How Resistance Money Is Chosen

About

Metanomia is a think tank focused on analyzing transformations in the cryptocurrency market and related technologies.

Researcher

Changjun Lee

Corresponding Author

Taemin Oh

Contents

01
Introduction

Money is both the primary currency of power and an instrument of control; at times, it also serves as a means of resistance to escape that very power. The fiat currency issued by a nation's central bank is the concrete manifestation of state sovereignty and governance. When an individual uses that currency, it implies an implicit endorsement of the state's economic order. What happens, then, when that order breaks down—when the value guaranteed by the state vanishes overnight? Where can individuals turn?

This report seeks to answer that question through the lens of **"Resistance Money."** Resistance money refers to alternative stores of value and payment instruments chosen to protect an individual's economic autonomy against state oppression or systemic financial failure. While earnest debate around this concept took off following the launch of Bitcoin in 2009, its historical roots run far deeper. People have always sought private safe havens to evade the reach of state-controlled money: physical gold, foreign bank notes, and cigarettes, as well as today's digital tokens.

Crucially, resistance money does not take a single, universal form. Bitcoin maximalists[1)] argue that Bitcoin alone represents true sovereign money[2)]. Their logic rests on its censorship resistance and hard-coded supply limit, which place it entirely beyond government intervention. Conversely, for financially excluded populations in developing nations, Bitcoin's extreme price swings represent an unbearable risk. For them, US dollar-pegged stablecoins, which offer the guarantee that tomorrow's purchasing power will match today's, serve as a far more immediate and practical lifeline.

The core thesis of this report is not about endorsing one asset over another. Resistance money is not tied to any single asset class. Neither Bitcoin, stablecoins, gold, cash, nor privacy coins like Monero and Zcash are resistance money by default; rather, an asset *becomes* resistance money only when held by a specific individual, under specific conditions, facing a specific threat.

There is no single "correct" form of resistance money. Instead, it is a dynamic set of optimal solutions emerging from the interplay between a power structure's vector of control and an individual's social context. Claims like "Bitcoin is the only answer" or "Stablecoins are sufficient" offer only partial truths that hold valid under narrow conditions. The primary question is not *which money is universally right*, but rather *who* chooses *what*, under *what circumstances*, to counter *what threat*.

1) Bitcoin Maximalist: A stance that views Bitcoin as the sole or most reliable decentralized currency distinct from other crypto-assets, expecting it to become the core monetary standard over the long term. Adherents regard Bitcoin as ideal "hard money" because a central entity cannot arbitrarily inflate its supply and its total issuance cap is fixed at 21 million units. While the intensity of views varies, maximalists generally prioritize Bitcoin's censorship resistance, decentralization, and capacity for self-custody, while maintaining a critical stance toward altcoins and centralized stablecoins. A strong form of maximalism projects "hyperbitcoinization," a scenario in which Bitcoin gradually replaces legacy fiat currencies.

2) Sovereign Money: In monetary and central banking literature, "sovereign money" generally refers to public money issued and guaranteed by the state or central bank, grounded in national monetary sovereignty. In Bitcoin discourse, however, the focus shifts to individual sovereignty, referring to "self-sovereign money," meaning currency directly controlled by the individual without relying on permission, custody, or third-party intermediaries such as states or banks.

Moving past binary debates, this paper draws on diverse case studies to examine which financial tools function as resistance money, for whom, and under what parameters. To establish this framework, we first examine how Bitcoin was initially conceptualized as resistance money, and then expand that framework to analyze a broader spectrum of currencies operating under real-world conditions.

02
Redefining Resistance Money

The Core Argument of Resistance Money

The term "Resistance Money" originally gained traction within the Bitcoin community. The theoretical framework positioning Bitcoin as an antidote to state power was systematically articulated in the 2024 book Resistance Money, authored by Andrew M. Bailey, Bradley Rettler, and Craig Warmke[1].

The authors begin with the premise that Bitcoin can serve wildly different agendas of resistance. It can act as a tool for illicit actors and hackers, just as easily as it serves as a financial lifeline for dissidents fighting censorship or refugees facing frozen bank accounts. Resistance itself carries no inherent moral alignment; its value depends entirely on what is being resisted. Classifying Bitcoin as resistance money does not mean it is exclusively used for noble ends, but rather that it carves out an economic domain where state power struggles to intervene.

The authors explain this capacity for resistance through the core metric of "trust minimization." Traditional digital monetary systems depend on central entities performing three distinct roles: custodians who hold funds (commercial banks), intermediaries who process transactions (credit card networks and payment processors), and issuers who control money creation (central banks and commercial banks). A single institution often performs multiple roles. While these entities facilitate secure custody, convenient payments, and monetary stability, they also represent critical single points of failure. Custodians can misplace or freeze funds; intermediaries can log transaction histories, block transfers, or extract fees; and issuers can debase currency through inflationary policies.

Evaluating traditional alternatives, such as gold, foreign fiat currencies, and physical cash, against these three pillars reveals that none fully escape reliance on trust. Physical gold does not depend on a central issuer, yet storing large quantities safely or transporting it across borders requires heavy reliance on third-party custodians and security networks. Holding foreign currency (such as US dollars) allows individuals to bypass domestic issuers, but leaves them exposed to the policy decisions of a foreign central bank and the domestic distribution networks required to exchange that currency. Physical cash permits peer-to-peer settlement without custodians or payment processors, yet users must still place total trust in the monetary in-

tegrity of the issuing state. Rather than eliminating trust, these traditional tools merely shift or shrink the scope of trust to sidestep immediate threats.

Bitcoin takes trust minimization a step further. It was engineered to bypass all three roles simultaneously. Users can hold their assets directly through self-custody and process transfers without third-party intermediaries, while new issuance follows a predictable, hard-coded schedule capped at 21 million coins. Altering these foundational parameters requires broad consensus across the network rather than an executive decree by a central authority. The authors designate Bitcoin as "digital cash" precisely because it removes the custody, settlement, and issuance of money from institutional discretion. This structural trust-minimization forms the backbone of Bitcoin's censorship resistance and its efficacy as resistance money.

That said, the authors do not present Bitcoin as an all-encompassing panacea. Their work weighs Bitcoin's structural advantages in privacy, censorship resistance, financial inclusion, and monetary predictability against its real-world costs and operational limitations. Nor do they argue that Bitcoin is the right choice for everyone in every situation. In this regard, their perspective maintains a clear boundary from Bitcoin maximalism.

While Bailey et al. focus their analysis on Bitcoin, the evaluation criteria they employ can also be applied to other currencies and payment methods. Alternatives to Bitcoin may reduce certain existing risks, but they may also create new challenges by introducing dependence on issuers, custodians, or payment infrastructure, or by raising concerns related to price volatility, accessibility, and regulation. The following discussion compares the potential for resistance and limitations of these alternatives through the lens of these trade-offs.

Five Criteria for Assessing Resistance Money

"Alternative currency" is a broad umbrella encompassing all stores of value and mediums of exchange outside standard fiat currency. It spans everything from retail loyalty points, in-game tokens, and local scrip to physical gold, foreign bank notes, Bitcoin, stablecoins, and mobile money rails. Regardless of form, any instrument that partially supplements or substitutes for state-issued fiat falls under this category.

However, not every alternative currency qualifies as resistance money. The defining line is not whether a tool is physical or digital, but whether it enables users to bypass institutional control and reclaim economic self-determination. Closed-loop corporate assets like airline miles or in-game currencies lack independent infrastructure; when targeted by an issuing authority, they offer no fallback options, making them ill-suited to act as resistance money.

By what criteria, then, can we determine whether a given tool functions as resistance money? Building on the concepts of trust minimization, privacy, censorship resistance, and financial inclusion laid out in Resistance Money,

this report establishes five core criteria to evaluate alternative monetary tools:

1. **Power Resistance:** The degree to which a currency withstands direct intervention by state or institutional authority, including asset freezes, account seizures, transaction blocks, and arbitrary censorship. The fundamental question is: "Can a central authority unilaterally block or seize this asset?" Held in a self-custody wallet,[3] Bitcoin demonstrates exceptionally high power resistance because freezing funds by choking off traditional intermediaries (banks or centralized exchanges) becomes nearly impossible. However, this does not grant total immunity against physical key confiscation or forced compliance. In contrast, centralized stablecoins like USDT and USDC carry lower power resistance than Bitcoin because their issuers can blacklist wallet addresses and freeze assets under regulatory pressure. Traditional bank deposits are the most vulnerable to capital controls and account freezes.

2. **Value Stability:** How effectively a currency protects an individual's purchasing power against value controls like rapid inflation and currency debasement. The fundamental question is: "Does this asset hold its purchasing power over time?" US dollars and dollar-pegged stablecoins provide high short-term purchasing power stability, though they remain bound to US monetary policy. Gold has served as the historic standard for value preservation over centuries, though it is poorly suited for daily commerce. Bitcoin, with its hard cap of 21 million coins, offers strong long-term defense against structural inflation, but suffers from significant short-term price volatility. Value stability depends on the specific time horizon an individual needs to protect.

