BITCOIN, DYNAMIC EFFICIENCY, AND THE ECONOMIC LIMITS OF "NAKAMOTO TRUST": AN AUSTRIAN REAPPRAISAL OF BUDISH'S ARGUMENT

JOEL SERRANO*

Date received: 11 December 2025
Date of acceptance: 5 March 2026

1. **Introduction**

The emergence of Bitcoin in 2009 sparked intense debate about the economic nature of decentralized monetary systems, their long-run viability, and their institutional implications. In recent years, one of the most influential critiques in academic economics has been advanced by Eric Budish, first in "The Economic Limits of Bitcoin and the Blockchain" (NBER Working Paper 24717, 2018) and later in its expanded and revised version, "Trust at Scale: The Economic Limits of Cryptocurrencies and Blockchains," published in *The Quarterly Journal of Economics* (Budish, 2025).

Budish's central thesis can be summarized in three ideas: (i) in competitive equilibrium, miners in a permissionless blockchain earn zero economic profit; (ii) for the system to be secure against a majority attack, the cost of such an attack must exceed its expected benefit; and (iii) taken together, these conditions imply an equilibrium restriction—namely, a necessary condition for the equilibrium described by the model to exist and remain sustainable—according

* The author holds a PhD in Social and Legal Sciences (Economics) from the International Doctoral School of Rey Juan Carlos University (URJC). He holds a Bachelor's degree in Philosophy and a Master's degree in Theoretical and Practical Philosophy from the National University of Distance Education (UNED), and a Master's degree in Austrian School Economics from Rey Juan Carlos University (URJC).
E-mail: jcol18@gmail.com; https://orcid.org/0009-0003-4855-5152.

Procesos de Mercado: Revista Europea de Economía Política
Vol. XXIII, nº1, Summer 2026, pp. 335-364
https://doi.org/10.52195/pm.v24i1.2011

to which the "flow cost" of maintaining blockchain security must be persistently large relative to the gains from attacking it. On this basis, Budish concludes that "Nakamoto Trust" is structurally expensive and that there are intrinsic limits to how economically significant Bitcoin can become as a monetary or settlement system (Budish, 2018, 2025).

In parallel, within the Bitcoin community and from perspectives more closely aligned with the Austrian School, a set of responses has emerged that challenges both the assumptions and the scope of those conclusions, stressing the dynamic, institutional, and entrepreneurial character of Bitcoin security. Notable contributions include the security model of Hasu, Prestwich, and Curtis (2019), which emphasizes the role of mining's sunk capital, and Garratt and van Oordt's analysis of the relevance of fixed costs and specific hardware (ASICs) in protecting against double-spend attacks (Garratt & van Oordt, 2020). In addition, several authors and specialized commentators have offered more informal yet economically substantive critiques of Budish's approach (Oasis Team, 2018).

The aim of this article is to reassess Budish's argument from the standpoint of the theory of dynamic efficiency developed by Huerta de Soto (2009), while also taking into account three dimensions that are crucial from an Austrian perspective and close to Bitcoin:

— The cost of sound money (a gold standard or a Bitcoin standard) relative to the visible and invisible costs of unsound fiat money managed by central banks.
— The legal-economic nature of Bitcoin ownership as a form of radically secure, decentralized, and practically unseizable property (Graf, 2013).
— The essential difference between Bitcoin—understood as a commodity money with an immutable supply—and cryptocurrencies, which in practice function as securities that can be manipulated by their promoters.

These three dimensions are developed in Serrano (2025).

The central claim of this article is as follows: if one adopts a genuinely dynamic notion of efficiency—focused on entrepreneurial

creativity, institutional quality, and the solidity of property rights—the expensive character of trust in Bitcoin is not a decisive argument against its viability, but rather a reflection of the price that must be paid for a monetary and property regime far more robust than the one prevailing under fiat money. The problem is not that Bitcoin is too costly, but that a static framework overlooks the opportunity cost of maintaining an inflationary system supported by bank credit and state discretion.

Methodology

This paper adopts a literature review and a theoretical-institutional approach. Specifically, it reconstructs Budish's argument (2018, 2025) as a consistency restriction on the security budget, contrasts its assumptions with recent contributions on security, sunk costs, and specific hardware, and reinterprets the debate through the lens of dynamic efficiency theory, emphasizing the role of institutions and property rights. The purpose is not to refute Budish's formal model on its own terms, but to reassess its scope under an alternative theoretical framework.

The sources used are mainly documentary (academic articles, working papers, and specialized literature), complemented by a comparative conceptual analysis. The criteria for bibliographic selection reflected theoretical relevance to the debate on the economic limits of PoW and its environmental sustainability, prioritizing peer-reviewed articles, widely cited working papers, and contributions representing both critical and supportive positions.

2. **"Nakamoto Trust": definition and basic features**

In contemporary discussions about Bitcoin, and particularly in Budish's work, the expression "Nakamoto Trust" has become popular to denote the specific type of trust that emerges from the so-called Nakamoto consensus, introduced by Satoshi Nakamoto in his foundational 2008 paper. This is not "trust" in the traditional sense—placed in identifiable authorities, institutions, or

intermediaries—but rather a set of probabilistic guarantees based on cryptography, game theory, and economic incentives.

In traditional payment and settlement systems, trust is placed in centralized entities: commercial banks, central banks, clearing houses, wholesale payment systems, and so on. These entities maintain accounting ledgers, validate transactions, and prevent fraud (such as double spending) through internal procedures, audits, and, ultimately, the backing of the state's coercive power. The typical user does not personally verify the integrity of the system; rather, they rely on the institutional and regulatory solidity of those intermediaries.

