CBDCs threaten financial freedom, potentially deterring support for political groups under government watch. Under highly controlled regimes, this is already evident. For example, China's digital yuan can link transactions to social credit scores, penalizing “undesirable” expenditures. Even in freer societies, the mere possibility of scrutiny and denial of access to funds creates an environment of hesitation and anxiety, as noted in an analysis by Ledger Insights, a leading publication on enterprise blockchain and distributed ledger technology.

Consider the act of donating to a political cause that challenges the established narrative. With a CBDC, every such donation is instantly traceable, creating a digital record that can be used for profiling or even retaliation. This pervasive knowledge of being watched leads individuals to pull back from actions that, while perfectly legal, might be perceived as non-conformist or politically inconvenient.

The negative impact on political dissent, independent journalism, and vulnerable populations cannot be overstated. Activists relying on donations to sustain their work can have their funding streams cut off or monitored with ease. Journalists protecting their sources can have their financial transactions tracked, revealing critical information. Dissidents in oppressive regimes, already facing immense pressure, lose their last vestige of anonymous financial support, leaving them entirely exposed. Even seemingly mundane purchases, such as certain medications or counseling services, can carry a social or professional stigma if they become part of a government-accessible ledger. The chilling effect does not merely deter illegal activities; it stifles legitimate and essential expressions of freedom as well as personal choices, fostering a culture of conformity and fear.

To the apologists of authoritarian power-grabs, the trite and facile notion that “if you have nothing to hide, you have nothing to fear” fundamentally misunderstands the essence of privacy and human dignity. It falsely equates personal discretion with unlawful activity, ignoring the vast spectrum of deeply private, non-illegal aspects of our lives – from health struggles and personal failures to intimate relationships and private thoughts – that each and every one of us conceal from public view. A demand for total transparency is not a genuine call for security, but instead, it is an insidious erosion of the personal autonomy and dignity essential to a free society.

Programmable Money: The Tool of Authoritarian Control

CBDCs introduce a form of money that governments can program at will, embedding rules directly into the currency itself. This programmability shifts financial power decisively toward the state, allowing officials to dictate how, when, where, and even if citizens can spend their own funds. Unlike cash or even traditional bank accounts, which offer a degree of anonymity and flexibility, programmable CBDCs enable precise controls that erode personal autonomy in everyday transactions. For instance, expiration dates can force funds to vanish if not spent by a certain time, compelling people to use them quickly or lose them altogether. Spending limits can cap how much an individual can allocate to certain categories, while restrictions on merchant types are able to block purchases from disfavored businesses, all enforced automatically through the digital ledger. This level of granular control over individual economic activity fundamentally redefines personal financial autonomy, shrinking the sphere of individual decision-making to an alarming degree.

Such control features are not merely hypothetical. Central banks are already exploring them as core elements of CBDC design. In India's digital rupee trials, for example, programmability allows for parameters like expiration dates and merchant category codes to be set, ensuring funds are used only in approved ways. Similarly, discussions around programmable payments highlight how CBDCs can automate rules for stimulus funds, preventing their use on items like alcohol or tobacco. This level of control extends to negative interest rates, which central banks could apply selectively to individual holdings. In a low-interest environment, a CBDC might deduct value from accounts over time, but unlike broad monetary policy, it could target

specific users – perhaps those deemed to be hoarding cash – pushing them to spend or invest in government-preferred ways. European Central Bank officials have noted that CBDCs could facilitate negative rates without the escape valve of physical cash, as holdings below certain thresholds might avoid penalties, but larger amounts would not. This results in a tool that nudges behavior in governmentally-favored ways through financial erosion.

Financial Geofencing

Geofencing adds yet another chilling layer of control. Geofencing – the ability to restrict where individuals' money can be spent, down to specific geographical locations – transforms their digital wallet into a virtual leash, effectively tethering economic activity to government-approved locations. For cross-border payments, geofencing might block non-residents from using a CBDC abroad, limiting its flow and enforcing capital controls. Imagine a scenario in which the places where you can spend your salary are restricted to local merchants or where protesters are barred from buying supplies beyond their immediate area. These are the kinds of restrictions that programmable money makes effortless. Central banks tout such programmable restrictions as a way to enhance efficiency, but clearly, they are also, and likely primarily, a highly effective means of control. The implications for personal mobility and freedom of association are stark and deeply concerning.

This is not just about hard geographical boundaries. Geofencing can extend to more subtle and insidious applications. For instance, geofencing can be dynamically tied to public health mandates, restricting purchases in areas with reported outbreaks (conversely, completely restricting the ability to spend funds outside of an outbreak area for those living there) or even limiting access to funds for those who have not complied with certain health directives within a specific zone. Similarly, during times of perceived crisis or emergency, the government could “geo-fence” funds to ensure they are spent only on government-approved “essential” goods and services, preventing purchases deemed “non-essential” or speculative. This granular ability to segment and control financial activity based on location and context creates a framework for unprecedented social and economic control.

Beyond the technical capabilities, the ability for censorship and financial exclusion woven into the fabric of CBDCs dwarfs similar capabilities with current systems. In

a traditional cash-based society, even in a highly digitalized one, there remains a degree of anonymity and a barrier to instantaneous, government-directed financial freezing. With a CBDC, the government possesses the unprecedented power to instantly freeze or seize funds without due process or delay. This is not hyperbole; it is a direct consequence of a centralized, programmable digital currency. Your ability to feed your family, pay your rent, or access medical care can be revoked with the click of a button, entirely at the discretion of the government. This ability extends to blocking transactions to or from specific individuals, organizations, or even entire regions. The government's ability to financially “blacklist” individuals based on their political views, social credit scores, or even their health status becomes terrifyingly easy, efficient, and pervasive with a CBDC.

Social Engineering

Critics warn that programmable money makes it disturbingly easy for social engineering and behavior modification. CBDC transaction data can reveal intimate details, from spending habits to affiliations, allowing governments to profile and penalize. In a system where every purchase is tracked, low social credit – tied to perceived disloyalty or non-conformity – could trigger automatic restrictions and punishment. Health status, which can be inferred from buying patterns like medications or gym memberships, can justify exclusions, such as denying access to certain locations, services, and even medical care during purported pandemics to those who refuse to be vaccinated. Democratic nations disingenuously frame this as a net positive for society, but in actuality, it gives the government unchecked power to define “undesirable” traits, turning financial inclusion into a privilege to be revoked at the whim of those in power.

This control morphs into outright social engineering, where CBDCs incentivize or punish behaviors through embedded rules. Governments can reward “green” spending – for instance, subsidies for electric vehicles or organic foods – while penalizing purchases of “fossil” fuels or processed snacks, all programmed into the currency. Taxes on unhealthy items, already used in some countries to curb consumption, can be amplified via CBDCs by automatically deducting extra fees for sugary drinks or fast food. While some argue these are noble goals, the underlying mechanism is one of coercion, not choice. It is about the state actively shaping individual

behavior, dictating what you should eat, how you should travel, and even how you should live your life, all based on the omnipresent CBDC. What begins as encouragement for perceived better choices results in a system that molds society from the wallet outward, prioritizing state goals over individual liberty.

The Canadian trucker protest of 2022 against vaccine mandates provides an ominous, real-world example of government leveraging financial infrastructure to crush dissent, even without a full CBDC. Invoking the Emergencies Act, which enabled measures to combat financing of activities deemed threats to public order, the Canadian government froze bank accounts and cryptocurrency wallets linked to protesters, blocking over \$3 million without court orders. Financial institutions and cryptocurrency exchanges operating in Canada swiftly complied, sanctioning dozens of crypto addresses and halting transactions for individuals who donated as little as \$50. But the crackdown did not end there. Over 200 bank accounts belonging to those donating to the protesters were also frozen, totaling millions of Canadian dollars.

The Canadian government had to rely on a network of third-party financial institu-

Stop Prison Profiteering: Seeking Debit Card Plaintiffs

The Human Rights Defense Center is currently suing NUMI in U.S. District Court in Portland, Oregon over its release debit card practices in that state. We are interested in litigating other cases against NUMI and other debit card companies, including JPay, Keefe, EZ Card, Futura Card Services, Access Corrections, Release Pay and TouchPay, that exploit prisoners and arrestees in this manner. If you have been charged fees to access your own funds on a debit card after being released from prison or jail within the last 18 months, we want to hear from you.

Please contact HRDC Legal Team at
HRDCLegal@humanrightsdefensecenter.org
Call (561) 360-2523
Write to: HRDC, SPP Debit Cards,
PO Box 1151, Lake Worth Beach, FL 33460

tions and a newly invoked Emergencies Act to carry out its goal of starving the protestors of funds. Although it was effective, the process required significant coordination, legal orders, and time. Had Canada possessed a CBDC at that time, such financial suppression could have been executed with alarming ease and near-instantaneous effect, bypassing traditional intermediaries and their procedural safeguards entirely.

The act of cutting off funds is an exceptionally potent and often devastating tactic for governments seeking to silence dissent. It attacks the very lifeblood of a protest movement on multiple critical levels: practical, logistical, psychological, and organizational. Practically, protestors face the immediate loss of basic necessities – food, water, fuel for their vehicles, and shelter – paralyzing their ability to sustain presence and operations. The inability to acquire essential equipment, from sound systems to medical supplies, diminishes their voice and resilience. In addition, access to legal counsel is crippled, making individuals more vulnerable to government prosecution and increasing the personal risks of engagement.

