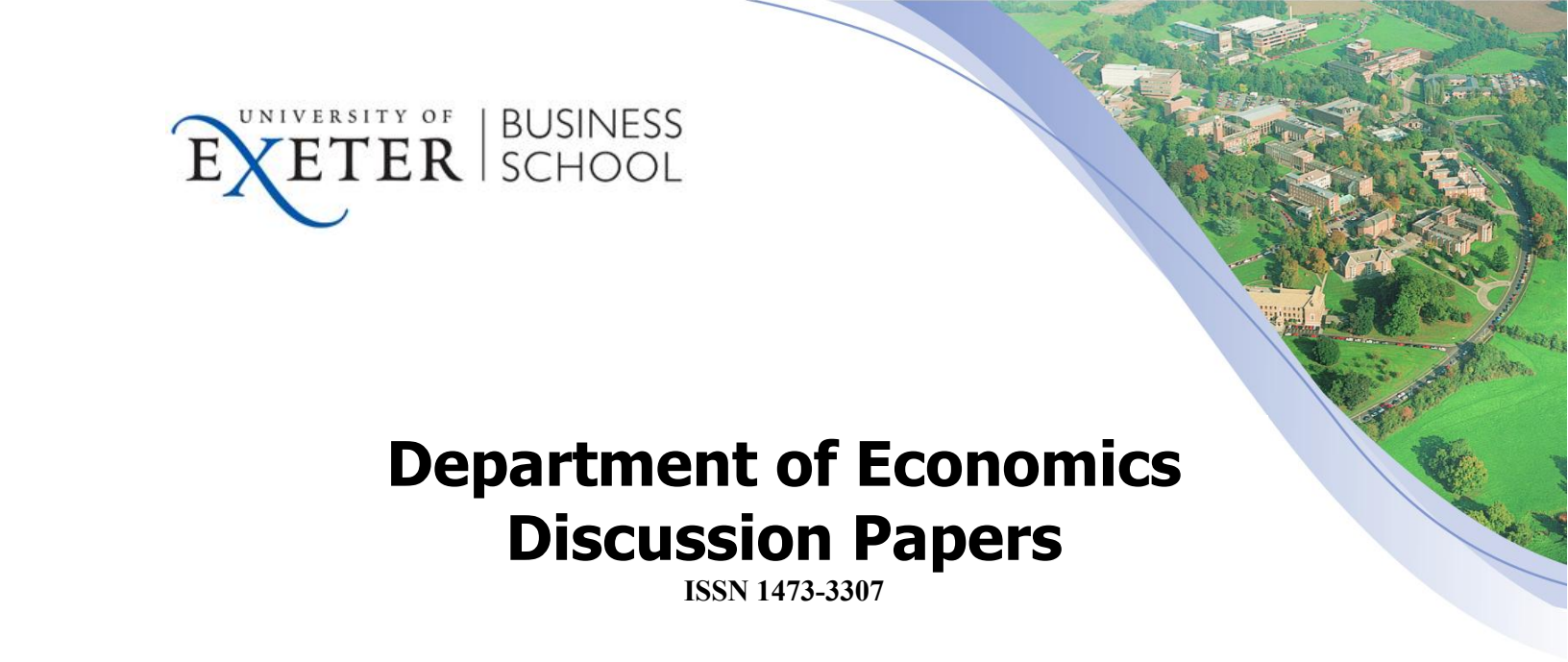

UNIVERSITY OF EXETER | BUSINESS SCHOOL

Department of Economics Discussion Papers

ISSN 1473-3307

False Premises, Failed Promises: BTC's Market Illusion and the Abandonment of Bitcoin's Design

Craig S. Wright

Paper number 25/02

RePEc page: https://ideas.repec.org/s/exe/wpaper.html

False Premises, Failed Promises: BTC's Market Illusion and the Abandonment of Bitcoin's Design

Craig S. Wright

University of Exeter Business School

cw881@exeter.ac.uk

July 1, 2025

Abstract

BTC, diverging fundamentally from the original Bitcoin protocol, has attained outsized market capitalisation despite abandoning Bitcoin's primary function as a scalable, traceable system for electronic cash. The Lightning Network, frequently misrepresented as a Layer 2 solution, is demonstrably a separate payment routing structure that never requires final settlement on-chain. This paper deconstructs the economic, technical, and ideological divergence of BTC from Bitcoin, critiques the architectural and empirical failure of Lightning, and examines the speculative mispricing driven by false narratives, branding confusion, and structural ignorance.

Keywords: BTC; Bitcoin; Lightning Network; digital cash; scalability; protocol divergence; Layer 2; micropayments; transaction finality; network economics

1 Introduction: Dislocating Function from Value

Bitcoin, as introduced in the original white paper [29], was intended to operate as an electronic cash system—traceable, scalable, and lawful. BTC, however, has emerged not as a

continuation of that system but as a structurally distinct financial product that maintains the name while abandoning its operational characteristics. The disjunction between protocol and branding has enabled market participants, institutional actors, and even regulators to conflate two incompatible systems. This has given rise to a speculative illusion: BTC is priced as if it were Bitcoin, while functioning according to an entirely different set of principles. Across the following subsections, we outline the core structure of this divergence. Subsection 1.1 examines the semantic capture of the term "Bitcoin" and the resulting protocol substitution. Subsection 1.2 outlines Bitcoin's original transactional purpose. Subsection 1.3 explains BTC's transition into a scarcity-based speculative asset. Subsection 1.4 introduces the Lightning Network as a mechanism falsely characterised as a scaling solution. Subsection 1.5 concludes with a roadmap for the paper's structure and argumentation.

1.1 The Misbranding of BTC as Bitcoin

BTC is not Bitcoin. The retention of the name "Bitcoin" following significant protocol-level changes has fostered semantic confusion and led to widespread misinterpretation of function, design, and purpose. As Sewell et al. argue, terminology in blockchain discourse is neither fixed nor neutral, but rather politically and economically loaded [37]. This semantic drift has allowed a substituted protocol to inherit the legitimacy, origin story, and symbolic capital of the original system—despite functioning according to wholly different rules.

The original Bitcoin protocol, released in 2009, was designed to support direct, peer-to-peer payments through on-chain settlement and simplified verification [29]. BTC, by contrast, introduced Segregated Witness, altered transaction finality through Replace-by-Fee, and imposed artificial block size constraints. These deviations are not minor optimisations but categorical redefinitions of how the system processes, validates, and accounts for transactions. Despite these changes, media outlets, exchanges, and institutional custodians continue to refer to BTC as "Bitcoin," reinforcing the linguistic capture described by Otabor-Olubor as interpretive divergence with material consequences [31].

This slippage has led regulators and market participants alike to build policies and portfolios around a version of "Bitcoin" that no longer aligns with its original function. It also inhibits accurate scholarly analysis by collapsing distinct systems under a common name.

As Allen and Chamberlain demonstrate in their study of Australian tax law, legal frameworks often misidentify economic substance when protocol divergence is masked by nominal continuity [2]. Misbranding is not simply a confusion of terms—it is a deliberate mechanism by which protocol power is laundered through historical reputation.

1.2 The Intended Function of Bitcoin: Electronic Cash

The original design of Bitcoin was never abstract or ambiguous: it was explicitly a peer-to-peer electronic cash system [29]. Its structure prioritised direct settlement, verifiability through simplified payment verification (SPV), and lawful traceability via a transparent ledger. The system incorporated a scripting language that enabled conditional payments and a linear incentive structure that rewarded miners for validating transactions at scale. Contrary to modern interpretations that treat blockchain systems as vessels for store-of-value theories or abstract decentralised ideals, Bitcoin's original role was grounded in practical functionality—processing real-world payments securely, efficiently, and without intermediaries.

Satoshi Nakamoto repeatedly affirmed that the protocol was capable of scaling to global transaction volumes. In archived discussions, Nakamoto dismissed the notion that Bitcoin could not handle Visa-scale throughput, citing both Moore's Law and the economic model of bandwidth-justified block growth. This design presumed and required growth on-chain, not off it. As Khan et al. observe in their systematic review of blockchain scalability challenges, the dominant constraints are rarely technical—they are narrative and ideological [22]. More recent comprehensive surveys corroborate that scaling Bitcoin through native protocol extension is viable and well understood, yet artificially restricted within BTC by policy, not principle [9].

The deliberate imposition of throughput ceilings in BTC breaks with the economic intent of Bitcoin. It shifts the model from inclusive, low-cost digital cash to an exclusive, high-fee settlement network for speculative purposes. This is not an evolution; it is a deviation that neuters the system's original purpose. The misrepresentation of this shift as continuity is a central distortion in the BTC narrative.

1.3 BTC as Speculative Asset: The Manufactured Myth of Digital Gold

BTC's present market characterisation as a "store of value" has no foundation in the original Bitcoin protocol. This framing emerged only after BTC Core developers disabled native scalability mechanisms and severed the system from its transactional roots. With its capacity to serve as electronic cash removed, BTC required a new narrative to justify its continued existence and market capitalisation. Thus was born the myth of "digital gold"—a term manufactured not from protocol design but from necessity, branding, and opportunistic analogies.