Nakamoto's model reverses this logic. Nakamoto consensus is a consensus mechanism for peer-to-peer networks that allows thousands of untrusted nodes to coordinate on the construction of a shared record of transactions (the blockchain) without requiring a central authority. The core of this mechanism is proof of work (PoW): miners compete in a computational lottery, repeatedly performing a large number of calculations until they can propose a valid block of transactions and add it to the chain.[1]

---

[1] It is often imprecisely claimed that miners "solve complex mathematical problems." In reality, the Proof-of-Work process does not consist of solving sophisticated equations but of a brute-force procedure. Each miner searches for an arbitrary number (a nonce) which, when combined with the block's data (set of transactions, timestamp, hash of the previous block, etc.) and processed through the SHA-256 cryptographic function, produces a hash that is less than or equal to a threshold set by the network, determined by the "difficulty" parameter. This hash must fall below a certain target (which in practice corresponds to beginning with a specified number of leading zeros in its hexadecimal representation), making it extremely unlikely to be found within a small number of attempts. There is therefore no deterministic "solution" to a mathematical problem, but rather a purely probabilistic process in which miners repeatedly compute hashes (millions or billions per second) until, by chance, one satisfies the required criterion. A common analogy is to imagine a die with one million faces that is rolled until a number lower than ten appears: no complex problem is being solved; the experiment is simply repeated until luck prevails. The greater the computing power (hashrate), the more "rolls of the die" a miner can perform per second and, therefore, the higher the probability of finding the block before competitors. The network automatically adjusts the difficulty every 2,016 blocks (approximately two weeks) to maintain an average block time of around ten minutes. The purpose of this Proof-of-Work mechanism is to require miners to demonstrate that they have incurred a real expenditure of resources (energy and hardware) in order to propose valid

The fundamental rule of Nakamoto consensus is that the valid chain is the one that accumulates the greatest amount of computational work—in practice, the "longest" chain in PoW terms. As long as the majority of mining power is controlled by honest agents, adding new blocks to the honest chain is faster and more likely than reconstructing an alternative history. To rewrite the transaction history (for instance, to execute a large-scale double spend), an attacker would need to control a very large fraction— in principle, more than 50%—of the network's total computing power for long enough, which in principle makes the attack extremely costly and risky.

In this context, Nakamoto Trust refers precisely to this peculiar form of trust: rather than trusting the honesty of a central institution, participants trust that (i) economic incentives align most mining power with honest behavior, and (ii) the amount of work accumulated in the dominant chain makes retroactive manipulation of the ledger impracticable except at prohibitive cost. "Trust" is thus placed in the combination of consensus rules, cryptography, and incentives—not in the goodwill of a third party.

This design has well-known advantages: a high degree of decentralization, radical transparency of the ledger (anyone can independently verify the validity of the chain), and the elimination of mandatory intermediaries in basic settlement. However, it also has limitations: the energy consumption associated with proof of work, scalability constraints at the base layer, and the possibility of majority attacks if mining power were to become significantly concentrated in coordinated hands. Budish's argument derives much of its force from these costs and risks. From the standpoint of Huerta de Soto's theory of dynamic efficiency and Austrian monetary theory more broadly, however, it becomes necessary to interpret more carefully what "trust" in Nakamoto Trust truly means and what role it may play within a broader market order.

---

blocks. The miner whose block is accepted receives the reward (newly issued bitcoins plus transaction fees). It is this real cost associated with mining that makes attempts to rewrite the chain's history and carry out fraud, such as double spending, prohibitively expensive.

3. Theoretical framework: static efficiency, dynamic efficiency, and the market order

Huerta de Soto's critique of the static efficiency paradigm and the Pareto optimum is well known in Austrian School literature. In contrast to a view that identifies efficiency with the allocation of resources given a fixed set of preferences, technologies, and endowments, dynamic efficiency theory redefines economic efficiency as the capacity of the market process to discover, generate, and coordinate new dispersed knowledge (Huerta de Soto, 2009).

In this framework:

— The central object of analysis is not equilibrium but the market process.
— The key is not the allocation of resources at a given moment but the entrepreneurial capacity to discover opportunities and correct discoordination.
— Institutions—especially property rights, contract enforcement, and the stability of the rules of the game—become central parameters of efficiency.

Huerta de Soto insists that dynamic efficiency is closely linked to ethical considerations: without strict respect for private property and for the fulfillment of contractual promises, the entrepreneurial function is distorted and the coordination process loses its capacity to generate social order (Huerta de Soto, 2009). It is precisely from this perspective that the Austrian critique of fiat money and fractional-reserve banking gains full force: systematic manipulation of interest rates and the money supply generates boom-bust cycles, distorts economic calculation, and undermines trust in basic social institutions (Huerta de Soto, 1998).

This dynamic conception of efficiency, in turn, implies a different criterion for evaluating technologies such as Bitcoin:

— It is not enough to ask whether its consensus mechanism is expensive in terms of energy or miner compensation.
— One must compare that cost with the cost of alternative trust-production mechanisms (the state apparatus, the

banking system, centralized payment networks) and, above all, with their cumulative effects on intertemporal coordination and individual freedom.

From this perspective, the relevant question is not whether Nakamoto Trust is expensive, but which institutional order is more dynamically efficient when we compare not only what is seen but also what is not seen, to use Bastiat's (1850) well-known distinction.

4. **Budish's argument and its scope**

Budish builds his critique of Bitcoin around three central equations (Budish, 2018, 2025). In simplified terms, his argument can be summarized as follows:

— A zero-profit condition for miners: in competitive equilibrium, expected revenue per block equals the marginal cost of mining. If expected income per block (subsidy plus fees) were persistently above the cost of energy and hardware, new miners would enter until economic profit is driven to zero. If it were below, some miners would exit until the hashrate fell and marginal profitability again equaled cost.
— An incentive-compatibility condition ensuring security against majority attacks: the cost of mounting an attack (in terms of the resources needed to control most mining power for the relevant time) must exceed the expected value of the attack. In other words, for a double-spend or systematic sabotage attack not to be attractive, the cost of temporarily acquiring sufficient hashing power—or diverting existing power to malicious ends—must exceed the potential gains.
— A necessary condition for the model's equilibrium to exist and be sustainable: this condition combines the previous equations and concludes that recurrent payments to miners ("security flow") must be large relative to the benefits of an attack ("stock of value to be captured") if network security is to be maintained. Put differently, if the system is in competitive equilibrium and is secure, this relationship between "security flow"

> and "stock of value to be captured" must hold. When expected revenue per block equals marginal mining costs in equilibrium, and one simultaneously requires attack costs to exceed the value that can be captured, one arrives at a proportionality relation between the security budget and exposed value: the more value the network aims to protect, the greater must be the continuous resource flow dedicated to sustaining the hashrate.

From this basic structure, Budish formalizes the problem as a repeated game between a potential attacker and honest miners. The attacker compares the economic value extractable from the network (e.g., via a double spend of a given magnitude) with the cost of acquiring or renting enough mining capacity for the time needed to reorganize the chain. Miners, for their part, adjust their supply of computing power until expected revenue per block equals their costs. A secure equilibrium therefore requires that, for relevant parameter values (Bitcoin's price, the volume of exposed transactions, the marginal cost of hashing, the time required for the attack), attack costs exceed the value that can be captured.