Psychologically, the impact is equally profound. Financial pressure creates immense personal stress, transforming participation from a civic act into a potentially ruinous personal sacrifice. The fear of personal ruin – losing savings, credit, and employment – extends to families, creating an agonizing dilemma for those involved. It fosters a sense of helplessness and isolation, as individuals feel cut off from the mainstream financial system because their actions are effectively delegitimized by governmental decree. Organizers lose the capacity to lead because their financial lifelines are severed, making it impossible to coordinate, communicate, or maintain momentum. The very trust that binds a movement together can rapidly erode when its financial foundations are suddenly removed.

Furthermore, the aggressive financial actions taken by the Canadian government sent a grim message beyond the active protestors themselves. Individuals who might otherwise offer even small donations to causes they believe in, but prefer to remain anonymous or simply avoid direct engagement, are now faced with the stark realization that their financial support could expose them to severe personal consequences, including frozen assets. This creates an intense chilling effect on

philanthropic freedom and civic participation, stifling future dissent and expression by making monetary support inherently risky.

Ultimately, cutting off financial lifelines serves as a powerful deterrent. It sends an unequivocal message from the government: “We are serious, we will use all available tools, and there will be severe economic consequences for participation.” The Canadian episode stands as an unnerving warning. It clearly demonstrates how financial pressure can and will be used against future movements, fostering a broader “chilling effect” on civil liberties and the fundamental right to protest. A CBDC will streamline and amplify these powers, making such actions instantaneous, pervasive, and virtually impossible to circumvent.

This is the dystopian future we risk if we fail to recognize the Trojan horse hidden within the promise of CBDCs. We must ensure one is never introduced in the U.S. Once programmable money takes hold, the line between economic policy and political repression disappears, empowering the government to silence opposition through its absolute control over the nation’s money.

False Promises: Deconstructing the Pro-CBDC Narrative

Governments and central banks around the world are increasingly touting CBDCs as a panacea for longstanding issues in the financial system. Proponents claim that these digital versions of fiat money, issued and backed by central authorities, will usher in an era of universal inclusion, enhanced efficiency, reduced crime, and cutting-edge advancements. However, upon critical examination, these promises collapse under the weight of practical limitations and unacknowledged dangers. Far from empowering individuals, CBDCs threaten to further entrench government surveillance and control at the expense of personal autonomy.

Financial Inclusion

One of the most frequently invoked justifications for CBDCs is their supposed ability to bridge gaps in financial access, particularly for underserved populations. Advocates contend that a CBDC could extend banking services to the unbanked and underbanked, enabling seamless participation in the economy without the need for traditional accounts. The International Monetary Fund has explored how CBDCs might address barriers related to access, cost, and trust, potentially shifting cash-reliant individuals toward digital alternatives. While the goal of universal financial

access is undeniably noble, the proposed solution of a CBDC is not merely insufficient; it is fundamentally flawed and potentially counterproductive.

At their core, CBDCs require digital literacy, access to smartphones or other digital devices, reliable internet connectivity, and verifiable identification. These elements may remain out of reach for some Americans, particularly in underserved communities, potentially limiting access to CBDCs. For them, mandating a CBDC without first bridging this gap would exclude those already marginalized, deepening their economic isolation rather than alleviating it.

The real path to financial inclusion lies in strengthening and innovating upon existing, proven solutions. Improving and expanding the reach of traditional banking infrastructure, promoting mobile banking solutions that are interoperable and accessible, and critically, preserving and supporting the use of physical cash are far more effective and less intrusive solutions than a CBDC.

Efficiency

Proponents also champion CBDCs for their potential to streamline payments, reduce transaction costs, and modernize outdated systems, i.e., make the financial system more efficient. They promise frictionless transactions, immediate settlement, and reduced costs compared to those associated with physical cash handling as well as the current digital structure in which multiple parties are involved in the settlement of transactions.

However, the alleged efficiency of a CBDC is directly proportional to its level of traceability. For a central bank to achieve the degree of oversight it truly desires, every transaction must be recorded and accessible. Such surveillance capabilities impose enormous operational burdens. Building and maintaining systems to monitor every transaction requires vast resources, from data storage to cybersecurity defenses, potentially offsetting any operational efficiency gains. This type of system does not make payments more efficient for the people, but it does make surveillance more efficient for the government.

Centralizing aspects of the monetary system, such as CBDC issuance and transaction oversight, within the central bank introduces systemic risks that far outweigh any perceived efficiency gains. The failure of a single, centralized digital system would have catastrophic consequences, paralyzing the entire nation’s economy. Unlike the distributed and relatively

resilient nature of the existing private payment network, a CBDC creates a single point of failure, making the financial system profoundly vulnerable to technical glitches, cyberattacks, or even targeted political disruptions.

Furthermore, the notion that a CBDC is necessary for payment innovation is simply false. The private sector has already demonstrated remarkable ingenuity in developing faster, more efficient payment solutions. Real-time payment systems, sophisticated mobile payment applications, decentralized cryptocurrencies such as Bitcoin, and stablecoins (privately issued digital currencies pegged to a stable asset like a fiat currency) currently enable rapid, low-cost transfers without central oversight. These systems are already addressing many of the supposed inefficiencies that CBDC proponents claim to solve. These private innovations arise from competition and market demand, creating a dynamic environment for technological advancement. In contrast, a government-mandated CBDC will stifle this organic innovation by discouraging private solutions and imposing a monolithic, state-controlled infrastructure.

The true efficiency lies in encouraging a vibrant, competitive ecosystem of payment providers, not in centralizing control under a single government-controlled entity.

Combating Illicit Finance

Perhaps the strongest, yet most disingenuous, argument for CBDCs is their alleged ability to combat illicit finance. Proponents often invoke the specter of money laundering, terrorism financing, and other criminal activities in arguing for fully traceable digital currency as the ultimate weapon in this fight. But this argument greatly overstates the potential effectiveness of CBDCs and, more importantly, serves as a transparent pretext for the expansion of mass surveillance and control.

Sophisticated criminals are highly adaptable. They operate at the fringes of the financial system precisely to evade detection. The deployment of a traceable CBDC would not eradicate illicit finance. It would simply force it deeper underground, driving bad actors to alternative, less regulated, or entirely untraceable methods, thereby rendering CBDC traceability less effective than claimed. This is not mere speculation. History is replete with examples of prohibition and stringent regulation pushing undesirable activities into the shadows, making them harder, not easier, to monitor.

The true danger of the CBDC “combatting illicit finance” narrative is that it erodes

the presumption of innocence by treating all users as suspects by default. Cash and privacy-preserving payment systems are not inherently criminal. They afford legitimate anonymity in a free society. Additionally, CBDCs undermine proportionality, as the vast data collection required far exceeds what is needed for targeted enforcement. With a CBDC, every purchase, every transfer, every financial interaction becomes a data point in a governmental ledger ripe for analysis, profiling, and potential misuse.

Privacy is not a crime. It is a fundamental human right that is essential for individual liberty, dissent, and the flourishing of a truly free society. To equate the desire for private transactions with criminal intent is a dangerous authoritarian fallacy but one with undeniable superficial appeal for many. The erosion of financial privacy under the guise of fighting crime is a price no free society should be willing to pay.

Innovation

Finally, proponents of CBDCs claim they will spur innovation in the financial sector. This is arguably the most ironic of the pro-CBDC arguments because a centralized, permissioned digital currency system is inherently antithetical to the very spirit of innovation. True innovation thrives in open, decentralized environments, driven by competition, experimentation, and user empowerment – precisely the characteristics that define the burgeoning cryptocurrency space.

By design, CBDCs are government-controlled financial instruments. Decisions regarding their architecture, features, and even their permitted uses are made by central planners, not by market forces or individual preferences. Such a top-down approach inevitably leads to stagnation and a lack of adaptability. Compare this to the dynamic, permissionless innovation seen in the world of decentralized cryptocurrencies, where developers from around the world can build new applications, services, and financial tools without seeking permission from a central authority. This open-source, collaborative model has led to an explosion of creativity and utility, demonstrating the power of true, bottom-up financial innovation.

The innovation promised by CBDCs is, in reality, innovation for the state, not for users. It is innovation geared toward enhanced control, surveillance capabilities, and the potential for new monetary policy tools. The focus shifts from empowering individuals and fostering

free markets to expanding state oversight and manipulation of economic behavior.

The arguments for CBDCs – financial inclusion, efficiency, combating illicit finance, and innovation – fail upon closer inspection. They are not genuine solutions to societal problems but rather thinly veiled justifications for an unprecedented expansion of governmental power. The costs to privacy, civil liberties, and a free society are immense and irreversible. CBDCs must be exposed for what they truly are – a pernicious step toward a cashless, surveilled, and controlled future.

The Cryptocurrency Contrast: Decentralization Versus Centralization

The rise of digital currencies has presented a fascinating paradox. On one hand, there is the revolutionary promise of cryptocurrencies, born from a desire for decentralization, individual sovereignty, and resistance to traditional gatekeepers. On the other, there is the emergence of CBDCs that are sold with the rhetoric of efficiency and modernization, but they are fundamentally antithetical to the very principles that make cryptocurrencies truly liberating.