3. **Privacy:** The degree to which a currency protects transaction histories and wallet balances from open surveillance. The fundamental question is: "Can an outside authority track who sent how much to whom, and when?" Physical cash provides strong transactional privacy, though it is constrained by physical storage limits and geographic boundaries. Bitcoin provides pseudonymity,[4] but because all transactions are recorded on a public blockchain, real-world identities can be unmasked through chain analysis. To restore cash-like privacy in digital environments, privacy-focused protocols[5] (like Monero and Zcash) alongside Bitcoin privacy tools (such as CoinJoin[6], the Lightning Network[7], and zero-knowledge proofs[8] were created. How these mechanisms counter surveillance control is examined further in Section 04.

3) Self-Custody Wallet: A method where users directly manage the private keys granting authority to transfer assets, rather than entrusting custody to third parties like exchanges or institutional custodians. While the individual bears sole responsibility for asset loss if private keys and recovery mechanisms are lost, it prevents third-party institutions from unilaterally freezing or transferring the assets.

4) Pseudonymity: The property of transacting under a pseudonym (public wallet address) rather than a real name. Unlike true anonymity, all transactions remain recorded on a public ledger; thus, the moment an address is linked to a specific identity, past transactions can be retroactively traced.

5) Privacy-Focused Protocols: Cryptocurrencies designed to conceal or obscure on-chain transaction details, such as the identities of transacting parties and transaction amounts. Monero hides senders, receivers, and amounts by default, while Zcash obscures transaction content using zeroknowledge proofs.

6) CoinJoin: A privacy-enhancing technique where multiple users pool their respective Bitcoins into a single joint transaction and disburse them to multiple output addresses, making it difficult for external observers to trace which input maps to which output.

7) The Lightning Network: A Layer-2 payment network operating on top of the Bitcoin blockchain. By opening payment channels, individual payments are processed off-chain within the channel, and only the final balance is settled on the blockchain upon channel closure, enabling fast and low-cost transactions. While it does not guarantee absolute anonymity, it reduces the public exposure of transaction data.

8) Zero-Knowledge Proofs: A cryptographic technology that mathematically proves a statement is true without revealing the underlying content of the information. For example, it proves knowledge of a password without disclosing the password itself. It allows verification of transaction validity while concealing the sender, receiver, and amount.

4. **Accessibility:** Whether a currency can be obtained, stored, and spent without requiring formal bank accounts, official identity verification, cross-border permissions, or legacy financial rails. The fundamental question is: "Can anyone use this tool without asking for permission?" According to World Bank Global Findex [2] data, approximately 21% of adults globally remain completely unbanked. Accessibility is the foundational requirement for all other criteria. Regardless of how censorship-resistant an asset is, if affected populations cannot access or store it, it cannot function as resistance money. The rapid adoption of mobile money and the widespread reliance on stablecoins across emerging economies stem directly from their low barriers to access.

5. **Acceptance Community:** The presence of a viable network of individuals and merchants who recognize and accept the asset as a medium of exchange. The fundamental question is: "Is there a counterpart willing to trade for this?" Money cannot function on technological merits alone. Without an active counterparty network, even the most sophisticated tool fails to act as a store of value or medium of exchange. Bitcoin served as an effective donor mechanism during the Canadian Freedom Convoy protests precisely because a global peer-to-peer network already existed to receive and route it. Where no local or global community accepts an asset, its utility as resistance money drops to zero. Alongside accessibility, an active acceptance community forms the practical baseline that allows all other criteria to operate in real-world scenarios.

These five criteria do not function in isolation. Power resistance, value stability, and privacy map directly against the state's three primary mechanisms of monetary control: **transaction control**, **value control**, and **surveillance control**. Meanwhile, accessibility and the acceptance community form the operational baseline required for any alternative currency to be deployed. Which asset functions as resistance money depends on where an individual's threat profile intersects with their available infrastructure and local community adoption.

How do state authorities deploy monetary control, and how far can individuals step out of reach? Section 03 examines this dynamic through the concept of "institutional distance."

03
Institutional Distance and Monetary Power

A Nearby Tyrant vs. a Distant Empire

As a British colony from 1841 to 1997, Hong Kong's residents had no voting rights in the British Parliament. From the perspective of democratic self-determination, this represented a clear democratic deficit. Yet the economic policies championed by Hong Kong's Financial Secretary, Sir John Cowperthwaite, transformed the territory into Asia's leading financial center.[3] Three structural pillars—the rule of law, economic freedom, and the protection of property rights—more than compensated for the absence of voting rights.

Meanwhile, in mainland China, the Great Leap Forward[9)] and the Cultural Revolution[10)] took place during and around Cowperthwaite's tenure as Financial Secretary. The famine caused by the Great Leap Forward claimed tens of millions of lives, while the Cultural Revolution was marked by widespread violence and persecution. Between residents of the mainland, who lived under the sovereign rule of their own government, and Hong Kong residents, who lived as subjects of a distant empire without even the right to vote, who was freer, and who was safer?

On the mainland, a nearby government exercised control not only over economic activity but also, in many cases, over the very conditions of survival. By contrast, the colonial government in Hong Kong maintained low tax rates and free trade while showing relative restraint in directly intervening in private decisions concerning production and investment. This contrast suggests that the freedom and security individuals enjoy may depend less on who holds governing power than on the extent to which that power intervenes in their lives and on the institutions that constrain it. In this sense, an institutionally constrained distant empire may sometimes be preferable to a nearby tyrant.

9) The Great Leap Forward: A radical industrialization and collectivization campaign led by Mao Zedong from 1958 to 1962. Unrealistic targets and policy failures triggered a massive famine that resulted in tens of millions of deaths.

10) The Cultural Revolution: A political and social movement led by Mao Zedong from 1966 to 1976. Under the banner of class struggle, intellectuals and political opponents were purged, causing severe societal upheaval and widespread persecution.

What Is Institutional Distance?

Institutional distance is a framework for analyzing the relationship between the extent of power's intervention in an individual's life and the autonomy the individual retains. The relationship between individuals and power is described in terms of "distance" because its essential dynamic lies in the bal-

ance between control and autonomy. The closer individuals are to power, the more their economic activities are exposed to surveillance and intervention; the farther away they are, the freer they become from such control. Institutional distance refers to this degree of proximity or distance, in other words, the extent to which an individual retains autonomy from the control of powerful institutions such as governments, corporations, and financial institutions.

This concept originated in international business as a metric to evaluate differences between the institutional environments of two countries (Kostova, 1999)[4, 11]. This report repurposes and redefines the concept, shifting the frame of reference from cross-national comparisons to the relationship between the individual and power. It maps an individual's capacity to conduct economic activity independent of central authority along a continuous spectrum ranging from absolute subordination to full economic sovereignty.

11) Kostova, 1999: In international business literature, institutional distance refers to the variance in institutional environments between a home country and a host country, spanning regulatory, normative, and cognitive dimensions. Originally conceptualized to explain the friction multinational enterprises face when transferring management practices across borders, distance here denotes inter-country institutional gaps. This report adapts only the underlying notion of "distance" rather than the cross-national metric itself, shifting the unit of analysis to the relationship between the individual and sovereign power.

This distance is not a fixed constant; rather, it is a dynamic variable constantly negotiated between power's push to intervene and the individual's drive to preserve autonomy. As power expands its reach into economic affairs, distance shrinks toward subordination; conversely, as individuals adopt mechanisms to sidestep intervention, distance expands toward sovereignty. Resistance money represents an individual choice to widen this distance through monetary means. How effectively a given currency expands this distance depends on which specific form of intervention it counters.

At one extreme of the spectrum lies absolute subordination. Here, an individual's assets and financial records are fully controlled by central authorities, leaving no room for economic self-determination. The total surveillance state of a totalitarian regime exemplifies this extreme. At the opposite end lies full sovereignty, an absolute state of autonomy free from any institutional interference. Because this state also implies a complete absence of institutional protections, it remains an unachievable ideal in practice. Most individuals navigate their daily lives somewhere between these two poles, negotiating a practical compromise between control and autonomy.

Table 1 summarizes these two polar extremes alongside the intermediate zones across the spectrum.

TABLE 01 **The Institutional Distance Spectrum**

	Dependent Group	Intermediate Zone	Sovereign Group
Status	Complete Dependence	Strategic Complementarity	Complete Sovereignty
Control	Controller	Separation of Powers	Individual
Data	Full Control over Personal Assets and Information	A Balance Between Disclosure and Convenience	Privacy Protection

Historically, institutional distance has been continuously reshaped by shifts in technology and structures of authority. Under medieval feudalism, the distance between serf and lord approached zero. Tied directly to the land, serfs possessed neither freedom of movement nor economic self-determination. The rise of the modern nation-state and the development of market economies dramatically expanded this distance. Institutional safeguards, such as private property rights, freedom of contract, and equality under the law, guaranteed individuals a meaningful buffer from central authority.

The twentieth century witnessed dramatic swings in this distance. Communist regimes in the Soviet Union and China compressed institutional distance back toward absolute subordination, whereas Western liberal democracies developed mechanisms to expand it. With the end of the Cold War, the world appeared briefly to enter an era of expanding institutional distance. However, twenty-first-century digital technologies have begun re-compressing this distance in unexpected ways.