Budish draws several implications from these relationships:

— A permissionless consensus system that seeks to protect a very large economic volume (e.g., Bitcoin as a global "digital gold") would be forced to sustain a very large security bill; otherwise, the incentive for a majority attack would grow until the equilibrium becomes likely to break down. That is, if the security budget (total payments to miners) does not rise roughly in proportion to the total value settled on the network, the inequality between attack cost and potential loot would reverse, and a sufficiently capitalized attacker might find it profitable to mount such an attack.
— The need to maintain those payments over time clashes with Bitcoin's finite issuance schedule, which reduces the block subsidy through successive halvings (until it disappears in 2140). Insofar as network security relies on the block reward, the transition to a scheme in which fees must by themselves sustain the hashrate poses a structural problem: if fee income does not rise sufficiently and stably, the security budget

would shrink, eroding the system's guarantees. From this perspective, Bitcoin's fixed supply—one of its main monetary virtues—would become, paradoxically, a source of long-run fragility. Whether transaction fees alone can sustain a sufficiently robust security budget over the long term remains an open empirical and theoretical question, whose resolution will depend on the evolution of demand for block space, second-layer adoption, and mining cost structures.

— Consequently, there would be intrinsic economic limits to the magnitude of the role that Bitcoin and similar technologies can play in the monetary and financial order (Budish, 2018, 2025). According to this logic, it would be unrealistic to expect a system based on proof of work and block rewards to protect, efficiently, a volume of wealth comparable to that of a global financial system without incurring disproportionate security costs. Hence the title of his work: the economic limits of Bitcoin and the blockchain.

Budish illustrates these ideas with quantitative comparisons between Bitcoin's security budget and the value of potentially exposed transactions. If the value settled on-chain grows faster than total payments to miners, the gap between "available loot" and the effective cost of attacking it widens. In principle, an actor with access to abundant capital—a hostile state, a large financial conglomerate—could coordinate a majority attack with a favorable cost-benefit ratio, especially if it does not fully internalize the reputational damage to the network or, for strategic reasons, values the harm inflicted more than the direct monetary benefit.

It is important to acknowledge that Budish's reasoning has explanatory power when applied to small blockchains with low security budgets, easily replicated tokens, and non-specialized consensus mechanisms. His analysis captures well why so many cryptocurrencies have suffered relatively cheap 51% attacks with devastating effects on trust and capitalization. Where the total value at stake is modest, the cost of coordinating an attack can remain below the potential loot, and the threat of a successful attack is real and frequent.

The essential question is whether that same logic can be applied without qualification to Bitcoin—with its specific combination of

proof of work, specialized hardware (ASICs), historical security track record, and ownership structure—and, further, whether it can be used to conclude that Nakamoto Trust is dynamically inefficient as the foundation of a long-run monetary order. The remainder of the article questions this extrapolation. It argues that Budish's model, understood as a static consistency restriction, omits key elements of dynamic efficiency: the sunk costs of mining capital, hardware specificity, path dependence, miners' reputational discipline, and, ultimately, the institutional value of a strong property regime and an immutable monetary supply.

5. **Budish's model as a security equation of exchange: a critique from dynamic efficiency**

Huerta de Soto's Austrian critique of the equation of exchange (MV = PT)—as developed by Mises, Hayek, and Rothbard, and systematized by Huerta de Soto (1998)—provides a fertile framework for evaluating the scope of Budish's mathematical model of the "economic limits" of Bitcoin. In both cases we face formal constructions that, while acceptable as definitional identities or simple aggregate restrictions (i.e., equalities that hold by virtue of how magnitudes are defined), are often used as if they contained a complete causal theory of complex phenomena: the purchasing power of money, in the case of the quantity equation; the security of a decentralized consensus system, in Budish's case.

From the standpoint of dynamic efficiency, the diagnosis is similar: both the equation of exchange and Budish's system of equations are static and mechanistic descriptions, incapable of capturing the microeconomic processes, the role of time, and the capital structure that characterize a real monetary economy.

5.1. *Formal tautologies and lack of causal content*

Huerta de Soto stresses that the equation of exchange (MV = PT) is ultimately a tautological identity: it asserts that total monetary expenditure (left-hand side) equals the monetary value of

transactions (right-hand side). The problem arises when one seeks to endow this identity with explanatory content regarding the price level or the value of money. Moreover, reducing heterogeneous transactions to an aggregate PT involves, as Rothbard argues, an "illogical leap": there is no solid basis for homogenizing goods and services of diverse nature into a scalar magnitude. The equation is thus reduced, in Huerta de Soto's words (1998), to a "mere ideogram" devoid of causal power.

Something similar occurs with Budish's central result. Combining miners' zero-profit condition with the attacker's incentive condition leads to an inequality of the form:

$$p\_block \geq V\_attack / (A\_star * t(A\_star)),$$

that is, the flow of payments to miners per block must be sufficiently large relative to the value of an attack and the time it requires. This relation is correct as a consistency restriction: no security system can be robust if the value that can be looted vastly exceeds the cost of violating it. It is a minimal condition of the system's logical coherence. If it does not hold, the system is not viable (it is inconsistent with the idea of "security"). But when taken as an "explanation" of Bitcoin's economic limits, it incurs a problem analogous to that of the equation of exchange: it merely expresses, in symbolic form, the idea that spending on security must exceed the potential gains from an attack, without providing a genuine theory of the process by which both terms are determined and adjust over time.

In both cases, the mathematical form has suggestive power that can lead one to mistake an identity of definitions for a causal explanation of how the economic process actually works.

5.2. *Parameters that are mishandled: from velocity V to V_attack, t(A), and the hashrate*

A central piece of Huerta de Soto's critique of the quantity equation is the concept of velocity of circulation V. From Irving Fisher to Milton Friedman, quantity theory tends to treat V as relatively stable or predictable, which allows one to infer that changes in M

translate, over time, into proportional changes in P. Against this, Huerta de Soto (1998) emphasizes that V is an artificial dependent variable, defined ex post to preserve the identity, with no autonomous economic content. One cannot rigorously speak of an "average velocity" applicable to individual agents who make specific transactions. Velocity is not a technical constant, but a residual that reflects the demand for cash balances and thus changing preferences and expectations.