At the heart of this divide lies a fundamental disagreement on the very architecture of digital money: decentralization versus centralization. Cryptocurrencies like Bitcoin emerged as a direct response to the perceived failures and vulnerabilities of centralized financial systems. They operate on decentralized networks, where no single entity holds dominion over the public ledger or transactions. This structure distributes power across a global network of participants who validate transactions and secure the ledger. This permissionless nature means anyone can participate, transact, and innovate without needing approval from a central authority. It is a system designed to be resistant to single points of failure, censorship, arbitrary intervention, and centralized control.

This stands in stark contrast to CBDCs that are, by definition, centralized. They were created as a calculated response from governments, mimicking the digital form of crypto while embedding mechanisms that could amplify state oversight and control. CBDCs are issued and controlled by a nation's central bank and represent the ultimate concentration of monetary power. Every transaction, every unit of currency, resides within a system ultimately beholden to state control.

Permissionless access further illustrates this divide. In decentralized cryptocurrency

ecosystems, anyone with an internet connection can participate without seeking approval from gatekeepers. Users generate digital wallets, mine tokens, or engage in transactions freely, embodying a permissionless ethos that democratizes finance and circumvents traditional barriers like banking requirements or geographic limitations. A digital or crypto wallet holds the private “key” – a secret code linked to the corresponding public address – that proves ownership of a specific amount of crypto located at the public address on the particular digital network (e.g., Bitcoin) and thereby grants the ability to authorize transactions.

Whereas, CBDCs are permissioned, meaning access and usage is regulated by authorities and likely require identity verification or compliance with state-mandated protocols. This design may streamline operations for central banks, but it introduces vulnerabilities where governments can deny access to dissidents, enforce spending restrictions, and track behaviors deemed undesirable. The permissionless model of decentralized crypto thus serves as a safeguard against exclusion, allowing even the unbanked to engage in global finance without intermediaries dictating terms.

Pseudonymity versus forced identity revelation is another critical distinction. Decentralized cryptocurrencies enable users to transact under pseudonyms. Transactions are recorded on a public ledger, but the identities of the participants are not directly linked to their wallet addresses. While sophisticated analysis can sometimes de-anonymize transactions, the fundamental design offers a degree of separation between one’s financial activities and their real-world identity. While not fully anonymous, this pseudonymity allows individuals to maintain control over their financial footprints, shielding them from unwanted and unwarranted scrutiny. This is not about enabling illicit activities; it is about safeguarding financial privacy, a fundamental principle of individual freedom.

CBDCs inherently lack this commitment to privacy. The very nature of a centralized, state-controlled digital currency means that the central bank, and by extension the government, has granular insight into all transactions, which are tied directly to verified users. Although proponents argue that “privacy safeguards” are possible, these are granted by design, not inherent to the system.

Consequently, such safeguards can be modified, revoked, or circumvented by legislative or executive fiat. The control remains with the issuer, not the individual. For CBDCs, that is a feature, not a flaw.

Beyond privacy, the concept of censorship resistance is another critical differentiator. In robust decentralized cryptocurrency networks, once a transaction is broadcast and confirmed, it is immutable and cannot be reversed or blocked by any single entity. Decentralized networks like Bitcoin achieve this through a consensus mechanism where “miners” – computers that solve complex mathematical puzzles to validate and secure transactions on the network – worldwide validate blocks, making it computationally infeasible for any single actor to alter or halt the chain without overwhelming majority control.

However, with a CBDC, that power is dangerously real. CBDCs represent the anti-crypto. They are the state’s attempt to co-opt the form of digital currency while stripping away its liberating core. The inherent vulnerability of a centralized system to political pressure, technical failures, and malicious attacks are risks that are far too great to countenance when the fundamental infrastructure of a nation’s money is at stake.

Retail and Wholesale CBDCs

CBDCs are often broken down into two main types: retail CBDCs and wholesale CBDCs. While both are digital currencies, they are designed for very different purposes and audiences. Understanding the distinction is key to grasping the full scope of CBDC development and implementation around the world.

Retail CBDC

A retail CBDC is essentially a digital version of cash available to the general public. It is a direct liability of the central bank, similar to physical cash. Depending on the design, a retail CBDC may allow individuals and businesses to hold accounts directly with the central bank, through commercial banks, or via other authorized intermediaries. This would enable secure, instant payments for everyday transactions, such as buying groceries or paying bills, without relying solely on traditional commercial banks or payment processors. The primary goal is to provide a safe, universally accessible, and efficient payment option for everyone, which could also promote financial inclusion for those without bank accounts. As a direct liability of the central bank, a retail CBDC eliminates commercial

bank credit risk, ensuring its stability is tied to the central bank’s credibility rather than private institutions. This distinguishes it from digital money held as deposits at commercial banks, which are liabilities of those banks, not the central bank.

Wholesale CBDC

A wholesale CBDC, in contrast, is designed for interbank settlements and large-value transactions among commercial banks, central banks, and other authorized financial institutions. It is not intended for public use. Instead, it would be a digital token used by these entities to settle payments. This type of CBDC aims to improve the efficiency, speed, and security of financial markets by enabling real-time settlements of large transactions, such as securities trading or cross-border payments. For example, in the current system, a cross-border payment can take several days to settle. With a wholesale CBDC, these payments could be executed almost instantly and around the clock, reducing both time and cost. It would also reduce counterparty risk in financial transactions because payments would be settled directly and definitively on a secure digital ledger.

Key Differences

The most significant difference between the two is their intended user and purpose. A retail CBDC is for the general public – individuals and businesses – and is meant for everyday payments and to encourage financial inclusion. It would be widely and universally accessible. A wholesale CBDC, on the other hand, is restricted to commercial banks, central banks, and other authorized financial institutions for interbank settlements and large-value transactions. Its accessibility is limited to these entities. While a retail CBDC eliminates commercial bank credit risk as a direct central bank liability, a wholesale CBDC focuses on reducing counterparty risk in financial markets. Ultimately, a retail CBDC has the potential to be transformative for public payments and banking, while a wholesale CBDC is more about revolutionizing the financial market infrastructure.

The Global CBDC Implementation Landscape

As the digital transformation of global finance accelerates, the Atlantic Council’s Central Bank Digital Currency Tracker reveals a remarkable shift in monetary policy worldwide: as of August 2025, 137 countries and currency unions – representing 98 percent of

global GDP – are or were actively exploring CBDCs. This represents a dramatic expansion from just 35 countries in May 2020, signaling an alarming global race toward digitizing sovereign currencies. Central banks advocate for CBDCs by citing compelling motivations for this transformation: enhancing financial inclusion for the unbanked, reducing transaction costs, improving cross-border payment efficiency, and enabling more precise implementation of monetary policy through programmable money.

However, this rapid adoption also introduces significant challenges and concerns, including vulnerability to cyberattacks, potential destabilization of traditional banking systems, and most critically, the erosion of financial privacy through comprehensive transaction monitoring that can enable mass surveillance and governmental control over individual economic activity. This section examines the diverse spectrum of CBDC implementation statuses worldwide – from fully operational systems to pilot programs and early-stage research – analyzing both the transformative potential and the fundamental risks these digital currencies present to the future of money and financial freedom.

CBDC Status in the United States

According to the Atlantic Council's CBDC Tracker, the U.S. has formally banned the development of a CBDC, making it the only country worldwide to do so. This status stems from President Trump's Executive Order 14178 issued in January 2025, which prohibits any U.S. agency from establishing, issuing, or promoting a CBDC, citing concerns over financial stability, privacy, and government overreach. The order effectively terminated any ongoing research or planning for a retail CBDC, which would be accessible to the general public for everyday transactions. Prior to this, the Federal Reserve had been exploring CBDC concepts through initiatives like Project Hamilton, but these efforts were discontinued following the executive action. However, executive orders remain vulnerable to political change – they can be revoked by future presidents, overturned by Congress, or challenged in court. This CBDC ban, while significant, represents a temporary reprieve rather than a permanent safeguard.

The U.S. continues to engage in limited research on wholesale CBDC applications, which are designed for interbank settlements and large-value transactions among financial institutions. Notably, the Federal Reserve is

participating in Project Agorá, a collaborative initiative with the Bank for International Settlements and six other central banks to explore tokenized commercial bank deposits and wholesale CBDCs for cross-border payments. This involvement indicates that while retail CBDC efforts are prohibited, the U.S. remains active in international discussions on wholesale digital currency innovations to enhance payment efficiency and interoperability without direct public issuance.

Legislatively, the U.S. House of Representatives passed the Anti-CBDC Surveillance State Act (H.R. 1919) in July 2025, which seeks to prohibit the Federal Reserve from issuing a CBDC or offering related services directly to individuals without explicit congressional authorization. As of August 2025, the bill has advanced to the Senate for consideration but has not yet become law. If enacted, it would codify the executive ban into statute, further solidifying the U.S. stance against CBDC exploration and positioning it as a global outlier amid widespread international pilots and launches.

Countries With "Operational" CBDCs

Three countries have moved beyond exploration to full CBDC implementation: the Bahamas with its Sand Dollar, Nigeria with the eNaira, and Jamaica with JAM-DEX. These pioneering implementations provide the world's first comprehensive case studies of government-issued digital currencies in operation, revealing both the technical possibilities and the significant challenges of digitizing national monetary systems. Despite official launch status, all three continue to face substantial adoption hurdles that highlight the complex relationship between central bank objectives and public acceptance of digital money.

