UNIVERSITÀ POLITECNICA DELLE MARCHE

FACOLTÀ DI ECONOMIA “GIORGIO FUÀ”

Corso di Laurea triennale in

Digital Economics and Business

Beyond Fiat: Decentralized Ideals and the Hybrid Future of Money

Relatore:

Prof. Francesco James Mazzocchini

Rapporto Finale di:

Leonardo Calcabrini

Anno Accademico 2025/2026

INDEX

Introduction

The modern financial system, built on state-managed fiat currency and fractional reserve banking, faced a crisis of confidence following the 2008 global financial collapse. This event catalyzed the search for decentralized alternatives, leading to the birth of the cryptocurrency movement. The purpose of this thesis is to analyze the evolution of digital money, evaluating the structural and economic trade-offs between traditional fiat systems, decentralized networks like Bitcoin, the institutional response of Central Bank Digital Currencies (CBDCs), and the market compromise of stablecoins.

The work is structured as follows:

Chapter 1 examines the foundational pillars of the traditional financial system and its inherent reliance on trust. It explores the ideological origins of the Cypherpunk movement and Satoshi Nakamoto's introduction of Bitcoin as a peer-to-peer solution to the double-spending problem and financial intermediation.

Chapter 2 dissects the technical architecture of Bitcoin, focusing on the Proof-of-Work consensus mechanism and the UTXO model. It analyzes how Bitcoin's perfectly inelastic supply creates a censorship-resistant "digital gold" but also results in the extreme volatility that hinders its use as a daily medium of exchange.

Chapter 3 provides a structural comparison between Central Banks and the Bitcoin network. It analyzes the rise of CBDCs as a sovereign counter-model designed to co-opt blockchain technology to preserve monetary control, highlighting the ethical tensions between individual privacy and state surveillance.

Chapter 4 investigates stablecoins as the connective tissue between the crypto-economy and fiat systems. Through the "Stablecoin Trilemma," it evaluates the risks of fiat-collateralized models, such as USDT, and the catastrophic collapse of algorithmic systems like Terra-Luna.

Finally, the Final Conclusions synthesize the findings by discussing the "Paradox of Retail Adoption". It argues that the market's reliance on centralized intermediaries suggests a hybrid future where blockchain technology upgrades, rather than replaces, the traditional financial order.

Chapter 1 – The Birth of Decentralized Finance and Bitcoin

1.1. Fiat Currency, Central Banks, and Their Criticisms

The architecture of the modern financial system is built upon an intricate, state-managed framework. To analyze the systemic vulnerabilities that prompted the search for alternatives, it is first necessary to define its three foundational pillars: the fiat monetary model, the institutional role of central banks, and the credit-creation mechanism of fractional reserve banking.

Fiat Money is a currency that a government has declared to be legal tender, but it is not backed by a physical commodity, such as gold or silver. Unlike commodity-backed money, its value is not intrinsic; rather, it is derived from two primary sources: the authority of the government that decrees it as legal tender for all debts, public and private, and the collective trust placed in the stability of that government and its managing institutions. Its supply is not constrained by the availability of a physical asset, which allows the central monetary authority to manage it elastically (expanding or contracting it) to meet, in theory, the needs of the economy and manage business cycles.

Central Banks are the apex institutions charged with managing a nation's (or a monetary union's) fiat currency and the broader monetary system. Their primary mandates typically revolve around two cores, and sometimes conflicting objectives: ensuring price stability and maintaining financial stability. To achieve these goals, central banks possess several critical functions: they hold the monopoly on the issuance of legal tender (base money), they implement monetary policy primarily by setting benchmark interest rates and managing the money supply through open market operations, they supervise and regulate commercial banks, and they act as the lender of last resort to provide emergency liquidity to solvent-but-illiquid financial institutions, aiming to prevent systemic collapse.

The Fractional Reserve System is the operational framework through which commercial banks, rather than the central bank, create the majority of the money in the economy (often called "broad money"). In this system, banks are legally required to hold only a fraction of their customer deposits as reserves (either as cash in their vaults or as deposits with the central bank). The remainder of the deposits can be loaned out to other borrowers. This process of lending is the fundamental mechanism of credit creation. When a bank issues a loan, it does so by creating a new deposit in the borrower's account. This act simultaneously creates a new asset (the loan) and a new liability (the deposit) on the bank's balance sheet, effectively expanding the total money supply. This system is inherently leveraged, as the total volume of deposits (money) is a multiple of the actual "base money" reserves.