The rhetorical pivot to scarcity as value is a retrofitted post hoc rationalisation. It relies on superficial comparison with gold: limited supply, cost of production (via mining), and presumed long-term appreciation. Yet Bitcoin's supply schedule was never meant to define its utility; it was a constraint within a broader transactional logic. As Selvam argues, this shift to store-of-value ideology relies not on economic performance, but on ideological persuasion, privileging narrative over function [35]. The utility vacuum created by BTC's refusal to scale is obfuscated by speculative demand and the recycling of financial tropes.

Empirical studies affirm this. Baur and Dimpfl demonstrate that BTC's volatility remains irreconcilable with characteristics expected of either a stable store of value or a medium of exchange [5]. Taskinsoy shows how the "digital gold" metaphor operates more as marketing heuristic than monetary classification, pointing to institutional buying patterns driven by hedging rhetoric rather than transactional adoption [40]. Jones et al. extend this critique further by exposing the environmental externalities of BTC mining, describing it as more akin to "digital crude" than anything resembling a functional monetary instrument [21].

The transformation of BTC into a speculative commodity marks not an evolution but a betrayal of the system's monetary function. It is a transformation built not on cryptographic innovation or economic coherence, but on the need to preserve narrative momentum after the system ceased to serve its foundational purpose.

1.4 BTC as Speculative Asset: The Manufactured Myth of Digital Gold

BTC's present market characterisation as a "store of value" has no foundation in the original Bitcoin protocol. This framing emerged only after BTC Core developers disabled native scalability mechanisms and severed the system from its transactional roots. With its capacity to serve as electronic cash removed, BTC required a new narrative to justify its continued existence and market capitalisation. Thus was born the myth of "digital gold"—a term manufactured not from protocol design but from necessity, branding, and opportunistic analogies.

The rhetorical pivot to scarcity as value is a retrofitted post hoc rationalisation. It relies on superficial comparison with gold: limited supply, cost of production (via mining), and presumed long-term appreciation. Yet Bitcoin's supply schedule was never meant to define its utility; it was a constraint within a broader transactional logic. As Selvam argues, this shift to store-of-value ideology relies not on economic performance, but on ideological persuasion, privileging narrative over function [35]. The utility vacuum created by BTC's refusal to scale is obfuscated by speculative demand and the recycling of financial tropes.

Empirical studies affirm this. Baur and Dimpfl demonstrate that BTC's volatility remains irreconcilable with characteristics expected of either a stable store of value or a medium of exchange [5]. Taskinsoy shows how the "digital gold" metaphor operates more as marketing heuristic than monetary classification, pointing to institutional buying patterns driven by hedging rhetoric rather than transactional adoption [40]. Jones et al. extend this critique further by exposing the environmental externalities of BTC mining, describing it as more akin to "digital crude" than anything resembling a functional monetary instrument [21].

The transformation of BTC into a speculative commodity marks not an evolution but a betrayal of the system's monetary function. It is a transformation built not on cryptographic innovation or economic coherence, but on the need to preserve narrative momentum after the system ceased to serve its foundational purpose.

1.5 Structure of the Argument: Reconstructing the Discontinuity

This paper proceeds by mapping the precise contours of divergence between Bitcoin as designed and BTC as implemented. Section 2 outlines the original structure of Bitcoin, focusing on native protocol features enabling scalable on-chain transactions, simplified verification, traceability, and lawful commercial application. It frames the protocol as an integrated monetary system—not an abstract asset layer.

Section 3 addresses the critical protocol changes enacted by BTC Core. It demonstrates that Segregated Witness, Replace-by-Fee, the artificial block size constraint, and the disabling of transaction scripting constitute foundational breaks from the Bitcoin system as released in 2009. These decisions are examined not only in technical terms, but through their economic implications and cumulative intent.

Section 4 deconstructs the Lightning Network, not as a Layer 2 solution, but as a parallel payment network operating independently of BTC's base chain. It examines how the structure, liquidity dynamics, routing failures, and custodial dependence of Lightning expose it as both non-layered and economically unscalable. Empirical studies on network centrality, failure rates, and capital inefficiencies are integrated to underscore this point.

Section 5 turns to the mechanisms of narrative insulation. It identifies the semiotic construction of BTC's legitimacy, the role of memes, language capture, and corporate sponsorships in maintaining the illusion of continuity. It draws on semiotic and economic literature to expose how ideological narratives have replaced protocol performance as the source of valuation.

The concluding sections address regulatory misclassification and monetary confusion, offering a reframing of BTC not as an evolved form of Bitcoin but as a distinct, incompatible system. This culminates in a call for formal terminological separation to restore analytical precision, legal coherence, and economic clarity.

2 Bitcoin's Design: Scaling by Protocol

The original Bitcoin system, as released in 2009, was constructed to scale through direct on-chain capacity, not layered abstractions. Its architecture centred on transparent, verifiable transaction processing, economic incentives for efficient validation, and a scripting language enabling payment conditions at the protocol level. The notion that Bitcoin required off-chain mechanisms for throughput or finality was a later imposition, not a foundational constraint. This section dissects the structural features that made Bitcoin scalable within its own protocol: block-level throughput, simplified verification (SPV), lawful traceability, and micropayment viability.

2.1 Native Throughput Capacity and the Role of Blocks

In Bitcoin, transaction throughput is determined by block size, block frequency, and the protocol's capacity to accept valid blocks that meet proof-of-work constraints. Nowhere in the original white paper is a fixed block size limit specified—only a 10-minute block interval target is noted, paired with a network difficulty adjustment mechanism [29]. Early versions of the software implemented a soft cap of 1MB as a temporary anti-spam measure, not a fundamental design ceiling.

Block size growth was assumed to track with advances in network bandwidth, storage, and processing power. Nakamoto explicitly stated that "[Bitcoin] can scale much larger than Visa with existing hardware," dismissing scaling concerns as unfounded given the hardware trends and economic incentives surrounding bandwidth cost [29]. The system was structured to incentivise miners to process ever-larger blocks as transaction volume increased, earning fees in addition to block rewards. This logic aligns with scaling by demand rather than fixed constraint—a principle consistent with economic systems of competitive service provision.

As Khan et al. observe, structural blockchain scalability is rarely limited by raw computation or bandwidth, but by imposed ideological or policy constraints [22]. Chen et al. reinforce this, documenting the viability of intra-chain scaling through protocol-level engineering, optimisation of validation workflows, and transaction aggregation methods [9].

Bitcoin's architecture placed no theoretical ceiling on throughput; it relied on market-driven miner incentives to adapt the ledger to usage demands.

The framing of a throughput ceiling was introduced much later by BTC Core, not as a design correction but as a strategic narrowing of the system's role. In its original form, Bitcoin relied on block throughput elasticity to handle transaction volume directly on-chain. Layer 1 was not merely a base; it was the system in full.

2.2 Native Throughput Capacity and the Role of Blocks

Bitcoin's throughput model is grounded in a simple economic and computational reality: more transactions require more space, and more space can be justified by falling bandwidth and storage costs. As nakamoto originally specified, transaction volume scales by increasing block size in line with resource availability [29]. The design assumed continual bandwidth growth, falling cost curves, and miner incentives to process larger blocks in exchange for fees. Contrary to later ideological interventions, there was no theoretical constraint limiting this scaling path.

The structure of the network aligns with Coase's theory of the firm, where organisational boundaries and responsibilities emerge from minimising internal transaction costs [10]. In Bitcoin, the marginal cost of transmitting and verifying larger blocks is borne by miners and infrastructure providers, not end-users. This separation of roles reflects an intentional economic specialisation. The attempt by BTC Core to enforce rigid caps contradicts this, artificially inflating costs for all participants and distorting the incentive structure.

Security in such a scaling model depends on the integrity of validation, not on state replication by all participants. Wright demonstrates through formal modelling that SPV clients operating under proof-of-work anchoring are not only computationally secure but economically efficient when compared with small-scale home node validation in constrained environments [43]. These results confirm that economic scale in Bitcoin derives from differentiated roles, not homogeneity.

In distributed blockchain-based systems beyond cryptocurrency, Kim et al. show that cost modelling validates bandwidth-intensive protocols when resource allocation is decentralised and incentive-aligned [23]. Similarly, Malempati's analysis of financial network infrastruc-

ture highlights that layered and adaptive load distribution ensures better scalability and performance in secure financial systems [26].

What is often ignored in BTC's current framing is that transaction throughput is not a side-effect—it is a design imperative. Hayek's work on decentralised knowledge systems applies directly here: protocols must assume asymmetric information and diverse resource availability, not impose universal constraints [17]. By enforcing rigid block limits, BTC rejects this epistemic insight and reintroduces bottlenecks in what was intended to be a self-adjusting system.

As brekke argues, the cryptoeconomic turn has often replaced technical architecture with ideological posturing, miscasting scale as antithetical to integrity [6]. Yet the original Bitcoin system was neither anarchic nor inefficient. It was a high-throughput, low-friction ledger designed to scale economically. The turn against throughput is not a failure of engineering—it is a rejection of Bitcoin's design logic.

2.3 Lawful Traceability and Script Expressiveness

The original Bitcoin protocol included a purpose-built scripting system designed for programmable payments—enabling functionalities such as multisignature enforcement, time locks, hash locks, and conditional execution directly on-chain [29]. This expressive capacity was not ornamental. It allowed contracts to be encoded into transactions in a transparent, verifiable, and legally meaningful manner. Rather than creating opaque execution environments, Bitcoin's Script was deliberately limited in complexity while maximising auditability and predictability.