The Bahamas: Sand Dollar – The Bahamas pioneered the global CBDC landscape with the launch of the Sand Dollar on October 20, 2020, making it the world's first fully implemented retail central bank digital currency. Issued by the Central Bank of the Bahamas, the Sand Dollar serves as a digital version of the Bahamian dollar with equivalent value and accessibility through mobile applications or physical cards for everyday payments. The program was designed to enhance financial inclusion, reduce cash dependency, and improve transaction efficiency across the archipelago, particularly benefiting remote islands where traditional banking infrastructure faces

significant challenges. Operating on a centralized ledger system, the Sand Dollar relies on authorized financial institutions to facilitate public access, and while adoption has grown by 2024, usage remains limited compared to traditional cash transactions and private digital payment methods.

However, the Sand Dollar's implementation has revealed significant concerns regarding privacy erosion, mass surveillance capabilities, and enhanced government control over individual financial autonomy. The centralized ledger architecture records all transactions while linking them to user identities through mandatory Know Your Customer requirements, creating comprehensive digital trails that eliminate the anonymity traditionally provided by cash transactions. This system enables the central bank or government to access detailed transaction histories that could potentially expose highly personal information including individual habits, political affiliations, or medical purchases, thereby threatening free expression and creating particular vulnerabilities for activists or minority populations. The infrastructure's real-time monitoring capabilities facilitate mass surveillance of financial activities, which proves especially concerning in a small nation like the Bahamas where dissent or political opposition often faces close scrutiny, potentially enabling targeted surveillance of individuals with data that could be shared with foreign governments under international agreements.

The centralized nature of the Sand Dollar grants the central bank unprecedented authority to freeze accounts or restrict transactions, creating substantial risks for authoritarian overreach that could manifest during periods of political unrest when governments might limit dissidents' access to funds, thereby stifling protest activities or suppressing free speech. The system's programmable features further amplify these concerns by potentially allowing authorities to impose restrictions on where or how Sand Dollars can be spent, fundamentally altering the relationship between citizens and their monetary system while expanding state control over individual financial decisions.

Jamaica: Jam-Dex – Jamaica entered the CBDC arena with the launch of Jam-Dex in July 2022, establishing its digital currency as legal tender under the authority of the Bank of Jamaica. Operating on a centralized platform accessible through digital wallets for retail transactions, Jam-Dex was designed to reduce cash usage and promote financial inclusion

throughout the country. The program has concentrated on expanding domestic reach by integrating the digital currency into everyday transactions including public transportation and retail purchases, achieving growing adoption by 2024, particularly among urban populations who have greater access to the necessary technological infrastructure.

Despite these implementation successes, Jam-Dex presents serious privacy and control concerns that mirror broader CBDC risks while reflecting Jamaica's specific political and social context. The system's mandatory user registration requirements link all transactions to individual identities, effectively eliminating the cash-like anonymity that traditionally protected sensitive personal financial information. This comprehensive tracking capability exposes citizens to potential misuse of their transaction data, particularly regarding purchases of political materials or donations to controversial causes, with the central bank's access to this information creating risks for abuse, especially significant given Jamaica's history of political polarization and social tensions.

The centralized ledger system enables real-time tracking of all financial transactions, establishing a surveillance apparatus capable of monitoring citizens' financial behavior with unprecedented precision. This monitoring capability proves particularly concerning for vulnerable populations including activists, journalists, and political dissidents who may face retaliation based on their spending patterns or financial associations. Furthermore, Jam-Dex's programmable features could enable the government to impose targeted restrictions during crises or against specific groups, potentially suppressing protests by cutting off funding sources or enhancing state control over dissenting voices, thereby fundamentally altering the balance of power between citizens and government authorities.

Nigeria: eNaira – Nigeria launched the eNaira on October 25, 2021, as the country's official central bank digital currency issued by the Central Bank of Nigeria. Built on a blockchain-based platform accessible through digital wallets, the eNaira was designed to reduce cash dependency, enhance financial inclusion, and combat illicit transactions within Africa's largest economy. The system supports both retail and wholesale transactions, though adoption has progressed slowly due to public skepti-

cism and significant infrastructure challenges that reflect Nigeria's complex economic and technological landscape. By 2024, the eNaira has achieved integration into some government payment systems and merchant transactions, though widespread adoption remains limited by various practical and cultural barriers.

The eNaira's implementation raises substantial concerns about privacy erosion within Nigeria's complex social and political environment. While the system operates on blockchain technology that appears distributed, the central bank maintains control over the ledger and requires comprehensive user identification for all transactions. This architecture eliminates financial anonymity and creates transaction records that could reveal highly sensitive information about individual purchases, including medical treatments or religious activities – information that could be weaponized against individuals in a country characterized by significant religious and ethnic tensions that often manifest in social and political conflicts.

The eNaira's comprehensive traceability capabilities enable mass surveillance that proves particularly troubling given Nigeria's historical record of government surveillance targeting activists, journalists, and political opposition figures. The system's data collection and monitoring capabilities could facilitate citizen profiling activities, especially during periods of political unrest when government authorities might seek to identify and suppress dissenting voices. The central bank's control over the eNaira infrastructure provides authorities with the ability to freeze accounts or restrict transactions, creating substantial risks in Nigeria's volatile political climate where such powers could be abused to silence opposition or target specific ethnic or religious groups. The currency's programmable features further amplify these concerns by potentially enabling discriminatory policies that could limit funding for certain communities or organizations, thereby reinforcing authoritarian control mechanisms and providing new tools for stifling dissent while expanding state surveillance capabilities over individual financial autonomy.

The Real-World Impact of CBDCs

The experiences of the Bahamas, Jamaica, and Nigeria reveal a disturbing pattern that transcends geographic, economic, and political differences: regardless of a nation's size, development level, or governmental structure, the implementation of CBDCs consistently creates identical mechanisms for

privacy destruction, mass surveillance, and authoritarian control. From the Caribbean archipelagos to West Africa, these pioneering systems have eliminated the fundamental anonymity that cash provides, replacing it with comprehensive digital tracking that exposes citizens' most sensitive financial behaviors to government scrutiny. The technical architecture may vary – from the Bahamas' centralized ledger to Nigeria's blockchain platform – but the outcome remains constant: citizens find themselves subject to real-time monitoring, account freezing capabilities, and programmable restrictions that can be weaponized against political dissent, activism, or any behavior deemed undesirable by the state.

Most tellingly, all three nations struggle with low adoption rates despite years of promotion, indicating that populations instinctively recognize the fundamental threat CBDCs pose to personal freedom and financial privacy. These early implementations serve not as success stories, but as proof-of-concept demonstrations that CBDCs function exactly as critics have warned – as sophisticated tools for financial surveillance and social control that governments can deploy regardless of their stated democratic values or constitutional protections, making the global expansion of this technology a clear and present danger to individual liberty worldwide.

Countries With "Pilot" CBDCs

While only three nations have fully launched CBDCs, a much larger group of 49 countries are currently operating pilot programs, representing the most extensive phase of CBDC development where theoretical concepts meet real-world testing. These pilot programs span diverse economic systems and regulatory environments, from authoritarian regimes to democratic societies, providing crucial insights into both the technical feasibility and public reception of government-controlled digital currencies. Among these pilot nations are some of the world's most influential economies, including China with its digital yuan, India's digital rupee, Japan's digital yen trials, Brazil's digital real program, and the European Union's digital euro development. These five economic powerhouses collectively represent a significant portion of global GDP and diverse monetary policy approaches, making their pilot experiences particularly revealing about the challenges and resistance patterns that emerge when central banks attempt to digitize national currencies. Their ongoing struggles with public adoption, privacy concerns, and competition

from existing payment systems offer encouraging lessons about the gap between central banking ambitions and citizen acceptance of financial surveillance infrastructure.

China (Digital Yuan/e-CNY): China's e-CNY pilot, launched in 2020 across multiple cities including Shenzhen, Suzhou, and Beijing, represents the world's most extensive CBDC testing program, yet it faces persistent adoption challenges despite years of development. Despite more than three years of piloting, the government is still struggling to find compelling applications and adoption has been minimal, with users reluctant to switch from established platforms like Alipay and WeChat Pay even after promotional events in pilot regions. The slow adoption suggests that existing electronic payment systems can be a significant deterrent to CBDC uptake, while privacy concerns and fears that the Communist Party could use it for surveillance have created resistance both domestically and internationally. The Atlantic Council notes that while adoption has been low, the broad range of applications suggests that testing, rather than adoption, is the current priority. Public statistics confirm that the digital yuan remains unpopular, with anecdotal evidence suggesting most people continue using traditional payment methods.

India (Digital Rupee/e-Rupee): India launched its digital rupee pilot in December 2022, targeting both wholesale and retail segments, but has encountered significant conceptual confusion and competitive challenges from existing payment systems. As of September 2024, the pilot operates with more than five million users across 16 participating banks, though the Reserve Bank of India emphasizes it is in "no rush" for full-scale launch. Indians are grappling with fundamental questions about CBDCs, including distinguishing between wholesale and retail versions, and there is significant ambiguity around India's public policy goals for the CBDC, with the pilot facing hurdles from UPI dominance and privacy concerns. Technical challenges include connectivity issues in rural India and interoperability problems with existing systems that the RBI must address. The International Monetary Fund has noted too many parallels between existing instant payment systems and CBDCs, which could restrict adoption of the new digital currency. The pilot's measured approach reflects recognition that India's already-successful UPI system may make a CBDC redundant for many use cases.