This architecture, composed of these three pillars, is fundamentally a "trust-based" model. The system's critical vulnerability, therefore, is the very necessity of this trust. Users must trust that central banks will not debase the currency, that commercial banks will act as prudent stewards of their deposits, and that the system will execute their transactions without censorship or counterparty risk. The traditional infrastructure for payments, particularly for cross-border transactions, has been documented as notoriously inefficient. The World Bank (2023), in its Remittance Prices Worldwide reports, consistently documents the global average cost of sending remittances as remaining stubbornly high (hovering above 6%), with banks being the most expensive channel, often charging in excess of 10% (World Bank, 2023).

This high-friction environment is not limited to cost. Adrian & Mancini-Griffoli (2021) analyze these deep-seated inefficiencies, identifying the high costs, slow settlement times (often taking days), and lack of financial inclusion in legacy systems as the primary drivers creating a potent demand for new forms of digital money. Their analysis suggests that the market itself was seeking a technological solution to the practical failures of the incumbent trust-based model, even before the 2008 crisis brought its solvency into question. This simmering discontent with the system's inefficiencies and its foundational reliance on fallible intermediaries was catalyzed into a full-blown crisis of confidence by the global financial crisis of 2008. The crisis served as a catastrophic failure analysis of the trust-based model, exposing systemic moral hazard and fragility. This event triggered a profound "weakening trust in the existing financial structure" and spurred a search for assets that were not correlated with the traditional system (Guesmi et al., 2019). The crisis, therefore, provided the immediate, real-world justification for a system designed to operate without the very intermediaries who had just failed.

1.2. The Ideological Quest for Decentralized Cash

The invention of Bitcoin was not an isolated event, nor was it merely a response to the 2008 financial crisis. On the contrary, it represents the culmination of decades of ideological and technological research conducted by a movement known as the Cypherpunks. Active primarily in the 1990s, this heterogeneous group of computer scientists, cryptographers, and libertarian activists shared a deep concern for the growing erosion of privacy in the digital age.

The Cypherpunks operated on a fundamental principle: in the face of society's digitalization, the only guarantee for individual liberty lay not in politics, but in cryptography. As famously expressed by Eric Hughes in A Cypherpunk's Manifesto (1993), in an era where private interactions were becoming traceable and permanent, "privacy is necessary for an open society in the electronic age." Theirs was not a purely theoretical opposition; their motto was "Cypherpunks write code."
Their objective was to use strong cryptography to build tools that restored power to the individual, removing it from the centralized control of governments and corporations. Although they initially focused on tools for private communication (such as PGP for encrypted email), they soon understood that true individual autonomy was unattainable as long as the financial system remained a centralized infrastructure of surveillance. The creation of a form of "digital cash"—anonymous, permissionless, and censorship-resistant—thus became one of the central and most technically complex objectives of the movement.

This ideological drive naturally led to the movement's most ambitious objective: the creation of "digital cash." This was envisioned as a form of money that could replicate the peer-to-peer and privacy-preserving properties of physical cash, but in the digital realm. Crucially, to fulfill the Cypherpunk mandate, this system had to function without any central authority, mint, or trusted third party, thereby eliminating the very points of control and surveillance identified in the traditional "trust-based" financial model. This quest was not merely theoretical. As Narayanan

& Clark (2017) meticulously document, Bitcoin did not emerge from a vacuum but was built upon a rich "academic pedigree" of prior attempts. Proposals like Wei Dai's "b-money" (1998) and Nick Szabo's "Bit Gold" (proposed 1998, architected 2005) were sophisticated blueprints for decentralized monetary systems. These concepts introduced crucial elements that would later appear in Bitcoin, such as the use of public-key cryptography for ownership and the idea of a distributed ledger maintained by a network of participants.

However, these precursors ultimately failed to gain traction because they could not provide a practical and robust solution to the most fundamental challenge of any digital monetary system: the "double-spending problem." In the physical world, double-spending is impossible, as one cannot hand the same physical coin to two different people. In the digital world, any piece of data—including a "digital coin"—can be duplicated.

The traditional financial system solves this by interposing a trusted third-party intermediary (a bank or payment processor) to maintain a central ledger. This central authority is the single source of truth that finalizes transactions, ensuring that once a unit of value is spent, it cannot be spent again. This created the central dilemma for the Cypherpunks: how could a decentralized network of untrusted peers collectively agree on a single, canonical history of transactions without a central coordinator? As Narayanan & Clark (2017) note, this was the specific technical hurdle that stalled the digital cash movement. While predecessors like Bit

Gold conceptualized parts of the solution, they did not provide a complete, working mechanism to achieve decentralized consensus, defining the precise problem Satoshi Nakamoto's white paper would soon claim to solve.

