LAST ASSET STANDING

Permission to Share

Free-Use Distribution License

The information contained in this White Paper is too important to be locked behind traditional copyright. As the authors, Peter J. Merrick and Adrian C. Spitters, we believe this work must remain freely accessible to anyone who seeks to understand it. To that end, we have adopted a Free-Use Distribution License.

You are permitted to:

- **Download & Share** – A free, shareable copy is available at ***www.ItStartsWithGold.com***.
- Write About It – Use the content as the basis for articles, reviews, or commentary, with proper attribution.
- **Discuss in Any Medium** – Talk about this work in podcasts, videos, social media, or public presentations, as long as the original source is acknowledged.
- **Create Memes** – Share memes or creative works inspired by this White Paper, provided they reference this White Paper clearly and do not alter the original message.

You may share, distribute, and use this White Paper for personal or professional use, as long as:

- The original text remains unaltered
- It is not modified, adapted, or used to create derivative works

This license is designed to encourage awareness, dialogue, and action. Truth should not be hidden behind paywalls.

Last Asset Standing

By Peter J. Merrick and Adrian C. Spitters, co-authors of the #1 International Bestseller It Starts With Gold™

Were Bitcoin and Other Cryptocurrencies Part of a Larger Control Grid?

This white paper explores the growing debate about the true origins of Bitcoin and other cryptocurrencies. It examines the theory that these systems may have been seeded or later co-opted by intelligence agencies, and now mirror state-backed surveillance architecture, including central bank digital currencies (CBDCs). The paper is presented as an open investigation, intended to inform, provoke thought, and invite contributions.

This story does not begin in 2008. In 1996, the United States National Security Agency quietly released a whitepaper titled *"**How to Make a Mint: The Cryptography of Anonymous Electronic Cash**."* It outlined a system of digital money strikingly similar to what Bitcoin would become. It featured public-key encryption, timestamped ledgers, and pseudonymity that was never truly anonymous. This early blueprint raises enduring questions about whether the financial freedom promised by Bitcoin was already designed with surveillance compatibility in mind.

Importantly, this technological vision did not emerge in isolation. It took shape within the expanding architecture of ***The Financial Industrial Complex,*** a network of governments, central banks, regulatory agencies, financial institutions, and surveillance technology firms. This system, largely unaccountable to the public, governs the flow of money, data, and digital identity across the globe. Bitcoin, rather than existing outside this complex, may have been designed to operate within it, or to condition the public for its next evolution.

To investigate that possibility, we apply two historical frameworks of strategic control: Operation Trust and the Hegelian Dialectic.

Operation Trust was a Soviet-era counterintelligence operation used to pacify dissent by convincing individuals that hidden patriots within the regime were fighting on their behalf. This false reassurance kept resistance passive while the state identified, monitored, and neutralized its opposition.

The Hegelian Dialectic, often summarized as *Problem, Reaction, Solution*, is a mechanism of engineered consent. A crisis is created or exploited, the public demands a fix, and a pre-planned solution is introduced. This solution typically expands centralized control. These frameworks are not relics of history. They remain embedded in modern governance and digital systems.

Together, these strategies form the lens through which this paper examines Bitcoin and its ecosystem. What if Bitcoin were not a rebellion against financial tyranny, but a sophisticated

instrument within it? A release valve that mapped dissident sentiment, normalized traceable money, and trained the public to accept digital ledgers under the illusion of decentralization?

As adoption spread, Bitcoin's architecture, public, timestamped, and surveillance-compatible, began to resemble a prototype for programmable finance. While it was marketed as peer-to-peer money without middlemen or censorship, many of its structural features align with long-standing state interests in behavioural monitoring and financial control.

The same logic now permeates the broader crypto ecosystem, including Ethereum, stablecoins, and other assets operating inside increasingly institutionalized infrastructure. What began as a vision of autonomy has been transformed into a compliance gateway.

This paper is not the final word. It is a living document, a work in progress designed to track, challenge, and expose what may be the most elaborate financial control system ever constructed. We explore the deeper implications of this surveillance-based architecture in our book *It Starts With Gold*™, where we argue that physical gold may represent one of the last real exits from a fully digitized economy.

If you have information technical, historical, institutional, or personal that can strengthen this thesis, we encourage you to contribute.

Adrian C. Spitters – Adrian@ItStartsWithGold.com
Peter J. Merrick – Peter@ItStartsWithGold.com

Together, we can uncover the truth before it disappears behind a wall of code, policy, and propaganda.

Some believe Bitcoin ushered in a new era of financial freedom. Others are beginning to recognize that what followed may have always been part of the plan. In a hyper-monitored financial ecosystem, nothing of systemic consequence is allowed to flourish unless it ultimately serves the goals of those shaping the grid.

We are piecing together a crime scene. A quiet global crime may have already been committed against humanity under the guise of innovation, convenience, and financial freedom.

To uncover whether Bitcoin's evolution was a coincidence or by design, we must start where few are willing to look: the timeline of surveillance infrastructure, long before 2008.

PART I: The Digital Trap Begins

The Internet Was Never Free

To understand what Bitcoin and cryptocurrencies have become, we need to understand where they came from. That trail leads not to cypherpunks in basements, but to military contractors and surveillance think tanks.

The modern internet began not as a tool for human connection, but as a Cold War weapon. In 1969, the United States Department of Defence launched the Advanced Research Projects Agency Network (ARPANET), a military communication network designed to withstand nuclear strikes and reroute digital traffic around damaged infrastructure.

What was sold to the public as innovation was, at its core, a network built for visibility and control. Early adopters were intelligence agencies, government laboratories, and defence-linked universities. Packet switching, Internet Protocol (IP) tracking, and Domain Name System (DNS) administration were never "open" systems. They were engineered from inception with traceability, redundancy, and centralized oversight.

By the time ARPANET gave way to the commercial internet in the 1990s, the architecture had already been set. This foundational architecture would later support not just Bitcoin, but the broader cryptocurrency ecosystem that inherited these same traceable, surveillable design elements.

In *It Starts With Gold*™, we break down how the infrastructure of surveillance was embedded into the internet from the beginning and how it quietly converged with ***The Financial Industrial Complex*** over time, shaping a system of control that now touches nearly every aspect of digital finance.

The NSA's Smoking Gun: How to Make a Mint (1996)

In 1996, the National Security Agency (NSA) published a little-known whitepaper titled "***How to Make a Mint: The Cryptography of Anonymous Electronic Cash***." Quietly released through MIT's cryptographic mailing list, the paper outlined a comprehensive method to build a digital currency using public-key cryptography, blind signatures, distributed ledgers, and timestamping all without needing a central bank.

The paper proposed a pseudonymous system, not truly anonymous, where transactions could remain visible to those with the right tools. It was not a theoretical exploration; it was a working blueprint. And it appeared twelve years before the release of Bitcoin and other cryptocurrencies.

In 2008, Satoshi Nakamoto published ***Bitcoin: A Peer-to-Peer Electronic Cash System***, proposing a decentralized currency that removed reliance on third-party trust. But the structural similarities between the two systems are too specific to ignore.

Both rely on public-key cryptography to authenticate ownership and secure transactions. Both use timestamping to establish a verifiable sequence of activity. The NSA paper proposed a spent-coin database to prevent double-spending. Bitcoin and cryptocurrencies achieved the same goal by publicly recording every transaction on a blockchain.

Crucially, both designs prioritize traceability over true anonymity. Bitcoin's pseudonymous nature reflects the NSA's original vision: a system that appears private but is ultimately transparent and observable. Even the language overlaps. The NSA described cryptographic transfers verified by a trusted system. Bitcoin and cryptocurrencies removed the issuer, but retained every core component: cryptographic signatures, irreversible transactions, and public timestamping.

Nakamoto's paper did not cite *How to Make a Mint*, but the architectural alignment is undeniable. Whether by influence or coincidence, Bitcoin's launch followed a surveillance-compatible model laid out over a decade earlier.

The surveillance-compatible design first outlined in 1996 has since been replicated across a wide range of cryptocurrencies, each built on similar ledger technologies that prioritize transparency, traceability, and institutional observability.

What began as a symbol of financial rebellion may have been the quiet rollout of a programmable ledger designed to satisfy both user demand and institutional control. Bitcoin and cryptocurrencies do not subvert surveillance. They refine it.

PART II: Surveillance Infrastructure Was Never Dismantled

Timeline of Major Events Leading to Today

Each entry in the timeline below marks a step not just in technological advancement, but in the steady centralization and control of what was once thought to be decentralized infrastructure.

1969 – ARPANET Launched

ARPANET was launched by the United States Department of Defence through its Defence Advanced Research Projects Agency. Publicly, it was framed as a project to ensure communication resilience during nuclear war. In reality, it created the first digital network in which every connection could be identified, logged, and controlled. It established the foundation of addressable digital nodes, which could be tracked and monitored at every level. Surveillance was not an afterthought. It was the starting blueprint.

1973 to 1989 – Internet Protocols Evolve

Key internet protocols such as Transmission Control Protocol (TCP), Internet Protocol (IP), and the Domain Name System (DNS) were developed during this period. These were not grassroots inventions. They were engineered through military and university contracts directed by the United States government. These protocols made it possible to trace every online movement from one machine to another. What emerged was not a web of freedom, but a grid of visibility. The architecture gave those with root access the ability to route, restrict, and review all digital traffic.

1990 – ARPANET Decommissioned

As ARPANET was officially shut down, the internet entered its commercial phase. New companies appeared, and the public was sold on the myth of a decentralized cyberspace. Behind the scenes, control over IP address allocations, root server management, and core infrastructure remained with organizations like the Internet Assigned Numbers Authority (IANA), which oversees global coordination of the DNS root, IP addressing, and protocol parameters, and the Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit organization responsible for managing and maintaining the DNS. These were not neutral entities. They were embedded in public-private partnerships tightly aligned with U.S. government policy. The power never left the original hands. It only hid better.

1996 – NSA Publishes “How to Make a Mint”

The National Security Agency (NSA) quietly published a whitepaper titled “***How to Make a Mint: The Cryptography of Anonymous Electronic Cash***” through an MIT mailing list. It described in detail how to construct a digital currency system with public-key encryption, blind

signatures, timestamping, and ledger verification. The paper proposed pseudonymity, but not true anonymity. It mirrored what Bitcoin would later become, down to its structural reliance on decentralized ledgers and cryptographic verification. It offered a system that could mimic financial freedom while remaining traceable. It was not a user guide. It was a trap disguised as a toolkit.

2001 – Secure Hash Algorithm 256 (SHA-256) was Released by the United States National Security Agency (NSA)

In August 2001, the United States National Security Agency (NSA) released Secure Hash Algorithm 256 (SHA-256), part of the SHA-2 family of cryptographic hash functions. It was published through the United States National Institute of Standards and Technology (NIST) and was promoted as an improvement over earlier hash standards. SHA-256 was rapidly adopted across digital authentication systems, certificate validation protocols, and secure data integrity applications.

SHA-256 would later become the foundational cryptographic function used in Bitcoin. It is responsible for securing transactions, validating proof-of-work through mining, and maintaining the integrity of Bitcoin's distributed ledger. While the algorithm is mathematically complex and publicly vetted, its origin raises deeper questions.

In the same year that the United States enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), the same intelligence agency released the cryptographic core of what would become the most prominent supposedly decentralized digital currency. This timing has led some observers to question whether SHA-256 was introduced as part of a longer-term architecture—one that positioned surveillance-compatible tools within open systems under the cover of transparency and innovation.