Far from anonymity-focused designs found in later blockchain iterations, Bitcoin prioritised traceability. Nakamoto's structure ensured that all transactions could be followed through a public chain of signatures, thus permitting forensic analysis, lawful recovery, and regulatory audit. As otabor-olubor argues, the interpretive divergence introduced by post-2014 BTC discourse mischaracterised this transparency as a flaw rather than a feature [31]. The original system was built for enforceable payments—not for black-box transfers.

This design aligns with the needs of enterprise and government-scale usage. Herold et al. provide a blockchain-specific categorisation of transaction cost outcomes under uncertainty,

showing that legally coherent audit trails reduce risk and streamline regulatory operations [18]. Mishra and Kaushik's recent work similarly identifies lawful provenance and accountability as essential to any blockchain's viability in sustainable financial systems [28]. Both studies validate Bitcoin's original model while implicitly rejecting BTC's increasing abstraction from these operational expectations.

Script's capacity for constrained conditionality also provides the foundation for regulated microcontracts. This structure is economically significant: it enables automatable rulesets for custody, release, dispute resolution, and compliance. As hong et al. show in their study of secure authentication models on permissionless networks, retaining visibility and determinism in script logic is key to maintaining verifiability and access control across decentralised systems [19].

BTC's gradual removal or deactivation of opcodes in the name of "safety" has not increased security. It has instead removed the system's ability to operate in legally aligned, rule-expressive environments. What was once a programmable, lawful, auditable system has become a static token layer with minimal logic and diminished functionality. The original Bitcoin system—by design—was compliant-capable, script-enabled, and traceable. Its removal was not a bug fix. It was a paradigm shift.

2.4 Economic Design for Micropayments

Bitcoin was not conceived as a high-fee settlement network for bulk transactions, but as an infrastructure for microeconomic activity. The protocol's fee model, incentive structure, and confirmation system were designed to support small-value transfers with minimal overhead. As nakamoto made clear, Bitcoin's core proposition was to serve as a peer-to-peer payment system capable of efficiently processing day-to-day transactions without reliance on centralised intermediaries [29].

The fee structure embedded in the original protocol supports this interpretation. Users attach optional fees, and miners prioritise transactions according to profitability. Under competitive conditions with increasing block size, fees tend toward marginal cost levels. As taskinsoy notes, the narrative pivot toward "store of value" ignores the protocol's microtransaction logic, substituting a scarcity-driven valuation model for one based on transactional

throughput and adoption [40].

Selvam extends this by demonstrating that Bitcoin's fee incentives were predicated on scale—low fees attracting volume, and volume providing incentive for security and validation infrastructure [35]. Any system that limits volume while requiring fixed income per block (e.g. via high fees) distorts this balance, leading to centralisation and reduced utility. This is not a flaw in Bitcoin's design but a rejection of it by the BTC implementation.

Wright's formal analysis confirms that SPV-based clients offer secure pathways for micropayment validation without the burden of full chain replication, supporting cost-effective user-side validation even in constrained environments [43]. Such an architecture enables viable microeconomic participation across a range of device classes, geographies, and infrastructure levels. It is inherently inclusionary.

Moreover, modern infrastructural perspectives validate this original model. Malempati shows that financial networks designed for low-latency, high-volume workloads require dynamic scalability at the infrastructure level, not abstracted payment rails layered atop frozen base chains [26]. Brekke's political economy critique reinforces this, observing that so-called "decentralised" architectures that abandon small-value throughput are structurally exclusionary [6]. High-fee models reproduce traditional gatekeeping under a technical guise.

Micropayments are not an afterthought—they are a test of architectural coherence. Bitcoin's capacity to process high volumes of low-value transactions is the definitive refutation of the notion that integrity and scale are incompatible. The abandonment of this function by BTC represents not just a change in use case, but a repudiation of Bitcoin's economic architecture.

2.5 Summary: Layer 1 Is the System

Bitcoin's design, as implemented in the 2009 release, was self-contained. It included all necessary components for a scalable, verifiable, and lawful electronic cash system within Layer 1. Block-level throughput was elastic. Verification was structured around SPV to maximise economic efficiency. Script enabled programmable, auditable contract logic. The fee model encouraged mass inclusion, and micropayment viability was essential to the system's intended function.

BTC's divergence from these principles—by capping throughput, disabling script, undermining SPV, and reframing high fees as a feature—constitutes a fundamental departure, not an evolutionary refinement. The shift was not technical; it was ideological. It recast Bitcoin from a lawful digital cash system into an exclusionary, scarcity-based settlement token layered beneath speculative abstractions.

Wright's formal analysis of SPV security underscores that Layer 1 was not reliant on hypothetical second-layer constructs or delayed finality [43]. Instead, it was anchored in direct proof-of-work confirmation and deterministic verification pathways. Hong et al. reinforce the necessity of Layer 1 transparency for authentication, accountability, and secure user access in decentralised systems [19].

BTC's post hoc justification of its narrowing—a claim that Layer 1 must be minimal to preserve decentralisation—contradicts foundational economic theory. Hayek's knowledge problem illustrates that scale arises from distributed specialisation, not artificial uniformity [17]. Coase's analysis of transaction costs shows that efficient systems externalise redundancy and internalise validation, precisely as Bitcoin's SPV structure does [10].

Bitcoin, properly implemented, is not a base layer waiting for a fix. It is a complete system—designed to operate openly, securely, and at global scale without dependency on separate mechanisms. This section closes by making that clear: Layer 1 is not the foundation of Bitcoin. Layer 1 is Bitcoin.

3 Protocol Substitution: Structural Divergence in BTC Core

BTC Core's stewardship of the codebase diverged sharply from the operational structure of Bitcoin as released in 2009. Rather than maintaining protocol compatibility with the original architecture, BTC Core implemented a series of revisions that cumulatively rewrote the system's assumptions, constraints, and functionality. These changes—justified through rhetorical appeals to security, decentralisation, and "technical debt"—have substituted one economic system for another while maintaining the same symbolic label. This section details

those divergences: the restructuring of transaction signatures through Segregated Witness; the deliberate break with finality via Replace-by-Fee; the hard enforcement of an artificial throughput ceiling; the deactivation of key transaction logic through opcode removal; and the ideological redefinition of network consensus through full-node dogma. Each modification is shown to be not a technical upgrade, but a structural repudiation of Bitcoin's purpose as scalable electronic cash.

3.1 Segregated Witness and the Removal of Signatures

Segregated Witness (SegWit), activated on BTC in 2017, fundamentally altered the Bitcoin transaction model by relocating the signature—witness data—outside the transaction hash used to identify a transaction. This change was introduced under the pretext of solving transaction malleability and increasing block efficiency, but in doing so, it broke the chain of digital signatures that defined Bitcoin's security model [29]. In the original design, each transaction referenced and cryptographically signed the hash of its parent transaction, forming a verifiable, tamper-evident chain. SegWit's structural separation nullifies this binding, turning a digital signature into an externally referenced metadata element.

This break undermines auditability and weakens the evidentiary link between spend and signature. Jain and Pilli's systemisation of Taproot and SegWit structures confirms that these changes not only alter the signature structure but introduce non-backward-compatible interpretive models for transaction verification [20]. Transactions are no longer verifiable through simple hash-linking, introducing additional parsing logic and diminishing the cryptographic simplicity of audit trails.

This undermines Bitcoin's legal enforceability. As Ahmad et al. argue, blockchain-based audit mechanisms derive strength from unbroken, fully verifiable state transitions [1]. By removing the witness from the transaction structure, BTC complicates this process, increasing reliance on contextual reconstruction rather than embedded verification. This is not a neutral design choice—it substitutes a linear signature graph for an interpretive witness schema.

The rhetoric used to justify SegWit mischaracterises transaction malleability as an "attack," framing it as a bug rather than a property of how signatures can be legally and

cryptographically altered before confirmation. Malleability did not compromise security or integrity—it merely allowed the same transaction content to be re-encoded. In systems where ordering and duplicate suppression matter, this is a protocol constraint to manage, not a threat to eliminate.

Garay et al. note that the integrity of the Bitcoin backbone protocol relies on verifiable inclusion paths anchored in proof-of-work, not abstract witness reassociation [14]. SegWit redefines the structure of that path, complicating verification logic and introducing alternative data hierarchies. In doing so, it weakens the Bitcoin model of digital cash secured by cryptographic commitment and replaces it with a modular, externally verified model more suited to token-based abstraction.

This signature displacement—marketed as a technical upgrade—represents a severance from Bitcoin's foundational structure. It is not simply a matter of format, but of function: SegWit transforms transactions from atomic units of cryptographic expression into objects requiring off-transaction context to verify.

3.2 Replace-by-Fee and the Destruction of Finality

Replace-by-Fee (RBF) was introduced to the BTC network as an opt-in policy allowing unconfirmed transactions to be replaced in the mempool with versions that pay a higher fee. Although presented as a method for improving transaction fee estimation and mempool hygiene, the introduction of RBF fundamentally altered Bitcoin's economic assurance model by breaking presumptive finality. Under the original protocol, transactions—once broadcast and accepted into the network—were treated as committed unless invalidated by a conflicting double spend included in a block. RBF, by contrast, openly permits and encourages replacement of a transaction with another version prior to inclusion, provided the new transaction offers a higher miner fee.