1.3. The Genesis of Bitcoin: Objectives and Satoshi Nakamoto’s White Paper

The resolution to the specific technical hurdle that had stalled the digital cash movement arrived on October 31, 2008. On that date, an entity operating under the pseudonym Satoshi Nakamoto published a document titled "Bitcoin: A Peer-to-Peer Electronic Cash System" on the Cryptography Mailing List. This white paper did not merely present a theoretical novelty; it functioned as an operational blueprint designed to bridge the gap between the Cypherpunks' ideological aspirations and technological reality. By directly addressing the double-spending problem that had plagued predecessors like Bit Gold, Nakamoto’s proposal offered a concrete solution to the vulnerabilities of the trust-based model described in previous sections.

As Nakamoto (2008) (Bitcoin: A Peer-to-Peer Electronic Cash System) reveals, the project's foundational objective was the total disintermediation of online commerce. In the document's abstract, the author explicitly defines the goal as the creation of a "purely peer-to-peer version of electronic cash" capable of allowing online payments to be sent directly from one party to another "without going through a financial institution" (Nakamoto, 2008) (Bitcoin: A Peer-to-Peer

Electronic Cash System). This objective was a direct response to the structural reliance on trust identified in the traditional financial architecture. Nakamoto argued that while the existing system functioned well enough for most transactions, it suffered from the "inherent weaknesses of the trust based model," specifically the reversibility of transactions and the mediation costs that made small, casual transactions practically impossible.

Consequently, the solution proposed was to replace the social contract of trust with "cryptographic proof." By utilizing digital signatures and a peer-to-peer network, Bitcoin was designed to allow two willing parties to transact directly without the need for a trusted third party to verify the exchange. This shift aimed to restore the properties of physical cash—such as censorship resistance and finality of settlement—to the digital realm, effectively eliminating the counterparty risk that had been so starkly exposed during the 2008 financial crisis.

While the removal of intermediaries was the philosophical goal, the engineering challenge remained the "double-spending" problem discussed in Section 1.2. As noted previously, without a central authority to maintain a master ledger, there was no established method to prevent a user from spending the same digital token twice. Narayanan & Clark (2017) (Bitcoin's Academic Pedigree) highlight that Nakamoto’s breakthrough was not the invention of entirely new mathematics, but rather the ingenious combination of existing cryptographic tools—such as public-key cryptography and digital signatures—with a novel consensus mechanism. The white paper’s specific answer to double-spending is the implementation of a distributed timestamp server using a Proof-of-Work (PoW) system.

Conceptually, this system replaces the private ledger of a bank with a public chain of transaction blocks, known as the blockchain, which is shared across all nodes in the network. To add a new block of transactions to this chain, network participants, known as miners, must expend significant computational energy to solve a cryptographic puzzle. This requirement creates a tangible cost for modifying the ledger. The network achieves consensus by agreeing to recognize the "longest chain"—that is, the chain with the greatest cumulative proof-of-work—as the single version of the truth. As Nakamoto (2008) (Bitcoin: A Peer-to-Peer Electronic Cash System) explains, this mechanism makes it computationally impractical for an attacker to alter past transactions, as they would need to control more computing power than the entire honest network combined. Thus, the double-spending problem is solved not by the decree of a central administrator, but by the economic and thermodynamic difficulty of falsifying the historical record.

The technological architecture of Bitcoin inherently dictates a specific economic model that contrasts sharply with the fiat monetary system analyzed in Section 1.1. Dwyer (2015) (The Economics of Bitcoin and Similar Private Digital Currencies) provides an economic analysis of this structure, categorizing Bitcoin as a "private digital currency" and emphasizing that its creation and governance occur entirely outside the purview of the state. This classification highlights two distinct economic characteristics derived from Nakamoto's code.

First, the system introduces a fixed and predictable supply schedule, often referred to as digital scarcity. Unlike central banks, which manage the money supply elastically to stabilize prices or respond to economic cycles, Bitcoin's supply is determined by an unchangeable algorithm that caps the total circulation at 21 million units. This design feature makes the currency inelastic, positioning it as a potential hedge against the arbitrary inflation and debasement associated with fiat currencies. Second, Bitcoin eliminates credit risk from the holding of money. In a fractional reserve banking system, a deposit represents a liability of the bank; in contrast, Dwyer (2015) (The Economics of Bitcoin and Similar Private Digital Currencies) notes that Bitcoin functions as a digital bearer asset. Possession of the private cryptographic key grants absolute control over the funds, transforming the nature of money from a credit relationship into a form of direct property ownership. Through these mechanisms, Nakamoto's white paper successfully synthesized the ideological quest of the Cypherpunks with a robust technical framework, launching a new era of decentralized finance.