The end result is that a digital monetary network often viewed as trustless and anonymous relies on cryptographic standards developed by the very agencies tasked with building global monitoring infrastructure. What appears to be secure may, in practice, be predictable to those who constructed the framework.

2001 – USA PATRIOT Act Expands Surveillance

In the aftermath of the September 11 attacks, the United States enacted the USA PATRIOT Act. It changed everything. ***The Financial Industrial Complex*** were turned into surveillance arms of the state. Know Your Customer (KYC) rules became mandatory. Suspicious Activity Reports (SARs) were institutionalized. Banks had to report anything that looked out of place. Privacy was equated with criminality. ***The Financial Industrial Complex*** was captured not with weapons, but with compliance. Every account became a potential threat, and every transaction was recorded.

Financial surveillance did not begin with Bitcoin. As early as the 1970s, intelligence-sharing alliances like the ECHELON network allowed Five Eyes (FVEY – Australia, Canada, New

Zealand, the United Kingdom, and the United States) partners to monitor global telecommunications, including banking data. After the September 11 attacks, the United States Department of the Treasury's Terrorist Finance Tracking Program (TFTP) began monitoring Society for Worldwide Interbank Financial Telecommunication (SWIFT) financial messages. These programs set the precedent for global financial visibility, long before blockchains arrived. Bitcoin and cryptocurrencies did not create the surveillance grid. It slotted into one already built.

We chart this digital encirclement of financial sovereignty step by step in *It Starts With Gold™,* exposing the real trajectory behind the promise of decentralization.

The following timeline illustrates a classic Hegelian Dialectic progression a manufactured crisis, a public reaction of outrage, and a pre-engineered digital solution that reshaped ***The Financial Industrial Complex*** under the illusion of decentralization.

2008 – Bitcoin Whitepaper Released Amid Global Market Collapse

Amid the 2008 global financial crisis, the Bitcoin whitepaper was released on October 31, authored by the pseudonymous Satoshi Nakamoto. The paper, titled *Bitcoin: A Peer-to-Peer Electronic Cash System*, proposed a decentralized, trustless digital currency that operated without banks or intermediaries.

The timing was not incidental. Just weeks earlier, Lehman Brothers collapsed, triggering a worldwide banking panic and eroding public trust in ***The Financial Industrial Complex***. Central banks were rushing to print money. Trillions in wealth had evaporated. Into this moment of engineered chaos came Bitcoin, a supposed technological escape route.

This moment fits the classic Hegelian Dialectic arc: first, the Problem, which was a manufactured collapse of housing and equity markets that triggered public devastation. Then, the Reaction, which included bailouts for the wealthy and mass outrage among ordinary citizens. And finally, the Solution, a decentralized-sounding digital system quietly introduced under the guise of financial freedom.

But what if this "solution" was pre-positioned? Bitcoin and cryptocurrencies arrived not as a rebellion, but as a Hegelian antidote. These decentralized illusions were offered precisely when confidence in central authority was breaking down. It captured the imagination of technologists, libertarians, and gold advocates, but its architecture would later prove ideal for surveillance, programmable control, and institutional capture.

While the public was being offered a digital lifeboat in the form of Bitcoin, central banks were quietly buying gold. The same institutions that printed trillions in fiat currency, which is government-issued money not backed by any physical commodity, were stockpiling physical reserves: real, tangible assets outside the digital grid. Fiat derives its value from legal decree and public trust. Unlike gold, it can be created in unlimited quantities at the discretion of central banks, leading to inflation and devaluation. As ordinary citizens explored a new "trustless" blockchain, sovereign entities were anchoring their wealth in the most trusted asset in human

history. This bifurcation reveals a deeper layer of strategy. It offered the masses a transparent, traceable financial system while consolidating real value out of reach.

Some critics have speculated that Satoshi Nakamoto may never have been a real person, but rather a symbolic signal or institutional alias. A fringe theory, circulating in some online communities, speculates that 'Satoshi Nakamoto' may be a constructed acronym: *Strategic Architecture for Tracking Operations, Surveillance, and Holistic Intelligence, Network Analysis Kernel for Autonomous Monitoring, Observation, Tracking, and Oversight.*

This interpretation is highly speculative and not supported by direct evidence. It is included here not as fact, but to illustrate the level of skepticism that exists around Bitcoin's origins within communities deeply concerned about surveillance and institutional control.

While this interpretation is speculative, it raises an unsettling possibility. Bitcoin may not have been launched in opposition to the surveillance state, but through it.

2009 – Bitcoin Network Goes Live

On January 3, 2009, the first Bitcoin block was mined. Known as the Genesis Block, it included a hidden message: *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."* This phrase was seen by early adopters as a declaration of financial independence.

In reality, it marked the start of a public, immutable transaction ledger that would record every action permanently. From the first transaction onward, Bitcoin's blockchain offered a live, global view of user behaviour, wallet balances, and movement patterns. Transparency became total. Privacy became optional. Anyone who understood network surveillance could already see what was coming.

As the Solution phase of the Hegelian Dialectic unfolded, Bitcoin appeared to offer freedom just as faith in fiat was collapsing. But its architecture ensured that all transactions could be observed, archived, and eventually controlled.

2011 – Occupy Wall Street Emerges, Bitcoin Quietly Gains Traction

In September 2011, the Occupy Wall Street movement erupted in New York City's financial district, catalyzing a global protest against central banking power, economic inequality, and institutional corruption. The phrase "We are the 99 percent" captured public outrage over bailouts, corruption, and rigged markets. As trust in legacy systems collapsed, many sought alternatives.

Bitcoin, still obscure at the time, quietly gained traction among privacy advocates and economic dissidents. It was marketed as a decentralized exit from centralized control. While retail enthusiasm surged toward cryptocurrencies, institutional players responded differently. From 2008 onward, global central banks reversed their role as net sellers and became consistent net buyers of gold. By 2010, they were accumulating over 1,000 tonnes annually.

This contrast, where retail investors rush into digital assets while institutions are fortified with physical bullion, underscores a deeper strategy. The implications of this divergence, and what it reveals about real versus illusory exits, are explored in Part V.

2013 – Snowden Reveals PRISM

In June 2013, Edward Snowden, a former contractor for the National Security Agency (NSA), leaked classified documents revealing the extent of global surveillance programs, including PRISM, the Planning Tool for Resource Integration, Synchronization, and Management. PRISM granted the NSA direct access to the servers of major technology companies, including Google, Microsoft, Facebook, Apple, and Yahoo. This gave the agency the ability to collect emails, video chats, file transfers, search history, and cloud-stored content, all without individual warrants.

It was a watershed moment. For the first time, the public saw evidence that the internet was not simply a decentralized system of free communication. It had become a global surveillance grid. Crypto developers, forum users, and early Bitcoin adopters were not building in a vacuum. They were already inside the net.

But it went deeper. Financial surveillance was not limited to blockchains or internet metadata. It was, and still is, omnipresent. All modern digital transactions leave a trace, and that trace feeds into an ecosystem of data analytics and behavioural monitoring.

Credit card networks like Visa and Mastercard log every purchase with timestamps, merchant identifiers, purchase amounts, and location data. In 2022 alone, Visa processed over 192 billion transactions. Every swipe becomes a data point. This information is routinely shared with banks, advertising platforms, and, through partnerships or subpoenas, with governments.

Retail surveillance adds another layer. Most major retailers in the United States, such as Walmart, Target, and CVS, use high-resolution security cameras integrated with facial recognition. In 2022, a U.S. Senate inquiry raised concerns about companies like Rite Aid and Lowe's deploying facial recognition systems without customer consent. The data, often collected under the guise of loss prevention, was sometimes shared with third-party analytics providers and law enforcement.

Internationally, biometric surveillance is even more advanced. In China, major retailers and financial institutions already link facial recognition with payment systems, allowing customers to pay with their face while feeding biometric and purchase data into national databases. Similar systems are emerging across Europe. In France, for example, facial recognition has been tested in airports and public transport under anti-terror frameworks, while Germany has explored biometric verification in digital banking systems.

These developments suggest that retail and financial sectors in many countries are converging toward an integrated surveillance environment, where purchasing behaviour, facial identity, and digital wallet use are synchronized under the pretext of convenience, fraud reduction, or ESG compliance.

As consumers tap their cards or scan digital wallets, the systems link their physical image to their financial transactions in real time. This data is stored and sometimes analyzed to build customer profiles or detect suspicious activity.

In urban environments, this extends even further. Smart city infrastructure powered by companies like Palantir, Hikvision, and Clearview AI uses a fusion of biometric surveillance, license plate readers, and geofencing to track individual movement. A person walking into a coffee shop in New York City, using tap-to-pay, and stepping onto a subway platform can be tracked continuously through face, card, route, and purchase data synchronized across platforms. Loyalty programs like Starbucks Rewards or Walgreens Balance Rewards quietly log spending behaviour across entire networks of affiliates.

Mobile apps are another backdoor. Even when crypto users employ privacy wallets or mixers, their phones may share background data with analytics providers. If the app uses GPS or Bluetooth, the user's location and social proximity can be inferred. For instance, Google Maps, Uber, and Facebook Messenger all request background location access, even when not in use.

In China, this infrastructure is formalized through the Social Credit System. In the United States and parts of Europe, it is emerging informally through digital ID proposals, carbon-tracking credit cards, and ESG-linked banking initiatives. Every digital action becomes either a point of access or a potential restriction.

The United States, along with countries like the Netherlands, Singapore, and the United Arab Emirates, has participated in biometric surveillance pilot programs tied to air travel. Under the Known Traveller Digital Identity initiative, backed by the World Economic Forum and international border agencies, biometric data, travel history, and behavioural profiles are combined to streamline border crossings. While marketed as a convenience measure, the program introduced a framework for integrating facial recognition and algorithmic risk scoring into broader infrastructure. It is a blueprint for how future financial systems could gate access based on data-driven eligibility.

In this context, the illusion of financial anonymity through cryptocurrency becomes dangerously misleading. Decentralization does not mean protection. It means exposure, especially when every layer of the transaction is embedded within a monitored system.

Privacy is no longer the default. It must be deliberately defended, if it can be defended at all.

2015 – Chainalysis was Founded

In 2015, the blockchain analytics company Chainalysis was launched. It pioneered software that could track cryptocurrency movements, link pseudonymous wallets to real-world identities, and provide surveillance reports to governments and banks. While Bitcoin was the original target, these surveillance tools were soon adapted to monitor Ethereum, stablecoins, privacy tokens, and virtually every major cryptocurrency. This development marked the formal fusion of blockchain and surveillance. Bitcoin's promise of anonymity was shattered. Every transaction was now a thread in a digital profile. The public ledger, once hailed as a breakthrough, became the forensic

foundation of behavioural monitoring. The system was not anonymous. It was engineered visibility.

2017 – Bitcoin Splits

In August 2017, years of debate over Bitcoin's block size culminated in a fork. The original chain split into Bitcoin Core and Bitcoin Cash. Bitcoin Core kept the smaller block size and retained high transaction fees and slower speeds. Bitcoin Cash expanded block sizes to enable faster, cheaper transactions in line with Satoshi's original vision of everyday peer-to-peer payments. The decision to keep Bitcoin Core as the dominant version had consequences. It made Bitcoin less useful for daily spending and more attractive to institutions. The network became easier to regulate, easier to track, and easier to control. It was no longer a currency. It was a speculative asset inside a ring-fenced system.