Advances in digital technology have vastly increased the capacity of states and corporations to monitor and direct individual economic behavior. Tools such as Central Bank Digital Currencies (CBDCs), digital ID networks, and real-time transaction monitoring systems act as forces compressing institutional distance toward subordination.

Money serves as the single most powerful lever leveraged by authority to shrink this distance. How, then, do governing structures utilize money to compress institutional distance? That question forms the core of the following section.

Three Mechanisms of Monetary Control

The state exercises control over money by leveraging the three essential actors in the financial architecture. By coercing or co-opting fund custodians, payment intermediaries, and currency issuers, governing authorities can constrain individual economic autonomy across three distinct dimensions. These interventions dictate the permissible scope of transactions, the purchasing power of money, and the visibility of economic activity, manifesting as transaction control, value control, and surveillance control.

First is transaction control. This occurs when authority intervenes in who may send or receive funds, and in what amounts. Key mechanisms include bank account freezes, capital controls, wire transfer blocks, and exclusion from global payment networks. When users store Bitcoin via self-custody, their resistance to transaction control is exceptionally high because state authorities cannot unilaterally freeze assets through central chokepoints like commercial banks or exchanges.

Second is value control. This addresses whether power can unilaterally dilute the purchasing power of an individual's assets. Key mechanisms include structural inflation, quantitative easing[12], currency redenomination, and deliberate devaluation. When a domestic currency is exposed to rapid inflation or sharp depreciation, U.S. dollar stablecoins can serve as a practical means of protection on this axis by drawing on the relative stability of the dollar while remaining accessible without a traditional bank account.

12) Quantitative Easing: A monetary policy where a central bank purchases large volumes of assets, such as government bonds, from the open market to inject liquidity into the economy. While it supports asset prices, expanding the monetary base can dilute the purchasing power of the currency.

Third is surveillance control. This concerns the extent to which an individual's economic life is exposed to outside observation, and how that operational data is utilized. This axis encompasses states leveraging transaction data for political control, Big Tech firms converting consumer spending patterns into predictive commercial products, and individuals unknowingly surrendering private data in exchange for platform convenience.

These three axes do not operate in isolation. Under totalitarian regimes, an individual's institutional distance across all three axes is forcibly compressed toward absolute subordination. Even in advanced liberal democracies, the surveillance axis quietly contracts as citizens surrender privacy for consumer convenience, while the transaction control axis can rapidly compress during crisis situations.

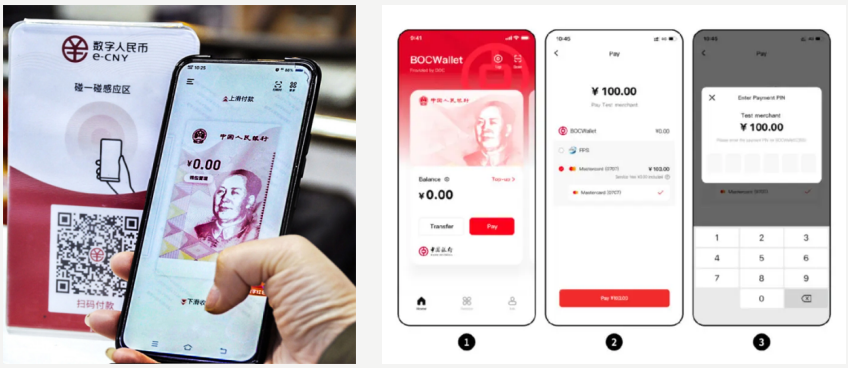
The reason Central Bank Digital Currencies (CBDCs) have sparked global debate lies precisely in their technical ability to calibrate all three control axes simultaneously. Where commercial bank deposits represent private bank liabilities and Bitcoin represents a decentralized asset, a CBDC is a central bank-backed fiat currency converted into digital form. The decisive shift from physical paper cash is that rules can be hard-coded into the currency itself. Issuers can dictate who can spend money, by when, and on what, creating so-called "programmable money."

Restricting permissible spending categories enforces transaction control; setting expiration dates to prevent saving enforces value control; and recording all ledger entries on a central server enforces surveillance control. However, how these technical features are implemented in practice varies widely by jurisdiction.

CBDCs are broadly split into wholesale models (used for interbank settlement) and retail models (issued directly to citizens). It is primarily retail CBDCs that bear a direct impact on daily individual freedom.

The most explicit manifestation of state control is China's digital yuan (e-CNY)[5]. Following internal testing in late 2019, the People's Bank of China launched public pilot programs in major hubs like Shenzhen and Suzhou in April 2020. The e-CNY supports smartphone app payments as well as offline, device-to-device transfers. While low-value payments feature near-anonymous settlement, authorities retain full technical capacity to unmask identities under the policy framework of "controllable anonymity" (可控匿名). In practice, transactions appear anonymous day-to-day, but the tracking switch remains firmly in the hands of the issuer.

FIGURE 01



China's e-CNY payment interface (left) and wallet app payment process (right).
Sources: Maeil Business Newspaper (left) and Registration China (right).

Conversely, the Sand Dollar of the Bahamas,[6] a retail CBDC deployed nationwide in October 2020, was designed primarily to expand financial inclusion and payment access across a geographically fragmented archipelago. Meanwhile, the European Central Bank's proposed Digital Euro has prioritized privacy from its inception, pledging cash-equivalent anonymity for offline transactions. In South Korea, the Bank of Korea's "Project Hangang" adopts an intermediated architecture: the central bank issues wholesale CBDCs exclusively to financial institutions, while commercial banks issue customer-facing deposit tokens[13)] on top of that system. This model prevents the central bank from directly inspecting private transactions. Furthermore, its core architecture embeds a dual-layer privacy protection scheme to prevent personally identifiable information from being logged by external entities uninvolved in the transaction. Thus, CBDCs are designed with vastly different balances of surveillance capacity, financial inclusion, and privacy protections based on each nation's policy objectives and institutional choices.

Consequently, a CBDC cannot be classified as a tool of state control by default. Nevertheless, because a CBDC functions as programmable money issued and managed by a central bank, its baseline architecture inherently aggregates transaction records at the center. While paper cash achieves privacy through the technical impossibility of tracing physical notes, a CBDC relies entirely on a policy promise not to track its users. Bridging the structural gap between this technical capacity and a legal commitment remains an unavoidable challenge for any CBDC architecture.

13) Deposit Tokens: Digital money issued by commercial banks on a blockchain backed by customer deposits. In South Korea, it is designed as a practical retail instrument operating on top of the Bank of Korea's wholesale CBDC infrastructure.

04
Resistance Money in Reality

Resistance to Transaction Control

In October 2020, protests erupted across Nigeria against police brutality by the Special Anti-Robbery Squad (SARS), coalescing under the #EndSARS movement[14)]. As state pressure intensified, the payment link on Flutterwave, the fintech platform utilized by organizers for fundraising, was disabled, and associated bank accounts were frozen. By weaponizing transaction control to sever the financial lifelines supporting medical, legal, and food assistance, authorities sought to suffocate the resistance without firing a single shot.

In response, protesters bypassed the traditional system by turning to Bitcoin. Immediately after bank accounts were blocked, organizers posted a Bitcoin donation address; by the time the protests subsided, Bitcoin accounted for roughly 40% of the approximately $387,000 raised[7]. Because Bitcoin operates without a centralized issuer or intermediary bank, government authorities could not block these contributions. This episode demonstrated to a global audience that Bitcoin's censorship resistance is not merely a theoretical virtue, but a practical lifeline in real-world crises. In an environment where political authorities can weaponize the financial system, uncensorable value transfer channels function as a vital defense mechanism to protect basic human rights.

14) The #EndSARS Movement: A nationwide protest movement in Nigeria in 2020 opposing torture, extortion, and extrajudicial killings by the police Special Anti-Robbery Squad (SARS). Originating as a social media hashtag, it expanded into widespread street demonstrations; despite the government announcing the dissolution of SARS, harsh crackdowns persisted.

FIGURE 02

The 2020 #EndSARS protests in Nigeria (left) and Jack Dorsey's tweet appealing for Bitcoin donations (right).
Source: Quartz Africa.

15) The "Freedom Convoy": A 2022 protest in Canada where truckers occupied downtown Ottawa to oppose COVID-19 vaccine mandates. The federal government invoked the Emergencies Act to freeze crowdfunding and bank accounts associated with the protest.

The events surrounding Canada's Freedom Convoy protests in 2022 demonstrated that the need for censorship-resistant money is not confined to developing economies. When truck drivers protesting COVID-19 vaccine mandates, organized as the "Freedom Convoy"[15)], occupied downtown Ottawa, financial channels were targeted first. On February 4, GoFundMe suspended the group's fundraising campaign, citing terms-of-service violations. On February 10, the Ontario Superior Court of Justice granted a government application to freeze funds collected via GiveSendGo. Four days later, on February 14, Prime Minister Justin Trudeau invoked the 1988 Emergencies Act for the first time in Canadian history. Under this declaration, approximately 210 bank accounts linked to the protests were frozen, locking up nearly CAD 7.8 million in assets[8].