1.4. Economic and Social Implications of Bitcoin's Genesis

The transition from the theoretical design of the white paper to operational reality occurred on January 3, 2009, when Satoshi Nakamoto mined the first block of the Bitcoin blockchain, known as the "Genesis Block." While the white paper outlined the technical solution to the double-spending problem, the Genesis Block established the project's ideological context. Embedded within the coinbase data of this first block was a hexadecimal string that decoded to the headline from that day’s edition of The Times: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."

As the network began to operate, it presented an immediate taxonomical challenge for economists and regulators. Bitcoin did not fit neatly into existing definitions of money, lacking both the legal tender status of sovereign currency and the physical utility of commodities like gold. Dwyer (2015) (The Economics of Bitcoin and Similar Private Digital Currencies) addresses this ambiguity by analyzing the economic nature of Bitcoin through the lens of monetary theory.

Dwyer (2015) (The Economics of Bitcoin and Similar Private Digital Currencies) argues that while Bitcoin was designed as a medium of exchange ("electronic cash"), its early economic behavior more closely resembled that of a speculative asset or a digital commodity. The protocol’s algorithmic scarcity and fixed supply schedule create a deflationary pressure that encourages hoarding—holding the asset for value appreciation—rather than spending it on goods and services. This dynamic led to significant debate regarding its viability as a unit of account. Dwyer (2015) (The Economics of Bitcoin and Similar Private Digital Currencies) notes that for a currency to be effective, its value must be relatively stable to facilitate trade. Bitcoin's volatility, driven by speculative demand and an inelastic supply, suggested that in its genesis phase, it functioned primarily as a high-risk, high-reward "private digital asset" rather than a stable substitute for fiat money.

While the economic classification remained debated, the social implications of Bitcoin's architecture were immediate and profound. By removing the central intermediary, Bitcoin introduced the concept of "permissionless" finance—a system where access requires no identification, credit check, or approval from a gatekeeper. Luther (2016) (Bitcoin and the Future of Digital Payments) explores this dimension, highlighting how Bitcoin creates a unique value proposition for individuals excluded from the traditional financial system.

Luther (2016) (Bitcoin and the Future of Digital Payments) posits that Bitcoin serves as a crucial alternative mechanism for the "bankless" population and for those living under repressive monetary regimes. In developed economies with stable currencies and robust payment systems, the social utility of Bitcoin might appear limited to privacy enthusiasts. However, Luther (2016) (Bitcoin and the Future of Digital Payments) argues that in scenarios of "monetary regime weakness"—where trust in the local currency has collapsed or where the state enforces strict capital controls—Bitcoin's censorship-resistant nature transforms it from a speculative asset into a vital tool for financial survival. The ability to transfer value globally without reliance on the SWIFT network or correspondent banks effectively democratized access to basic financial services, fulfilling the Cypherpunk vision of separating money from the state.

The evolution of Bitcoin from a cryptographic novelty to a functioning economic network with social utility inevitably drew the attention of global financial authorities. Initially, institutions dismissed the phenomenon as a niche experiment with little impact on the broader economy. However, as adoption grew and the "permissionless" nature of the asset became clear, regulators began to perceive it as a potential disruption to monetary sovereignty.

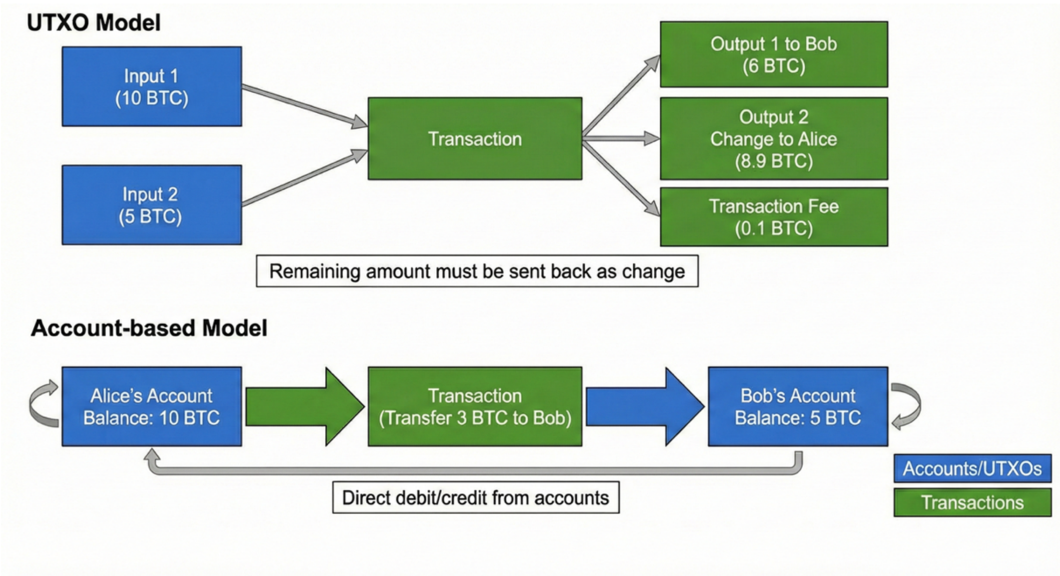
This shift in perception is evident in early institutional literature, such as the reports published by the European Central Bank (ECB) starting in 2012. In these early analyses, the ECB categorized Bitcoin as a "Virtual Currency Scheme," acknowledging for the first time that a non-state actor could issue a digital unit of value. While these reports initially focused on consumer protection and the risks of volatility, they laid the groundwork for a deeper existential realization: that the technology underlying Bitcoin—the Distributed Ledger Technology (DLT)—offered a superior infrastructure for settlement than legacy banking systems. This realization would eventually prompt central banks to move from observation to imitation, catalyzing the research into Central Bank Digital Currencies (CBDCs). Bitcoin's genesis, therefore, did not destroy the central banking model, but it arguably forced it to evolve, marking the beginning of the era of digital monetary competition.