2020 – Digital Yuan and Bahamas Sand Dollar Launch

In 2020, China formally launched the digital yuan, also known as the e-CNY, through the People's Bank of China. It became the world's first major central bank digital currency (CBDC) pilot tied to a major economy. Unlike cryptocurrencies, the digital yuan was fully centralized and controlled by the Chinese state. It featured biometric integration, time-based spending rules, and programmable restrictions. Transactions could be blocked or expired remotely. That same year, the Bahamas launched its own CBDC, the Sand Dollar, making it the first country to roll out a fully operational digital state currency. These were not academic trials or proof-of-concept demonstrations. They were live systems that allowed governments to control how, when, and where money was used. These programs marked a turning point. Central banks now had the tools to bypass commercial banks and interact directly with citizens' digital wallets.

Monetary sovereignty moved from people to programmable code.

2022 – Canada Freezes Convoy Crypto

In February 2022, during the Freedom Convoy protests in Ottawa, the Canadian government invoked the Emergencies Act and took unprecedented steps to freeze the financial assets of protestors. This included traditional bank accounts, crowdfunding platforms such as GoFundMe and GiveSendGo, and, for the first time in Canadian history, cryptocurrency wallets. Exchanges were ordered to block wallets linked to organizers. Even Bitcoin, long considered censorship-resistant, proved vulnerable. The majority of affected wallets were held on custodial platforms, which complied immediately with government instructions. This shattered the myth of autonomy in digital assets. If your crypto lives on a platform controlled by someone else, then it is no different than a bank account. Financial freedom, it turned out, was an illusion. The infrastructure was already compliant.

During the crackdown, Bitcoin was promoted as an anonymous solution among protest supporters, positioned as a lifeline after donations through GoFundMe and GiveSendGo were either blocked or confiscated. Some have since speculated that this may have served a secondary purpose: to train the Canadian public in the mechanics of Bitcoin usage under duress. What

appeared to be an escape route may have doubled as a live demonstration of how cryptocurrency functions within a compliance-capable system.

2023 – Tornado Cash Developer Arrested

In August 2023, a developer associated with Tornado Cash, an open-source privacy protocol, was arrested in the Netherlands. The crime was not fraud or theft. It was writing and publishing code that enabled anonymous transactions. Tornado Cash allowed users to obfuscate their cryptocurrency history, which angered financial regulators and law enforcement. This arrest marked a turning point. It was no longer about prosecuting criminal use of privacy tools. It was about criminalizing the very idea of privacy. Developers now faced legal risk simply for creating technology that ran counter to the surveillance agenda. Code was no longer treated as free speech. It became a form of resistance, and resistance was met with arrest.

2024 – CBDC Frameworks Released

In 2024, both the United States and Canada released official frameworks for their upcoming central bank digital currencies. These documents, published by the U.S. Federal Reserve and the Bank of Canada, respectively, outlined how CBDCs would be structured, monitored, and integrated into society. Key features included programmable spending limits, wallet ID requirements, and built-in surveillance functions. The systems would link to national tax agencies and social benefit programs, creating a unified digital infrastructure for financial and social oversight.

In Canada, consultation papers and early-stage design proposals for the digital dollar have referenced environmental, social, and governance (ESG) considerations, including exploratory discussions on integrating carbon-tracking or behavioural incentives. While not yet enforced, these features are actively being tested through pilot programs and digital ID frameworks under development, pointing toward future integration with social scoring or programmable restrictions.

Some elements of this scoring architecture are already operational. Mastercard's DO Black card, released in select markets, imposes carbon limits on user spending and automatically declines purchases that exceed a personal carbon allowance. This is no longer theoretical. ESG-linked payment systems are already being normalized under the guise of sustainability and personal responsibility.

2025 – CBDC Laws Passed During War Distraction

In March 2025, amid global tensions in the Middle East, the United States launched a major federal payment modernization effort. Executive Order 14247, titled *Modernizing Payments To and From America's Bank Account*, requires all federal agencies to discontinue paper checks for most disbursements, including vendor payments, tax refunds, and Social Security benefits, by September 30, 2025. It mandates the use of electronic funds transfer methods such as direct deposit, debit and credit cards, digital wallets, and real-time payments. While the Order explicitly states it does not authorize a central bank digital currency, its requirement for

programmable wallets and digital payment infrastructure sketches out the blueprint necessary for a future CBDC rollout.

In the United States, the groundwork for a programmable digital dollar had already been tested. Project Hamilton, a collaboration between the Federal Reserve Bank of Boston and MIT, successfully processed over 1.7 million transactions per second in its 2022 pilot. This prototype demonstrated that CBDC infrastructure is no longer theoretical. It is scalable, operational, and already being refined for deployment. The project did not ask whether this system should be built. It simply proved that it could be and soon would be.

Bitcoin vs Reality (and How Other Cryptocurrencies Followed Suit)

Bitcoin was designed to be a true peer-to-peer cash system. That vision has not held.

Today, Bitcoin and many cryptocurrencies no longer function as peer-to-peer money. Transactions that once promised minimal fees now spike in cost during periods of network congestion, making microtransactions impractical.

While Bitcoin and many cryptocurrencies that followed initially offered the hope of private and anonymous exchange, they are now heavily tracked. Know Your Customer (KYC) laws and blockchain analytics have turned it into one of the most surveilled financial tools on earth.

The principle of self-custody, central to Satoshi's original design, is now the exception, not the rule. Most users hold their assets on regulated exchanges.

Although Bitcoin was built to operate without intermediaries, today the vast majority of activity flows through centralized custodians and institutions.

This evolution has raised a deeper question. Were Bitcoin and other cryptocurrencies always meant to function this way?

Some believe it began as an altruistic project to escape central bank control. Others argue it was seeded from the beginning as a prototype for a global compliance-ready ledger. Its architecture, including timestamped ledgers, public blockchains, and traceable keys, aligns more closely with surveillance infrastructure than resistance.

What was supposed to free people from financial control has, in many cases, become a gateway right back into it, across the broader crypto ecosystem.

PART III: The Quiet Capture of Crypto

When Control Replaces Code

The tipping point was not a single moment. It was gradual. A soft capture.

Between 2013 and 2017, the major turning points began. As the adoption of Bitcoin and other cryptocurrencies grew, regulatory agencies began imposing rules. Exchanges adapted. They asked for identification. Linked accounts to bank transfers. Froze withdrawals.

By 2022, the shift was undeniable.

During protest movements in several countries, including Canada, governments ordered cryptocurrency platforms to freeze accounts associated with civil disobedience. It worked. Although Bitcoin itself cannot be censored, individuals who own it through custodians were blocked. This was the turning point for many. The same applies across the crypto ecosystem. Major altcoins and tokens are subject to the same custody risks, surveillance enforcement, and identity-linked compliance architecture.

Regulators worldwide issued guidance, effectively deputizing exchanges. They now report suspicious activity. They comply with subpoenas. They restrict privacy tools like mixers and self-hosted wallets.

Even self-custody tools such as Wasabi and Samourai Wallet have come under pressure. In 2023, the developers of Tornado Cash were arrested, setting a precedent for prosecuting the code itself. In the eyes of governments, financial privacy is now a threat.

But the shift from code to control did not just enable compliance. It enabled prediction.

As blockchain surveillance matured, the financial data collected became more than just a record of transactions. It became a dataset for profiling. What you buy, how much you hold, when you move it, and where it goes is no longer just historical. It is behavioural.

With the rise of artificial intelligence and behavioural analytics, institutions and governments can now use these datasets to identify future risks. Your spending patterns, donation history, IP address, browser fingerprint, and wallet associations can feed algorithms that flag dissident behaviour before a law is even broken.

The public ledger is not just a record. It is a forecast engine. And once tied to real-world identity through Know Your Customer (KYC) requirements and wallet tracking, it becomes the raw fuel for predictive policing.

What began as open-source freedom has become the foundation of pre-crime finance. The blockchain remembers everything. And now, it predicts.

From Blockchain to Pre-Crime: Minority Report Was a Warning

In 2002, the film *Minority Report* portrayed a dystopian future where predictive algorithms and state surveillance were used to arrest individuals before they committed crimes. It was marketed as science fiction. But in light of today's blockchain analytics, artificial intelligence, and behavioural profiling, it now reads more like a policy manual.

The movie introduced the concept of Precrime, a state agency that forecasts criminal behaviour using data from clairvoyants. In the real world, clairvoyants have been replaced by algorithms. Financial transactions, digital footprints, and online behaviour are fed into models to predict who might pose a risk, not based on what someone has done, but on what the system thinks they might do.

This predictive logic now governs much of the blockchain surveillance ecosystem. Wallets are flagged not for criminal acts, but for “suspicious patterns.”

Transactions are monitored, not because they are illegal, but because they deviate from normative models. Donating to the wrong cause, transacting at the wrong time, or using privacy tools like mixers may place individuals under scrutiny, well before any law is broken.

The shift from probable cause to predictive suspicion is the hallmark of digital authoritarianism. It transforms justice from a reactive process into a pre-emptive weapon. When that logic is built into financial infrastructure, as it now is through blockchain surveillance, it means your money becomes your profile, and your profile becomes your sentence.

In *Minority Report*, the system eventually collapses under the weight of its own moral contradictions. But in reality, today's digital surveillance regime is not apologizing. It is expanding. Blockchain has given it the perfect memory to do so.

What began as decentralized money is now part of a pre-crime economy. Autonomy is exchanged for algorithmic permission, and privacy is treated as deviance.

The Rise of ETFs and Institutional Capture

The rise of Bitcoin Exchange Traded Funds (ETFs) was celebrated as a milestone.

ETFs are publicly traded investment vehicles that track the price of an underlying asset, such as Bitcoin, without requiring the investor to hold the asset directly. Investors buy shares in the fund, while the underlying Bitcoin is held by custodians and managed by institutions.

This convenience comes at the cost of ownership, privacy, and decentralization. What was intended to be an alternative to the fiat system is now tightly integrated into it.

ETF shares are custodied, insured, and traded just like traditional securities, removing direct ownership and placing control in the hands of third-party institutions. Similar structures are now

applied to other cryptocurrencies, embedding them within a compliance-first framework that mirrors traditional finance.

This structural shift is not just about control of assets. It is also about control of perception.

They also allow institutions, not individuals, to shape the narrative. Most crypto ETF investors never touch the underlying asset, never use a wallet, and never leave the traditional financial system.

This is not decentralization. It is delegation. And the power has been delegated to the same corporate actors who helped build the current system.

Platforms like Coinbase, custodians like Anchorage Digital, and blockchain surveillance firms like Chainalysis have embedded chokepoints that reroute Bitcoin's original purpose. A custodian is a third-party institution that holds and manages digital assets on behalf of users, often subject to regulatory oversight and legal obligations. In this model, users do not control their own private keys, meaning they do not truly own the asset. Compliance is no longer optional. It is the infrastructure.

The Financial Industrial Complex and blockchain surveillance firms are not just involved in Bitcoin. They are structuring it. They are the ones writing the operating procedures for custody, access, and reporting. The tools of surveillance are being baked into wallets, exchanges, and interfaces before most users even realize it.

The enforcement of the Bitcoin control grid is no longer just a government project. It has been outsourced to a powerful network of private sector partners. ETF providers, exchanges, custodial platforms, and blockchain compliance firms now operate as the front line of surveillance.

These institutions are often more aggressive than governments because they are not constrained by constitutional protections or democratic oversight. They do not need public approval. They operate with legal immunity, market incentives, and embedded access to user data. They profit from access, regulation, and control. In many cases, they write the rules before lawmakers catch up.