Japan (Digital Yen Pilot): Japan's central bank began CBDC experimentation in 2021 and has progressed through multiple phases of testing, though the Bank of Japan maintains a cautious approach toward full implementation. The pilot program has focused primarily on basic functionality testing, including issuance, distribution, and redemption of digital currency, with particular attention to offline payment capabilities and privacy features. While technical testing has progressed smoothly, Japanese officials have emphasized that any decision on actual issuance will depend heavily on public acceptance and clear demonstration of benefits over existing payment systems. The Bank of Japan has been particularly concerned about potential impacts on the banking system and has designed its pilot to minimize disintermediation risks. Recent phases have included limited private sector participation to test real-world scenarios, though adoption metrics remain limited. The central bank has indicated that any full launch would require extensive collaboration with private financial institutions and robust legal frameworks.

Brazil (Digital Real Pilot): Brazil's central bank launched its CBDC pilot program in 2023, focusing on both domestic payments and potential integration with existing payment infrastructure like PIX, the country's highly successful instant payment system. The pilot has tested various use cases including offline payments, smart contracts for conditional payments, and integration with government social programs, though early results show limited adoption beyond testing participants. Brazilian officials have expressed particular interest in using CBDCs for targeted social spending and financial inclusion initiatives, especially in underbanked regions. However, the pilot has faced challenges competing with PIX, which already provides instant, free digital payments and has achieved massive adoption since its 2020 launch. Privacy advocates have raised concerns about the potential for enhanced government surveillance through the digital real, particularly given Brazil's history of financial monitoring. The central bank has emphasized that any full rollout would maintain strong privacy protections, though technical specifications remain under development.

European Union (Digital Euro): The European Central Bank's digital euro project entered its preparation phase in 2021, with the Governing Council set to decide by the end of 2025 whether to move to the next phase,

though final issuance decisions await EU legislative framework adoption. The project faces numerous challenges including privacy concerns, the complexity of coordinating across 27 EU member states, a lack of compelling consumer use cases, and competition with existing digital payment solutions like cards and wallets. Testing has focused on technical architecture, privacy features, and potential limits on individual holdings to prevent bank disintermediation, with particular attention to offline functionality and cross-border payments within the eurozone. While no technical barriers were identified during preliminary planning phases, the project must navigate complex political considerations as different member states have varying priorities and concerns about monetary sovereignty. The ECB has emphasized that the digital euro would complement, not replace, cash and existing payment methods, though critics worry about potential impacts on commercial banking and financial privacy across Europe's diverse regulatory landscape.

A Global Pattern of Skepticism and Resistance

Across these five major economies piloting CBDCs, a consistent pattern of public resistance and reluctant adoption has emerged, suggesting widespread skepticism about transitioning from existing payment systems to government-controlled digital currencies. In China, concerns about heightened surveillance by the government have compounded resistance to adoption, while users continue preferring established platforms like Alipay and WeChat Pay despite years of government promotion and incentives. India faces similar challenges as citizens question the necessity of a digital rupee when the highly successful UPI system already provides instant, free digital payments, with privacy advocates raising concerns about enhanced government monitoring capabilities. Japan's cautious approach reflects public wariness about financial privacy and banking system disruption, while Brazil's pilot struggles to demonstrate advantages over the popular PIX payment system, with civil society groups voicing surveillance concerns. In the European Union, the digital euro project confronts resistance from privacy advocates, concerns about banking disintermediation, and skepticism from member states worried about monetary sovereignty and surveillance capabilities. This collective resistance across diverse political and economic systems suggests that populations worldwide intuitively

Central Bank Digital Currencies (cont.)

recognize the fundamental trade-offs CBDCs represent: the surrender of financial privacy and autonomy in exchange for promised efficiencies that existing systems often already provide, creating a natural barrier to adoption that central banks have yet to overcome despite extensive technical development and promotional efforts.

Countries in CBDC “Development” Stage

Countries in the “development” stage have progressed beyond theoretical research to active CBDC system construction. According to the Atlantic Council’s CBDC tracker, approximately 20 nations are currently in this development stage, having made strategic decisions to move from research into tangible implementation efforts. This stage involves sophisticated technical architecture development, regulatory framework drafting, and preliminary system testing, distinguishing itself through concrete progress toward creating functional CBDC systems with clearly defined use cases for either retail consumer transactions or wholesale interbank settlements.

The development stage encompasses key

technical and operational milestones demonstrating serious commitment to CBDC implementation. Countries actively design core system architectures using blockchain technology, centralized ledger systems, or hybrid models while crafting comprehensive regulatory frameworks addressing monetary policy integration, financial stability implications, and compliance requirements. Internal testing protocols evaluate system performance, security vulnerabilities, and operational efficiency before advancing to public pilot programs. Notable countries in this phase include Colombia, Mexico, Peru, and the United Kingdom, each approaching CBDC development with distinct national priorities and technical strategies.

The development stage introduces significant concerns regarding centralized infrastructures that fundamentally alter citizen-government monetary relationships. As these countries design CBDC architectures, they embed capabilities for comprehensive transaction tracking, mandatory KYC requirements, and programmable money features enabling unprecedented government control over individual financial behavior. These technical design decisions create powerful surveillance mechanisms transcending tradi-

tional banking privacy protections, allowing governments to monitor, restrict, or reverse transactions in real-time. This represents a fundamental shift from cash anonymity toward fully monitored digital monetary systems, raising concerns about CBDCs as tools for expanding government authority over personal economic autonomy.

Countries in CBDC “Research” Stage

Countries in the “research” stage represent the foundational tier of global CBDC exploration, encompassing approximately 36 nations conducting preliminary investigations into the feasibility, implications, and potential frameworks for CBDCs. These countries – including major economies and emerging markets like Argentina, Canada, Egypt, Kenya, and Pakistan – are engaged in comprehensive theoretical work spanning economic impact assessments, policy analysis, and stakeholder consultations. The research stage typically involves commissioning detailed studies on CBDC benefits such as enhanced financial inclusion, improved monetary policy transmission, and payment system efficiency, while simultaneously examining potential risks including banking sector disruption,

Criminal Legal News

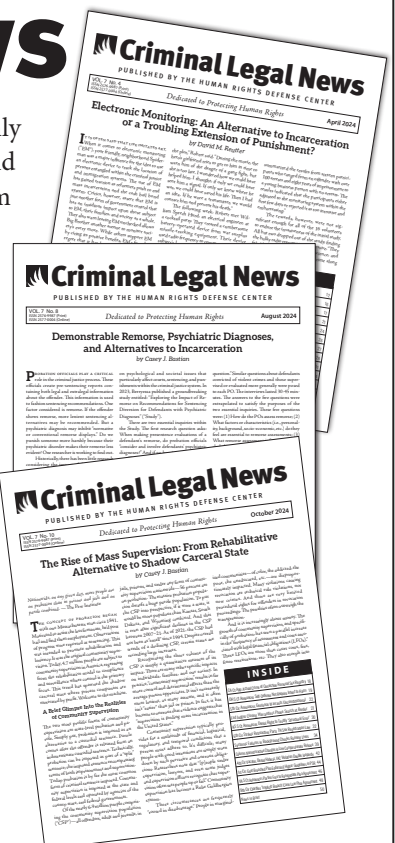
Criminal Legal News is the sister publication of *Prison Legal News*. Both are published monthly by the Human Rights Defense Center, Inc. Same timely, relevant, and practical legal news and features as *PLN*, BUT *CLN* provides legal news you can use about the criminal justice system prior to confinement and post-conviction relief. Coverage includes:

- Criminal Law & Procedure
- Prosecutorial/Police Misconduct
- Ineffective Counsel
- Militarization of Police
- Junk Science
- False Confessions
- Witness Misidentification
- Post-Release Supervision
- Due Process Rights
- Police Brutality
- Habeas Corpus Relief
- Sentencing Errors & Reform
- Surveillance State
- Wrongful Convictions
- Search & Seizure Violations
- Paid/Incentivized Informants
- Police State in America

Between the two publications, every possible interaction with the criminal justice system is reported, analyzed, and exposed.

“STOP RESISTING” and subscribe today!

Subscriptions to *CLN* are \$48/year for prisoners/individuals and \$96/year for professionals/entities. To subscribe, send payment to: Criminal Legal News, P.O. Box 1151, Lake Worth Beach, FL 33460; (561) 360-2523. www.criminallegalnews.org



cybersecurity vulnerabilities, and macroeconomic stability concerns.

The research stage encompasses broad analytical activities designed to establish whether CBDC implementation aligns with national economic and regulatory objectives. Central banks conduct feasibility studies examining technical architecture options from blockchain-based distributed ledger systems to centralized database approaches, while evaluating operational complexities of integrating digital currencies with existing financial infrastructure. This process involves establishing policy objectives and success measures while identifying and quantifying risks, creating comprehensive decision-making frameworks. Economic impact assessments analyze potential effects on monetary policy effectiveness, banking sector stability, and payment system competition, while regulatory reviews examine necessary legal frameworks, consumer protection measures, and anti-money laundering compliance requirements.