Chapter 2 – The Technical and Economic Functioning of Bitcoin

2.1. Bitcoin Technology: PoW, Cryptography, and Structure

While the first chapter analyzed the ideological and historical trajectory that necessitated a decentralized currency, the robustness of Bitcoin is not rooted in its philosophy, but in its rigid technological architecture. From an analytical perspective, Bitcoin acts as a state-transition machine—a protocol that governs the updating of a shared database without a central administrator. This section dissects the technical mechanisms that allow the network to secure property rights and achieve consensus, shifting the focus from the "why" of decentralization to the specific "how" of its operational execution.

The foundational layer of this architecture is the blockchain, which serves as the distributed public ledger. However, contrary to the intuitive understanding of digital banking, Bitcoin does not utilize an "account-based" model where the ledger tracks the net balance of every user. Instead, as Narayanan et al. (2016) explain, the protocol employs a "Unspent Transaction Output" (UTXO) model.

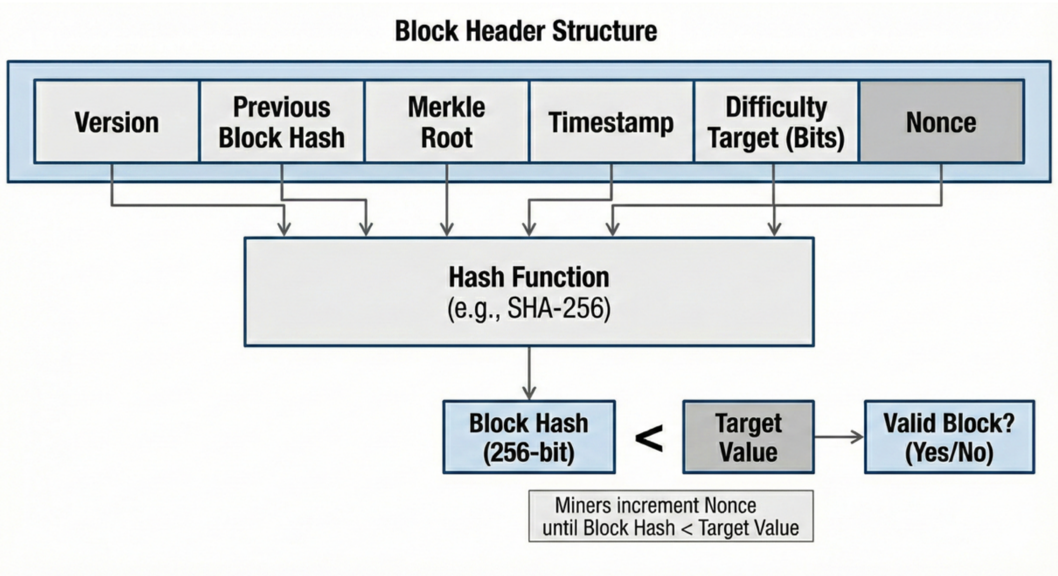


The Unspent Transaction Output (UTXO) transaction model vs. Account-based model. Adapted from Narayanan et al. (2016).