This modification destabilises commerce. Zero-confirmation transactions, once relied upon for rapid payment settlement in high-frequency and retail contexts, are rendered economically insecure. The change removes the practical utility of real-time transactions and forces users to wait for confirmation, even in contexts where trust was previously modelled on observed network propagation. As milkau notes, payment intermediaries historically pro-

vided temporal certainty; RBF shifts this burden onto users, forcing them to internalise payment risk without any institutional mitigation [27]. Bitcoin was designed to eliminate that intermediary function, not to reproduce its risk asymmetries.

The result is a payments environment where senders can non-deterministically reverse a transaction up to the point of confirmation. This violates a fundamental principle of cash-like exchange: the irreversibility of a valid, transmitted payment. Fabi's modelling of blockchain latency trade-offs demonstrates that throughput under high replacement policy leads to increased average confirmation delays, congestion in mempool state maintenance, and probabilistic instability in miner prioritisation [13]. This is not an efficiency improvement—it is the insertion of temporal uncertainty into what was meant to be a deterministic system.

RBF also compromises miner signalling and transaction prioritisation, encouraging fee-driven opportunism over consistent inclusion logic. Sarenche et al. show that under volatile block rewards, mempool statistics become crucial to miner revenue projections [34]. The presence of RBF introduces exploitable variance, allowing well-resourced actors to submit competing replacement chains, undermining fairness for economically marginal users. The result is a system increasingly optimised for fee-sensitivity rather than payment reliability.

Swambo's recent analysis of custody practices reinforces this point from an infrastructure perspective: wallets and service providers must now build safeguards and delays into systems that were once responsive and instant [39]. This increases friction, degrades UX, and recreates centralised buffering layers—all to compensate for the intentional erosion of trust assumptions.

There is no indication in the original protocol or white paper that RBF-like behaviour was envisaged, tolerated, or desired. On the contrary, Bitcoin's model assumed that a transaction broadcast and accepted by the network was authoritative barring clear invalidity. RBF introduces a double-spend race condition by design, replacing network agreement with individual economic coercion. It transforms Bitcoin from a tool of instant settlement to a contest of latency and pricing power.

3.3 Block Size Constraint and Engineered Scarcity

The imposition of a fixed block size constraint—formalised through policy rather than necessity—marked a decisive shift in the economic logic of BTC. The original Bitcoin protocol did not prescribe a hard limit on transaction volume. While the early implementation included a 1MB soft ceiling, it was understood as a spam prevention mechanism, not an economic throttle. BTC Core's decision to institutionalise this constraint, even in the face of network congestion and fee spikes, was an ideological assertion: that scarcity should be manufactured and preserved, not overcome.

This artificial bottleneck introduced predictable economic effects. Transactions competed for limited space, driving up fees and introducing inclusion uncertainty. As cole et al. quantify, the economic value of blockchain transactions becomes skewed under throughput constraints, prioritising high-value, low-frequency settlements over routine exchange [11]. The result is a redefinition of Bitcoin from a tool of mass commerce to a gated ledger of elite transfers.

Garay et al. demonstrate that the security of the Bitcoin protocol rests on continual usage and inclusion—not static preservation [14]. Fee-based models under fixed block space decouple miner income from transaction diversity, reducing the alignment between network growth and validation incentives. Fabi's modelling further confirms that under artificial constraints, latency and congestion emerge not from demand, but from policy-induced frictions [13]. This is not market optimisation—it is deliberate suppression of transactional capacity.

Azouvi's analysis of decentralisation and governance reveals how this constraint was not merely technical but political: a decision by a concentrated group of developers to redefine what Bitcoin should be, without reference to the system's origin or function [4]. Whitford and Anderson situate such governance shifts within broader frameworks of regulatory and institutional misclassification, where systems are relabelled based on emergent power dynamics rather than technological consistency [41].

This transformation mirrors Austrian critiques of engineered scarcity: supply is deliberately restricted, not due to natural limitation, but to manufacture value perception. Pecis et al. analyse this discursive process directly, showing how BTC communities substitute

ideology for utility, constructing "trust" through symbolic austerity rather than systemic performance [32].

The outcome is exclusionary by design. As sarenche et al. show, constrained block environments produce volatility in mempool statistics that disadvantage low-fee users and encourage speculative bidding wars over confirmation timing [34]. This directly undermines the use of Bitcoin as a low-cost, frictionless payment tool and reorients the network toward hoarding and delayed settlement.

Bitcoin's original design presumed capacity growth with adoption. BTC's refusal to scale does not represent conservatism—it represents regression. It replaces functionality with narrative, volume with symbolism, and monetary exchange with scarcity theatre.

3.4 Opcode Removal and the Crippling of Script

One of the most fundamental design elements of Bitcoin is its native scripting system—an intentionally limited, stack-based programming language designed to encode conditional payments, automate transaction logic, and facilitate auditable smart contracts directly at the protocol level [29]. The early Bitcoin implementation included a suite of opcodes enabling functionalities such as multi-signature checks, time locks, and various forms of value constraints. These features were not extraneous; they enabled contract enforcement, escrow, delegation, and legal compliance directly within Layer 1.

BTC Core progressively disabled or deprecated large portions of this script functionality under the pretext of safety. This included disabling opcodes like OP_EVAL, OP_CHECKSIGVERIFY, and others, and never re-enabling them despite advances in validation and sandboxing models. These decisions stripped Bitcoin of its capacity to perform rule-based enforcement without intermediaries. As sambana explains in his review of blockchain systems, this results in a system that functions not as programmable money but as static asset transfer, removing programmability in favour of token simplicity [33].

Fabi's research on blockchain capacity management reinforces the role of script complexity in throughput optimisation [13]. Contrary to BTC Core's assumptions, constrained conditionality does not compromise scalability; it enables parallelism and delegation without reliance on trusted intermediaries. The removal of these opcodes reflects a failure to

understand the role of deterministic logic in distributed verification.

This loss of expressiveness also undermines Bitcoin's compliance potential. Ahmad et al. demonstrate that effective audit trails depend on transparent, enforceable transaction logic, not merely immutable state changes [1]. With scripting capacity disabled, BTC fails to deliver transaction-level accountability required for institutional adoption.

From an economic perspective, Milkau's work on payment intermediaries becomes relevant again here: the original scripting model was designed to remove the need for human arbitration and institutional custodianship [27]. By removing programmability, BTC reintroduces the need for off-chain contractual enforcement, reversing the gains in transactional autonomy that Bitcoin originally enabled.

More critically, this regression is not accompanied by innovation elsewhere. No Layer 2 construct restores what Script once enabled. Swambo's study on custody highlights that institutions are forced to design their own mechanisms for ruleset enforcement, increasing both complexity and risk [39].

The disabling of Bitcoin's scripting layer is not neutral. It is a decisive step away from functionality toward ideological minimalism. It has reduced Bitcoin to a passive transport protocol, incapable of encoding obligation, condition, or structured rights transfer. What was once lawful programmable cash has been reduced to a mute token.

3.5 Node Dogma and the Rejection of Economic Hierarchy

A pivotal yet underexamined transformation in the BTC protocol lies in its redefinition of network roles—particularly the elevation of full nodes as the central authority in validating consensus. This ideological shift, originating in BTC Core discourse post-2015, reframed Bitcoin's architecture as one in which "everyone must run a full node" to ensure trust, replacing the original economic logic of differentiated participation with a homogenised, inefficient model of universal validation.

This narrative stands in direct contradiction to the SPV model defined in the original protocol [29]. In that model, most users operate as economic nodes—verifying payments via Merkle proofs and trusting the longest chain of proof-of-work, not by replicating the entire chain state. Wright's formal security model confirms that SPV clients maintain cryp-

tographic assurance under realistic adversarial conditions, while full nodes impose high resource overhead with diminishing marginal benefit [43]. By imposing full node participation as normative, BTC imposes barriers to entry and shifts the protocol away from global usability.

The resulting network model is one where participants are required to perform roles they neither need nor benefit from. This contradicts Hayek's knowledge theory, where distributed systems operate efficiently only when local actors are not burdened with the full informational scope of the system [17]. Bitcoin was designed to allow resource-constrained participants to validate their own payments without full-system replication. BTC's inversion of this is both epistemically inefficient and economically regressive.

Coase's framework is equally relevant here. Transaction cost minimisation is central to Bitcoin's design—delegating archival roles to miners and infrastructure operators while allowing users to economically validate their transactions [10]. Forcing all actors to be archival nodes distorts the division of labour and increases systemic friction.

This shift also facilitated a narrative recasting of decentralisation. Azouvi documents how definitions of decentralisation in cryptocurrencies often obscure concentration of power through rhetorical techniques, masking the ideological control of protocol development beneath the language of trustlessness [4]. Pecis et al. reinforce this by demonstrating how BTC's community structures construct legitimacy through ritualised narratives—full node identity, self-validation, and minimalism—rather than through performance or access [32].

Governance landscapes become central in this redefinition. Whitford and Anderson explain that the perceived neutrality of decentralised technologies often conceals structured gatekeeping, where influence is exercised not through mining or transaction validation but through protocol-level norms and discourse control [41]. BTC's emphasis on full nodes has facilitated this control structure—filtering consensus not by hashpower, but by cultural conformity.

This reorganisation of Bitcoin's social and technical hierarchy effectively rejected the economic node model in favour of doctrinal consensus. It elevated performative redundancy over functional verification. The result is a system less inclusive, less scalable, and more ideologically rigid than the protocol it supplanted.