In Budish's model we find a similar use of aggregate parameters:

— the value of an attack *V_attack*,
— the expected duration of an attack *t(A)*,
— the equilibrium hashrate *N_star*,
— and the unit mining cost *c*.

These parameters are treated as if they were technological or environmental data for comparative statics. Yet each of these magnitudes is in fact the result of microeconomic decisions, expectations, and capital structures:

— *V_attack* depends on patterns of Bitcoin use (treasury holdings, retail payments, derivatives), the confirmation policies of exchanges and merchants, the degree of development of layer-2 solutions that reduce the value exposed on the base chain, and expectations about the social and technical response to an attack.
— *t(A)* is conditioned not only by relative mining power, but also by the speed and effectiveness of potential countermeasures (defensive forks, software upgrades, coordinated changes in the rules followed by nodes).
— *N_star* and *c* embody investment decisions in specific ASICs, technological learning, long-term energy supply contracts, and regulatory constraints across jurisdictions.

Treating these parameters as exogenous and relatively stable is, from Huerta de Soto's perspective, akin to treating V as a constant: it freezes the outcome of human action and institutional evolution into "symbols" then taken as "technological" givens.

5.3. *Concealment of microeconomic effects and the capital structure*

Huerta de Soto further criticizes the equation of exchange for, by focusing on the "general price level" P, obscuring changes in relative prices and the redistribution of income that accompany processes of monetary and credit expansion. New money does not enter neutrally or simultaneously, but sequentially through specific channels (banking, public spending, large borrowers), generating the well-known Cantillon effects: some agents benefit from still-low prices while already holding more money, while others face higher prices without yet seeing their nominal income rise. This distorts the productive structure, artificially lengthens the stages of production farther removed from consumption, and ultimately leads to unavoidable recessions (Huerta de Soto, 1998, 2009).

Budish's model, centered on aggregates such as *V_attack* or total hashrate, suffers an analogous bias: it obscures microeconomic heterogeneity and the capital structure involved in Bitcoin security. It does not distinguish, for example:

— between internal potential attackers (large mining pools that have invested in specific infrastructure) and external attackers (hostile states, conglomerates with strategic interests), whose incentives and constraints differ sharply;
— between different types of Bitcoin holders (retail users, firms, financial institutions, long-term *hodlers*) who would experience the impact of an attack (or an attempted attack) differently;
— between different forms of specific capital—mining farms, long-term energy contracts, software and know-how—that could be sharply devalued if trust in the network were to erode.

Just as MV = PT collapses to an aggregate P that says nothing about the capital structure and the production process, Budish's scheme reduces Bitcoin security to a relation among a few aggregate magnitudes, without tracking how changes affect the balance sheets and expectations of the various agents involved.

5.4. *Illusory neutrality and the absence of a value theory: from money to security*

Quantity theory often rests on the idea that money is "neutral" in the long run: changes in M translate mainly into changes in P, leaving T unchanged. Huerta de Soto, following Mises and Hayek, denies this neutrality: monetary and credit expansion not only raises prices, but also alters the structure of production, generates malinvestments, and leads to cyclical crises. The equation of exchange, lacking a theory of capital and time, cannot account for these effects (Huerta de Soto, 1998).

In Budish's model we find a form of implicit neutrality assumption: for a given level of Bitcoin use, there would exist a "sufficient security budget" ensuring system resilience, independently of the concrete capital and contractual structure surrounding the network. In practice, it is suggested that if the flow of payments to miners (from subsidies and fees) satisfies the relevant inequality, the system will be secure, without much regard for how that cost is distributed, what forms of mining organization prevail, or what complementary institutions emerge (layer-2 solutions, custodians, insurers, arbitration mechanisms).

From an Austrian viewpoint, this neutrality is illusory for two reasons:

— Because the value of security itself is not neutral: having a medium of exchange with a strictly limited supply, censorship resistance, and practical unseizability profoundly alters patterns of saving, investment, and capital allocation. It is not enough to say that "X is spent on security"; one must understand what effects that security has on the market process.
— Because the way in which the security budget is built (via subsidies, fees, or hybrid models) has implications for the temporal structure of mining capital and for the distribution of risks between users and security providers.

In both cases, the underlying problem is the one Huerta de Soto identifies in the quantity equation: a lack of a theory of value and

capital capable of correctly interpreting the aggregates being manipulated.

5.5. *Passive macro-aggregates vs human action, entrepreneurship, and institutional evolution*

Finally, Huerta de Soto criticizes the thoroughly macro-aggregate and mechanistic character of the equation of exchange: individuals are subsumed into aggregates (M, V, P, T) that are manipulated algebraically, without making visible concrete decisions, intertemporal coordination (or discoordination) of plans, or processes of learning and error correction. Austrian business cycle theory, by contrast, starts from human action and reconstructs step by step how bank credit expansion alters the intertemporal structure of production and leads to recession (Huerta de Soto, 1998, 2009).

Budish's model commits, mutatis mutandis, a similar bias. The mining industry is represented as a set of identical agents who enter and exit until profits are exhausted; users and exchanges as passive recipients of a consensus rule; the attacker as an abstract player comparing a benefit and a cost in a single move. Left out are:

— mining entrepreneurship (new business models, vertical integration with energy production, hardware innovation, geographic relocation in response to regulation);
— institutional innovation (Lightning Network, custody solutions, private insurance against operational failures, contract clauses that allocate risks);
— the evolution of the protocol itself and associated social norms (defensive hard forks, adjustments in confirmation policies, coordination among relevant actors on how to respond under extreme scenarios).

From Huerta de Soto's dynamic efficiency theory, these elements—entrepreneurial action, learning, and institutional evolution—are precisely what define the long-run viability of a market order. Just as MV = PT cannot capture the logic of the business cycle or capitalist development, Budish's model, taken literally,

cannot capture the real dynamics of Bitcoin security, which is an emergent product of an ongoing discovery and coordination process.