In this framework, the state of the economy is defined exclusively by the set of all currently unspent outputs. A user's "balance" is merely an abstraction derived from the aggregation of all UTXOs they can cryptographically unlock. Technically, a valid transaction consumes one or more existing UTXOs as inputs and creates new UTXOs as outputs. This distinction is critical for the system's auditability: once an output is used as an input in a valid transaction, it is permanently recorded as "spent" and cannot be reused. This creates a transparent, unbroken chain of ownership for every unit of value, tracing back to the "coinbase" transaction where the coin was originally mined.

To navigate this ledger without a central gatekeeper to verify identity, the protocol relies on asymmetric cryptography. Bitcoin implements the Elliptic Curve Digital Signature Algorithm (ECDSA), specifically using the secp256k1 curve (Narayanan et al., 2016), to manage authorization. This system assigns each user a key pair consisting of a private key and a public key. The private key acts as a randomly generated secret that grants the user absolute control over specific UTXOs, allowing them to sign transactions and mathematically prove ownership without ever revealing the key itself. The public key, derived from the private key, allows the network to verify these signatures. When a transaction is broadcast, network nodes act as validators, using the public key to confirm that the digital signature on the input matches the owner of the referenced UTXO. Thus, the system effectively replaces the legal concept of ownership with the cryptographic concept of knowledge: to possess the private key is to own the asset.

While cryptography secures individual transactions, the synchronization of the ledger across a global network of untrusted peers requires a solution to the "Byzantine Generals Problem." Bitcoin achieves this via the Nakamoto Consensus, which utilizes Proof-of-Work (PoW). As detailed in sections 3 and 4 of the white paper (Nakamoto, 2008), PoW functions primarily as a distributed timestamp server. Its technical purpose is to impose a thermodynamic cost on the modification of the ledger, thereby preventing double-spending. The mining process is effectively a global, probabilistic competition based on the SHA-256 hashing algorithm. To propose a new block, a miner must construct a block header that includes the "Merkle Root" (a hash of all pending transactions), the hash of the previous block, and a variable known as a "nonce."



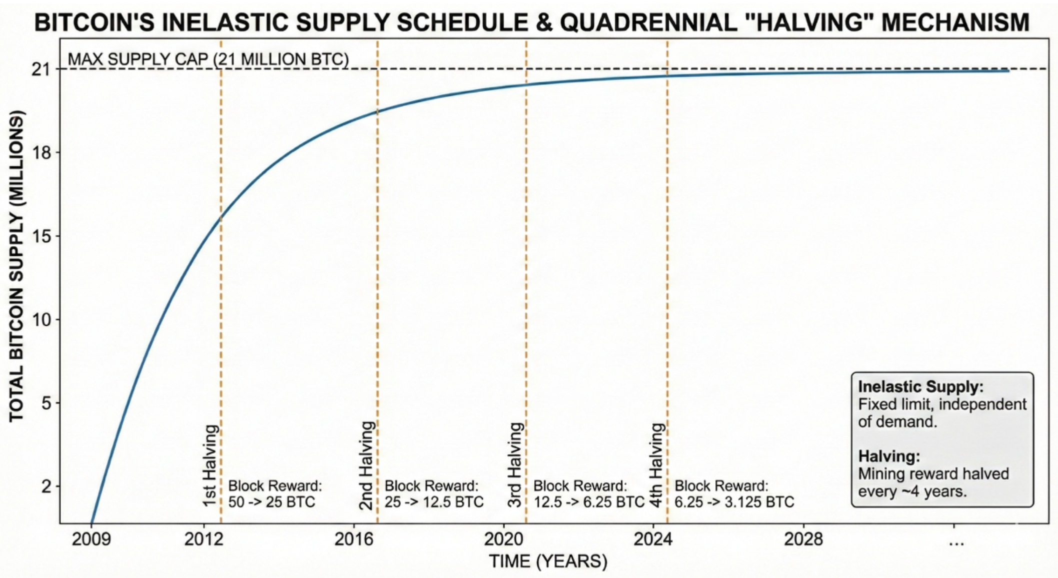
The Proof-of-Work hashing mechanism and block header structure. Adapted from Nakamoto (2008).

The core mechanic of this consensus lies in the "difficulty target." The miner must repeatedly hash the block header, incrementing the nonce with each attempt, until the resulting hash is lower than a specific target value defined by the network. Visually, this results in a hash that begins with a specific number of zero bits. Because the output of SHA-256 is pseudo-random and unpredictable, there is no algorithmic shortcut to finding this value; it requires a brute-force search consuming significant CPU or ASIC cycles. As Nakamoto (2008) asserts, "one-CPU-one-vote," meaning that the validity of the history is determined by the chain with the greatest cumulative proof-of-work. This mechanism introduces a Game Theoretic equilibrium: since the cost of attacking the network (by re-mining the chain) exceeds the potential rewards of a double-spend, rational actors are incentivized to cooperate rather than defect.