4 The Lightning Network: Autonomy, Abstraction, and the Collapse of Settlement Finality

The Lightning Network has been mischaracterised as a Layer 2 scaling solution to Bitcoin. Rather than extending the base protocol, it operates as a structurally independent system with no enforced requirement to close or reconcile transactions on the blockchain [43]. Its architecture redefines transaction logic, shifting from time-stamped, traceable entries in a global ledger to probabilistic, conditional payment flows across private channels. This not only undermines auditability and legal finality, but also severs the transactional chain of accountability inherent to Bitcoin's original design [29].

The economic narrative surrounding Lightning is one of efficiency, latency reduction, and microtransaction enablement. Yet the core function of the network introduces abstractions that compromise the determinism and auditability essential to digital cash. Rather than congestion relief, Lightning forms a separate network of capital-locked bilateral agreements with no settlement imperative. It is this disjunction that renders it not merely an external service, but an economic counter-model with a different set of incentives. In the following subsections, we explore the lifecycle of Lightning channels, incentive incompatibilities, the breakdown of finality, and the false equivalence of "scaling" as framed by BTC Core advocates.

4.1 Channel Lifecycle and Autonomy

As shown by Grötschla et al., Lightning payment channels exhibit non-deterministic closure behaviour, with no enforced obligation to settle on the base layer within any finite period [15]. Unlike the Bitcoin protocol, where each transaction is final and broadcast across a global state, Lightning operations are pre-signed IOUs contingent upon future closure. This enables routing across non-transparent intermediaries, whose liquidity status and intentions are unknown to the sender or receiver.

The supposed efficiency of Lightning comes at the cost of system-wide traceability and predictable enforcement. Audit trails are fragmented and off-chain, removing the ability

to reconstruct value flows or detect systemic abuse [25]. This bifurcated state mechanism detaches accountability from protocol-level enforcement. Rational actors, facing asymmetric information and risk, are incentivised to hoard liquidity and delay closure [8]. These game-theoretic outcomes, rather than resolving Bitcoin's throughput concerns, instantiate a distinct market of channel arbitrage that contradicts the principle of direct, cash-like payments.

4.2 Incentive Misalignment and Channel Economics

The Lightning Network introduces a fundamental shift in the economic model of transaction propagation. Unlike Bitcoin, where transaction validation is rewarded in proportion to proof-of-work and incorporated into a universally verifiable ledger, Lightning introduces capital lock-up as a gating mechanism [12]. Participants must front liquidity into payment channels, which in turn incentivises large hubs to centralise control and extract routing fees from less-capitalised users [3]. Rather than fostering peer-level economic empowerment, the structure privileges intermediated liquidity pathways reminiscent of traditional correspondent banking.

Moreover, the asymmetry in time preference and reward distribution creates misaligned incentives. Users seeking final settlement must rely on unregulated, unauditable intermediary nodes whose operational security, uptime, and reliability are opaque. The resulting economic behaviour leads to hoarding, fee maximisation, and selective routing, all of which distort the transactional neutrality envisioned in the Bitcoin whitepaper [29]. As shown by Dasaklis and Malamas, the economic logic underpinning Lightning resembles a competitive telecom network more than a cash infrastructure, with the associated risks of congestion, service degradation, and non-neutral fee practices.

This misalignment exposes a contradiction in Lightning's positioning: while marketed as a decentralised microtransaction layer, its structural incentives mirror platform capitalism and centralised rent extraction. Economic finality and transparency are sacrificed in favour of throughput, yet without the systemic protections or legal recourse found in traditional financial intermediaries [16]. Consequently, Lightning fails to deliver on both technical and economic fronts as a supplement to digital cash.

4.3 Disconnection from Base Layer Security and Auditability

One of the critical failures of the Lightning Network lies in its structural and operational disconnection from the base Bitcoin protocol. The Lightning Network does not require regular settlement back to the blockchain, undermining the core principle of transparent auditability that Bitcoin was designed to uphold [42]. As noted by Wright, Lightning is not a Layer 2 in any formal system architecture—it is a separate overlay with an independent logic and security model. This decoupling strips away the proof-of-work assurances that underpin Bitcoin's integrity and instead relies on unverified state transitions between transient, ephemeral payment channels.

This structural independence leads to severe consequences in terms of transparency and accountability. Since off-chain transactions are not subject to global consensus, there is no mechanism to ensure uniform agreement on the network's state or to resolve disputes without defaulting to base layer closure. Yet, paradoxically, the very design of Lightning discourages closing channels due to cost and complexity, resulting in long-lived off-chain interactions with no public verification path [8].

Moreover, the presumption of trustlessness in Lightning collapses under scrutiny, as the system depends on watchtower services, channel monitoring, and timely access to dispute resolution mechanisms—all of which reintroduce points of failure and surveillance that Bitcoin was explicitly constructed to avoid [25]. In practice, these systems cannot be guaranteed across jurisdictions, time zones, and edge cases, further detaching Lightning's model from the base layer's universal auditability.

Lightning's inability to offer immutable, timestamped records of transaction flow not only undermines the security model but invalidates its use as a forensic or regulatory tool. The economic and legal viability of a payment system hinges on deterministic traceability and non-repudiation—requirements Lightning fails to meet by design. Thus, Lightning does not enhance Bitcoin's cash properties; it contradicts them.

4.4 Disconnection from Base Layer Security and Auditability

The Lightning Network introduces a structurally separate transaction environment that undermines the fundamental auditability and security guarantees of Bitcoin. Unlike a true layered solution, Lightning operates independently of the base protocol, circumventing the transparency and immutability assured by proof-of-work validation [42]. This detachment compromises verifiability: transactions executed off-chain are not secured by the global network consensus, but by bilateral state agreements between participants, exposing them to disputes, fraud, and silent failure without recourse to deterministic finality.

As Carotti et al. demonstrate, economic actors within Lightning channels are motivated by rational fee-seeking behaviour, not by network robustness [8]. Combined with the operational necessity of watchtowers, timing constraints, and monitoring agents, Lightning embeds layers of conditional trust, in stark contrast to the non-intermediated and timestamped assurances of on-chain Bitcoin. The result is a system that bypasses the original intent of a cash protocol that guarantees integrity through public validation [29].

Furthermore, the assumption that Lightning can be supervised or verified retroactively through optional base-layer settlement is flawed. As Macharia et al. observe, experimental overlays detached from base-ledger finality inhibit public accountability and forensic transparency [25]. Lightning thus devolves into a private, selectively visible payment scheme that forfeits the legal and technical reliability Bitcoin is premised upon. The system's detachment is not a scaling solution; it is a departure.

4.5 The Abstraction of Utility: Framing Lightning as Settlement Without Finality

The Lightning Network has been promoted as a high-throughput "settlement layer" to address Bitcoin's perceived scalability limits. However, this conceptualisation detaches utility from the fundamental notion of settlement finality inherent to Bitcoin's design. Settlement on Bitcoin, as outlined by [29], is not merely transactional throughput—it is irrevocability bound to block confirmation. Lightning introduces a counterparty-dependent system where finality is contingent on cooperation or punitive channel closure, not cryptographic proof.

This creates an abstraction that undermines Bitcoin's original proposition as digital cash [35]. As [8] argue, rational actors in the Lightning Network may engage in behaviours that maximise liquidity availability without actually completing transfers on-chain. This fosters a pseudo-settlement economy where transaction finality becomes economically optional. Moreover, as [42] demonstrates, this abstraction distorts incentives and introduces layers of uncertainty that cannot be reconciled with the deterministic framework envisioned for Bitcoin's base layer.

Thus, what is claimed as "settlement" becomes a linguistic sleight-of-hand: an economic ritual absent the definitive anchoring of on-chain resolution. This discursive inflation of capabilities reflects broader marketing narratives in cryptocurrency that detach claims from architectural substance [37]. The result is not just conceptual confusion, but structural misallocation of capital and degraded systemic integrity.

5 Misconstruing Network Value: Metrics, Liquidity, and Market Fictions

This section dissects the misrepresentation of the Lightning Network's economic viability through misleading metrics. While proponents assert that LN reflects scalable liquidity and transactional efficiency, the actual topology and functionality betray this narrative. Capacity is conflated with utility, routing is idealised despite failure rates, and network liquidity is marketed without acknowledging directional imbalance, fragmentation, or lock-in. This misrepresentation distorts market perception and enables ideological promotion devoid of operational truth.

5.1 Liquidity Theatre: Channel Capacity and Misrepresented Spendability

The Lightning Network's reported liquidity is structurally misleading. Most public metrics report gross channel capacity across the network but neglect economic usability. Liquidity is not fungible across the network: it is path-constrained, fragmented, and directionally limited.

Channels may remain open indefinitely with inactive balances or require rebalancing that is economically unviable. Metrics platforms such as 1ML and Amboss fail to disclose actual spendability conditions, misleading analysts and investors alike.

Empirical analyses have demonstrated that declared liquidity does not equate to economic throughput. Gritschla et al. [16] document the inert nature of stale channels and highlight topological imbalance. Zabka et al. [44] show that centrality and liquidity concentration skew network access and exacerbate routing asymmetries. IoT payment trials on LN further demonstrate structural fragility in sparse or unbalanced states [23]. Kumble and Roos [24] evaluate how different routing clients exhibit inconsistent success rates across similar paths, undermining claims of robust liquidity. Finally, Seo and Kim [36] show that aggregation techniques designed to improve throughput are limited by the fundamental liquidity fragmentation of LN's architecture. Together, these studies reveal that LN's public liquidity claims are theatrical illusions rather than economic truths.