Fundraising via Bitcoin, however, unfolded along a markedly different trajectory. According to CBC reporting, protest-linked wallets raised approximately 20.7 BTC (valued at roughly CAD 1.06 million), of which Canadian authorities managed to freeze only 5.96 BTC[9].

The legal mechanisms deployed by authorities targeted the institutional perimeter around Bitcoin rather than the protocol itself. The Emergency Economic Measures Order issued under the Emergencies Act classified virtual currencies as freezable property and imposed regulatory compliance obligations on crypto crowdfunding platforms. Simultaneously, the Royal Canadian Mounted Police (RCMP) circulated a blacklist of 34 crypto wallet addresses to domestic exchanges, demanding a cessation of transactions[10]. Furthermore, a Mareva injunction issued by the Ontario Superior Court in a civil lawsuit brought by Ottawa residents explicitly named cryptocurrencies as frozen assets, compelling certain defendants to surrender wallet control to court-appointed escrow agents.

Conversely, Nunchuk, a self-custody wallet provider, replied to the court that because it does not hold user private keys, it possessed neither the technical capacity to freeze user assets nor visibility into their existence or magnitude[11]. While authorities could order centralized exchanges to block transactions and mandate wallet owners to transfer assets, they remained powerless to block transfers of self-custodied Bitcoin without possessing the underlying private keys. Moreover, because the majority of donated funds were dispersed across multiple wallets immediately before the Mareva injunction took effect, most of the capital successfully evaded confiscation.

This incident demonstrated that even within a fundamentally different structural context, a Western liberal democracy operating under the rule of law and a stable economy, states can and do weaponize financial infrastructure, and that Bitcoin's censorship resistance remains functionally effective against such pressure.

Similar evasive tactics emerged during the 2019 Hong Kong protests. Fearing that transaction logs on their Octopus transit cards would serve as physical evidence of protest participation, demonstrators purchased subway tickets using physical cash; meanwhile, overseas donations that did not require

immediate liquidation were accepted in cryptocurrency. When confronted with transaction controls, individuals systematically partitioned their use of physical cash and cryptocurrency based on the specific nature of the threat they faced[12].

Resistance to Value Control

For the past several decades, the US dollar has served as the world's most widely used instrument of resistance. In countries where the domestic currency lost public trust, such as Zimbabwe, Argentina, Venezuela, and Lebanon, what individuals held tightly in their hands was the dollar. From a microeconomic perspective centered on the individual rather than a macro-level state perspective, holding dollars when a national currency collapses represents an unmistakable act of resistance.

Dollarization refers to the official or unofficial use of the U.S. dollar in place of a country's domestic currency. In Argentina, individuals repeatedly chose dollars outside official channels to escape the debased peso; in contrast, Panama and Ecuador officially adopted the dollar as legal tender. In Zimbabwe, both paths unfolded in sequence. During the height of hyperinflation in 2008, as citizens pushed the Zimbabwean dollar out of daily commerce in favor of foreign currencies, the government formally recognized this reality by establishing a multi-currency system in February 2009[13].

To be sure, dollarization does not grant complete independence from political authority. Because U.S. monetary policy is set by the Federal Reserve, adopting the dollar shifts a country's exposure from its own government's monetary policy to that of the United States. In effect, individuals step out of the reach of a nearby tyrant only to enter the shadow of a distant empire. Nevertheless, when facing a collapsing domestic currency, this trade-off functions as a viable form of resistance. By choosing a distant power that cannot easily intervene in their daily lives over a proximate power actively eroding their purchasing power, individuals mitigate immediate monetary risk and secure a degree of economic autonomy. Dollarization thus demonstrates that selecting resistance money is not a matter of securing absolute sovereignty, but rather of calibrating one's distance from power based on specific threats and contexts. This logic also implies that when the threat originates from the US government or the US-centric financial system itself, tools other than the dollar become necessary to secure distance from authority.

Instruments used to counter value control are not modern inventions of the digital age. When domestic fiat currencies lose purchasing power, people have long turned to gold as an alternative store of value and medium of exchange. Venezuela provides a vivid case study of how this age-old defense mechanism re-emerged in the twenty-first century. Suffering from chronic hyperinflation for years, Venezuela's consumer price index soared by approximately 130,000% year-over-year in December 2018[14]. Amid this total collapse of currency value, residents in Tumeremo, a mining town in the

southern state of Bolivar, began using gold flakes for daily transactions. Half a gram of gold covered a one-night hotel stay, a quarter-gram paid for a two-person lunch, and local shops and restaurants displayed prices directly in grams of gold.

According to on-the-ground reporting by Bloomberg, residents carried gold flakes in their pockets and wrapped them in worthless bolívar banknotes to execute trades[15]. When state-issued currency turned to scrap paper, individuals defaulted back to gold—humanity's universal store of value for thousands of years. This serves as a reminder that resistance money is rooted not merely in technological innovation, but in an instinctive human response to monetary decay.

FIGURE 03

Gold pieces wrapped in bolívar banknotes are weighed on a scale in Tumeremo, Venezuela.
Source: Bloomberg.

While Venezuela defaulted back to physical gold, Argentina adopted stablecoins as its primary resistance money. In 2023, Argentina's annual inflation rate reached 211.4%[16], and the peso lost over 99% of its value against the US dollar over a single decade, plummeting from 8.5 pesos per dollar at the end of 2014 to 1,031 pesos per dollar by late 2024. Although the government capped individual foreign currency purchases at $200 per month starting in 2019, citizens systematically bypassed these capital controls by purchasing USDT and USDC on their smartphones, a restriction that was lifted only in April 2025[17].

The 2025 report from Chainalysis categorizes Latin America as a region where chronic inflation, currency volatility, and strict capital controls combine to drive a structural demand for stablecoins[16]. The same report noted that Argentina's annual cryptocurrency transaction volume reached $93.9 billion, ranking second in Latin America behind Brazil[18]. Rather than a state-directed initiative, this trend represents a bottom-up process of digital dollarization driven by individuals choosing stablecoins to counter inflation and capital controls.

16) Chainalysis: A US-based blockchain data analytics firm that tracks and analyzes on-chain transactions, providing forensic intelligence to governments, law enforcement agencies, and cryptocurrency exchanges globally.

Value control does not always manifest as gradual inflation. India's 2016 demonetization episode demonstrated how a government can nullify currency value overnight. When the Modi administration abruptly invalidated ₹500 and ₹1,000 banknotes, approximately 86.9% of India's circulating currency in value (roughly ₹15.4 trillion) became void overnight[19]. Although officially intended to curb the shadow economy, the move dealt its harshest blow to hundreds of millions of unbanked people who relied on the informal economy. These individuals held physical cash, but they lacked accessible channels to convert those notes into new currency or alternative assets quickly. This case illustrates that while physical cash possesses strong resistance to surveillance and transaction controls, it remains highly vulnerable to value controls executed directly by the issuing authority. It further reveals that the efficacy of resistance depends not only on the intrinsic properties of an asset, but also on an individual's access to financial infrastructure and viable alternatives.

Resistance to Surveillance Control

"Surveillance Capitalism,"[17] conceptualized by Shoshana Zuboff (2019), demonstrates that the compression of institutional distance is not driven exclusively by government action[20]. Big Tech platforms such as Google, Meta, and Amazon harvest users' behavioral data, transform it into prediction products, and monetize those products by selling advertisers access to targeted audiences.

17) "Surveillance Capitalism": An accumulation regime in which firms extract behavioral data from users as raw material to construct behavioral prediction products traded in futures markets. It differs from industrial capitalism in that revenues derive from automated data capture of everyday human experience rather than labor power alone.

Where traditional capitalism extracted surplus value from labor, surveillance capitalism extracts behavioral data. Individuals continually compress their institutional distance without fully recognizing the real costs behind the free access and convenience offered by these platforms. Unlike forced submission under political tyranny, this represents a form of unconscious dependence captured through convenience, making it far harder for individuals to recognize.

Google predicts user intent through search histories and location telemetry; Meta maps interpersonal networks through social graphs; and Amazon anticipates consumer desire by analyzing purchasing patterns. The deployment of this data extends beyond basic ad targeting into what Zuboff terms "behavioral modification," shifting from passive observation to actively steering user behavior via nudging, reward mechanics, and notifications.

Within the financial domain, surveillance operates even more directly. Credit card companies record every transaction entry, while fintech applications analyze user spending patterns, income levels, and financial habits in real time. The financial data surrendered by individuals in exchange for convenience is ingested to construct credit scores, set insurance premiums, and underwrite loans. Although individuals generate data through their own activity, corporations hold exclusive ownership and interpretive rights over it. This dynamics forms the core of what Zuboff calls "behavioral surplus," the portion of user-generated data exceeding what is strictly necessary for service improvement, diverted directly into corporate profits.