This model is no longer just technocratic. It is a modern form of financial fascism. Control is no longer exercised solely by government agencies but delegated to private corporations that enforce surveillance, compliance, and censorship without democratic accountability. By merging state interests with corporate infrastructure, the system creates the illusion of private enterprise while consolidating power in the hands of unelected actors. This is governance without consent, outsourced and unrestrained.

The surveillance state is not coming. It has already been built. And it is being run by ***The Financial Industrial Complex***.

This is not accidental. It is strategic. By embedding surveillance into the infrastructure of investment, ***The Financial Industrial Complex*** has become the enforcer of the new system.

Governments do not need to ban privacy. They just need to make it incompatible with modern finance.

What was once a decentralized escape has become a permissioned portal into a monitored economy.

For those who hold Bitcoin only through custodians or ETFs, the door to peer-to-peer freedom is already shut. Their assets are embedded in a permissioned system with no off-ramp, unless they start over from scratch.

PART IV: Global Financial Gatekeepers — DTC, IMF, World Bank and BIS

The DTC and the Clearinghouse Model

Before examining the DTC model, it is important to clarify the difference between beneficial ownership and direct ownership.

Beneficial ownership refers to a legal structure in which an individual or entity holds the right to benefit from an asset (such as receiving dividends or interest), but does not hold legal title to it. Instead, the legal title is held by a nominee or intermediary, such as a brokerage firm or a central depository.

In contrast, direct ownership grants the individual full legal title and control over the asset without reliance on any third party. In systems of indirect or beneficial ownership, access to the asset depends on the solvency, compliance, and permission of the intermediaries.

This distinction becomes critical in times of systemic stress, platform failure, or political overreach. Direct ownership, particularly of tangible assets like physical gold, remains one of the last forms of sovereign control.

The Depository Trust Company (DTC) is the core infrastructure behind U.S. securities settlement, consolidating trillions of dollars in assets into a single institutional clearinghouse. Its role is often hidden, but its power is absolute. Every publicly traded security in North America, including stocks, bonds, and exchange-traded funds, is ultimately settled through the DTC or a partner system. This model operates on indirect ownership, where individuals do not own securities directly but merely hold a beneficial interest recorded by intermediaries. The true legal title remains with the DTC and its nominees.

This arrangement creates a layered custody chain that masks who actually owns what. If a brokerage becomes insolvent, if a clearing partner fails, or if regulators impose restrictions, investors have little to no legal recourse to claim their assets directly. It Starts With Gold™ explains this vulnerability in depth, contrasting it with direct ownership, where individuals possess full legal title to a tangible, identifiable asset without needing permission from intermediaries. Physical gold held outside the financial system remains one of the few remaining assets that offer this level of sovereign control.

By embedding ownership inside centralized systems, the DTC structure introduces an invisible dependency. Access to assets is conditional upon the system itself remaining solvent, secure, and compliant. In a programmable future, that conditionality becomes even more dangerous.

Bitcoin and cryptocurrencies were originally designed to eliminate such intermediaries. Yet as Bitcoin is increasingly routed through custodians like Anchorage Digital and Coinbase, and packaged into institutional exchange-traded products, it begins to mirror the very system it set out to disrupt. The crypto asset may be decentralized in design. However, once placed inside

custodial wrappers or exchange-traded products, it is reabsorbed into the beneficial ownership model, subject to legal, regulatory, and systemic control.

This is a pivotal moment. A system marketed as a rebellion against financial control is being routed back into the very architecture of surveillance and dependency. The illusion of ownership replaces actual control.

The International Monetary Fund (IMF), the World Bank, and the Bank for International Settlements (BIS): Architects of Programmable Global Finance

These three supranational institutions now function as the architects of a coordinated global financial system, one built on interoperability, programmable payments, identity-linked transactions, and behavioural oversight.

The International Monetary Fund (IMF) serves as a global lender and regulator, issuing policy guidance, infrastructure blueprints, and coordination frameworks for digital currencies across jurisdictions.

The World Bank finances development projects and supports emerging-market infrastructure. In recent years, it has pivoted toward shaping digital financial systems that align with environmental, social, and governance (ESG) criteria.

The Bank for International Settlements (BIS), known as the central bank for central banks, is headquartered in Basel, Switzerland. It provides technical infrastructure, policy guidance, and prototype development for central bank digital currencies (CBDCs). Its Innovation Hub is actively testing cross-border settlement systems, real-time digital ID verification, and smart contract enforcement.

In its 2023 publication Crypto-Assets and Central Bank Reserve Portfolios, the World Bank warned that traditional cryptocurrencies are too volatile and speculative to be included in official reserve holdings. Yet the same paper encouraged central banks to experiment with digital reserve assets, programmable, traceable, asset-backed tokens that serve the interests of global stability and compliance. The report openly advocated for interoperability frameworks embedded with ESG enforcement, identity verification, and behavioural conditions for financial access. In effect, crypto-assets are dismissed, but the control logic behind them is retained, refined, and scaled.

Meanwhile, the IMF has issued guidance on regulatory coordination across jurisdictions, CBDC infrastructure design, and anti-fragmentation strategies to manage the risks posed by decentralized finance. Its stated objective is to prevent digital assets from undermining monetary sovereignty or capital controls. In practice, this means that decentralized currency must either be outlawed or absorbed into a programmable financial grid. The crypto rebellion was tolerated only long enough to perfect the tools of its capture.

The BIS plays a central implementation role in building cross-border CBDC infrastructure. Through two flagship initiatives, Project Icebreaker and Project mBridge, the BIS has demonstrated how programmable money systems can operate internationally with identity-based restrictions and built-in compliance.

Project Icebreaker, conducted with the central banks of Israel, Norway, and Sweden, tested a hub-and-spoke model for cross-border retail CBDC payments. It enabled real-time currency conversion, identity verification, and transaction-level compliance checks, all embedded directly into the payment process.

Project mBridge, a collaboration with the central banks of China, Thailand, the United Arab Emirates, and Hong Kong, pilots a shared distributed ledger for wholesale CBDCs. It supports programmable, cross-border payments with built-in policy restrictions, including transaction expiry, destination controls, and identity-linked authorization. Access to funds can be conditioned on jurisdictional approval or geopolitical alignment.

These are not abstract prototypes. They are active demonstrations of how programmable finance can be enforced at the infrastructure level. They embed surveillance, conditionality, and centralized control into the core of the monetary system.

The Looming Web of Global Surveillance

While companies like Chainalysis bring blockchain visibility to local law enforcement and regulators, the IMF, World Bank, and BIS are building the infrastructure for global compliance enforcement. As of 2025, over 130 countries are developing or piloting central bank digital currencies, many based on BIS-developed templates that standardize interoperability, surveillance mechanisms, and digital ID integration across jurisdictions.

These systems are being coded not just for transaction clearing, but for programmability, the ability to approve or deny transactions in real time, based on who you are, what you bought, where you bought it, and how it aligns with predetermined social or environmental targets. This is not future speculation. It is the present policy blueprint of supranational institutions that now sit atop the global financial stack.

From SHA 256 to Global Ledger Compliance

It Starts With Gold™ warns that the same cryptographic algorithm used in Bitcoin, SHA 256, is also used across state-controlled surveillance infrastructure and may form the backbone of future global CBDC ledgers. This convergence allows decentralized platforms to be absorbed into centralized governance systems under the banner of security, compliance, and global coordination. Once integrated into this programmable money grid, decentralization becomes a cosmetic feature. Surveillance and control remain hard-coded.

The institutions now leading this transformation are not startups or cypherpunks, but the IMF, the World Bank, and the BIS, operating under the influence of unelected global technocrats.

Their goal is not financial liberty. It is a global compliance infrastructure enforced at the transaction level.

Implications and Call to Action

Bitcoin and crypto were once seen as the tools of resistance, permissionless, peer-to-peer, and borderless. But today, those tools are being co-opted to build a programmable financial grid governed by the very institutions they once claimed to bypass.

The Depository Trust Company, the IMF, the World Bank, and now the BIS are shaping the future of money into something traceable, behavioural, and contingent. Not because crypto failed, but because it succeeded just enough to prove the model could work.

The next phase is not about decentralization. It is about consolidation under global rules, programmable tokens, and identity-based access.

But infrastructure alone does not guarantee control. To ensure adoption, systems of financial surveillance must also win public trust. That trust is not always earned. It is often engineered. Throughout history, powerful institutions have relied not only on architecture but on psychology. The most effective forms of control are not imposed with force but adopted voluntarily, under the illusion of choice. As financial power consolidates, so too does the use of psychological operations designed to pacify dissent, redirect resistance, and make surveillance feel like safety.

To fully understand Bitcoin’s possible role in this transformation, we must examine how hope itself has been weaponized.

PART V: The Illusion of Resistance

The Blueprint of Controlled Opposition: Operation Trust and the Psychology of Entrapment

To understand how Bitcoin may have been used to funnel dissidents into a surveillance system, it helps to revisit a historical blueprint: Operation Trust.

In the early 1920s, Soviet intelligence launched Operation Trust, a counterintelligence program run by the Cheka, the Soviet Union's first secret police. The Cheka later evolved into the Gosudarstvennoye Politicheskoye Upravlenie (GPU), the State Political Directorate, then the Narodny Komissariat Vnutrennikh Del (NKVD), the People's Commissariat for Internal Affairs, and eventually the Komitet Gosudarstvennoy Bezopasnosti (KGB), or Committee for State Security.

The operation created a fake resistance movement to lure anti-communist dissidents into exposing themselves. Believing they were joining a real underground effort, targets were monitored, profiled, and dismantled. Operation Trust did not rely on force. It relied on hope. It offered the illusion of resistance to neutralize real opposition.

A century later, the same strategy appears to be playing out through Bitcoin.

Launched during a global crisis of trust in fiat currencies and central banks, Bitcoin was marketed as a decentralized escape from the system. It attracted privacy advocates, libertarians, and critics of ***The Financial Industrial Complex***. But its architecture public ledgers, traceable transactions, and timestamped blocks mirrored the very surveillance structure many thought they were leaving behind.

And the trap may have been laid long before Bitcoin's release.

In 1996, the United States National Security Agency quietly published a whitepaper titled "***How to Make a Mint: The Cryptography of Anonymous Electronic Cash***." It outlined, in technical detail, a digital currency system strikingly similar to what Bitcoin would later become. It featured public-key encryption, timestamping, distributed ledgers, and pseudonymity that was never truly anonymous. Though framed as an academic proposal, the paper effectively served as a blueprint for a surveillance-compatible form of programmable money. It was released quietly, twelve years before Bitcoin appeared.

If Operation Trust offered false underground movements to pacify dissidents, *How to Make a Mint* may have pre-seeded the technological framework for a future digital capture system. It planted the seeds of a tool that looked like liberation but functioned as a mirror of the surveillance state.

As Bitcoin adoption grew, its infrastructure was absorbed into the system. Know Your Customer (KYC) and Anti-Money Laundering (AML) rules were enforced. Custodial platforms became

compliance chokepoints. Blockchain analytics firms like Chainalysis created real-time tracking tools for governments and financial regulators.

The Committee for State Security (KGB) perfected this method: create a system that feels like freedom, then use it to map, monitor, and contain.

Just as Operation Trust offered a false resistance to map dissent, Bitcoin may have done the same. It offered an illusion of freedom while recording every move. Hope was the bait. Surveillance was the outcome.

That may have been the point.