In summary, the analogy is limited but instructive: Budish's system of equations plays, in the analysis of Nakamoto Trust, a role analogous to that of the equation of exchange in classical monetarism. In both cases, the tools are useful as restrictions but dangerous if elevated to the status of complete theories. Of course, security spending must be of a certain order of magnitude for the system to make sense. But if one overstates this idea (e.g., the inference that below a certain security threshold Bitcoin would necessarily become unviable), one moves from a minimal consistency condition to a purported total causal law. From an Austrian perspective, and specifically from Huerta de Soto's dynamic efficiency theory, any judgment about Bitcoin's "economic limits" based exclusively on such equations risks ignoring precisely what matters: human action, capital structure, time, and institutional evolution.

6. The cost of sound money: gold, Bitcoin, and the analysis of what is not seen

A classic objection to the gold standard, articulated in the monetarist tradition, holds that a monetary system based on a scarce good competitively produced—gold—entails an excessive resource cost: capital, labor, and land that could have been devoted to other productive ends. That same objection has been transferred almost unchanged to Bitcoin: mining would consume too much energy and too much hardware "merely" to maintain a transaction record (Serrano, 2025).

However, a more careful analysis, in Bastiat's (1850) spirit, requires comparing not only the visible cost of producing gold or securing Bitcoin, but also the hidden costs associated with an inflationary fiat monetary regime.

From this viewpoint:

— It is true that issuing fiat money has a seemingly negligible direct cost (through keystrokes at a central bank).

— But its indirect cost—in terms of boom-bust cycles, malinvestments induced by artificially low interest rates, rising public and private indebtedness, expansion of the state, and erosion of the purchasing power of savings—is enormous. Huerta de Soto has extensively documented how the combination of fractional-reserve banking and central banking generates a recurrent sequence of unsustainable expansions and crises, with large capital losses and intertemporal discoordination (Huerta de Soto, 1998, 2009).

If one focuses only on "what is seen"—Bitcoin mining's electricity bill or the cost of extracting gold—sound money will always appear expensive relative to fiat. Yet if we take what is not seen seriously, the comparison changes radically.

In Bitcoin's case, the large amount of resources devoted to proof of work is not technical waste, but the price the market voluntarily pays for a medium of exchange that offers unprecedented institutional properties: perfectly predictable supply, political neutrality, resistance to censorship and confiscation, global liquidity 24/7, and an ownership structure difficult to attack by legal or extralegal means (Serrano, 2025). That millions of ASICs run hash functions is not a system flaw, but a reflection of the subjective valuation participants place on those monetary properties.

In strictly economic terms, the relevant cost is not the book-keeping operating cost of mining, but its opportunity cost. Here the contrast is stark:

— The opportunity cost of a gold standard or a Bitcoin standard is foregoing an unsound fiat monetary regime and a structurally expansive state: giving up inflation as a hidden fiscal tool, discretionary manipulation of interest rates, and the sustained expansion of the political-bureaucratic apparatus.
— The opportunity cost of an unsound fiat monetary regime is foregoing sound money and a more limited state: giving up an institutional framework that favors long-term saving, prudent investment, fiscal discipline, and a reduction in discretionary monetary intervention.

If we consider dynamic efficiency, what ultimately matters is not only how much it costs to secure the monetary system in terms of resource flows, but what kind of institutional order is sustained by that cost. From Huerta de Soto's perspective, it is economically coherent that part of society's capital be devoted to maintaining a sound monetary system if doing so reduces the frequency and severity of cycles, improves economic calculation, and constrains discretionary monetary power.

In this context, Budish's claim that Nakamoto Trust is very expensive is incomplete: it correctly describes that Bitcoin's security budget must be large relative to protected value, but it does not compare that budget with the dynamic cost of the alternative monetary regime.

Environmental critiques and measuring the energy impact

From an Austrian perspective, the relevant point is not to count "energy per transaction"—a particularly misleading metric under PoW because security does not scale linearly with the number of payments—but to understand that energy expenditure is the economic anchor of ledger immutability: the observable cost of preventing double spending without a trusted third party. Precisely for that reason, the environmental debate requires carefully separating electricity consumed from carbon footprint (and avoiding metrics that conflate the two): the former is a physical magnitude; the latter depends on the electricity mix, the timing of consumption, and—above all—which generation is marginal in each system. Along these lines, part of the public critique relies on questionable carbon accounting—for instance, when it imputes to mining indirect emissions or system averages that do not identify which generation actually covers the additional consumption; or when it introduces duplications in emissions accounting and assumptions that are difficult to verify about what consumption or emissions would have occurred in the absence of mining (Carter, 2021; Rochard, 2023). None of this eliminates possible externalities; on the contrary, it forces us to discuss them with data (electricity mix, hashrate elasticity, hardware efficiency, mining location and mobility) and to

compare them with the institutional reference framework: what visible and invisible costs are incurred in securing and disciplining fiat money, its intermediaries, and its payments infrastructure.

Given that public debate about PoW often focuses on energy consumption, it is useful to incorporate the academic literature that quantifies and discusses it: there are estimates based on techno-economic models and hardware data (de Vries, 2018; Stoll, Klaaßen & Gallersdörfer, 2019), life-cycle assessment approaches (Köhler & Pizzol, 2019), and reviews synthesizing the state of the question (Vranken, 2017). In general, results depend on assumptions about hardware efficiency, electricity prices and contracts, regional carbon intensity, and patterns of mining relocation, which calls for prudence when extrapolating and, again, for distinguishing between "consumption" and "emissions". In parallel, an argument line emphasizes that mining can behave as flexible, interruptible demand, absorbing surpluses or "stranded" energy (e.g., unevacuated renewable generation) and, in certain contexts, helping reduce emissions through methane mitigation from flared or vented gas (Saylor, n.d.; Batten, n.d.). Tracking and evidence-aggregation tools, such as BEEST, aim to organize this discussion with comparable indicators, but their usefulness depends on methodological transparency and the quality of the underlying data (Batten, n.d.).

In sum, the state of knowledge suggests avoiding categorical conclusions: the environmental assessment of PoW is highly sensitive to assumptions and to observable variables such as the local electricity mix, the marginal generation that covers additional demand, and grid constraints. For this reason, rigorous discussion should rely on replicable measurements, carefully distinguish metrics, and ultimately compare institutional costs and benefits against the relevant monetary and payments alternative.

None of these considerations eliminates the possibility of significant local externalities, which should be evaluated case by case.