TABLE 02 **Structural Similarities: Authoritarian Regimes vs. Platform Economy**

Dimension	Individuals Under Authoritarian Regimes	Consumers in the Platform Economy
Power Holder	Totalitarian Autocrats	Platform Corporations (Big Tech)
Means of Control	Account Freezes and Censorship	Algorithms and Digital Control
Distance Dynamics	Forced Compression	Unconscious Compression (Via Convenience)
Resistance Tools	BTC, Stablecoins (Censorship/Freeze Resistance)	Privacy Technologies, DeFi (Data Sovereignty)
Outcome	Institutional Compression (Forced)	Institutional Compression (Voluntary/Unconscious)

Resistance money is needed both by individuals living under authoritarian regimes and by consumers in a system of surveillance capitalism; only its form and priorities differ. Unlike transaction control or value control, however, surveillance control is not usually perceived as an immediate threat in everyday life. Account freezes and currency collapses are visible and immediate, but transaction data is collected quietly, and the costs of that collection may not become apparent until much later. Yet once such data is used as a basis for sanctions, surveillance control can become just as restrictive as the other two forms of control. In response to this threat, resistance money may take the form of technologies that restore transactional anonymity and unlinkability.[18)]

Physical cash remains the oldest circumventive tool. Because physical notes leave no digital record, cash functions as an increasingly potent privacy shield in digitized societies. Privacy coins represent the effort to recreate this physical attribute within digital environments. Monero uses ring signatures and stealth addresses to obscure senders, receivers, and transaction amounts by default. Zcash utilizes zero-knowledge proofs to enable shielded transactions that verify transaction validity without exposing underlying details. Unlike Bitcoin, these protocols embed privacy directly into their foundational architecture rather than leaving it as an opt-in overlay.

18) Unlinkability: The property preventing external observers from linking multiple transactions together to infer that they originate from or belong to the same entity.

Efforts to enhance privacy within the Bitcoin ecosystem have also progressed steadily. CoinJoin aggregates transactions from multiple users into a single batch to break the link between specific inputs and outputs. While originally designed as a scaling mechanism, the Lightning Network executes small-value transfers within off-chain payment channels, keeping individual transactions off the public ledger. Nevertheless, its privacy protections remain conditional, as routing nodes can still observe transaction paths.

That these tools pose a genuine challenge to central authority is evidenced by the state's own regulatory reactions. In 2022, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned Tornado Cash, an Ethereum-based mixing protocol; in 2024, developers of the Bitcoin privacy wallet Samourai Wallet were indicted on charges of conspiracy to commit money laundering and operating an unlicensed money transmitting business[21]. That same year, Wasabi Wallet, another prominent CoinJoin service, ceased operating its central coordinator[22]. That political authorities targeted the anonymity mechanism rather than the base currency paradoxically confirms that surveillance control is a vital pillar of state power, and that privacy technologies represent effective instruments of resistance against it. In November 2024, the US Court of Appeals for the Fifth Circuit ruled that Tornado Cash's immutable smart contracts do not constitute "property" under applicable sanctions statutes, concluding that OFAC exceeded its statutory authority, and the Treasury Department subsequently removed the protocol from its sanctions list in March 2025[23]. However, criminal prosecution of individual developers continued after the protocol-level sanctions were lifted. In July 2025, Samourai Wallet's two co-founders pleaded guilty to conspiracy to operate an unlicensed money transmitting business, receiving prison sentences of five and four years respectively in November 2025. For Tornado Cash co-developer Roman Storm, a jury found him guilty only on the unlicensed money transmitter count in August 2025 while failing to reach a verdict on money laundering and sanctions evasion conspiracy charges, prompting prosecutors to request a retrial on the remaining counts in March 2026. The institutional tension between state authority and privacy technologies remains actively ongoing.[24]

To be sure, state and corporate surveillance is frequently justified as necessary to combat money laundering, cut off terrorist financing, prevent financial fraud, and enforce tax compliance. Granting unrestricted privacy can turn anonymity into a sanctuary for criminal activity, providing the rationale state authorities use to target privacy technologies. Surveillance control is therefore not a simple moral binary, but a perpetual tug-of-war between surrendering distance for regulatory protection and preserving distance for individual autonomy. Complete transparency leads to political subordination, whereas absolute opacity risks losing the collective security guarantees of a community. What resistance money seeks to restore is not the complete elimination of oversight, but the individual's agency to calibrate that distance on their own terms.

Nevertheless, an individual's capacity to adjust distance on the surveillance axis is narrower than on the other two axes. Transaction controls under au-

thoritarian regimes arrive through visible force, such as account freezes or blocked transfers, making both the adversary and the moment of resistance explicit. Corporate power, by contrast, presents itself under the guise of platform benefits: free web search, instant payments, and personalized recommendations. Individuals voluntarily yield their data by clicking "agree" on terms of service agreements, and the true cost is never felt at a single, disruptive moment like a frozen bank account. In a structure based on voluntary surrender rather than overt seizure, identifying what to resist becomes uniquely difficult.

This explains why Table 2 identifies Decentralized Finance (DeFi) alongside privacy tools as resistance mechanisms available to platform consumers. By executing deposits, loans, and trades via public code without central intermediaries like commercial banks or card networks, DeFi provides a pathway to access financial services without surrendering personal identity or transaction histories to corporate entities. Yet this buffer remains constrained. Entering or exiting fiat currency still requires passing through regulated intermediaries enforcing identity verification; more importantly, for consumers who see no immediate reason to sacrifice convenience, DeFi struggles to emerge as a practical alternative.

Consequently, individual monetary choices alone are insufficient to preserve institutional distance along the surveillance control axis. The primary force effectively checking corporate power has been another institutional authority: state regulation. Regulatory frameworks such as the European Union's General Data Protection Regulation (GDPR) illustrate how statutory limits on data collection and usage can serve as a counterweight. Where individuals previously fled a nearby tyrant by seeking shelter under a distant empire, they now turn to state regulation to restrain corporate power embedded deep within daily life through convenience. Institutional distance is secured not merely by moving further away from power, but also through institutional frameworks where competing powers hold each other in check. This dynamic highlights yet another reason why resistance money cannot be reduced to a single, universal solution.

Across the three control axes—transaction, value, and surveillance—the central battlegrounds have centered on power resistance, value stability, and privacy, respectively. Yet even when confronting threats along the same axis, individuals have chosen differently among Bitcoin, gold, dollars, stablecoins, and privacy technologies. What functions as resistance money is determined not only by the nature of the threat itself, but also by the structural conditions surrounding the individual facing that threat. What, then, are the decisive conditions that shape this selection? The following section examines these parameters through time preferences, distance optimization, societal infrastructure, community networks, and the tiered structures of power.

05
Dynamic Equilibrium Framework

Time Preferences and Distance Optimization

Time preference refers to the relative weight an individual assigns to present satisfaction versus future satisfaction. An individual who prioritizes accumulating assets through saving or investment over immediate consumption exhibits a low time preference; conversely, one who prioritizes present survival or immediate consumption over the future exhibits a high time preference. The Bitcoin community actively elevates a low time preference to a central virtue, as reflected in its iconic slogan, “HODL,” popularly interpreted as “Hold On for Dear Life,” which encourages investors to hold Bitcoin for the long term rather than sell it or spend it on immediate consumption. Yet this framework assumes an environment where saving and investment remain structurally viable. In most of the real-world case studies examined above, that baseline assumption had already collapsed.

Consider an individual in 2023 Argentina, where annual inflation reached 211%, watching their monthly peso salary lose purchasing power before the next month arrived, or residents of Tumeremo in Venezuela, where 2018 inflation topped 130,000%, rendering the bolívar effectively worthless. For financially excluded populations living under sovereign monetary decay, the paramount requirement is not an asset that might appreciate multifold over a decade, but a stable medium that guarantees tomorrow's purchasing power will match today's.

Time preference, therefore, is not merely an innate personal trait; it can also be a condition forcibly imposed by circumstance. Under forced time preference, where domestic fiat currency makes long-term saving or investment impossible, adopting stablecoins or physical gold to stabilize value represents a rational survival strategy. Leveraging resistance money to lower one's effective time preference is thus one manifestation of securing institutional distance. This survival strategy is not limited to value stability alone; power resistance, privacy, accessibility, and acceptance communities all operate interdependently to support it.

Just as individuals attempt to manage forced time preferences, they instinctively seek to optimize their distance from political authority. Positioning

oneself too close to power results in a loss of freedom; positioning oneself too far away results in a loss of protection. Within this paradoxical tension, individuals constantly search for an optimal balance.

This optimal point is not a fixed constant, but a dynamic variable. Even for the same individual, the optimal distance shifts as circumstances change. During stable periods, individuals willingly compress this distance for convenience, surrendering personal data to governments, banks, credit card networks, and platforms. However, when a crisis erupts, whether through hyperinflation, account freezes, capital controls, or political repression, they immediately seek to expand that distance. Resistance money serves as the precise instrument for this distance calibration.

From an institutional perspective, the state functions as a "stationary bandit"[19)] that extracts revenue through taxation in exchange for providing order and security (Olson, 1993)[25]. Individuals accept this arrangement so long as the benefits of protection outweigh the costs of extraction. When extraction exceeds protection, manifesting as hyperinflation, deposit freezes, or draconian capital controls, the primary recourse remaining for the individual is "exit"[26]. When people become dissatisfied with a system, they can either stay and seek change or leave. Cryptocurrency allows individuals to exit a country's monetary system without crossing national borders or relying on a bank's permission. Unlike traditional exits via gold or foreign fiat, which entailed heavy transport, custody, and regulatory friction, the threshold for executing a monetary exit has been lowered dramatically.