5.2 Liquidity Centralisation: Economic Failure of Decentralised Assumptions

The core narrative promoting the Lightning Network (LN) as a decentralised scaling solution collapses under empirical scrutiny. Despite theoretical claims of peer-to-peer balance, actual liquidity provisioning on LN is dominated by a handful of well-funded hubs that perform de facto custodial functions. These liquidity centres—often operated by exchanges, fintechs, or intermediated service layers—distort the topology and negate decentralised network assumptions. Empirical data show that the majority of routing activity, payment volume, and reliable throughput is processed through a small set of privileged nodes, whose dominance increases as payment volume scales [45].

This centralisation yields compounding fragility. As noted by Gritschla et al., once a node acquires routability dominance, users preferentially establish channels with it, reinforcing its power and disincentivising participation in more peripheral nodes [16]. The resulting network resembles a payment cartel rather than a trustless mesh. Furthermore, Kumble and Roos [24] demonstrate that routing heuristics and fee structures are optimised around these

supernodes, leading to effective path centralisation even when topological alternatives exist. Such configurations introduce single points of economic failure, as shocks to dominant nodes disproportionately affect network-wide payment viability.

The result is not decentralised liquidity but a tiered system where only well-funded actors provide reliable access. Far from embodying Bitcoin's original model of distributed control and user-level verification, LN substitutes this with systemic trust in liquidity overlords—creating a paradoxical dependency on entities that the base protocol was designed to eliminate.

5.3 Scaling Pathologies: Capital Lock-Up and Throughput Constraints

Contrary to marketing narratives, the Lightning Network (LN) imposes severe throughput limitations due to its structural reliance on locked capital and bounded channel liquidity. While theoretically capable of facilitating numerous off-chain transactions, each channel must be pre-funded with sufficient liquidity in both directions to ensure routing success. This design creates systemic inefficiencies in capital utilisation. Funds are immobilised across the network not for yield or productive deployment, but merely to sustain potential transaction pathways [36].

As Fabi's analysis on blockchain latency shows, LN introduces a paradox: the more participants join, the more fragmented the liquidity landscape becomes, increasing payment failure rates and network friction [13]. Attempts to mitigate these effects—such as circular rebalancing, dual-funded channels, and aggressive fee tuning—often backfire, introducing even greater complexity and cost. Moreover, simulations and empirical evaluations confirm that overall payment success does not scale linearly with node count, especially under realistic fee and balance constraints [24].

This creates what can be termed a scaling pathology: increased user adoption degrades network efficiency, necessitating greater central coordination or external liquidity injections. Such a system deviates sharply from the autonomous, permissionless scalability envisioned in Bitcoin's original protocol design [29]. The Lightning Network's inherent throughput

ceiling, liquidity dependency, and adverse scaling profile render it structurally incapable of supporting global digital cash functionality.

5.4 Custodial Gravity and Structural Centralisation

The Lightning Network, in its architectural and economic implementation, creates gravitational pull toward custodial infrastructure. This pull is not merely a by-product of convenience but a structural necessity born from its capital inefficiencies, routing fragility, and liquidity fragmentation. Custodial wallets like Wallet of Satoshi, Strike, and BlueWallet dominate usage precisely because they eliminate the friction endemic to self-hosted LN interaction—replacing protocol guarantees with trust-based abstractions that contradict the Bitcoin model of non-intermediated cash transfers [42].

Studies including Kumble and Roos's comparative routing client analysis demonstrate how reliance on liquidity hubs and pathfinding heuristics scales poorly and centralises network architecture [24]. The inability of users to reliably open, maintain, and rebalance channels on their own results in consolidation into large, well-capitalised intermediaries, effectively reinventing the financial system LN claims to disrupt. These custodians increasingly mediate Lightning payments off-chain, storing user balances in internal ledgers, and only occasionally interfacing with the actual LN protocol.

This leads to two-layered centralisation: economic (control of liquidity and routing) and technical (channel and node management). Far from disintermediating finance, LN introduces new opaque intermediaries whose incentives are not aligned with user sovereignty or Bitcoin's design as digital cash. As Wright has shown mathematically, the Lightning Network's need for external liquidity provision and non-settled IOUs structurally decouples it from Bitcoin's ledger-based trust model, collapsing peer-to-peer guarantees into proxy banking [42].

5.5 Narrative Engineering: Lightning as Marketing Veneer

The institutional and popular embrace of the Lightning Network (LN) has not been driven by technical merit or empirical performance, but by a concerted effort to engineer narratives

that preserve BTC's stagnation as a virtue. The portrayal of LN as a triumphant Layer 2 innovation serves as a rhetorical smokescreen for the refusal to scale the base layer—a refusal justified through misrepresentation of economic principles and technical feasibility [32]. Rather than enabling mass adoption, LN diverts attention from the base protocol's incapacity to process global transaction volume under hard-coded constraints.

Promotional material, especially in nation-state contexts like El Salvador, frames LN as functional without disclosing the underlying custodial mechanics or user friction. Research by Pecis et al. reveals that trust in LN is maintained not through performance, but through ideological reinforcement and selective visibility of success cases. Similarly, Whitford and Anderson identify a pattern in crypto governance whereby infrastructural decay is masked by appeals to decentralisation and innovation narratives [41]. This discursive reinforcement of LN as a solution rather than a patch deflects scrutiny and enables its positioning in policy, media, and speculative investment.

Wright has demonstrated that this divergence between rhetoric and architecture is not accidental but constitutive: LN is not designed to scale Bitcoin, but to defend BTC's low-throughput architecture under a guise of innovation [42]. Its systemic failure is thus not a bug—it is the feature that allows BTC to remain ideologically static while appearing progressive. The result is a simulacrum of scalability: a non-functional mythology that serves institutional interests while degrading Bitcoin's original purpose.

6 Market Illusion and Media Narrative

BTC no longer derives its market capitalisation from functionality but from the systematic construction of narratives designed to overwrite the original purpose of Bitcoin. In place of a functional micropayment system, BTC is marketed as "digital gold," a store of value unencumbered by usage constraints, despite its systemic failures to support day-to-day transactions. This section demonstrates that BTC's value is not anchored in economic use but in linguistic appropriation, institutional reinforcement, and investor-facing rhetoric that disguises technological stagnation as intentional design. The economic and semiotic strategy behind BTC's illusion of utility is dissected across media, regulation, and market practice.

6.1 The Substitution of Narrative for Function

The redefinition of Bitcoin away from digital cash to a deflationary store of value was not an organic evolution but a deliberate discursive shift. The phrase "peer-to-peer electronic cash" has been actively suppressed in promotional and institutional literature in favour of terms like "digital gold." This rhetorical displacement masks structural failure: transaction fees remain volatile, block space is limited by policy, and the system's inability to support micropayments contradicts its original function [35, 5]. Proponents cite scarcity as value, yet this overlooks essential monetary characteristics—fungibility, divisibility, and transactional accessibility. The substitution of function for myth creates a system where belief substitutes for utility, and volatility becomes a feature rather than a flaw [40, 32]. The strategic omission of use-case capability permits the perpetuation of an asset whose only success is narrative control.

6.2 Misclassification and Regulatory Evasion

BTC-based Lightning wallets are routinely marketed as "non-custodial" despite their actual operational model reflecting custodial architecture. Services such as Strike and Wallet of Satoshi require pooled liquidity, centralised control over key management, and user reliance on internal ledgers—replicating the very intermediated financial structure Bitcoin was designed to displace [42, 39]. These services disguise their architecture behind technical terminology, creating ambiguity that regulators are often ill-equipped to unravel.

This misclassification leads to both under-regulation and user misinformation. Apparent adherence to decentralisation is belied by custodial practices that nullify user sovereignty. The illusion of non-custodianship not only undermines regulatory clarity but creates systemic legal arbitrage, wherein custodial entities avoid oversight by merely rebranding their service layer [27, 41]. The practical result is user exposure to institutional counterparty risk under the veneer of decentralised independence. Such deliberate rhetorical engineering perpetuates the BTC narrative of trustless systems while surreptitiously reinstating centralised control.

6.3 Narrative Substitution: From Peer-to-Peer Cash to Digital Mythology

BTC has displaced the original vision of Bitcoin as digital cash with a mythos centred on "store of value" rhetoric, where transactional throughput, cost, and accessibility are sacrificed for the illusion of scarcity-driven valuation [29, 35]. This narrative shift enables BTC proponents to ignore economic utility, promoting illiquid, speculative holding over transactional functionality. The foundational economic principle of a medium of exchange is thus supplanted by appeals to digital austerity.

The emergence of Lightning Network is cast within this mythology, not as a technical necessity but as narrative scaffolding—used to rationalise BTC's refusal to scale Layer 1 [42, 8]. High transaction costs and delays are reframed as virtues: a mechanism to prevent "spam" rather than evidence of architectural failure. Custodial wallets like Strike and Wallet of Satoshi inherit this mythology, cloaking financial centralisation in the language of freedom. In this way, ideological substitution operates as a mechanism of control, repackaging limitations as features and deflecting scrutiny from BTC's deviation from the Bitcoin protocol's original economic model.