It Starts With Gold™ explores this strategy in greater depth. It shows how manufactured hope can act as a trap, delaying action until the doors are already closed.

What if Bitcoin were never outside the system? What if it was the system's next phase?

Rather than ban dissent, the central banking cartel offered it a digital flag to rally behind. Bitcoin, and later the broader cryptocurrency movement, became the honeypot.

The Hegelian Dialectic: Problem, Reaction, Solution

To understand how Bitcoin may have functioned as a control mechanism rather than a tool of liberation, it is essential to examine the Hegelian Dialectic: Problem, Reaction, Solution. This strategic model involves either creating or exploiting a crisis, provoking a predictable public response, and then offering a pre-engineered solution that consolidates power and advances control, under the guise of solving the original crisis.

Viewed through this lens, Bitcoin may not have been a rebellion against financial control. It may have been the problem introduced to justify a more advanced surveillance-based solution.

In the realm of digital finance, the 2008 global financial crisis marked the initial problem. Trust in fiat currencies and central banks collapsed. Millions lost their homes, savings, and belief in the legitimacy of the system. The public demanded an alternative, something that promised sovereignty, privacy, and freedom from centralized control.

The reaction came swiftly. Bitcoin emerged as a decentralized, peer-to-peer digital currency, supposedly beyond state interference. It attracted technologists, libertarians, and others disillusioned by legacy finance. It was not just a tool. It became a movement.

Then came the solution, not the one the people believed they were choosing, but perhaps the one the system intended all along. Bitcoin introduced a public, permanent ledger that recorded every transaction. Custodial exchanges implemented strict Know Your Customer (KYC) regulations. Blockchain surveillance firms like Chainalysis made de-anonymization routine. Users trained themselves to use digital wallets, abandon cash, and normalize traceable transactions, behaviours

critical for the eventual rollout of identity-linked, programmable central bank digital currencies (CBDCs).

As Bitcoin adoption grew and the illusion of decentralization faded, a new problem emerged: volatility, fraud, and illicit use cases. The public and regulators called for safety and oversight. The next solution arrived in the form of state-backed digital currencies, fully programmable, centrally controlled, and permanently linked to individual identities.

And so, the dialectic cycle repeated: Problem, Reaction, Solution. Each phase advanced digital control, all while being marketed as progress.

What began as financial rebellion may have been an engineered pathway to digital containment. Through the Hegelian Dialectic, the public was not forced into surveillance. It was led there through belief.

The Protest That Changed Nothing and Set the Stage for Everything

Occupy Wall Street erupted in 2011 as a populist protest against financial corruption, corporate power, and growing inequality. It gave voice to the mass outrage following the 2008 financial collapse. Millions had lost homes, jobs, and savings while the same financial institutions that caused the crisis were bailed out with taxpayer money.

Occupy embodied the Reaction phase in the classic Problem, Reaction, Solution formula. The crisis, the 2008 collapse, was the Problem. The public outrage and protest movement were the Reaction. And into this void emerged the Solution: Bitcoin, marketed as a decentralized alternative that bypassed central banks and corporate control.

But that may have been the point. Occupy's energy was never allowed to restructure the system. It was redirected into a digital escape valve. The timing was not coincidental. Just as protestors were demanding justice, a new system appeared, one that promised liberation but was built on traceable, timestamped, and surveillable infrastructure.

Bitcoin became the chosen lifeboat, but few noticed the growing divergence beneath the surface. While retail investors poured into crypto hoping to exit the broken system, central banks and state-aligned institutions were executing a different strategy: buying gold.

From 2008 onward, the world's central banks flipped from net sellers to net buyers of gold. In 2010, that trend accelerated. Nations like China, Russia, Turkey, and India led the charge. By 2022, even the Bank for International Settlements, the so-called central bank of central banks, was settling interbank transactions in gold rather than fiat. Between 2008 and 2024, central banks accumulated over 1,000 tonnes of gold per year, according to the World Gold Council.

They were not speculating. They were preparing.

This accumulation was not without precedent. As we outline in It Starts With Gold, the last time the U.S. government dramatically shifted its gold policy was during a crisis. In 1933, Executive

Order 6102 forced Americans to hand over their gold under threat of imprisonment. Weeks later, the government revalued gold from $20.67 to $35 per ounce, a 69 percent increase, enacted by decree. This one act allowed the U.S. Treasury to instantly expand its monetary base and reset its debt obligations without public debate.

A similar mechanism remains in place today.

In May 2025, the ***Financial Accounting Manual for Federal Reserve Banks*** confirmed that the U.S. Treasury is authorized to issue gold certificates to the Federal Reserve. These certificates, backed by physical gold, can be used to credit the Treasury General Account without selling the gold itself. This is not theory, it is formal policy. The Federal Reserve can accept the revalued certificates as balance sheet assets, functionally creating money backed by gold without going to market.

This is not theory, it is formal policy. The Federal Reserve can accept the revalued certificates as balance sheet assets, functionally creating money backed by gold without going to market.

As detailed in our July 2025 article "***Is a Global Gold Revaluation the Next Debt Reset Tool?***", this mechanism could allow the U.S. Treasury to reprice its 260 million ounces of gold from the legacy accounting value of $42.22 per ounce to $20,000 per ounce. This would instantly unlock over $5 trillion in balance sheet capacity. The Federal Reserve would then accept newly issued gold certificates at that higher valuation and credit the Treasury's account, enabling debt reduction without selling bonds or raising taxes. This is functionally no different than quantitative easing. The key difference is that the new money creation would be tied to a finite, tangible reserve.

While the public was taught that Bitcoin was the exit, institutions were anchoring themselves in gold. While retail investors celebrated digital wallets, the system was quietly preparing a hard-asset realignment.

Occupy Wall Street was never about ending the system. It was about redirecting resistance. It allowed people to feel heard without changing anything of consequence. And in the background, the real strategy was already underway, one that did not rely on blockchain, but on bullion.

This dual-track response, one for the public, one for the institutions, reveals the deeper nature of the trap. What appeared to be financial empowerment may have been engineered exposure. What was framed as revolution may have been stage-managed containment. The only parties who truly exited the system were the ones accumulating physical gold.

In the end, Occupy Wall Street did not fail. It succeeded in changing the battlefield from the streets to the blockchain. It taught the public to think in digital terms, to abandon privacy, and to accept traceability in the name of progress. And when the next crisis arrives, that same digital infrastructure will be used to lock the exits.

Unless you have already found the one that cannot be frozen, tracked, or reprogrammed.

It starts with gold.

Was Bitcoin a Trojan Horse?

The question can no longer be avoided. Was Bitcoin truly a grassroots rebellion against ***The Financial Industrial Complex***, or was it a carefully designed lure to bring dissidents into a controlled digital matrix?

At first glance, Bitcoin appeared revolutionary. A pseudonymous creator. An open-source codebase. A decentralized ledger that promised freedom from central banks. For a generation disillusioned by Wall Street bailouts and fiat devaluation, it looked like salvation.

But hindsight reveals a darker possibility.

Whether by design or evolution, Bitcoin and the structure now replicated across many cryptocurrencies have laid the groundwork for something even more dangerous. That same groundwork is now mirrored across countless tokens whose architecture reflects Bitcoin's traceable, timestamped, and surveillable design.

Perhaps the most brilliant aspect of the Bitcoin experiment is not technical at all. It is psychological.

Bitcoin and cryptocurrencies were marketed as tools of liberation. They attracted individuals who rejected authority, distrusted central banks, and sought an exit from the fiat system. Libertarians, privacy advocates, anti-globalists, gold holders, and technophiles all saw in them the promise of a parallel economy.

But the very values that drew them in made them vulnerable. Bitcoin did not ask for trust in a government. It asked for trust in code. In doing so, it bypassed skepticism and gained adoption more quickly than any surveillance tool ever could.

By convincing people they were opting out, the system funnelled them in.

Bitcoin created the illusion of escape while quietly enabling the greatest financial mapping tool ever deployed. It recorded every transaction, every movement, every timestamp, and every wallet address. And it did so with full transparency, under the banner of decentralization.

What began as a movement became a honeypot. The same community that distrusted government and rejected surveillance handed over their financial lives to a system that logs every transaction permanently for anyone with the tools to trace it.

The genius of the trap was that people walked into it voluntarily, believing it was their escape.

What was sold as a weapon against tyranny may have been the very foundation of the control grid now forming around us.

But then came the solution, not the one the people thought they were choosing, but the one the system may have intended all along. This followed the classic Problem, Reaction, Solution script: offer a technological escape, such as Bitcoin, just as public trust in ***The Financial Industrial Complex*** collapses, then use it to shepherd the population into an even more controllable digital system.

The blockchain does not forget. And neither does the system built on top of it.

Whether Bitcoin was created as a surveillance system from the start or later captured through strategic absorption, the outcome is now the same.

We lean toward the second view. While the early architecture may have had sincere decentralization goals, Bitcoin was ultimately co-opted by powerful interests who saw in it the ideal vehicle to normalize traceable digital finance.

The infrastructure of control did not need to invent its own system. It only needed to absorb the one already trusted by the public. By presenting itself as a tool of resistance, Bitcoin became easier to incorporate into the very surveillance regime it was meant to challenge.

PART VI: CBDCs: From Prototype to Digital Prison

Bitcoin vs CBDC: Infrastructure Reused

On the surface, Bitcoin and central bank digital currencies (CBDCs) may appear to operate on similar digital rails. But their underlying structures serve very different purposes and outcomes.

Bitcoin, like many cryptocurrencies, operates on a public, pseudonymous ledger. Anyone can view the transactions, but the identities behind them are obscured unless linked through external data. In contrast, CBDCs use private, state-controlled ledgers with full visibility into every transaction by design.

Control is another key difference. Bitcoin was built to be decentralized, at least in theory. No single authority governs the network. CBDCs, in contrast, are fully programmable. Central banks can impose restrictions, conditions, and expiration dates on how the digital money is used.

Access also diverges sharply. With Bitcoin, individuals can hold their assets in self-custody, outside the control of any institution. CBDCs are permissioned and revocable. Access is granted and can be taken away by the issuing authority.

Surveillance is already a concern in the Bitcoin space due to Know Your Customer (KYC) regulations and blockchain analytics tools. But CBDCs go further, enabling real-time, granular surveillance of every transaction, down to the individual level.

Finally, Bitcoin operates independently of central bank monetary policy. No one can arbitrarily inflate its supply or manipulate its use. CBDCs are the opposite. They give governments direct influence over monetary flow, velocity, and even the behaviour of citizens through programmable incentives or penalties.

The architecture may look familiar. The outcomes are not.

Enter CBDCs: Bitcoin’s Evil Twin

Central bank digital currencies (CBDCs) are already in pilot stages across the globe.

In 2024, several countries expanded consultations on programmable digital currencies. The focus shifted from technical feasibility to social engineering, embedding transaction-level controls, behavioural nudges, and automated restrictions. These systems mimic the structure of Bitcoin wallets and ledgers, but they eliminate all plausible deniability and all financial autonomy.

The overlap is undeniable. Both systems use wallets, cryptographic keys, and digital ledgers. While some cryptocurrencies attempt to distance themselves from this model, most remain tethered to systems of institutional oversight and digital visibility.

What began as a model for financial independence has now become a template for financial surveillance.

As CBDCs become normalized and legacy cash systems are phased out, financial escape will no longer be an option. Every transaction, every interaction, and every act of commerce will occur within the digital perimeter.

The implications go far beyond monetary policy.