19) "Stationary Bandit": A concept formulated by Mancur Olson comparing the state to a bandit settled in a fixed territory. Unlike a "roving bandit" who plunders and moves on, a stationary bandit who exercises long-term control over a domain institutionalizes plunder as taxation and provides public goods—such as law enforcement and property rights protection—to maximize revenue extraction.

Why, then, does this exit option remain largely unexercised during stable periods? Prospect theory, developed by behavioral economists Daniel Kahneman and Amos Tversky, offers a clear explanation[27]. Human decision-making weights losses far more heavily than gains of equal magnitude. In peacetime, the gains from convenience are immediately tangible, whereas the loss of privacy is discounted as an abstract and distant concern. The moment bank accounts are frozen or assets are threatened, however, that loss transforms into an immediate and concrete reality. Driven by loss aversion, the individual's optimal distance expands abruptly. The explosive surge in demand for resistance money during crises is not an irrational panic, but a predictable outcome of human cognitive architecture.

Managing forced time preferences and optimizing distance from authority represent two expressions of the same underlying drive. In ordinary times, this drive leads individuals to compress distance for convenience; in times of crisis, it leads them to expand distance to avoid loss. Yet for these instinctive choices to function effectively as resistance money, specific societal conditions, namely infrastructure and community networks, must be in place.

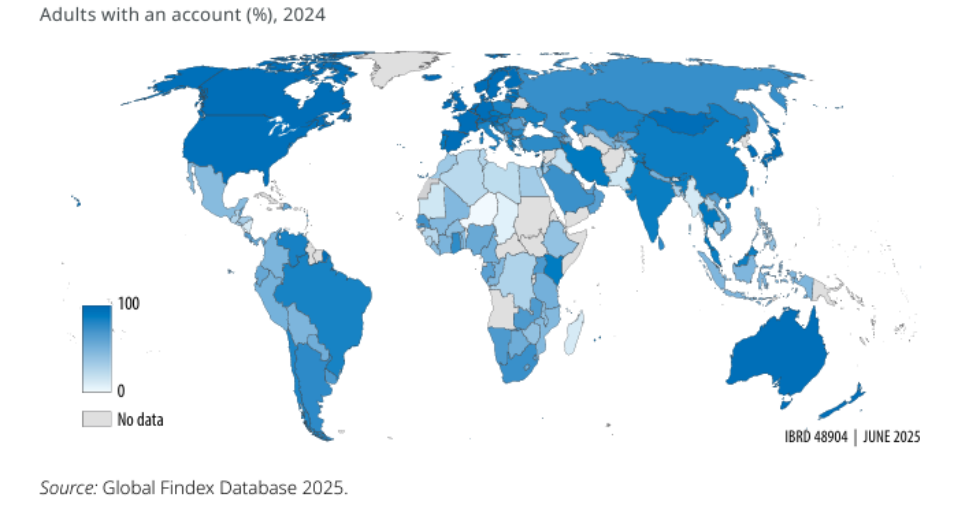
Infrastructure and Acceptance Communities

For an individual's monetary choice to result in actual transactions and value storage, specific supporting societal conditions must be met. Among the five

analytical dimensions, accessibility and acceptance communities represent these precise conditions.

Accessibility concerns the physical and technological foundations that enable the actual use of resistance money. The approximately 21% of the world's adult population currently excluded from formal finance fall into two main categories of exclusion. The first consists of practical barriers to accessing financial services. In rural Sub-Saharan Africa, bank branches are located far from residential areas, and requirements such as official government IDs, proof of address, and minimum deposit balances pose steep hurdles for impoverished populations. The second category involves institutional exclusion driven by sovereign authority, such as autocratic regimes freezing the accounts of political opponents, or legal frameworks and societal norms restricting women from engaging in independent financial activities.

FIGURE 04



Global Adult Account Ownership Rates (2024). Account ownership rates are lower in lower-income regions.
Source: World Bank, Global Findex Database

Kenya’s M-Pesa represents a landmark case of overcoming this exclusion. Launched in 2007 by telecommunications operator Safaricom, this mobile money system requires neither a traditional bank account, nor a smartphone, nor internet access. Users transfer funds via simple SMS text messages on basic feature phones, depositing and withdrawing cash at localized agent counters operating out of neighborhood shops and kiosks. Even in rural areas lacking bank branches, financial transfers and everyday payments became accessible through a single basic mobile phone and a nearby agent. This expansion of financial accessibility translated directly into poverty reduction: M-Pesa is estimated to have lifted approximately 194,000 Kenyan households, roughly 2% of the country's households, out of extreme poverty, an effect particularly pronounced in female-headed households[28].

FIGURE 05

Kenya's M-Pesa Service Interface (Left) and Mobile Money Transaction (Right).
Source: Wikimedia Commons.

However, mobile money possesses virtually no resistance to sovereign power. The telecom operator retains complete records of all transactions, can freeze accounts upon government request, and hosts the entire service on centralized servers. Nevertheless, the success of M-Pesa demonstrates that what users ultimately prioritize in daily survival is not ideologically pure decentralization, but immediate, functional accessibility.

In this context, accessibility serves as a decisive criterion determining which currency is selected as resistance money. Even if a currency offers the highest theoretical resistance to sovereign power, it cannot function as a tool of resistance if users cannot access or operate it. This explains why, when facing identical structural threats, societies with widespread smartphone adoption and fintech penetration turn to stablecoins, whereas regions with thinner digital infrastructure opt for gold or physical fiat currency.

An acceptance community refers to the network of economic actors who recognize a given money as valuable. Currency can circulate only when there are recipients willing to accept it. Physical gold fragments functioned as money in Tumeremo, Venezuela, precisely because local merchants and restaurants accepted them as payment; similarly, foreign fiat dollars emerged as resistance money in dollarized economies because individuals and merchants already trusted and accepted them. M-Pesa succeeded in Kenya because it rested upon a dense acceptance network connecting users, agents, and local merchants.

The consequences of confronting a crisis without an established acceptance community or supporting infrastructure were vividly demonstrated in South Korea. On the night of December 3, 2024, when martial law was declared, Bitcoin was not treated as a safe-haven asset on domestic exchanges. Instead, its price fell by more than 30%. On Upbit, South Korea's largest cryptocurrency exchange, Bitcoin's price dropped from approximately USD 92,000 (KRW 132.51 million) to USD 61,000 (KRW 88.26 million) in roughly 20 minutes. It then recovered to around USD 90,000 (KRW 130 million) by midnight, shortly before the National Assembly passed a resolution demanding the lifting of martial law[29].

The reason Bitcoin on Korean exchanges traded like a high-risk asset rather than functioning as resistance money during a political crisis can be traced to two main factors. First, there was no shared recognition within the local community viewing cryptocurrency as a safe haven during systemic crises. Second, the underlying infrastructure through which those trades occurred dictated user behavior. Bitcoin's resistance to political power derives primarily from self-custody, where individuals hold their own private keys. In South Korea, however, the vast majority of cryptocurrency transactions occur via accounts on centralized exchanges like Upbit and Bithumb. Bitcoin held on a centralized exchange remains subject to state control, susceptible to compliance orders, account freezes, or withdrawal suspensions, making it structurally identical to commercial bank deposits or domestic stocks. In an environment where the foundational practice of self-custody is virtually absent, Bitcoin is perceived not as resistance money, but as an asset class for trading and speculation.

Ultimately, even for the exact same asset, it functions as resistance money only within a society equipped with both a community that accepts it as a safe haven and the requisite infrastructure for individual self-custody. The true nature of resistance money is determined not by the intrinsic properties of the asset itself, but by the surrounding community and structural infrastructure.

Furthermore, even when infrastructure and acceptance networks are firmly in place, resistance money does not bypass all forms of authority equally. Sovereign power does not exist as a single monolithic layer; determining which specific tiers of control resistance money can actually evade is the subject of the next subsection.

Tiered Power Structures and Controllability

The power individuals face comes from multiple sources and operates at different levels. The state can control economic activity through account freezes, currency issuance, and transaction surveillance. Platform companies that control payments and user data can exercise similar control by blocking accounts and analyzing consumers' spending records. In this sense, the three forms of control—transaction, value, and surveillance—can recur at different levels of power. Resistance money does not offer the same protection at every level. One form of money may bypass state control over transactions while remaining vulnerable to platform surveillance; another may protect against surveillance but sacrifice price stability.

Stablecoins clearly illustrate this asymmetry. In economies suffering from monetary collapse, stablecoins provide a mechanism to bypass domestic monetary policy and access dollar-denominated value. However, they remain tethered to the administrative power of private issuers such as Tether and Circle, as well as the US-centric regulatory and sanctions regime. Issuers retain the technical authority to blacklist specific addresses, permanently blocking token transfers[30], while the token's underlying purchasing power

remains bound to US monetary policy. Thus, the exact same stablecoin can offer potent resistance against one tier of power while remaining inherently vulnerable to another.