The diversity of countries reflects varying motivations across different economic contexts. Developed economies like Canada focus on maintaining monetary sovereignty and payment system resilience, while emerging markets pursue CBDCs for enhancing financial inclusion, reducing correspondent banking reliance, and addressing currency stability challenges.

However, even this preliminary phase establishes foundational surveillance infrastructure elements. The research process requires central banks to engage with digital platforms, establish technology partnerships, and collect extensive data on payment patterns and consumer behavior. Central banks necessarily examine transaction tracking capabilities, identity verification requirements, and programmable money features – research that normalizes surveillance mechanisms within monetary policy frameworks, creating pathways toward financial privacy erosion before any CBDC system becomes operational.

Countries in CBDC “Inactive” or “Canceled” Stage

As global CBDC momentum accelerates with 137 countries and currency unions exploring digital currency initiatives, a critical but overlooked category emerges: nations that have abandoned, canceled, or allowed their CBDC programs to become inactive. Countries including Belize, Ecuador, Uganda, Vietnam, and Zambia have either implemented CBDCs that failed and were abandoned or explored

digital currencies before canceling them, providing crucial insights into the practical challenges and inherent risks of centralized digital currency systems.

The “inactive” classification encompasses countries that previously engaged in substantive CBDC exploration – including research, development, or pilot testing – but have ceased all activities without formal cancellation announcements. This dormant status typically results from shifting governmental priorities, insufficient resources, insurmountable technical challenges, or political changes redirecting focus away from digital currency implementation. Twenty-one countries are listed in the inactive stage, including Denmark, Iceland, Kuwait, Venezuela, and North Korea.

The “canceled” stage represents decisive rejection of CBDC implementation, where countries formally discontinued efforts following assessments revealing unacceptable risks or obstacles. Ecuador and Senegal have officially canceled programs, demonstrating explicit policy decisions to terminate development after initial exploration. These cancellations frequently stem from banking sector disruption concerns, cybersecurity vulnerabilities, regulatory complexities, or privacy and financial autonomy concerns. Ecuador exemplifies this dynamic, where central bank refusal to support digital money has created significant skepticism among government and banking officials. The inactive designation reveals the volatile nature of centralized digital currency adoption, where political and economic pressures can rapidly transform ambitious CBDC programs into abandoned initiatives.

From a surveillance perspective, both inactive and canceled programs present ongoing risks transcending apparent abandonment. Foundational infrastructure developed during active phases often remains embedded within central banking systems, leaving behind intelligence-gathering capabilities, technological partnerships, and monitoring protocols that create persistent privacy vulnerabilities. These dormant surveillance infrastructures could be reactivated under different political circumstances, meaning canceled programs may represent temporary setbacks rather than permanent rejections of centralized monetary control.

Countries With CBDC Status of “Other”

The “other” classification within the Atlantic Council’s CBDC Tracker encompasses countries and jurisdictions whose digital currency

activities resist conventional categorization, representing a complex landscape of ambiguous, transitional, or uniquely structured CBDC engagements that fall outside standard research, development, pilot, or launch phases. This category includes nations participating in innovative cross-border initiatives such as Project mBridge, which involves the Hong Kong Monetary Authority, the Bank of Thailand, the Central Bank of the United Arab Emirates, the Saudi Central Bank, and the Digital Currency Research Institute, with the IMF and more than 19 central bank observers. Similarly, the U.S. presents a unique case where President Trump issued an executive order to halt all work on a retail CBDC while continuing to engage in wholesale cross-border payments research through Project Agorá in collaboration with six other major central banks.

Countries classified as other frequently represent exploratory or informal activities where governments have expressed interest in CBDCs without establishing formal programs, engaging instead in preliminary discussions, public consultations, or private sector collaborations that lack clear research or development frameworks. This category also encompasses jurisdictions with paused or undefined efforts that have initiated CBDC-related activities but suspended them without official cancellation, creating ambiguous status due to lack of public updates or transparent communication about future intentions. Some countries participate in hybrid or non-standard initiatives that blend CBDC exploration with other digital currency projects, such as stablecoin partnerships or blockchain experiments, that do not align strictly with traditional central bank issuance models.

From a surveillance perspective, the other classification represents perhaps the most insidious category, as it masks countries’ digital currency involvement while potentially facilitating covert surveillance infrastructure development. The ambiguous nature provides governments with plausible deniability regarding CBDC intentions while enabling participation in data collection, technology partnerships, and cross-border monitoring systems through seemingly benign collaborative projects, advancing financial privacy erosion through incremental and largely invisible means.

Conclusion

CBDCs stand as a profound threat to the fabric of free societies, weaving together unprecedented surveillance, programmable control, and the erosion of personal autonomy

under the guise of modern convenience. Throughout this examination, the evidence has mounted: from the granular tracking embedded in systems like China's e-CNY, where tiered accounts demand identity verification and create permanent records of daily life, to the programmable features in India's digital rupee trials that enforce expiration dates and spending restrictions. These are not abstract perils but concrete mechanisms that central banks are actively building, enabling governments to monitor every transaction, infer personal details, and dictate economic behavior. The panopticon analogy holds firm – citizens, aware of constant oversight yet uncertain of when they are targeted, would self-censor their choices, avoiding donations to dissenting causes or purchases that might draw scrutiny. This chilling effect, as documented in analyses of existing financial surveillance, stifles dissent, journalism, and vulnerable communities, transforming money from a tool of individual empowerment into an instrument of state dominance.

The global landscape underscores the urgency of resistance. As of August 2025, 137 countries and currency unions, encompassing 98 percent of global GDP, are pursuing CBDCs in various stages – from full launches in the Bahamas, Jamaica, and Nigeria to pilots in economic giants like China, India, Japan, Brazil, and the European Union. In these pilots, the promised efficiencies falter against the reality of surveillance infrastructures that link transactions to identities, cross-reference with government databases, and enable geofencing or negative interest rates to coerce behavior. Even in development and research stages, nations like Colombia, Mexico, Peru, the United Kingdom, Argentina, Canada, Egypt, Kenya, and Pakistan are laying groundwork for similar controls, normalizing data collection that could be weaponized against citizens. Inactive or canceled programs in places like Belize, Ecuador, Uganda, Vietnam, and Zambia offer false comfort; the surveillance capabilities developed often linger, ready for reactivation under shifting political winds.

Yet amid this tide, the U.S. emerges as a critical outlier, having formally prohibited retail CBDC development through Executive Order 14178 in January 2025, which halted all related work to safeguard privacy and prevent overreach. This executive action,

reinforced by the House-passed Anti-CBDC Surveillance State Act (H.R. 1919) awaiting Senate consideration as of August 2025, positions America as the sole nation to outright ban such currencies, while permitting limited wholesale research in projects like Agorá for interbank efficiency. This stance is no accident but a deliberate rejection of the dangers that have materialized elsewhere – the loss of cash-like anonymity, the politicization of payments, and the fusion of economic policy with repression, as seen in the Canadian trucker protests where financial freezing foreshadowed CBDC-enabled suppression. By preserving decentralized alternatives like cryptocurrencies, which offer pseudonymity and censorship resistance through permissionless networks, the U.S. upholds a model where innovation serves individuals, not states.

The false narratives peddled by proponents – financial inclusion, efficiency, crime reduction, and innovation – crumble under scrutiny. Inclusion rings hollow when CBDCs demand digital access that excludes the underserved, efficiency masks surveillance burdens that create single points of failure, anti-crime rhetoric justifies treating all as suspects, and innovation stifles private-sector creativity in favor of top-down stagnation. These are not solutions but pretexts for control, echoing historical abuses where financial levers silenced opposition. In authoritarian regimes, CBDCs already amplify social credit systems and transaction penalties; in democracies, they risk the same slide, integrating with health mandates or environmental nudges to engineer society from the wallet.