6.4 The Illusion of Scalability: Misusing Layer 2 to Mask Economic Failure

The promotion of the Lightning Network as a scalability solution functions primarily as a public relations mechanism, not a technical resolution. While marketed as a Layer 2 system, LN is structurally decoupled from Bitcoin's base chain and fails to deliver sustained throughput, reliability, or accessibility [42, 38]. Its architectural dependency on capital lock-up, fragile routing paths, and hub-based liquidity undermines any claim to decentralised scaling. Despite these constraints, LN is cited by institutional actors to justify BTC's incapacity to scale Layer 1—a deflection that facilitates the maintenance of BTC's restricted protocol limits.

Economic analyses demonstrate that LN fails to offer proportional throughput gains

per additional user [36, 24]. Liquidity exhaustion, indirect routing failures, and reliance on centralised custodians negate any cost-efficiency advantages. Meanwhile, off-chain settlement erodes the auditability and security that originally underpinned Bitcoin's value proposition. The mythology of LN scalability is thus a facade: its real function is to obscure BTC's abandonment of the original design, all while enabling speculation and narrative control.

6.5 Confusion as Strategy: Custodial Wallets Masquerading as Non-Custodial

BTC advocates frequently conflate custodial Lightning wallets with non-custodial applications, obfuscating the erosion of user agency and traceability. Wallets such as Wallet of Satoshi, Strike, and others operate under centralised control, often without user-held keys, relying on internal ledger updates to simulate Lightning transactions [39, 27]. This misrepresentation serves to bolster the illusion that BTC remains aligned with Bitcoin's original peer-to-peer architecture, despite effectively restoring the intermediated model of financial control.

Such wallets introduce traditional banking trust dependencies, negating the fundamental purpose of cryptographic financial sovereignty. Regulatory arbitrage becomes possible as providers hide custodianship behind technical jargon and UI sleight-of-hand [42]. Users unknowingly surrender control, subject to blacklisting, censorship, and surveillance—all while believing they are using a system with no intermediaries. The confusion is not incidental but essential: it preserves the BTC narrative and secures institutional comfort while betraying the core protocol promises.

7 Implications for Regulation and Economics

BTC's adoption in legal frameworks as "Bitcoin" introduces systemic risk:

- Custodial Lightning exposes users to counterparty risk without protection.
- Obfuscated routing undermines anti-money laundering enforcement.

- Economic models assuming BTC utility are based on false technical premises.
- Policy recommendations grounded in BTC's structure misunderstand Bitcoin's original function and potential.

7.1 Misidentification of BTC in Legal Definitions

The incorporation of BTC into legislative and policy frameworks under the label "Bitcoin" constitutes a misclassification with significant regulatory consequences. Statutory language and jurisprudence often refer to Bitcoin as a decentralised cash system, yet what is codified reflects the economic and structural properties of BTC—an asset marked by high volatility, limited throughput, and extensive custodial exposure. The use of this misidentification affects tax rulings, monetary designation, and the enforcement of securities laws, all while excluding the architectural foundations originally established in [29]. As Otabor-Olubor [30] outlines, interpretive divergence in cryptocurrency taxonomies drives institutional errors. Whitford and Anderson [41] further note that regulatory frameworks struggle to keep pace with evolving technical substrates. Economic confusion results: monetary designations are applied to deflationary, speculative tokens incapable of acting as money. The mislabeling has redefined Bitcoin not as a micropayment system, but as a speculative instrument backed by rhetorical scarcity.

7.2 Custodial Systems and Counterparty Risk

BTC's integration of Lightning Network custodial wallets introduces direct counterparty exposure, reviving the trust dependencies Bitcoin originally sought to eliminate. Unlike SPV or direct base-layer interaction, systems such as Wallet of Satoshi, Strike, or custodial LN hubs require users to forfeit private key control and accept IOU-based accounting within closed ledgers. This introduces banking-like risk profiles without accompanying consumer protection mechanisms. As noted by Wright [42], such architectures reflect economic centralisation hidden beneath a façade of decentralisation. The systemic risk is compounded as these custodial actors remain unregulated in many jurisdictions, exposing users to service termination, withdrawal freezes, or legal seizure without recourse.

Regulatory frameworks treating these entities as mere "wallets" rather than financial custodians enables loopholes in KYC, AML, and fiduciary compliance obligations. Brekke [6] outlines how such architectures realign economic agency around centralised cryptoeconomic engineers, reintroducing the very trust asymmetries Bitcoin's original white paper explicitly eliminated [29]. This misclassification affects monetary velocity, introduces opacity in settlement finality, and collapses the auditability advantages of blockchain-based systems. Such economic misalignment demands reassessment in regulatory architecture.

7.3 Opacity and Enforcement: Obfuscated Routing and AML Failures

The Lightning Network's routing architecture introduces inherent opacity, frustrating anti-money laundering (AML) enforcement and regulatory traceability. HTLC-based routing, multi-hop anonymisation, and the absence of persistent ledger entries for payments undermine standard compliance frameworks that depend on end-to-end visibility of transactions. Unlike Layer 1 blockchain settlements, Lightning payments are not permanently recorded, creating an environment where illicit transfers can avoid detection under the pretext of privacy and efficiency [14, 45].

This structural design raises profound issues for both legal enforcement and macroeconomic surveillance. As noted by Whitford and Anderson [41], effective governance mechanisms over emergent technologies rely on accurate classification and observability. By misidentifying BTC transactions as being on-chain when routed through Lightning, regulatory oversight is bypassed unintentionally or by design. Cai et al. [7] demonstrate how off-chain scaling techniques, while technically appealing, demand a different enforcement framework—one BTC advocates avoid acknowledging. This not only hampers enforcement efforts but also distorts cost models, market assumptions, and broader economic analytics.

AML, fraud prevention, and tax compliance mechanisms fail when transactional trails are intentionally obfuscated. Lightning undermines these functions while posing as a scaling innovation, creating a dual-layered risk profile: invisible systemic threat and public regulatory misdirection.

7.4 Faulty Economic Models Built on Technical Misconceptions

Mainstream economic analysis often adopts assumptions about BTC's scalability, transaction throughput, and security that do not hold when scrutinised against the protocol's actual functionality. Models treating BTC as an efficient means of exchange ignore the reliance on off-chain solutions like Lightning Network, whose scalability is bounded by liquidity lock-in, custodial concentration, and low routing reliability [13, 44, 46]. These assumptions create flawed projections of network efficiency, adoption rates, and long-term fee sustainability.

Wright [42] has shown that the economic behaviour of participants within BTC diverges radically from the rational-agent assumptions in classical monetary theory, given the strategic use of custodians, frozen balances, and arbitrarily high confirmation delays. Moreover, as Cole et al. [11] demonstrate, the true economic value of Bitcoin-based transactions diminishes when trust assumptions are reinstated via intermediaries.

Layer 2 projections often assume near-zero marginal cost and linear scalability, violating empirical observations. Sarenche et al. [34] illustrate that mempool behaviour and volatile block rewards complicate throughput, while Fabi's latency trade-offs [13] expose critical inefficiencies in managing demand surges. These misalignments corrupt macroeconomic analyses and affect national and global policymaking where BTC is misclassified as a functional payments infrastructure.

7.5 Misaligned Policy: Substituting Ideology for Economic Evidence

Policy built on BTC often inherits ideological assumptions instead of empirical foundations. Regulatory proposals referencing "Bitcoin" routinely adopt BTC's constraints—artificially small block sizes, irreversible transaction finality assumptions, and Layer 2 dependence—as if they were innate to all instantiations of the protocol. This conflation results in legislation, tax rulings, and compliance frameworks that favour custodial intermediaries, undercutting the potential of traceable, enforceable digital cash systems.

Azouvi [4] and Pecis et al. [32] document how regulatory frameworks have been shaped by discourse steeped in decentralisation myths and narratives of trustless networks. When

systems like BTC obfuscate control through pseudo-decentralised custodianship and marketing sleight, regulators misjudge risk, classifying pseudo-banks as peer-to-peer systems. Whitford and Anderson [41] further show how such errors create governance landscapes that distort innovation, misallocate public trust, and delay the maturation of effective oversight.

The result is policy failure: stable regulatory environments are compromised by the incoherence between technology and its perceived properties. Misidentification leads to failure in tax treatment, consumer protection, anti-money laundering, and cross-border enforcement—reinforcing systemic fragility where economic integrity is most required.

8 Conclusion: The Coming Correction

BTC is not Bitcoin. It is a structurally limited system propped up by marketing, not merit. Its inability to scale, dependence on a separate non-Layer 2 solution, and abandonment of core principles ensure it cannot deliver what it promises. When utility is repriced into markets, the divergence will collapse.

8.1 Reasserting Technical and Economic Findings

This paper has demonstrated, in explicit technical and economic terms, that BTC diverges from Bitcoin not merely in implementation, but in fundamental purpose. The original system, defined clearly by Nakamoto [29], was intended as peer-to-peer digital cash: scalable, low-cost, traceable, and enforceable. BTC abandoned this path. By imposing artificial block size constraints and externalising transaction volume to the Lightning Network—shown here to be neither Layer 2 nor compatible with the protocol's economic assumptions—BTC removed itself from viability as a transactional system.