Once programmable CBDCs are tied to carbon scores, social behaviour, vaccine status, tax history, or political activity, citizens will find themselves inside a dynamic control system. Spending will no longer be a right. It will be a conditional privilege.

In China, digital wallets linked to the social credit system have already demonstrated how programmable currency can adjust permissions based on obedience. In Europe and Canada, ESG scoring frameworks are laying the groundwork for similar restrictions. Access to digital services, financial products, and even food rations may one day depend on behavioural compliance with shifting policy goals.

As detailed in It Starts With Gold™, CBDCs are not just a payment method. They represent a programmable command system that governs what, when, and where you can transact and whether you are permitted to do so at all.

The ability to save, donate, travel, or transact will depend not on your wealth, but on your compliance.

In many jurisdictions, digital IDs are already being tied to biometric verification. India's Aadhaar system links fingerprints and retina scans to citizen bank accounts and welfare programs. Several African pilot projects backed by the United Nations are exploring similar systems, merging identity, payments, and biometric data into a unified digital profile. These programs are being promoted as models for future CBDC deployment. Once implemented, the simple act of spending could require biometric approval.

There will be no grey market, no side channel, and no off-ramp unless you exit the system entirely. Without physical cash or assets outside the digital framework, opting out will no longer be possible.

Financial autonomy will become a relic of the past. Programmable money will mean programmable lives. And the system will not need your consent to include you. It will only require your silence.

Officials have made it clear that privacy is not the goal. In 2023, European Central Bank President Christine Lagarde stated bluntly, "We do not want a completely anonymous digital euro." With this admission, the illusion that digital currencies might preserve privacy was dismantled. The objective was always control transparent, programmable, and enforceable.

Lightning Network and the Centralization Creep

The Lightning Network is a Layer 2 protocol built on top of the Bitcoin blockchain. It was designed to enable faster and cheaper transactions by routing payments off-chain through specialized payment channels.

The Lightning Network was promoted as Bitcoin's scaling solution. Faster, cheaper transactions. It sounded ideal.

However, it comes with trade-offs. In practice, Lightning has encouraged centralization through large payment hubs, custodial mobile wallets, and infrastructure operated by a handful of providers.

A 2023 Stroom report found that over 80 percent of Lightning volume flowed through fewer than 10 dominant nodes, most run by exchanges or custodial services.

While the Lightning protocol remains technically decentralized and open-source, real-world usage has gravitated toward central nodes due to ease of use, speed, and the low technical barriers presented by custodial wallet apps. This user-driven centralization introduces systemic risks that mirror those of the traditional banking sector, where traffic is routed through chokepoints vulnerable to monitoring, censorship, and state-corporate coordination.

This concentration was no accident. Many of the most widely promoted Lightning wallets offered simple, custodial setups that required no technical knowledge, conditioning users to trade sovereignty for convenience without realizing they had entered a monitored environment.

And worse, they have opened the door to real-time surveillance. If your payments are routed through a third-party Lightning node, especially one linked to an exchange or bank, you can be monitored.

These custodial setups do more than enable surveillance. They also serve as a gateway for future government absorption. As regulations tighten and central bank digital currencies are deployed, custodial crypto wallets may be repurposed or mandated to function as conversion tools. Governments do not need to crack cryptographic algorithms. They only need to enforce compliance among wallet providers, especially those already integrated with exchanges or payment processors. In the event of a crisis, emergency laws could require the migration of crypto holdings into government-backed digital currencies. This would turn crypto wallets into on-ramps for financial control. Without realizing it, users may find themselves using Bitcoin within the same monitored and programmable framework they tried to escape.

This is not theoretical. This pattern of centralization is not limited to Bitcoin. Other Layer 2 solutions on Ethereum and other blockchains show similar tendencies, especially where user access depends on custodial platforms.

Similar surveillance-enabling trends are now seen across Ethereum's Layer 2 protocols, Solana validators, and custodial platforms for stablecoins, making centralized chokepoints a universal feature across crypto.

Similar centralization trends are emerging in other crypto networks and Layer 2 scaling solutions.

Custodial Bitcoin Is Not Yours

This cannot be repeated enough. If you do not control the private keys, you do not own the Bitcoin.

Digital Wallets: Illusions of Safety in a Compromised System

Even for those who control their private keys, digital wallets are not as secure as they seem. Most wallets rely on a chain of trust that includes mobile devices, app stores, firmware, Bluetooth protocols, USB connections, and software libraries. Each of these layers introduces potential attack vectors. A wallet is not an island. It is part of an ecosystem of devices and networks designed for surveillance.

Mobile wallets often leak metadata, link to background location services, or run on compromised operating systems. Even hardware wallets, widely seen as the most secure option, are not immune. Closed-source firmware, over-the-air updates, and supply chain tampering introduce invisible risks. Once a device is compromised, every transaction becomes a disclosure.

Even seed phrases, the cornerstone of self-custody, may be generated or stored insecurely. Some wallets have been found to transmit unencrypted analytics during setup, exposing user behaviour and network information to third-party servers. Others auto-sync to cloud backups without user awareness, introducing custodial risk even in so-called non-custodial apps. This was not theoretical.

In 2023, Ledger introduced a controversial feature called Ledger Recover, which proposed splitting user seed phrases into encrypted shards stored by third parties. Although marketed as a safety net, this feature was criticized by security experts for creating a backdoor to user funds and undermining self-custody principles. The backlash underscored how even hardware wallets, long viewed as secure, are vulnerable to firmware updates, closed-source components, and institutional pressure.

In the end, even when the private keys remain yours, the tools may not be. Surveillance is not just in the blockchain. It is in the firmware, the routers, the interfaces, and the systems that wrap around your wallet.

If you do not control every layer, you are still in the cage. You just cannot see the bars.

But even outside of self-custody traps, the illusion of ownership becomes even more dangerous under custodial models. Holding Bitcoin in a regulated exchange means your assets are subject to foreign policy, domestic legislation, and even platform failure.

From Celsius and FTX to QuadrigaCX, the record is clear. Custodians fail. Assets vanish. And in the end, the user is left with nothing but a line on a screen and a bankruptcy court claim.

Bitcoin and Cryptocurrencies held in custodial accounts are no more outside the system than mutual funds. What you do not control, you do not own.

By 2024, more than 70 percent of all Bitcoin was held on custodial platforms such as exchanges, ETFs, or regulated financial institutions. This meant that most users no longer controlled their private keys or owned their Bitcoin in any meaningful sense. The principle of decentralization had become a marketing slogan, replaced in practice by compliance architecture and third-party control.

In *It Starts With Gold™,* we explain why the promise of self-sovereignty is often an illusion when your assets remain inside the digital system and how physical gold held outside the system can serve as your final backstop.

But the risk is no longer just financial. It is structural.

Know Your Customer (KYC) rules are not simply about taxation or anti-money laundering compliance. They are the foundation of something far larger, an identity-linked architecture of control.

Once your wallet is tied to your legal name, mobile device, and geolocation data, your financial activity becomes the skeleton key to your entire digital footprint. That wallet is no longer just a tool for transactions. It becomes your core identity.

This identity connects in real time to everything else. Credit scores. Health records. Employment history. Biometric databases. Social media accounts. Travel patterns. Voting records. ESG compliance. The integration is already underway.

What begins as a financial ID quickly evolves into a behavioural profile. It maps what you spend, where you go, what you support, and who you interact with.

The wallet becomes your passport, your tracker, your ration book, and your leash. It is a financial tether that links you to a network that can now assign permissions, impose restrictions, and revoke access based on algorithmic determinations.

In this new system, ownership is no longer about possession. It is about permission.

And once permission becomes programmable, freedom becomes optional.

If you are a financial professional, policy analyst, dissident, or simply someone seeking to protect your wealth and privacy before the window closes, we encourage you to reach out directly.

Email Adrian C. Spitters at Adrian@ItStartsWithGold.com or Peter J. Merrick at Peter@ItStartsWithGold.com.

Whether your concern is asset protection, off-grid wealth preservation, or preparing for the programmable future, we will connect you with trusted solutions that still exist for now.

Do not wait for the next freeze, lockdown, or wallet restriction. Action must be taken before the digital cage locks shut.

PART VII: The Only Escape Left

Gold: The Last Asset Standing

While Bitcoin was the first and most prominent example, many other cryptocurrencies have since followed the same path toward surveillance, compliance, and institutional capture. Despite their branding as decentralized alternatives, most operate within the same monitored financial infrastructure.

If Bitcoin's freedom has become conditional, then the only true escape may lie in what predates the digital system entirely.

Individuals who recognize the scale of the shift underway are no longer waiting for institutional reform. They are acting now to secure what still holds value.

As real estate markets unravel, debt burdens grow, and the traditional financial system becomes more unstable, many are turning to a more permanent store of value: physical gold.

Physical gold offers direct ownership, tangible value, and immunity from digital interference. It does not require a financial intermediary, a custodial platform, or a compliant digital ID to access. It exists outside the programmable financial infrastructure now forming around us.

Once cash is gone, and wallets are tied to your carbon score, there will be no 'opt out.' Only compliance. Gold is not just a hedge. It is the firewall between autonomy and algorithmic rule.

Those preparing for what lies ahead are reallocating portions of their wealth into hard assets. They are removing exposure to centralized platforms and preserving purchasing power in the one asset that has survived every financial system collapse.

Every day you wait, the cost of real money rises. Do not let the next crisis catch you unprepared. The time to build a reserve of real, sovereign wealth is now.

Gold Has No Protocol

Gold does not require a wallet. It cannot be hacked. It is not tracked, traced, tokenized, or tied to a compliance regime.

It has never been weaponized by a state because it cannot be.

Bitcoin and much of the broader crypto ecosystem now operate within the very architecture they were designed to escape. Gold remains tangible, sovereign, and ancient.

We are not against Bitcoin. We are against the illusion that it still serves the purpose it was built for.

Why Gold Still Wins

Bitcoin may be digital, but gold is immutable. The research presented throughout this paper shows that globalist institutions, blockchain compliance firms, and state-aligned exchanges have reshaped Bitcoin's foundational architecture. Its code is vulnerable to governance, forks, and institutional capture.

Gold, by contrast, is inert. It exists beyond regulation, beyond narrative manipulation, and beyond algorithmic failure.

No permission is required to hold it. No software update can alter it. No government can print it. That is why gold remains the one true asset that defies capture.

The Real Asset Revolution Begins with Gold

Bitcoin's original vision was noble. It inspired millions and launched a global movement.

But movements can be co-opted. Protocols can be rewritten. And faith in digital systems can be misplaced.

Gold's nature has never changed. It cannot be printed. It cannot be hacked. And no government can inflate it away.

The financial control grid is no longer theoretical. It is already operational. Digital assets may offer speed, but not sovereignty.

That is why real change begins not with digital speculation, but with the ownership of physical, sovereign assets.

When the next crisis arrives, there may be no off-ramp left. By the time the system locks into place, it will be too late to leave it**.**

If Bitcoin was the lure, gold is the exit. This white paper was your warning.

Our book ***It Starts With Gold*™** is a roadmap for that exit, laying out not just what is happening, but what you can still do to preserve your privacy, property, and sovereignty.