7. **Bitcoin's economic security and bitcoiner critiques of Budish**

Several authors close to the Bitcoin ecosystem have pointed to additional limitations in Budish's approach. A useful, though

informal, synthesis appears in Oasis Team's (2018) response, which criticizes several key model assumptions:

— Overestimation of the value of an attack: Budish approximates the potential value that an attacker could capture as a multiple of the total value of transactions included in certain blocks. In practice, however, an attacker can only benefit from the bitcoins they already control and attempt to spend twice, so the maximum exploitable value is only a fraction of total volume.
— Ignoring price reactions to frequent attacks: if a majority attack succeeds and becomes recurrent, confidence in Bitcoin would collapse, and with it the asset's price. The value of what is "stolen" would fall quickly, reducing endogenously the incentive to repeat the attack. The model treats Bitcoin's market value as exogenous to protocol credibility, whereas in reality the two are tightly linked.
— Assuming constant marginal costs and abundant, easily redeployable mining capacity: the analysis simplifies the cost structure as if mining equipment could scale without constraints, when in practice there are bottlenecks in chip manufacturing, logistical constraints, and, in the case of highly specific ASICs, a large sunk-cost component.[2]

Along these lines, Garratt and van Oordt (2020) show that the presence of significant fixed costs and specific hardware in Bitcoin mining strengthens system security: when miners must invest capital in ASICs with little alternative use, their supply of mining power reacts less to Bitcoin price drops, reducing vulnerability to double-spend attacks and weakening the most pessimistic predictions about future network security.

[2] A sunk cost is an expenditure that has already been incurred and cannot be recovered, or can only be recovered marginally, even if the project is abandoned. In the context of Bitcoin mining, a significant portion of the investment in specialized hardware and infrastructure constitutes sunk capital: if the network were to lose value or confidence in it were to collapse, that capital would have little alternative use and its liquidation value would be far below the initial investment.

For their part, Hasu, Prestwich, and Curtis's (2019) model emphasizes the importance of miner commitment: to operate a mining farm, an operator must invest today an amount of capital whose present value is roughly equivalent to half the bitcoins they expect to mine over the next two years. This means miners hold, in the form of specific physical capital, an economic position analogous to that of a large long-term Bitcoin holder. Any behavior that seriously damages the network—such as systematic double spending or sabotage—would erode the value of that capital and is therefore strongly disincentivized even if a one-off attack might be profitable in static terms.

In dynamic-efficiency terms, these approaches highlight that Bitcoin security:

— is not only a function of the current flow of rewards, but also of the amount of sunk capital whose value depends on the system's health;
— is not only a matter of incentives at the margin, but also of historical trajectory: after seventeen years of operation without catastrophic attacks, participants have developed expectations, routines, and informal rules that reinforce the protocol's coordinated stability.

None of this invalidates Budish's core observation (that the security budget must be high relative to protected value), but it does substantially soften the force of his more alarmist conclusions about the supposed inevitability of an attack if Bitcoin becomes very important as a store of value. Bitcoin security is an institutional and dynamic phenomenon, not a comparative-statics exercise with two equations.

8. **Property, anonymity, and responsibility: Bitcoin as a new type of property**

An essential aspect of the debate, rarely addressed in more formal literature, is the nature of Bitcoin ownership. Unlike bank deposits, cryptocurrencies, and fiat money itself, Bitcoin offers a property regime that combines:

— radical transparency of the ledger (the blockchain contains the full transaction history),
— pseudonymity of identities (units are associated with addresses and UTXOs, not with particular persons),
— exclusive control via private keys.

Functionally, this implies that the owner and the possessor tend to coincide: only whoever controls the private keys that allow spending particular UTXOs can dispose of those bitcoins. Except in cases of negligence, there is no separation between the right and the fact of possession.

Authors aligned with the Austrian framework have emphasized that Bitcoin meets the classic criteria of property: it is exclusively appropriable, effectively controllable, and constituted by discrete units perfectly identifiable in a public record reflecting the chain of title (UTXOs) (Graf, 2013; Serrano, 2025).

The institutional novelty is twofold:

— Bitcoin property is not guaranteed by the state. It does not depend on a central registry, on courts that can order forced transfers, or on authorities that can confiscate or freeze balances. The ultimate guarantee lies in cryptography, social consensus around the protocol, and users' custody practices.
— Bitcoin introduces, for the first time in history, a form of property that is practically unseizable and highly portable. By memorizing (or securely storing) a twelve-word seed phrase, an individual can "move" their bitcoins across borders and jurisdictions without the state having the technical capacity to prevent it.

The counterpart to this sovereignty is strict individual responsibility: the user must take charge of their own security and accept that mistakes (lost keys, sending to the wrong address, etc.) are not reversible. This has several implications for evaluating Nakamoto Trust:

— the product a user purchases with the network's security budget is not only a payment and settlement service, but a high-quality property regime, outside political discretion;

— cost analysis must incorporate the value agents place on holding a form of wealth resistant to inflation, confiscation, and censorship—particularly relevant in contexts of institutional instability or high inflation;
— the combination of relative anonymity, absence of a central authority, and cryptographic security is not a technological whim, but the condition for such property to exist at the margin in an environment where the state, by design, tends to expand its control over money and financial assets.

From the perspective of Huerta de Soto's theory of dynamic efficiency, this transformation in the property regime is not neutral: by radically improving the institutional quality of ownership of the medium of exchange, Bitcoin can expand the scope for entrepreneurship—whether as a long-term savings asset, as collateral in private contracts, or as the base layer for higher-level financial services built on voluntary custody and market rules.

9. **Bitcoin versus cryptocurrencies: the immutability of the essence of property**

The implications of the foregoing become clearer when comparing Bitcoin with two other universes: (i) fiat money issued by central banks; and (ii) the myriad "cryptocurrencies" launched over the past decade.

In the case of fiat money, one can argue that the monetary balances individuals hold as deposits and cash resemble a kind of security sui generis—what I call *security-fiat*, that is, a monetary asset whose quantitative and qualitative attributes ultimately depend on discretionary decisions by a central authority—rather than genuine commodity money. The central bank and the state retain the capacity to alter both the utility (via inflation, negative rates, regulatory changes) and the essence of what is held (e.g., leaving the gold standard in 1971 or introducing new forms of digital control over payments). In this sense:

— one dollar is, and will be, an ever smaller fraction of the total dollar supply;

— minority holders of that *security-fiat* have no guarantee of quantitative or qualitative stability of what they hold (Serrano, 2025).