Empirical data from Lightning Network architecture [44, 24] has confirmed its structural reliance on intermediated liquidity hubs, its routing failures, and its unsuitability for economic scaling. The result is a return to custodial infrastructure, undermining both traceability and the foundational trust model. Section 5 exposed that BTC's narrative has replaced utility: myths of scarcity, "digital gold", and protocol sanctity substitute for throughput, performance, and transactional integrity. Regulatory risk, systemic confusion, and a collapse

in economic coherence follow.

By integrating studies in cryptographic implementation [20], scaling economics [13, 9], and policy exposure [41, 4], this paper repositions Bitcoin as a protocol rooted in function, not fantasy. BTC is a deviation—a high-volatility, low-utility asset promoted through abstraction. It is not sustainable. Correction is not only inevitable—it is necessary.

References

[1] A. Ahmad, M. Saad, M. Al Ghamdi, D. Nyang, and D. Mohaisen. Blocktrail: A service for secure and transparent blockchain-driven audit trails. *IEEE Systems Journal*, 16(1):1367–1378, 2021.

[2] C. M. Allen and D. G. Chamberlain. Lost and found coins: Cryptocurrency chain splits in australia. In *Australian Tax Forum*, volume 38, pages 509–542, Sydney, NSW, 2023. Tax Institute.

[3] D. W. Allen, C. Berg, A. M. Lane, and J. Potts. Daos are adaptive governance engines. *Available at SSRN*, 2024.

[4] S. Azouvi. *Levels of decentralization and trust in cryptocurrencies: consensus, governance and applications*. Doctoral dissertation, University College London, 2021.

[5] D. G. Baur and T. Dimpfl. The volatility of bitcoin and its role as a medium of exchange and a store of value. *Empirical Economics*, 61(5):2663–2683, 2021.

[6] J. K. Brekke. Hacker-engineers and their economies: The political economy of decentralised networks and 'cryptoeconomics'. *New Political Economy*, 26(4):646–659, 2021.

[7] T. Cai, W. Chen, K. E. Psannis, S. K. Goudos, Y. Yu, Z. Zheng, and S. Wan. On-chain and off-chain scalability techniques. In *Blockchain Scalability*, pages 81–96. Springer Nature Singapore, Singapore, 2023.

[8] A. Carotti, C. Sguanci, and A. Sidiropoulos. Rational economic behaviours in the

bitcoin lightning network. In *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 594–601. IEEE, 2024.

[9] B. Chen, L. Ma, H. Xu, J. Ma, D. Hu, X. Liu, and K. Li. A comprehensive survey of blockchain scalability: Shaping inner-chain and inter-chain perspectives. `https://arxiv.org/abs/2409.02968`, 2024.

[10] R. H. Coase. The nature of the firm. *Economica*, 4(16):386–405, 1937.

[11] B. M. Cole, A. H. Dyhrberg, S. Foley, and J. Svec. Can bitcoin be trusted? quantifying the economic value of blockchain transactions. *Journal of International Financial Markets, Institutions and Money*, 79:101577, 2022.

[12] T. K. Dasaklis and V. Malamas. A review of the lightning network's evolution: Unraveling its present state and the emergence of disruptive digital business models. *Journal of Theoretical and Applied Electronic Commerce Research*, 18(3):1338–1364, 2023.

[13] M. Fabi. Latency tradeoffs in blockchain capacity management. Technical Report 2024-10, Center for Research in Economics and Statistics, 2024.

[14] J. Garay, A. Kiayias, and N. Leonardos. The bitcoin backbone protocol: Analysis and applications. *Journal of the ACM*, 71(4):1–49, 2024.

[15] F. Grötschla, L. Heimbach, S. Richner, and R. Wattenhofer. On the lifecycle of a lightning network payment channel. *arXiv preprint arXiv:2409.15930*, 2024.

[16] F. Grötschla, L. Heimbach, S. Richner, and R. Wattenhofer. On the lifecycle of a lightning network payment channel. *arXiv preprint arXiv:2409.15930*, 2024.

[17] F. A. Hayek. The use of knowledge in society. *The American Economic Review*, 35(4):519–530, 1945.

[18] D. M. Herold, S. Saberi, M. Kouhizadeh, and S. Wilde. Categorizing transaction costs outcomes under uncertainty: a blockchain perspective for government organizations. *Journal of Global Operations and Strategic Sourcing*, 15(3):431–448, 2022.

[19] H. J. Hong, S. Y. Chang, W. Fan, S. Wuthier, and X. Zhou. Secure and efficient authentication using linkage for permissionless bitcoin network. *Computer Networks*, 254:110840, 2024.

[20] A. Jain and E. S. Pilli. Sok: Digital signatures and taproot transactions in bitcoin. In *International Conference on Information Systems Security*, pages 360–379, Cham, 2023. Springer Nature Switzerland.

[21] B. A. Jones, A. L. Goodkind, and R. P. Berrens. Economic estimation of bitcoin mining's climate damages demonstrates closer resemblance to digital crude than digital gold. *Scientific Reports*, 12(1):14512, 2022.

[22] D. Khan, L. T. Jung, and M. A. Hashmani. Systematic literature review of challenges in blockchain scalability. *Applied Sciences*, 11(20):9372, 2021.

[23] M. Kim, K. Kim, and J. H. Kim. Cost modeling for analyzing network performance of iot protocols in blockchain-based iot. *Human-centric Computing and Information Sciences*, 11, 2021.

[24] S. P. Kumble and S. Roos. Comparative analysis of lightning's routing clients. In *2021 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, pages 79–84. IEEE, 2021.

[25] D. Macharia, A. Kara, and A. Jabbar. Distributed ledger technology niches and experimentation in central banks payment systems functions: A thematic analysis. *Available at SSRN 5275486*, 2025.

[26] M. Malempati. Leveraging cloud computing architectures to enhance scalability and security in modern financial services and payment infrastructure. *European Advanced Journal for Science & Engineering (EAJSE)*, 2(1), 2024.

[27] U. Milkau. What are (payment) intermediaries good for? *Journal of Payments Strategy & Systems*, 17(2):115–129, 2023.

[28] L. Mishra and V. Kaushik. Application of blockchain in dealing with sustainability issues and challenges of financial sector. *Journal of Sustainable Finance & Investment*, 13(3):1318–1333, 2023.

[29] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. `https://bitcoin.org/bitcoin.pdf`, 2008.

[30] I. Otabor-Olubor. Critical reflections on the interpretive divergence of decentralised cryptocurrencies. *SSRN Electronic Journal*, 2021. Available at SSRN 4945730.

[31] I. Otabor-Olubor. Critical reflections on the interpretive divergence of decentralised cryptocurrencies. `https://ssrn.com/abstract=4945730`, 2024.

[32] L. Pecis, L. Cervi, and L. Introna. In blockchain we trust: Ideologies and discourses sustaining trust in bitcoin. *Information and Organization*, 35(2):100573, 2025.

[33] B. Sambana. Blockchain technology: Bitcoins, cryptocurrency and applications. `https://arxiv.org/abs/2107.07964`, 2021.

[34] R. Sarenche, A. Aghabagherloo, S. Nikova, and B. Preneel. Bitcoin under volatile block rewards: How mempool statistics can influence bitcoin mining. `https://arxiv.org/abs/2411.11702`, 2024.

[35] V. Selvam. 10. a store of value. In *Principles of Bitcoin*, pages 146–159. Columbia University Press, 2025.

[36] J. Seo and J. Kim. Enhancing scalability with payment requests aggregation in lightning network. In *2022 IEEE International Conference on Blockchain (Blockchain)*, pages 340–347. IEEE, 2022.

[37] O. Sewell, L. Robb, and J. Flood. Asset, token, or coin? a semiotic analysis of blockchain language. *International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique*, 37(1):1–35, 2024.

[38] H. Song, Z. Qu, and Y. Wei. Advancing blockchain scalability: An introduction to layer 1 and layer 2 solutions. In *2024 IEEE 2nd International Conference on Sensors, Electronics and Computer Engineering (ICSECE)*, pages 71–76. IEEE, 2024.

[39] J. T. G. Swambo. Evolving bitcoin custody. `https://arxiv.org/abs/2310.11911`, 2023.

[40] John Taskinsoy. Bitcoin: A new digital gold standard in the 21st century? `https://ssrn.com/abstract=3941857`, 2021.

[41] A. B. Whitford and D. Anderson. Governance landscapes for emerging technologies: The case of cryptocurrencies. *Regulation & Governance*, 15(4):1053–1070, 2021.

[42] C. S. Wright. The autonomy of the lightning network: A mathematical and economic proof of structural decoupling from btc. *arXiv preprint arXiv:2506.19333*, 2025.

[43] C. S. Wright. Formal security analysis of spv clients versus home-based full nodes in bitcoin-derived systems. `https://arxiv.org/abs/2506.01384`, 2025.

[44] P. Zabka, K. T. Foerster, S. Schmid, and C. Decker. Empirical evaluation of nodes and channels of the lightning network. *Pervasive and Mobile Computing*, 83:101584, 2022.

[45] P. Zabka, K. T. Förster, C. Decker, and S. Schmid. A centrality analysis of the lightning network. *Telecommunications Policy*, 48(2):102696, 2024.

[46] H. N. D. Şenyapar. Cryptocurrency on social media: Analyzing the digital discourse towards the coin market. *İktisadi İdari ve Siyasal Araştırmalar Dergisi (İKTİSAD)*, 9(23):202–223, 2024.