Take Action Before the Gate Closes

The urgent themes discussed here are expanded on in our #1 international best-selling book, ***It Starts With Gold*™**, co-authored by Peter J. Merrick and Adrian C. Spitters. Visit ***www.ItStartsWithGold.com***

Order your own copy of *It Starts With Gold*™ from Amazon today. *CLICK HERE*

References

1. Cryptographic Foundations & Bitcoin Origins

1. National Security Agency. (1996). *How to Make a Mint: The Cryptography of Anonymous Electronic Cash.* Retrieved from https://groups.csail.mit.edu/mac/classes/6.805/articles/money/nsamint/nsamint.htm
2. American University Law Review. (1997). *How to Make a Mint.* Retrieved from https://digitalcommons.wcl.american.edu/aulr/vol46/iss4/6/
3. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved from https://bitcoin.org/bitcoin.pdf
4. Wikipedia. (2025). *Blockchain Analysis.* Retrieved from https://en.wikipedia.org/wiki/Blockchain_analysis
5. Wikipedia. (2025). *Lightning Network.* Retrieved from https://en.wikipedia.org/wiki/Lightning_Network

2. Surveillance Infrastructure and Financial Monitoring

6. The Guardian. (2013). *PRISM leaks: NSA surveillance exposed.* Retrieved from https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
7. Privacy International. (2001). *Interception Capabilities 2000: ECHELON Report.* Retrieved from https://irp.fas.org/eprint/ic2000/ic2000.htm
8. U.S. Department of the Treasury. (2006). *Terrorist Finance Tracking Program (TFTP).* Retrieved from https://home.treasury.gov/system/files/246/Terrorist-Finance-Tracking-Program-Questions-and-Answers.pdf
9. Chainalysis. (2022). *Blockchain Analytics, National Security & AML Enforcement.* Retrieved from https://www.chainalysis.com/blog/blockchain-analysis-national-security-law-enforcement/
10. Chainalysis. (2024). *Testimony to the U.S. House Committee on Agriculture.* Retrieved from https://agriculture.house.gov/uploadedfiles/levin_testimony_package.pdf
11. Wired. (2022). *Most Criminal Cryptocurrency Funnels Through Just 5 Exchanges.* Retrieved from https://www.wired.com/story/cryptocurrency-money-laundering-chainalysis-report/
12. Wired. (2019). *Inside the Bitcoin Bust That Took Down the Web's Biggest Child Abuse Site.* Retrieved from https://www.wired.com/story/tracers-in-the-dark-welcome-to-video-crypto-anonymity-myth/
13. Time. (2022). *Why Crypto Scams Are Driving an Online Crime Boom.* Retrieved from https://time.com/6162350/crypto-scams-online-crime-boom/
14. Greenberg, A. (2022). *Crypto Is Anything But Private. Time.* Retrieved from https://time.com/6239364/crypto-criminals-andy-greenberg/
15. Wikipedia. (2025). *Cryptocurrency and Crime.* Retrieved from https://en.wikipedia.org/wiki/Cryptocurrency_and_crime
16. Associated Press. (2022). *Justice Dept. Charges Russian Founder of Cryptocurrency Firm.* Retrieved from https://apnews.com/article/a503fdd97e1d8a91b36e2ee4a933e0c3

3. Bitcoin Custody, ETFs & Institutional Capture

17. CoinDesk. (2024). *The Biggest Bitcoin ETF Threat No One Is Talking About.* Retrieved from https://www.coindesk.com/opinion/2024/01/11/the-biggest-bitcoin-etf-threat-no-one-is-talking-about
18. CryptoSlate. (2025). *BlackRock Adds Anchorage Digital Alongside Coinbase.* Retrieved from https://cryptoslate.com/blackrock-adds-new-bitcoin-custodian-anchorage-digital-alongside-coinbase/
19. The New Yorker. (2022). *How a Young Couple Failed to Launder Billions in Stolen Bitcoin.* Retrieved from https://www.newyorker.com/business/currency/how-a-young-couple-failed-to-launder-billions-of-dollars-in-stolen-bitcoin

4. Lightning Network Centralization

20. CoinDesk. (2020). *Bitcoin's Lightning Network Is Growing 'Increasingly Centralized'.* Retrieved from https://www.coindesk.com/tech/2020/02/20/bitcoins-lightning-network-is-growing-increasingly-centralized-researchers-find/
21. Cointelegraph. (2020). *Bitcoin's Lightning Network Found More Centralized Than Expected.* Retrieved from https://cointelegraph.com/news/bitcoins-lightning-network-found-more-centralized-than-expected-by-researchers
22. Stroom Blog. (2023). *Lightning Network Centralization Challenges.* Retrieved from https://stroom.network/blog/2023/09/centralization-on-lightning-network/
23. Breez Technology. (2023). *Sources of Centralization on Lightning (and Why They Matter).* Retrieved from https://blog.breez.technology/sources-of-centralization-on-lightning-and-why-they-matter-b7aa3352231f
24. MDPI. (2023). *A Review of the Lightning Network's Evolution.* Retrieved from https://www.mdpi.com/0718-1876/18/3/68
25. Zabka, M., et al. (2022). *A Centrality Analysis of the Lightning Network. arXiv.* Retrieved from https://arxiv.org/abs/2201.07746
26. arXiv. (2020). *A Second Path to Centralization in the Bitcoin Economy.* Retrieved from https://arxiv.org/abs/2005.00114
27. arXiv. (2020). *Bitcoin Transaction Networks: Overview of Recent Results.* Retrieved from https://arxiv.org/abs/2111.13494
28. arXiv. (2021). *The Weighted Bitcoin Lightning Network.* Retrieved from https://arxiv.org/abs/2104.01492

5. Canadian CBDC, Freedom Convoy & Financial Censorship

29. CoinDesk. (2022). *Court Freezes Freedom Convoy Crypto Donations.* Retrieved from https://www.coindesk.com/policy/2022/02/18/private-lawsuit-freezes-canadian-freedom-convoy-crypto-fundraising/
30. Global News. (2022). *Canadian Government Freezes Bitcoin Accounts.* Retrieved from https://globalnews.ca/news/8610512/givesendgo-fundraiser-trucker-convoy-frozen/
31. Blockworks. (2022). *Federal Judge Rules Crypto Freeze Unlawful.* Retrieved from https://blockworks.co/news/crypto-freeze-unlawful-canada

6. Tornado Cash Precedent & Crypto Privacy Crackdown

32. Associated Press. (2023). *Tornado Cash Founders Arrested, Sanctioned.* Retrieved from https://apnews.com/article/cryptocurrency-treasury-crypto-sanctions-russia-north-korea-88115029d0a033b7b8b3e3a34dccf00c
33. Axios. (2024). *Dutch Court Sentences Tornado Cash Developer Alexey Pertsev.* Retrieved from https://www.axios.com/2024/05/14/tornado-cash-alexey-pertsev-crypto
34. Reuters. (2025). *U.S. Lifts Tornado Cash Sanctions.* Retrieved from https://www.reuters.com/business/finance/us-scraps-sanctions-tornado-cash-crypto-mixer-accused-laundering-north-korea-2025-03-21/

7. Central Bank Digital Currencies (CBDCs) & Global Interoperability

35. Bank of Canada. (2024). *Digital Canadian Dollar: Consultation Paper.* Retrieved from https://www.bankofcanada.ca/wp-content/uploads/2024/10/sdp2024-16.pdf
36. Bank of Canada. (2024). *Analytical Note on CBDC Impact.* Retrieved from https://www.bankofcanada.ca/2024/03/analytical-note-cbdc-implications/
37. CIGI. (2024). *How Central Banks Are Shaping the Future of Digital Currencies.* Retrieved from https://www.bankofcanada.ca/2024/12/staff-analytical-note-2024-27/
38. Brookings Institution. (2022). *China's Orwellian Social Credit Score Isn't Real.* Retrieved from https://www.brookings.edu/articles/chinas-orwellian-social-credit-score-isnt-real/
39. MIT Digital Currency Initiative. (2022). *Project Hamilton: Phase 1 Executive Summary.* Retrieved from https://www.bostonfed.org/publications/one-time-pubs/project-hamilton-phase-1-executive-summary.aspx
40. European Central Bank. (2023). *The Digital Euro: Privacy Options and Programmability.* Retrieved from https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.degov220404_privacy.en.pdf
41. European Central Bank. (2023). *Lagarde: "We Do Not Want a Completely Anonymous Digital Euro".* Retrieved from https://finbold.com/ecb-chief-says-the-digital-euro-cbdc-will-not-be-entirely-anonymous/

8. Financial Deplatforming & Regulatory Overreach

42. BBC. (2023). *Nigel Farage De-Banked by Coutts for Political Views.* Retrieved from https://www.bbc.com/news/uk-politics-66354476
43. U.S. House of Representatives. (2014). *Operation Choke Point Report.* Retrieved from https://republicans-oversight.house.gov/wp-content/uploads/2014/05/Staff-Report-Operation-Choke-Point1.pdf

9. Video & Cultural Commentaries

44. James Jani. (2021). *Crypto: The World's Greatest Scam?* [YouTube]. Retrieved from https://www.youtube.com/watch?v=ORdWE_ffirg

45. Unknown. (2022). *Has Bitcoin Been Hijacked by Intelligence Agencies?* [YouTube]. Retrieved from https://www.youtube.com/watch?v=iFqyKLXEuYo
46. Office of the Privacy Commissioner of Canada. (2020). *Investigation into Cadillac Fairview's use of facial recognition technology.* Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/
47. United States Government. (1933). *Executive Order 6102: Gold Confiscation Order.* Retrieved from https://www.federalreservehistory.org/essays/gold-reserve-act
48. Merrick, P. J., & Spitters, A. C. (2025). *It Starts With Gold™.* Chapter 4: The 1933 Gold Reset. Retrieved from https://www.ItStartsWithGold.com

Glossary of Terms

Aadhaar
A biometric digital ID system implemented in India. Links identity, financial accounts, and government services. Cited as a model for integrated digital ID and CBDC platforms.

Addressable Digital Node
A device or endpoint on a network that can be uniquely identified, tracked, and monitored through IP addresses or other identifiers. Used in early ARPANET and modern internet infrastructure.

Air Miles
A Canadian customer loyalty program that tracks consumer purchases across partnered retailers. Data collected may be used to profile consumer behaviour and link purchasing activity to financial and identity systems.

AI (Artificial Intelligence)
Software systems capable of processing large datasets, detecting patterns, and making predictions. In this context, used to analyze blockchain data for behavioural profiling and predictive financial surveillance.

Algorithmic Governance
The use of software code, machine learning, or programmable rules to control user permissions, access, or activity. Found in both smart contracts and programmable CBDCs.

Anchorage Digital
A regulated cryptocurrency custodian that holds assets on behalf of institutions. It plays a role in Bitcoin ETF structures and compliance infrastructure.

Anti-Money Laundering (AML)
A legal framework that requires financial institutions to prevent, detect, and report money laundering and terrorist financing. Often used as a justification for surveillance of crypto users.

API (Application Programming Interface)
A software interface that allows different applications to communicate. APIs are used by surveillance firms, exchanges, and banks to share user data and integrate financial controls.

Apple
A major U.S. technology company whose servers were accessed through PRISM, according to the Snowden revelations. Mentioned in context of mass data surveillance partnerships with intelligence agencies.

ARPANET
The U.S. Department of Defense's original packet-switching network, launched in 1969. Considered the precursor to the internet and designed for traceability, redundancy, and control.

Asset Forfeiture
The legal process where government authorities seize assets suspected of being linked to crime or non-compliance. Increasingly applied to crypto wallets through custodians or blockchain analytics.

Beneficial Ownership
A legal structure where the rights to an asset are held by a party other than the legal titleholder. Common in custodial and ETF structures, where investors hold interest but not direct title to underlying assets.