The stability of this system is maintained by the Difficulty Adjustment Algorithm, which links the digital protocol to physical constraints. The network is programmed to ensure blocks are produced approximately every ten minutes. Every 2,016 blocks (roughly two weeks), the protocol calculates the total hashing power deployed by the network. If blocks have been generated too quickly, the difficulty target decreases, making the hash harder to find; if too slowly, it increases. This self-regulating mechanism creates a barrier against attacks. To reverse a transaction (a "51% attack"), an adversary would need to rewrite the blockchain history by re-mining the block containing the transaction and all subsequent blocks faster than the honest network can extend the current chain (Nakamoto, 2008). By making the cost of such an attack prohibitively expensive in terms of hardware and electricity, the technical architecture transforms economic incentives into network security

2.2. Economics and Volatility: Supply, Halving, and Price Dynamics

Bitcoin operates on a rigid monetary policy known as "algorithmic determinism," representing a fundamental divergence from modern monetary theory. Unlike the fiat system, where central banks manage the money supply elastically to target inflation or stabilize exchange rates, Bitcoin adheres to a predetermined supply schedule that is completely unresponsive to changes in demand. In traditional macroeconomics, the supply of money is a policy variable; in Bitcoin, the supply curve is vertical, representing perfect inelasticity. The protocol dictates that the total supply will asymptotically approach, but never exceed, 21 million units.



Bitcoin’s inelastic supply schedule and the quadrennial "Halving" mechanism.

This cap is enforced by the consensus rules of the network and cannot be altered by political pressure or economic necessity. Consequently, Bitcoin lacks the stabilizing mechanism inherent in fiat currencies. Since the quantity of Bitcoin cannot adjust to match fluctuations in demand, the entire burden of adjustment falls upon the price. This creates a market dynamic where even minor shifts in adoption or sentiment result in disproportionate price swings, a phenomenon that is not a temporary anomaly but a direct function of its unyielding issuance schedule.

The mechanism that enforces this scarcity is the "Halving," a programmatic event embedded in the source code that reduces the issuance rate of new Bitcoins by 50% every 210,000 blocks, or approximately every four years. This event acts as a recurring, exogenous supply shock. Historically, the Halving has served as a catalyst for market cycles, disrupting the equilibrium between miners (sellers) and investors (buyers). When the block subsidy is halved, the daily supply of new coins entering the market drops significantly. If demand remains constant or increases, the reduced flow of new supply creates an immediate shortage, placing upward pressure on the price. This mechanism transforms Bitcoin into a disinflationary asset, contrasting sharply with the inflationary tendency of fiat currencies. However, this predictable reduction in supply also introduces speculative anticipation, where market participants attempt to price in the supply shock before it occurs, leading to boom-and-bust cycles that have characterized Bitcoin's economic history.

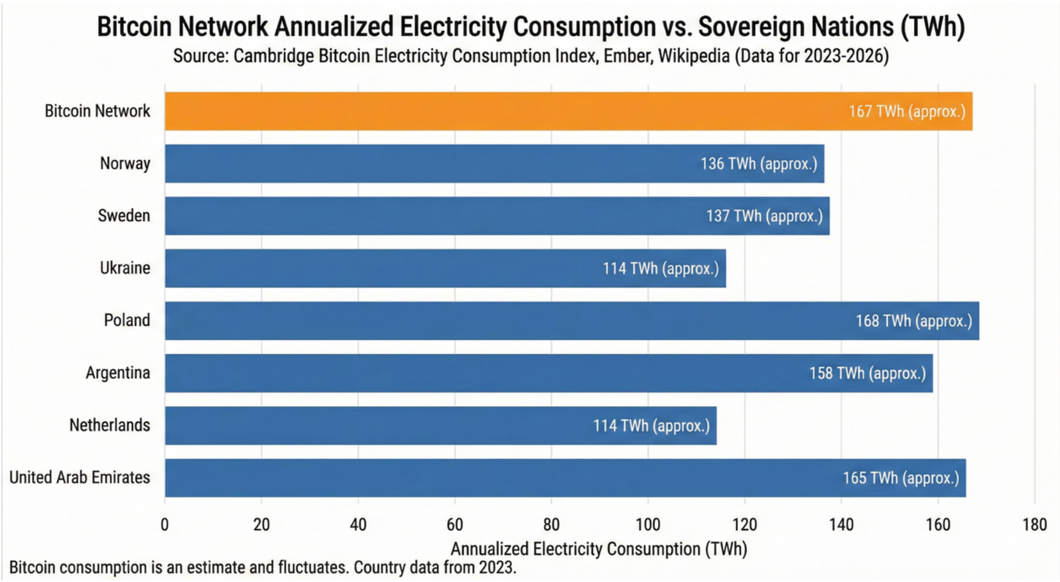
The interplay between this inelastic supply and fluctuating speculative demand results in the extreme volatility that defines Bitcoin's market performance. This characteristic has been the primary subject of economic criticism regarding Bitcoin’s viability as money. Yermack (2013), in his analysis "Is Bitcoin a Real Currency?", argues that this excessive volatility prevents Bitcoin from fulfilling the classic functions of money, particularly that of a "unit of account." For a currency to be useful in commerce, merchants must be able to price goods in it without facing the risk that the currency’s value will shift drastically between the time of sale and the time of conversion. Yermack (2013) posits that Bitcoin’s behavior is more akin to a high-risk speculative stock than a currency, concluding that its instability imposes prohibitive costs on anyone attempting to use it for daily transactions. According to this view, the very feature that makes Bitcoin scarce—its rigid supply—simultaneously disqualifies it from becoming a stable medium of exchange in the traditional sense.