A similar reasoning applies to cryptocurrencies.[3] Behind them we typically find:

— an identifiable set of promoters and developers with the ability to change protocol rules (issuance, reward policy, consensus mechanism);
— a highly concentrated ownership structure that allows insiders to decisively influence system evolution;
— formal or informal governance mechanisms that make it possible, in practice, to alter the token's essence to suit the interests of majority holders.

In this framework, the minority holder of a cryptocurrency is in a position analogous to that of a minority shareholder: their property is subject to potential dilution, changes in associated rights, and so on. Qualitative and quantitative uncertainty about what is actually owned is high.

Bitcoin, by contrast, operates as a form of commodity money in the strongest sense:

— its total supply is capped at 21 million units by protocol design, and this rule enjoys extraordinary social and technical protection, making changes extremely costly and highly unlikely in practice;

[3] The institutional essence of cryptocurrencies is fundamentally different from that of Bitcoin. Of the core features that define Bitcoin—decentralization, scarcity, unforgeability, immutability of monetary policy, irreversibility of transactions, censorship resistance, stability, credibility, voluntariness, proof of work, and pure property—cryptocurrencies, in general, satisfy only voluntariness (no one is forced to use them) and, in some cases, proof of work (PoW), always with the latent possibility that this mechanism may be abandoned—something that, in practice, cannot occur in Bitcoin without it ceasing to be recognized as such by its users. From this perspective, no cryptocurrency reproduces the remaining essential features of Bitcoin. The logical consequence is that Bitcoin and cryptocurrencies constitute two distinct institutional categories that should not be conflated (Serrano, 2025).

— any attempt to modify this core monetary rule would meet coordinated opposition from users, node operators, and much of the community and would, in practice, be forced to express dissent as a split chain without meaningful economic backing;
— owners—majority or minority—can reasonably expect that 1 bitcoin will always be at least one twenty-one-millionth of the total supply, even though its purchasing power fluctuates (Serrano, 2025).

From Huerta de Soto's perspective, this institutional stability of the essence of the monetary good is crucial for dynamic efficiency. A market order in which entrepreneurs can plan knowing that monetary policy will not be modified discretionarily offers far more fertile ground for intertemporal coordination and long-term investment (Huerta de Soto, 2009).

In sum, Bitcoin and cryptocurrencies do not belong to the same institutional genus. Extending to Bitcoin objections that are valid for highly centralized tokens is equivalent to conflating a commodity-money regime characterized by rule stability with a security-fiat asset subject to discretionary modification by its issuers.

10. Bitcoin, the legal order, and dynamic efficiency: substitute or complement?

A common objection—one that Budish implicitly captures—is that securing the ownership and settlement of very valuable assets in an anonymous, "lawless" environment is extremely expensive. From this, it is concluded that Bitcoin can only function as a marginal component within a broader legal order with property, reputation, contracts, courts, etc., and not as the core of an extensive market order.

From the perspective of Huerta de Soto's theory of dynamic efficiency, and in light of the preceding arguments, this objection can be qualified in several respects:

— Bitcoin does not deny private property or legal institutions; rather, it introduces a layer of property that is prior to, and

resistant to, state interference. On top of this layer, many contractual, entrepreneurial, and legal arrangements can be built: from professional custody services and private insurance to arbitration and private-law courts specialized in disputes involving keys, access, inheritance, and so on.

— The fact that sovereign custody is possible (self-custody) does not imply that all agents will choose it. Many will legitimately prefer to delegate part of the responsibility to trusted third parties, entering the realm of contracts enforceable by traditional legal systems. When this happens, what the user directly holds is no longer pure Bitcoin but an IOU (with different risks). That decision, however, is voluntary and reversible: the underlying good continues to exist as property in its sovereign form (Bitcoin in self-custody).

— As for the supposedly "excessive cost" of securing valuable transactions in an anonymous environment, it is worth recalling that Bitcoin anonymity is relative and that the system is evolving toward second-layer solutions (e.g., Lightning Network) that increase transaction volume without raising the base-layer security budget linearly.

More importantly, from dynamic efficiency theory the evaluation criterion is not only the cost of operating a system at a point in time, but its capacity to foster entrepreneurship, protect property rights, and limit discretionary power. From this perspective, Bitcoin can be seen not as a total substitute for the legal order but as a key component of a polycentric order of private institutions:

— at the structural level, the Bitcoin network guarantees a property register and an immutable monetary policy without requiring trust in the state;

— at other levels, firms, contracts, and reputational mechanisms emerge that coordinate more complex uses—from financial services to payment infrastructures—always arbitraging between the security of sovereign custody and the convenience of intermediation.

This view is coherent with Huerta de Soto's general thesis: a dynamically efficient market order tends to rely on institutions that emerge evolutionarily, respect private property, and leave ample room for free enterprise (Huerta de Soto, 2009). Bitcoin fits this pattern well.

The claim that it makes no sense to expect a system seeking to replace the logic of private property and legal institutions to be dynamically efficient at scale must be reformulated: what is dynamically inefficient is a system that replaces private property with discretionary promises of third parties (states or token issuers). Bitcoin does the opposite: it radicalizes private property, makes it technically more defensible, and invites a rethinking of higher-level institutional arrangements on firmer foundations.

11. **Conclusions**

This article has reassessed Budish's critique of the economic limits of Bitcoin and the blockchain from a theoretical framework distinct from static efficiency and partial-equilibrium analysis. In particular, it has argued that an adequate evaluation of Bitcoin requires incorporating dynamic efficiency, the entrepreneurial function, and institutional analysis, along the lines developed by Huerta de Soto (2009).

From this perspective, the high cost of Nakamoto Trust is not interpreted as waste, but as the institutional price of sustaining a monetary and property regime with more rigid and verifiable rules without the need for a trusted third party. That cost must be assessed together with its counterpart: the opportunity cost of forgoing unsound money and an institutional framework that facilitates monetary discretion, credit expansion, and, ultimately, business cycles, with persistent effects on saving, investment, and fiscal discipline.

The paper has also incorporated contributions from more recent specialized analyses (Hasu et al., 2019; Garratt & van Oordt, 2020; Oasis Team, 2018) that help nuance key assumptions in Budish's argument by introducing dynamic elements: sunk costs, specific hardware, path dependence, and reputational discipline mechanisms that influence miners' and participants' incentives.