Citizens must recognize this Trojan horse for what it is: a gateway to a cashless dystopia where governments hold absolute sway over economic life, freezing funds, restricting mobility, and punishing non-conformity with a keystroke. The line between policy and repression vanishes, turning free markets into command economies at the micro level. Resistance is not optional but imperative – through advocacy, legislation, and support for privacy-preserving alternatives like cash and decentralized crypto such as Bitcoin. The window to act is narrowing as global adoption accelerates. History teaches that power unchecked corrupts absolutely. When it comes to money, that corruption is total, irrevocable, and devastating to personal freedom. 📌

Sources: Bhatia, Nik. "Layered Money: From Gold and Dollars to Bitcoin and Central Bank

Digital Currencies." 2021; Atlantic Council. "Central Bank Digital Currency Tracker." 2025; Bank for International Settlements. "Central Bank Digital Currencies: Foundational Principles and Core Features." 2020; Carstens, Agustín. "Digital Currencies and the Future of the Monetary System." 2021; Cato Institute. "The Risks of Central Bank Digital Currencies to Financial Freedom." 2022; Electronic Frontier Foundation. "Financial Privacy and the Threat of Surveillance." 2021; Federal Reserve. "Project Hamilton: Technical Papers on Central Bank Digital Currency." 2022; International Monetary Fund. "The Rise of Digital Money." 2019; Ledger Insights. "Central Bank Digital Currencies: Privacy and Surveillance Concerns." 2023; Li, Bo. "The Future of Programmable Money." 2021; American Civil Liberties Union. "Financial Privacy in the Digital Age." 2020; Bowman, Michelle. "The Risks of Central Bank Digital Currencies." 2022; Reserve Bank of India. "Digital Rupee Pilot: Progress and Challenges." 2024; Bank of Jamaica. "Jam-Dex: Implementation and Adoption." 2023; Central Bank of Nigeria. "eNaira: Design and Implementation." 2022; Central Bank of the Bahamas. "Sand Dollar: The World's First CBDC." 2021; Bank of Japan. "Digital Yen Pilot: Technical Assessment." 2024; Central Bank of Brazil. "Digital Real Pilot: Early Findings." 2024; White House. "Executive Order 14178: Prohibition on Central Bank Digital Currency." 2025; U.S. House of Representatives. "Anti-CBDC Surveillance State Act (H.R. 1919)." 2025; CoinDesk. "China's Digital Yuan: Surveillance and Adoption Challenges." 2024; The Economist. "The Global Race for Central Bank Digital Currencies." 2023; Forbes. "CBDCs and the Threat to Financial Privacy." 2023; World Economic Forum. "Central Bank Digital Currencies: Opportunities and Risks." 2022; Mises Institute. "Central Bank Digital Currencies: A Threat to Liberty." 2022; Council on Foreign Relations. "The Geopolitics of Digital Currencies." 2023; Brookings Institution. "Central Bank Digital Currencies: Balancing Innovation and Risk." 2022; Bitcoin Magazine. "Bitcoin vs. CBDCs: The Battle for Financial Freedom." 2022; PwC. "Central Bank Digital Currencies: A Global Perspective." 2022; Federal Reserve Bank of St. Louis. "Exploring CBDCs: Risks and Benefits." 2022; Journal of Financial Innovation. "CBDCs: Technology and Policy Considerations." 2023; Quarterly Journal of Economics. "The Economics of Digital Currencies." 2022; Coin Center. "Policy Implications of Central Bank Digital Currencies." 2023; Blockchain Association. "Decentralized Finance vs. CBDCs." 2022.

Human Rights Defense Center Book Store

FREE SHIPPING on all book orders OVER \$50 (effective 9-21-2022 until further notice). \$6.00 S/H applies to all other book orders.

Prison Profiteers: Who Makes Money from Mass Incarceration, edited by Paul Wright and Tara Herivel, 323 pages. **\$24.95**. This is the third book in a series of Prison Legal News anthologies that examines the reality of mass imprisonment in America. Prison Profiteers is unique from other books because it exposes and discusses who profits and benefits from mass imprisonment, rather than who is harmed by it and how. **1063**

Prison Education Guide, by Christopher Zoukis, PLN Publishing (2016), 269 pages. **\$24.95**. This book includes up-to-date information on pursuing educational coursework by correspondence, including high school, college, paralegal and religious studies. **2019**

The Habeas Citebook: Ineffective Assistance of Counsel, 2nd Ed. (2016) by Brandon Sample, PLN Publishing, 275 pages. **\$49.95**. This is an updated version of PLN's second book, by former federal prisoner Brandon Sample, which extensively covers ineffective assistance of counsel issues in federal habeas petitions. **2021**

Prison Nation: The Warehousing of America's Poor, edited by Tara Herivel and Paul Wright, 332 pages. **\$54.95**. PLN's second anthology exposes the dark side of the 'lock-em-up' political agenda and legal climate in the U.S. **1041**

The Ceiling of America, An Inside Look at the U.S. Prison Industry, edited by Daniel Burton Rose, Dan Pens and Paul Wright, 264 pages. **\$24.95**. PLN's first anthology presents a detailed "inside" look at the workings of the American justice system. **1001**

The Criminal Law Handbook: Know Your Rights, Survive the System, by Attorneys Paul Bergman & Sara J. Berman-Barrett, 16th Ed, Nolo Press, 648 pages. **\$39.99**. Explains what happens in a criminal case from being arrested to sentencing, and what your rights are at each stage of the process. Uses an easy-to-understand question-and-answer format. **1038**

Represent Yourself in Court: How to Prepare & Try a Winning Case, by Attorneys Paul Bergman & Sara J. Berman-Barrett, 10th Ed, Nolo Press, 600 pages. **\$39.99**. Breaks down the civil trial process in easy-to-understand steps so you can effectively represent yourself in court. **1037**

Writing to Win: The Legal Writer, by Steven D. Stark, Broadway Books/Random House, 303 pages. **\$19.95**. Explains the writing of effective complaints, responses, briefs, motions and other legal papers. **1035**

The Blue Book of Grammar and Punctuation, by Jane Straus, 201 pages. **\$19.99**. A guide to grammar and punctuation by an educator with experience teaching English to prisoners. **1046**

Legal Research: How to Find and Understand the Law, 19th Ed., by Stephen Elias and Susan Levinkind, 368 pages. **\$49.99**. Comprehensive and easy to understand guide on researching the law. Explains case law, statutes and digests, etc. Includes practice exercises. **1059**

All Alone in the World: Children of the Incarcerated, by Nell Bernstein, 303 pages. **\$19.99**. A moving condemnation of the U.S. penal system and its effect on families" (Parents' Press), award-winning journalist Nell Bernstein takes an intimate look at parents and children—over two million of them - torn apart by our current incarceration policy. **2016**

Blue Collar Resume, by Steven Provenzano, 210 pages. **\$16.95**. The must have guide to expert resume writing for blue and gray-collar jobs. **1103**

Protecting Your Health and Safety, by Robert E. Toone, Southern Poverty Law Center, 325 pages. **\$10.00**. This book explains basic rights that prisoners have in a jail or prison in the U.S. It deals mainly with rights related to health and safety, such as communicable diseases and abuse by prison officials; it also explains how to enforce your rights, including through litigation. **1060**

Spanish-English/English-Spanish Dictionary, 2nd ed., Random House. 694 pages. **\$15.95**. Has 145,000+ entries from A to Z; includes Western Hemisphere usage. **1034a**

The Merriam-Webster Dictionary, 2016 edition, 939 pages. **\$9.95**. This paperback dictionary is a handy reference for the most common English words, with more than 75,000 entries. **2015**

Roget's Thesaurus, 709 pages. **\$9.95**. Helps you find the right word for what you want to say. 11,000 words listed alphabetically with over 200,000 synonyms and antonyms. Sample sentences and parts of speech shown for every main word. Covers all levels of vocabulary and identifies informal and slang words. **1045**

Beyond Bars, Rejoining Society After Prison, by Jeffrey Ian Ross, Ph.D. and Stephen C. Richards, Ph.D., Alpha, 224 pages. **\$14.95**. Beyond Bars is a practical and comprehensive guide for ex-convicts and their families for managing successful re-entry into the community, and includes information about budgets, job searches, family issues, preparing for release while still incarcerated, and more. **1080**

Directory of Federal Prisons: The Unofficial Guide to Bureau of Prisons Institutions, by Christopher Zoukis, 764 pages. **\$99.95**. A comprehensive guidebook to Federal Bureau of Prisons facilities. This book delves into the shadowy world of American federal prisoners and their experiences at each prison, whether governmental or private. **2024**

Merriam-Webster's Dictionary of Law, 634 pages. **\$19.95**. Includes definitions for more than 10,000 legal words and phrases, plus pronunciations, supplementary notes and special sections on the judicial system, historic laws and selected important cases. Great reference for jailhouse lawyers who need to learn legal terminology. **2018**

The Best 500+ Non-Profit Organizations for Prisoners and Their Families, 5th edition, 170 pages. **\$19.99**. The only comprehensive, up-to-date book of non-profit organizations specifically for prisoners and their families. Cross referenced by state, organization name and subject area. Find what you want fast! **2020**

Deposition Handbook, by Paul Bergman and Albert Moore, 7th Ed. Nolo Press, 440 pages. **\$34.99**. How-to handbook for anyone who conducts a deposition or is going to be deposed. **1054**

Please Note: Book orders are mailed via the U.S. Postal Service with delivery confirmation. PLN does not assume responsibility to replace book orders once their delivery to the destination address (facility) is confirmed by the postal service. If you are incarcerated and placed a book order but did not receive it, please check with your facility's mailroom before checking with us. If books ordered from PLN are censored by corrections staff, please file a grievance or appeal the mail rejection, then send us a copy of the grievance and any response you received

Prisoners' Self-Help Litigation Manual, updated 4th ed. (2010), by John Boston and Daniel Manville, Oxford Univ. Press, 928 pages. **\$69.95.** The premiere, must-have "Bible" of prison litigation for current and aspiring jail-house lawyers. If you plan to litigate a prison or jail civil suit, this book is a must-have. Includes detailed instructions and thousands of case citations. Highly recommended! **1077**

How to Win Your Personal Injury Claim, by Atty. Joseph Matthews, 9th edition, NOLO Press, 411 pages. **\$34.99.** While not specifically for prison-related personal injury cases, this book provides comprehensive information on how to handle personal injury and property damage claims arising from accidents. **1075**

Sue the Doctor and Win! Victim's Guide to Secrets of Malpractice Lawsuits, by Lewis Laska, 336 pages. **\$39.95.** Written for victims of medical malpractice/neglect, to prepare for litigation. Note that this book addresses medical malpractice claims and issues in general, not specifically related to prisoners. **1079**