Bitcoin (BTC)
The original cryptocurrency, launched in 2009 by Satoshi Nakamoto. Initially promoted as decentralized peer-to-peer cash, now largely absorbed into regulated, surveilled financial infrastructure.

Bitcoin Cash (BCH)
A fork of Bitcoin created in 2017 to support larger block sizes and lower transaction fees. Intended to restore Bitcoin's original purpose as peer-to-peer money.

Bitcoin Core (BTC)
The main implementation of Bitcoin, maintained by a core development team. Often associated with smaller block sizes, slower speeds, and institutional alignment.

Blockchain
A cryptographically secured, time-stamped digital ledger used to record transactions. Designed for transparency, but easily used for traceability and behavioural analytics.

Blockchain Analytics
A field focused on analyzing blockchain data to track transactions, identify user behaviours, and link wallet addresses to real-world identities.

Carbon Score
A behavioural metric that measures an individual's carbon emissions or compliance with environmental standards. Often discussed in relation to ESG-linked digital currencies or digital IDs.

Carbon Tracking Credit Cards
Financial products that monitor the carbon footprint of user purchases. Promoted as part of ESG frameworks and discussed in the context of programmable money and social credit applications.

CBDC Interoperability
The technical and policy frameworks that allow CBDCs from different countries to work together across borders. Often designed using International Monetary Fund or Bank for International Settlements templates.

Central Bank Digital Currency (CBDC)
A programmable, centrally issued digital currency designed to replace physical cash and allow governments to monitor, restrict, and control financial behaviour at the individual level.

Centralized Exchange (CEX)
A cryptocurrency platform that acts as an intermediary for buying, selling, and custody of digital assets. Requires KYC and is subject to government regulations.

Cadillac Fairview
A Canadian commercial real estate company investigated in 2023 for deploying facial recognition technology in mall directories without user consent. Cited as evidence of domestic biometric surveillance.

Chainalysis
A major blockchain surveillance company providing tools for transaction monitoring, risk scoring, and compliance. Used by governments, regulators, and private firms to de-anonymize users.

Cheka
The first Soviet state security organization. Precursor to the GPU, NKVD, and KGB. Ran Operation Trust to trap dissidents under false pretenses of underground resistance.

Clearview AI
A controversial facial recognition company that scrapes public images to build biometric profiles. Referenced in relation to smart city surveillance infrastructure in Canada.

Coin Mixer
A tool that anonymizes cryptocurrency transactions by pooling and redistributing coins to obscure origins. Example: Tornado Cash.

Cold Wallet
A cryptocurrency wallet not connected to the internet. Provides offline storage and greater protection from hacking and surveillance.

Compliance Infrastructure
The embedded legal and technological framework that enforces government or institutional rules on financial platforms. Includes KYC, AML, geofencing, and blacklists.

Custodian
An entity, often regulated, that holds and manages digital assets for users or institutions. Users who store funds with custodians do not control their private keys or asset access.

- **Custodial Platform**

A third-party service that holds digital assets on behalf of users. Custodial models are subject to regulatory compliance and can freeze, block, or surveil user activity.

Cypherpunk
A 1990s-era movement advocating for the use of strong cryptography and decentralized systems to protect privacy and individual sovereignty.

Dark Wallet
An experimental privacy-focused Bitcoin wallet developed in 2014. Targeted by regulators due to its anonymity features. Predecessor to tools like Wasabi and Samourai Wallet.

Decentralized Finance (DeFi)
A system of blockchain-based financial services that operate without centralized intermediaries. Increasingly subject to regulation and surveillance pressure.

Digital Dollar (Canada or U.S.)
A proposed central bank digital currency in Canada or the United States. Would allow real-time tracking, control of citizen transactions, and integration with ESG or identity scoring.

Digital ID
A digital identity tied to an individual's legal, biometric, or behavioural information. Used to access services and link to payment systems like CBDCs.

DNS (Domain Name System)
A naming system for internet-connected devices. Developed under government control and allows tracing and routing of all online communication.

DOJ (U.S. Department of Justice)
The law enforcement agency responsible for prosecuting crypto-related crimes, often relying on blockchain analytics firms for evidence.

Doxing
Publishing personal information online, often through de-anonymization of crypto wallets, forums, or social media.

End-to-End Traceability
The ability to follow digital activity from its origin to final use, enabling complete behavioural mapping. Built into blockchain systems by design.

ESG (Environmental, Social, and Governance)
A framework for evaluating compliance with environmental and social goals. Increasingly tied to financial access, including programmable currency and credit scoring.

ESG Scoring
A numeric or weighted system that rates individuals or entities based on ESG criteria. Can be tied to financial permissions under CBDCs.

Executive Order 14247
A 2025 U.S. policy requiring all federal payments to use digital rails. Although not a CBDC law, it lays the groundwork for programmable payments and surveillance.

Fiat Currency
Government-issued currency not backed by a commodity like gold. CBDCs are digital fiat currencies with programmable features.

Five Eyes
An intelligence-sharing alliance between the United States, Canada, United Kingdom, Australia, and New Zealand. Mentioned in context of global surveillance programs like ECHELON.

The Financial Industrial Complex
A term used in this paper to describe the interconnected system of governments, central banks, financial institutions, regulatory bodies, surveillance technology firms, and international organizations that operate together to enforce financial compliance, monitor behaviour, and shape the future of programmable money systems—often with little or no democratic oversight.

Fork (in blockchain)
A change in the blockchain protocol that creates a new version of the blockchain, such as the split between Bitcoin and Bitcoin Cash.

Freedom Convoy
A 2022 Canadian protest against COVID-19 mandates. Became the first major Western event where crypto wallets were frozen by government order.

FTX
A failed cryptocurrency exchange where billions in user assets were lost. Highlighted the risk of custodial platforms and lack of investor protections.

GPU (Soviet GPU)
The successor to the Cheka and forerunner of the KGB. Played a key role in suppressing dissent and running operations like Trust.

Hot Wallet
A cryptocurrency wallet connected to the internet. Easier to use but more vulnerable to surveillance and hacking.

ICANN
Internet Corporation for Assigned Names and Numbers. Manages domain names and IP address allocation globally, reinforcing centralized control of internet infrastructure.

IANA
Internet Assigned Numbers Authority. Coordinates IP address allocation and protocol parameters, operating within centralized internet governance.

Institutional Capture
The process by which large financial or regulatory institutions absorb or co-opt decentralized technologies to serve centralized control mechanisms.

IP Address
A unique identifier for an internet-connected device. Enables geolocation, surveillance, and traceability online.

KGB (Committee for State Security)
The Soviet intelligence agency that succeeded the NKVD. Known for psychological operations, surveillance, and suppression of dissent.

Know Your Customer (KYC)
A regulatory requirement for financial services to verify users' identities. Ties all transactions to real-world identities, ending pseudonymity.

Layer 2
A secondary protocol built on top of an existing blockchain to increase scalability. Often introduces new chokepoints and surveillance vectors, such as Lightning Network.

Lightning Network
A Layer 2 protocol for Bitcoin that enables faster, cheaper transactions. It has become increasingly centralized, with traffic flowing through a small number of nodes.

MIT
Massachusetts Institute of Technology. Its mailing list was used to publish the NSA's 1996 whitepaper *How to Make a Mint*. Also partnered in Project Hamilton.

MIT Cryptographic Mailing List
The online venue where the NSA released its 1996 *How to Make a Mint* paper, which outlined a pseudonymous electronic cash system.

Minority Report
A 2002 film depicting predictive policing. Used as a metaphor for modern financial surveillance and algorithmic profiling.

Mixer
A privacy tool that scrambles cryptocurrency transaction paths. Frequently targeted by regulators and banned in some jurisdictions.

NSA
National Security Agency. U.S. intelligence agency responsible for cryptographic standards like SHA-256 and the 1996 *How to Make a Mint* paper. Foundational in shaping surveillance-compatible cryptographic systems.

Operation Trust
A Soviet counterintelligence program used to lure dissidents into false resistance cells. Used in this paper as an analogy for Bitcoin's potential role in surveillance entrapment.

P2P (Peer-to-Peer)
A network where participants interact directly without intermediaries. Bitcoin was originally designed as a P2P payment system.

PRISM
A U.S. government mass surveillance program that accessed user data from major tech companies. Exposed by Edward Snowden in 2013.

Private Key
A secret cryptographic key used to access and authorize transactions from a crypto wallet. Whoever holds the private key controls the asset.

Programmability
The core feature of CBDCs that enables money to be conditional, expirable, or restricted. Often linked to digital ID, ESG metrics, or behaviour.

Programmable Currency
Digital money that contains embedded rules for how, where, or when it can be used. Central banks can use it to enforce restrictions or incentives.

Project Hamilton
A pilot CBDC infrastructure project led by the Federal Reserve Bank of Boston and MIT, processing 1.7 million transactions per second. Serves as a proof-of-concept for scalable CBDCs.

Public Key
A cryptographic key that allows others to verify transactions or send funds. Paired with a private key in blockchain systems.

QR Code (in crypto)
A machine-readable code often used to share wallet addresses. Can be scanned to send funds but also used for surveillance and tracking.

Real-Time Payments
Digital payment systems that process and settle transactions instantly. Often serve as the foundation for CBDC infrastructure.

Samourai Wallet
A privacy-focused Bitcoin wallet that includes coin mixing, transaction obfuscation, and stealth addresses. Frequently targeted by regulators.

Satoshi Nakamoto
The pseudonymous creator of Bitcoin. Some theories suggest the name could represent an institutional or government-backed effort.

Self-Custody
Maintaining personal control over crypto assets by holding private keys independently. Considered a cornerstone of financial sovereignty.

Smart Contract
A self-executing contract with rules coded into blockchain. Executes automatically when conditions are met. Enables automation, but also control.

Social Credit System
A behavioural scoring system used to control access to goods and services based on compliance with rules or political norms. Piloted in China and increasingly referenced in Western ESG systems.

Stablecoin
A cryptocurrency pegged to fiat money or another asset to maintain stable value. Examples include USDC, USDT, and government-backed tokens.

Stroom Report
A 2023 analysis showing that over 80% of Lightning Network volume flows through fewer than 10 nodes, highlighting centralization risk.

Surveillance Capitalism
An economic model where data collected from individuals is used to predict and control behaviour for profit and power.

Surveillance State
A political system where citizen activity is continuously monitored and recorded, often under the pretext of national security or financial compliance.

Timestamp
A precise record of the time a blockchain transaction or block was validated. Used to establish chronological and legal records.

Tokenization
The process of converting physical or digital assets into blockchain-based tokens. Often touted as innovation but enables traceability and surveillance.

Tornado Cash
An Ethereum-based privacy protocol shut down by regulators. Its developer was arrested in 2023 for enabling anonymous transactions.

Traceability
The ability to track transactions or digital interactions across time and networks. Built into blockchain by design and increasingly used for profiling.

Trojan Horse
A strategy or system disguised as beneficial that hides a harmful or deceptive intent. Used in the white paper to describe Bitcoin's possible role.

USA PATRIOT Act
A post-9/11 law that expanded surveillance authority in the U.S., including mandatory reporting by financial institutions.

Wasabi Wallet
A Bitcoin wallet that integrates privacy features like CoinJoin. Monitored or restricted by many centralized exchanges.

Wallet
A digital or physical tool for storing cryptocurrency. Can be custodial, where control lies with a third party, or non-custodial, where the user holds the private keys.