Controllability is similarly a double-edged sword. A power's capacity to control individuals simultaneously represents its capacity to protect them. Just as protection stands opposite extraction in Olson's protection-extraction balance, expanding one's distance from power to evade control inevitably surrenders the institutional protections provided by that authority. A commercial bank's capacity to freeze a transaction also enables it to recover stolen funds; a payment network's capacity to censor a transaction also enables it to reverse fraudulent charges.

This duality is clearly illustrated by voice-phishing scams. As long as the stolen money remains in a bank account, institutional protections such as payment suspension and fund recovery can still be used. But once the money is converted into Bitcoin or stablecoins and transferred to a self-custody wallet, recovery becomes nearly impossible. Criminal organizations favor cryptocurrencies because of their irreversibility and censorship resistance, while individuals rely on these same properties to protect themselves from government intervention, such as account freezes. The same properties that protect donations to protesters can also make it impossible to recover money lost to fraud. In other words, irreversibility and censorship resistance can free individuals from institutional control while making it harder for institutions to provide relief when things go wrong.

Because of these trade-offs, most individuals choose to live in close proximity to power during normal times. While loss aversion (Kahneman & Tversky) drives individuals to expand their distance from power during systemic crises, the prospective loss of institutional protection acts as a counterweight in ordinary times, pulling them toward closer proximity. Consequently, selecting resistance money is not a matter of casting off authority to enter a state of total exposure, but rather a deliberate weighing of which tier of control to accept and which to evade.

Ultimately, no single currency can counter control across all tiers of power simultaneously. Choosing resistance money is therefore not a search for an absolute solution, but a continuous exercise in striking a dynamic balance.

There Is No Single Right Answer

The preceding case studies demonstrate that the exact same asset functions differently depending on the structural context in which it is situated. Bitcoin served as resistance money for protesters whose bank accounts were frozen; however, in countries where the domestic fiat currency continued to function normally, it failed to fulfill that role. Similarly, when facing value control, individuals chose either physical gold or stablecoins depending on the available technological infrastructure. Resistance money is not a single, universal tool; rather, the optimal choice depends on the specific forms of control an individual faces and the circumstances in which they operate.

Furthermore, nothing is absolute. The character of a currency can invert entirely as circumstances change. In the hands of Nigerian protesters resisting state censorship, Bitcoin functioned as resistance money; on the night of South Korea's martial law declaration, where no surrounding community recognized it as a financial refuge, Bitcoin reacted not as resistance money, but as a plummeting speculative asset. No asset is inherently resistance money, nor does an asset remain resistance money forever simply because it once fulfilled that role. The character of money is not etched into the asset itself; rather, it is continuously assigned anew by the threats, contexts, and communities that surround it. Thus, there is no fixed, definitive answer to what constitutes resistance money; the optimal choice exists only as a dynamic equilibrium constantly recalibrated as conditions shift.

From this perspective, one cannot declare any single form of resistance money superior to another. Bitcoin comes closest to the ideal of absolute sovereignty against state censorship and asset seizure, whereas stablecoins safeguard daily survival today in the face of a collapsing domestic currency. One provides long-term sovereignty; the other provides immediate survival. The two are not competitors vying for the exact same niche. Physical gold, foreign fiat currencies, physical cash, mobile money networks, and privacy technologies can each function as effective instruments of resistance within their respective contexts.

The preceding discussion can be synthesized into a single analytical decision framework. By integrating the five criteria (Section 02), the three control axes (Section 03), and the choice conditions outlined in this section, determining the optimal resistance money narrows down by sequentially asking five diagnostic questions:

1. Threat Diagnosis: Which control axis—transaction, value, or surveillance—presents the immediate threat?

2. Temporal Condition: Is the objective long-term sovereignty or immediate survival?

3. Usage Condition: Are the necessary infrastructure and access channels in place?

4. Community Condition: Is there a surrounding community that accepts the medium as valuable?

5. Control Risk: What institutional protections are surrendered in exchange for evading control?

The optimal tool emerges at the intersection of these five answers, and shifting even a single condition alters the outcome. Table 3 applies this decision framework to the case studies examined throughout this report.

TABLE 03 **Dynamic Equilibrium Framework: Decision Process and Case Applications**

Context	Threat Diagnosis	Temporal Condition	Usage Condition (Access & Infrastructure)	Community Condition	Control Risk	Selected Tool
Nigeria & Canada Protests (Account Freezes & Crowdfunding Blocks)	Transaction Control (Censorship)	Immediate Transfer	Self-custody & P2P available	Borderless Bitcoin network	Avoids state freezes but accepts volatility and irreversibility	Bitcoin
South Korea Martial Law (Dec. 2024)	Transaction Control (Potential Transaction & Value Threat)	Crisis Moment	Centralized exchange–centric (weak self-custody)	No community that views Bitcoin as a safe haven	Exchanges can freeze assets, so resistance fails	No Resistance Money (Bitcoin treated as a speculative asset)
Argentina (2023 High Inflation)	Value Control	Immediate Survival (High Time Preference)	Widespread smartphone & fintech adoption	Merchants & individuals accept USD	Vulnerable to issuer control and U.S. monetary policy	U.S. Dollar Stablecoins
Tumeremo, Venezuela (Hyperinflation)	Value Control	Immediate Survival	Lack of reliable electricity & telecommunications infrastructure	Local shops accept gold	Storage and transportation risks; limited portability	Physical Gold
Surveillance Capitalism & Platform Economy	Surveillance Control	Ongoing (Potential)	Technical barriers to understanding & adoption	Narrow user base	Gains anonymity but sacrifices convenience and access to lawful payment channels	Privacy Technologies & Cash

06
Conclusion

The tug-of-war between the individual and power over institutional distance is growing only more acute as digital technology deepens. As physical cash disappears and payment rails migrate fully onto electronic networks, realtime records capture who buys what and when. Surveillance capitalism harvests even consumption and attention into data, arming power with tools to compress institutional distance more precisely than ever.

Yet counter-forces seeking to widen that distance are growing too. Zero-knowledge proofs and privacy coins build anonymity against surveillance and control; self-custody widens individuals' room to hold their own keys and transact directly; and stablecoins, as they move into the mainstream financial system, let more people hold an alternative to collapsing domestic currencies.

Ultimately, what decides the future is not which currency wins. It is whether power narrows that distance faster than individuals can widen it back, and how much room individuals can preserve to calibrate that distance on their own terms. The future of resistance money depends not on the price of any one asset, but on this balance of power.

Resistance money cannot be nailed down to a single name. So long as power tightens its grip on individual life, and so long as individuals exist who want out from under that pressure, whatever fills that space, whether gold, dollars, Bitcoin, or something not yet even named, becomes resistance money. Resistance money is not a fixed asset; it is the name of a possibility, rewritten anew as circumstance demands.

Notes

1. Andrew M. Bailey, Bradley Rettler, and Craig Warmke, *Resistance Money: A Philosophical Case for Bitcoin* (New York: Routledge, 2024).

2. World Bank, *The Global Findex Database 2025: Connectivity and Financial Inclusion in the Digital Economy* (Washington, DC: World Bank, 2025), https://www.worldbank.org/en/publication/globalfindex, accessed April 25, 2026.

3. Neil Monnery, *Architect of Prosperity: Sir John Cowperthwaite and the Making of Hong Kong* (London: London Publishing Partnership, 2017).

4. Tatiana Kostova, "Transnational Transfer of Strategic Organizational Practices: A Contextual Perspective," *Academy of Management Review* 24, no. 2 (April 1999): 308–24.

5. People's Bank of China, *Progress of Research & Development of E-CNY in China* (Beijing: PBOC, July 2021), https://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021072014364791207.pdf, accessed April 25, 2026.

6. Central Bank of The Bahamas, "Project Sand Dollar," https://www.sanddollar.bs/, accessed April 25, 2026; European Central Bank, "Digital Euro," https://www.ecb.europa.eu/euro/digital_euro/html/index.en.html, accessed April 25, 2026; Bank of Korea, "Project Hangang Phase 1 Real-Transaction Pilot Final Report", October 2025, https://www.bok.or.kr/portal/bbs/B0000232/view.do?menuNo=200725&nttId=10094317, accessed July 24, 2026.

7. Yomi Kazeem, "How Bitcoin Powered the Largest Nigerian Protests in a Generation," *Quartz Africa*, October 26, 2020, https://qz.com/africa/1922466/how-bitcoin-powered-nigerias-endsars-protests, accessed April 25, 2026.

8. GoFundMe, "Statement on the Freedom Convoy 2022 Fundraiser," February 4, 2022; "Ontario Court Freezes Access to Funds Raised for Protest Convoy on GiveSendGo Platform," *CBC News*, February 10, 2022, https://www.cbc.ca/news/canada/toronto/freedom-convoy-2022-donations-frozen-give-send-go-1.6347345, accessed July 23, 2026. For the invocation date of the Emergencies Act, see Department of Justice Canada, "February 14, 2022 Declaration of Public Order Emergency," https://www.justice.gc.ca/eng/csj-sjc/section58.html, accessed July 23, 2026. For the scale of account freezes, see "Banks Have Started to Freeze Accounts Linked to the Protests, Freeland Says," *CBC News*, February 17, 2022, https://www.cbc.ca/news/politics/ottawa-protests-frozen-bank-accounts-1.6355396, accessed July 23, 2026. The Department of Finance reported to the House of Commons committee that up to 210 accounts, totaling approximately 7.8 million CAD, were frozen under the emergency financial measures.