A central result of the discussion is the importance of the property regime made possible by Bitcoin: the combination of pseudonymity, practical unseizability, and extreme portability constitutes a singular institutional innovation, consistent with the Austrian defense of property rights and with the critique of fractional-reserve banking (Graf, 2013; Serrano, 2025). In this sense, the paper has also emphasized the need to clearly distinguish between Bitcoin and cryptocurrencies: whereas the latter tend to reproduce, in private form, features typical of security-fiat (promises alterable by their controllers), Bitcoin approaches commodity money with an immutable essence—an especially relevant feature for dynamic efficiency in the long run.

None of the above implies that Bitcoin is a perfect system or that the challenges highlighted by Budish—particularly the transition toward a security regime based almost exclusively on fees—should be minimized. The long-term sustainability of a fee-driven security model remains contingent upon factors that are still evolving, including transaction demand, technological innovation, and miners' capital commitments. It implies, rather, that its evaluation requires attending (i) to the costs of what is seen and what is not seen (Bastiat, 1850; Serrano, 2025); (ii) to the institutional dimension of money and property (Graf, 2013; Huerta de Soto, 1998, 2009; Serrano, 2025); and (iii) to the creative, open, and entrepreneurial nature of the market process (Huerta de Soto, 2009).

From this perspective, the relevant question is not whether Bitcoin will fully replace the prevailing monetary and legal order, but rather to what extent its existence and expansion contribute to making that order more dynamically efficient by offering a sounder monetary base, less exposed to political arbitrariness and more consistent with a strict conception of property rights. In this sense, Bitcoin can be interpreted as a significant step in the evolution of monetary institutions toward forms of social coordination less dependent on the state and more aligned with market processes and human entrepreneurship.

Conflict of interest

The author declares that he has no conflict of interest.

References

Bastiat, F. (1850/2011): *That Which Is Seen and That Which Is Not Seen*. In *The Bastiat Collection* (2nd ed., pp. 1-48). Auburn, AL: Ludwig von Mises Institute.

Batten, D. (n.d.): BEEST (Bitcoin Energy & Emissions Sustainability Tracker). https://batcoinz.com/beest/ (accessed February 25, 2026).

Böhme, R., Christin, N., Edelman, B., and Moore, T. (2015): "Bitcoin: Economics, technology, and governance." *Journal of Economic Perspectives*, 29(2), 213-238.

Budish, E. (2018): "The economic limits of Bitcoin and the blockchain." NBER Working Paper No. 24717. Cambridge, MA: National Bureau of Economic Research. https://www.nber.org/papers/w24717 (accessed February 25, 2026).

— (2025): "Trust at scale: The economic limits of cryptocurrencies and blockchains." *The Quarterly Journal of Economics*, 140(1), 1-62.

Carter, N. (2021): "Noahbjectivity on Bitcoin mining: A response to Noah Smith" (March 29). https://medium.com/@nic__carter/noahbjectivity-on-bitcoin-mining-2052226310cb (accessed February 25, 2026).

de Vries, A. (2018): "Bitcoin's growing energy problem." *Joule*, 2(5), 801-805.

Garratt, R.J., and van Oordt, M.R.C. (2020): "Why fixed costs matter for proof-of-work-based cryptocurrencies." Staff Working Paper 2020-27. Ottawa: Bank of Canada. https://www.bankofcanada.ca/2020/07/staff-working-paper-2020-27/ (accessed February 25, 2026).

Garrison, R. W. (1992): "The costs of a gold standard." In Rockwell, L. H., Jr. (ed.): *The Gold Standard: Perspectives in the Austrian School* (pp. 61-80). Auburn, AL: Ludwig von Mises Institute.

Graf, K. S. (2013): "On the origins of Bitcoin: Stages of monetary evolution." https://static1.squarespace.com/static/5720adbdc6fc0891cbcce17c/t/580d685959cc689a7b411ba4/1477275058522/On+the+Origins+of+Bitcoin+Graf+03.11.13.pdf (accessed February 25, 2026).

Hasu, Prestwich, J., and Curtis, B. (2019): "A model for Bitcoin's security and the declining block subsidy (v1.06)." https://

uncommoncore.co/wp-content/uploads/2019/10/A-model-for-Bitcoins-security-and-the-declining-block-subsidy-v1.06.pdf (accessed February 25, 2026).

Huerta de Soto, J. (1998/2016): *Money, Bank Credit, and Economic Cycles*. Madrid: Unión Editorial.

— (2009): *The Theory of Dynamic Efficiency*. Oxfordshire: Routledge.

Köhler, S., and Pizzol, M. (2019): "Life cycle assessment of Bitcoin mining." *Environmental Science & Technology*, 53(23), 13598-13606.

Krause, M.J., and Tolaymat, T. (2018): "Quantification of energy and carbon costs for mining cryptocurrencies". *Nature Sustainability*, 1, 711-718.

Kroll, J.A., Davey, I.C., and Felten, E.W. (2013): "The economics of Bitcoin mining, or Bitcoin in the presence of adversaries." *Twelfth Workshop on the Economics of Information Security (WEIS)*.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016): *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton, NJ: Princeton University Press.

Oasis Team (2018): "Response to economic limits of Bitcoin and the blockchain by Eric Budish." https://medium.com/@oasiscryptowonderland/response-to-budish-paper-economic-limits-of-bitcoin-and-the-blockchain-79908f3d9899 (accessed February 25, 2026).

Rochard, P. (2023): "Fractional reserve carbon accounting is an attack on Bitcoin mining" (March 20). https://bitcoinmagazine.com/culture/carbon-accounting-attacks-bitcoin-mining (accessed February 25, 2026).

Rockwell, L. H., Jr. (ed.) (1992): *The Gold Standard: Perspectives in the Austrian School*. Auburn, AL: Ludwig von Mises Institute.

Saylor, M. (n.d.): "Bitcoin mining and the environment." https://www.michael.com/en/resources/bitcoin-mining-and-the-environment (accessed February 25, 2026).

Serrano, J. (2025): *Bitcoin as Sound Money: An Interpretation of Bitcoin in Light of the Austrian School of Economics*. Doctoral dissertation, Universidad Rey Juan Carlos.

Stoll, C., Klaaßen, L., and Gallersdörfer, U. (2019): "The carbon footprint of Bitcoin." *Joule*, 3(7), 1647-1661.

Vranken, H. (2017): "Sustainability of Bitcoin and blockchains." *Current Opinion in Environmental Sustainability*, 28, 1-9.