Disciplinary Self-Help Litigation Manual, by Daniel Manville, 355 pages. **\$49.95.** By the co-author of the Prisoners' Self-Help Litigation Manual, this book provides detailed information about prisoners' rights in disciplinary hearings and how to enforce those rights in court. Includes state-by-state case law on prison disciplinary issues. This is the third book published by PLN Publishing. **2017**

The PLRA Handbook: Law and Practice under the Prison Litigation Reform Act, by John Boston, 576 pages. **Prisoners - \$84.95, Lawyers/Entities - \$224.95.** This book is the best and most thorough guide to the PLRA provides a roadmap to all the complexities and absurdities it raises to keep prisoners from getting rulings and relief on the merits of their cases. The goal of this book is to provide the knowledge prisoners' lawyers – and prisoners, if they don't have a lawyer – need to quickly understand the relevant law and effectively argue their claims. **2029**

Everyday Letters for Busy People: Hundreds of Samples You Can Adapt at a Moment's Notice, by Debra May, 287 pages. **\$21.99.** Here are hundreds of tips, techniques, and samples that will help you create the perfect letter. **1048**

Federal Prison Handbook, by Christopher Zoukis, 493 pages. **\$74.95.** This leading survival guide to the federal Bureau of Prisons teaches current and soon-to-be federal prisoners everything they need to know about BOP life, policies and operations. **2022**

Locking Up Our Own, by James Forman Jr., 306 pages. **\$19.95.** In *Locking Up Our Own*, he seeks to understand the war on crime that began in the 1970s and why it was supported by many African American leaders in the nation's urban centers. **2025**

Jailhouse Lawyers: Prisoners Defending Prisoners v. the U.S.A., by Mumia Abu-Jamal, 286 pages. **\$16.95.** In *Jailhouse Lawyers*, Prison Legal News columnist, award-winning journalist and death-row prisoner Mumia Abu-Jamal presents the stories and reflections of fellow prisoners-turned advocates who have learned to use the court system to represent other prisoners—many uneducated or illiterate—and in some cases, to win their freedom. **1073**

The Habeas Citebook: Prosecutorial Misconduct, by Alissa Hull, 300 pages. **\$59.95.** This book is designed to help pro se litigants identify and raise viable claims for habeas corpus relief based on prosecutorial misconduct. Contains hundreds of useful case citations from all 50 states and on the federal level. **2023**

Arrest-Proof Yourself, Second Edition, by Dale C. Carson and Wes Denham, 376 pages. **\$16.95.** What do you say if a cop pulls you to search your car? What if he gets up in your face and uses a racial slur? What if there's a roach in the ashtray? And what if your hot-headed teenage son is at the wheel? If you read this book, you'll know exactly what to do and say. **1083**

Caught: The Prison State and the Lockdown of American Politics, by Marie Gottschalk, 496 pages. **\$27.99.** This book examines why the carceral state, with its growing number of outcasts, remains so tenacious in the United States. **2005**

Encyclopedia of Everyday Law, by Shae Irving, J.D., 11th Ed. Nolo Press, 544 pages. **\$34.99.** This is a helpful glossary of legal terms and an appendix on how to do your own legal research. **1102**

*** ALL BOOKS SOLD BY PLN ARE SOFTCOVER / PAPERBACK ***

To Pay by Credit Card, Go to Our Website: www.criminallegalnews.org or Call Us at 561-360-2523

Subscription Rates

| | 1 Year | 2 Years | 3 Years | 4 Years |
|--|-------------|--------------|--------------|--------------|
| Prisoners/Individuals | \$48 | \$96 | \$144 | \$192 |
| Professionals (attorneys, agencies, libraries) | \$96 | \$192 | \$288 | \$384 |

Mail Payment
and Order to:

Human Rights Defense Center
PO Box 1151
Lake Worth Beach, FL 33460

Please Change my Address to what is entered below: ☐

Ship Order To:

Name: _____
DOC #: _____
Suite/Cell: _____
Agency/Inst: _____
Address: _____
City/State/Zip: _____

Subscription Bonuses

2 year subscription include 2 extra issues
3 year subscription include 4 extra issues
4 year subscription include 6 extra issues

(All subscription rates and bonus offers are valid as of 1/1/2022)

Subscribe to Criminal Legal News

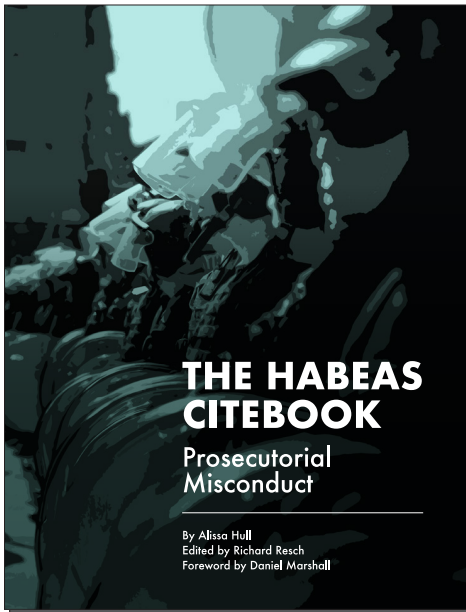
6 month subscription (prisoners only) - \$28 _____
1 yr subscription _____
2 yr subscriptions (2 bonus issues) _____
3 yr subscriptions (4 bonus issues) _____
4 yr subscriptions (6 bonus issues) _____
Single back issue or sample copy of CLN - \$6.00 _____

Book Orders

_____ _____
_____ _____
_____ _____
_____ _____
Add \$6.00 S/H to BOOK ORDERS under \$50 _____
FL residents ONLY add 7% to Total Book Cost _____
TOTAL Amount Enclosed: _____

*** NO REFUNDS on CLN subscription or book orders after orders have been placed. ***

*** We are not responsible for incorrect addresses or address changes after orders have been placed. ***



The Habeas Citebook: Prosecutorial Misconduct

By Alissa Hull

Edited by Richard Resch

The Habeas Citebook: Prosecutorial Misconduct is part of the series of books by Prison Legal News Publishing designed to help pro se prisoner litigants and their attorneys identify, raise and litigate viable claims for potential habeas corpus relief. This easy-to-use book is an essential resource for anyone with a potential claim based upon prosecutorial

misconduct. It provides citations to over 1,700 helpful and instructive cases on the topic from the federal courts, all 50 states, and Washington, D.C. It'll save litigants hundreds of hours of research in identifying relevant issues, targeting potentially successful strategies to challenge their conviction, and locating supporting case law.

The Habeas Citebook: Prosecutorial Misconduct is an excellent resource for anyone seriously interested in making a claim of prosecutorial misconduct to their conviction. The book explains complex procedural and substantive issues concerning prosecutorial misconduct in a way that will enable you to identify and argue potentially meritorious claims. The deck is already stacked against prisoners who represent themselves in habeas. This book will help you level the playing field in your quest for justice.

—Brandon Sample, Esq., Federal criminal defense lawyer, author, and criminal justice reform activist

The Habeas Citebook: Prosecutorial Misconduct

Paperback, 300 pages

\$59.95

(includes shipping)

Order by mail, phone, or online. Amount enclosed _____

By: ☐ check ☐ credit card ☐ money order

Name: _____

DOC/BOP Number: _____

Institution/Agency: _____

Address: _____

City: _____ State: _____ Zip: _____



Human Rights Defense Center
Dedicated to Protecting Human Rights

PO Box 1151 • Lake Worth Beach, FL 33460 • Phone # 561-360-2523
WWW.PRISONLEGALNEWS.ORG • WWW.CRIMINALLEGALNEWS.ORG



Criminal Legal News

PO Box 1151
Lake Worth Beach FL 33460

CHANGE SERVICE REQUESTED

Non-Profit Org.
U.S. Postage
PAID
Portland OR
Permit No. 3142

9/25 — Subscription Renewal

The above mailing address for CLN subscribers indicates how many issues remain on the subscription. For example, if it says "10 LEFT" just above the mailing address, there are 10 issues of CLN remaining on the subscription before it expires. IF IT SAYS "0 LEFT," THIS IS YOUR LAST ISSUE. Please renew at least 2 months before the subscription ends to avoid missing any issues.

Change of Address

If you move or are transferred, please notify CLN as soon as possible so your issues can be mailed to your new address! CLN only accepts responsibility for sending an issue to the address provided at the time an issue is mailed!

The screenshot shows a web browser window with the address bar displaying www.criminallegalnews.org. The main heading on the page is "Criminal Legal News is online!". Below this, the text states: "Full issues of CLN are available on our website at www.criminallegalnews.org." It then continues: "In addition to the content available in CLN's print issues, our website contains updated criminal justice related news stories, subscribing and book ordering information, ability to search all past articles, HRDC Litigation Project information, and much more!" The final line of text is: "Visit us online today for all your criminal justice related news and information!"

Criminal Legal News is online!

Full issues of CLN are available on our website at www.criminallegalnews.org.

In addition to the content available in CLN's print issues, our website contains updated criminal justice related news stories, subscribing and book ordering information, ability to search all past articles, HRDC Litigation Project information, and much more!

Visit us online today for all your criminal justice related news and information!