9. David Fraser, "Digital Currency Donations for Freedom Convoy Evading Seizure by Authorities," *CBC News*, March 21, 2022, https://www.cbc.ca/news/canada/ottawa/freedom-convoy-cryptocurrency-asset-seizure-1.6389601, accessed April 25, 2026.

10. Emergency Economic Measures Order, SOR/2022-22, *Canada Gazette*, Part II, vol. 156, Extra no. 1 (February 15, 2022), ss. 2(1)(c), 3(k), https://gazette.gc.ca/rp-pr/p2/2022/2022-02-15-x1/html/sor-dors22-eng.html, accessed July 10, 2026; Alexandra Posadzki, James Bradshaw, and Temur Durrani, "RCMP Identify Dozens of Financial, Crypto Accounts Tied to Convoy Protests," *Globe and Mail*, February 16, 2022, https://www.theglobeandmail.com/business/article-rcmp-asks-cryptocurrency-exchanges-to-halt-trading-for-accounts/, accessed July 10, 2026.

11. *Li v. Barber*, 2022 ONSC 1176 (Ont. Sup. Ct. J., February 17, 2022); Annabel Oromoni, "Freedom Convoy Crypto Holdings to Remain Frozen and in Escrow Pending Lawsuit by Ottawa Residents," *Law Times*, March 2, 2022, https://www.lawtimesnews.com/news/general/freedom-convoy-crypto-holdings-to-remain-frozen-and-in-escrow-pending-lawsuit-by-ottawa-residents/364490, accessed July 10, 2026; Nunchuk (@nunchuk_io), Disclosure of official response sent to the Ontario Superior Court of Justice, X (formerly Twitter), February 18, 2022, https://x.com/nunchuk_io/status/1494885897577271299. The Mareva injunction explicitly targeting cryptocurrencies in this case is noted as likely being the first reported precedent of its kind in Canada. See Mark Jewett, Simon Grant, and Joseph Blinick, "Mareva Injunction over Cryptocurrencies in the Freedom Convoy Class Action," *Bennett Jones*, March 1, 2022.

12. Andrea O'Sullivan, "Hong Kong Protests Show Dangers of a Cashless Society," *Reason*, July 2, 2019, https://reason.com/2019/07/02/hong-kong-protests-show-dangers-of-a-cashless-society/, accessed July 17, 2026; Leigh Cuen, "Global Protests Reveal Bitcoin's Limitations," *CoinDesk*, November 21, 2019, https://www.coindesk.com/tech/2019/11/21/global-protests-reveal-bitcoins-limitations, accessed July 17, 2026.

13. For the concept of dollarization and official adoption cases, see Åke Lönnberg and Luis I. Jácome, "Implementing Official Dollarization," *IMF Working Paper* WP/10/106 (Washington, DC: International Monetary Fund, April 2010), https://doi.org/10.5089/9781455200658.001.A001, accessed July 17, 2026. For Zimbabwe's unofficial dollarization and the official institutionalization of a multi-currency system in February 2009, see Vitaliy Kramarenko et al., "Zimbabwe: Challenges and Policy Options after Hyperinflation," *IMF Departmental Paper* (Washington, DC: International Monetary Fund, June 2010), https://doi.org/10.5089/9781462309184.087.A001, accessed July 17, 2026.

14. Economic Commission for Latin America and the Caribbean (ECLAC), "Bolivarian Republic of Venezuela," in *Economic Survey of Latin America and the Caribbean 2019: The New Global Financial Context: Effects and Transmission Mechanisms in the Region* (Santiago: United Nations, 2019), 9, table 2, https://repositorio.cepal.org/server/api/core/bitstreams/e0b0150e-8f00-4ca8-b276-298f49f207a7/content, accessed July 23, 2026.

15. Alex Vasquez and Ezra Fieser, "Venezuelans Break Off Flakes of Gold to Pay for Meals, Haircuts," *Bloomberg*, October 20, 2021, https://www.bloomberg.com/news/articles/2021-10-20/venezuelans-break-off-flakes-of-gold-to-pay-for-meals-haircuts, accessed April 25, 2026.

16. Instituto Nacional de Estadística y Censos (INDEC), *Indice de precios al consumidor (IPC), Diciembre 2023* (Buenos Aires: INDEC, January 2024), https://web.archive.org/web/20241112210626/https://www.indec.gob.ar/uploads/informesdeprensa/ipc_01_24DBD5D8158C.pdf, accessed April 25, 2026. Cumulative 12-month consumer price inflation reached 211.4% in December 2023.

17. The USD/ARS exchange rate according to official Central Bank of the Argentine Republic (BCRA) disclosures was approximately 8.5 pesos per dollar at year-end 2014 and approximately 1,031 pesos per dollar at year-end 2024. Foreign exchange controls limiting individual dollar purchases to $200 per month (*cepo cambiario*) were introduced in September 2019 and lifted in April 2025.

18. Chainalysis Team, "Latin America Emerges as a Crypto Powerhouse Amid Volatile Growth," *Chainalysis*, October 2, 2025, https://www.chainalysis.com/blog/latin-america-crypto-adoption-2025/, accessed May 30, 2026.

19. Reserve Bank of India, *Macroeconomic Impact of Demonetisation: A Preliminary Assessment* (Mumbai: RBI, March 2017), 1, https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/MID10031760E85BDAFEFD497193995BB1B6DBE602.PDF, accessed April 25, 2026.

20. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019).

21. U.S. Department of the Treasury, “U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash,” press release JY0916, August 8, 2022, https://home.treasury.gov/news/press-releases/jy0916, accessed July 27, 2026; U.S. Attorney’s Office, Southern District of New York, “Founders and CEO of Cryptocurrency Mixing Service Arrested and Charged with Money Laundering and Unlicensed Money Transmitting Offenses,” press release, April 24, 2024, https://www.justice.gov/usao-sdny/pr/founders-and-ceo-cryptocurrency-mixing-service-arrested-and-charged-money-laundering, accessed July 27, 2026.

22. zkSNACKs, “zkSNACKs Is Discontinuing Its Coinjoin Coordination Service 1st of June,” May 2, 2024, https://web.archive.org/web/20241007122748/https://blog.wasabiwallet.io/zksnacks-is-discontinuing-its-coinjoin-coordination-service-1st-of-june/, accessed July 27, 2026. The coordinator ceased operations effective June 1, 2024.

23. Van Loon v. Department of the Treasury (5th Cir., November 26, 2024); U.S. Department of the Treasury, “Tornado Cash Delisting,” press release SB0057, March 21, 2025, https://home.treasury.gov/news/press-releases/sb0057, accessed July 27, 2026.

24. United States v. Rodriguez and Hill, No. 1:24-cr-00082 (S.D.N.Y.). The two defendants pleaded guilty on July 30, 2025, and were sentenced that November to 60 months and 48 months of imprisonment, respectively. United States v. Roman Storm, No. 1:23-cr-00430 (S.D.N.Y.). On August 6, 2025, the jury convicted Storm only on the charge of conspiring to operate an unlicensed money transmitting business, deadlocking on the money laundering and sanctions evasion conspiracy charges; prosecutors moved for a retrial on the unresolved counts in March 2026.

25. Mancur Olson, “Dictatorship, Democracy, and Development,” *American Political Science Review* 87, no. 3 (September 1993): 567–76.

26. Albert O. Hirschman, *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States* (Cambridge, MA: Harvard University Press, 1970).

27. Daniel Kahneman and Amos Tversky, “Prospect Theory: An Analysis of Decision under Risk,” *Econometrica* 47, no. 2 (March 1979): 263–91.

28. Tavneet Suri and William Jack, “The Long-Run Poverty and Gender Impacts of Mobile Money,” *Science* 354, no. 6317 (December 9, 2016): 1288–92, https://doi.org/10.1126/science.aah5309.

29. "'Virtual Asset Panic'... Domestic Exchanges Halt Operations Amid Emergency Martial Law Declaration", *ZDNet Korea*, December 3, 2024, https://zdnet.co.kr/view/?no=20241203231615, accessed July 23, 2026; "Bitcoin, XRP, and Dogecoin Plummet Simultaneously on Upbit Following Yoon's Declaration of Emergency Martial Law", *Digital Asset*, December 4, 2024, https://www.digitalasset.works/news/articleView.html?idxno=23759, accessed July 23, 2026. Market prices based on Upbit exchange data.

30. Tether has routinely frozen specific wallet addresses pursuant to requests from law enforcement agencies and OFAC sanctions designations, with cumulative frozen assets exceeding $4.4 billion according to Tether disclosures. Circle has similarly blocked USDC addresses based on court orders or sanctions designations. Tether, "Tether Supports Freeze of More Than $344 Million in USD in Coordination with OFAC and U.S. Law Enforcement," https://tether.io/news/, accessed July 23, 2026.

How Resistance Money Is Chosen

Researcher

Changjun Lee johan000623@gmail.com

Corresponding Author

Taemin Oh

Editor

Hyemin Son

Translator

Samuel J. Hahn