While volatility undermines Bitcoin’s utility as a transactional currency, other economic analyses suggest it strengthens its case as an alternative asset class. If Bitcoin is not "money" in the operational sense, it may function as "digital gold." Baur et al. (2018) investigate this property by analyzing Bitcoin’s correlation with traditional financial assets like stocks, bonds, and commodities. Their findings suggest that Bitcoin exhibits distinct return characteristics that are largely uncorrelated with the mainstream market. Baur et al. (2018) argue that this lack of correlation allows Bitcoin to serve as a diversification tool within an investment portfolio and, potentially, as a safe haven during periods of specific market stress, distinct from the broader financial system. This perspective reframes volatility not as a failure of the currency, but as the process of "price discovery" for a nascent, finite asset that is being monetized in real-time. Thus, the economic reality of Bitcoin presents a trade-off: the protocol sacrifices short-term price stability to guarantee long-term censorship resistance and absolute scarcity

2.3. Environmental Sustainability and Criticism of Mining

The security model of Bitcoin, as established in the previous sections, relies on the assumption that rewriting the ledger is computationally, and therefore energetically, prohibitive. This reliance on Proof-of-Work transforms the network into a massive consumer of electricity, generating one of the most contentious externalities of the protocol: its environmental impact. From an economic perspective, this energy expenditure is not an inefficiency but a "costly signal." In game theory, a costly signal is an action that is reliable specifically because it is expensive to fake. For Bitcoin, the thermodynamic cost serves as the barrier to entry for malicious actors; if the energy cost were trivial, the security of the ledger would be negligible. However, as the network has scaled, the aggregate magnitude of this consumption has triggered a polarized debate regarding its sustainability and alignment with global Environmental, Social, and Governance (ESG) standards.

The primary critique focuses on the absolute scale of energy usage and the resulting carbon footprint. De Vries (2018), through the "Digiconomist" index, has been a leading voice in quantifying this impact, frequently comparing the network's total energy consumption to that of medium-sized sovereign nations.



Bitcoin network annualized electricity consumption compared to sovereign nations. Source: Cambridge Bitcoin Electricity Consumption Index.

The central argument posits that the mechanism of "brute-forcing" hash functions is inherently wasteful, as the computation serves no purpose other than securing the network and is immediately discarded once a block is found. De Vries (2019) extends this criticism to electronic waste, noting that the specialized hardware

(ASICs) used for mining becomes obsolete rapidly, creating physical waste comparable to the IT sectors of small countries. Under this framework, the social utility of a censorship-resistant currency is outweighed by the environmental damage caused by its maintenance, particularly when the electricity fueling the ASICs is derived from fossil fuels like coal or natural gas.

Conversely, alternative economic analyses argue that focusing on total consumption ignores the crucial nuance of the energy mix and the geographical mobility of miners. Unlike traditional industrial consumers, Bitcoin miners are location-agnostic and interruptible; they can operate anywhere with an internet connection and can shut down instantly without damaging their equipment. This unique flexibility drives miners to act as "energy arbitrageurs," seeking the cheapest available electricity globally. CoinShares (2019) and subsequent studies suggest that this economic incentive naturally aligns mining with renewable energy sources. In many hydroelectric regions, such as parts of Scandinavia or formerly in Sichuan, electricity is often overproduced relative to local demand. In these scenarios, the marginal cost of hydro energy approaches zero. By utilizing this "stranded assets"—energy that has been generated but cannot be transported to population centers—miners provide a revenue stream for renewable infrastructure that would otherwise face curtailment.

This dynamic has led to the emergence of the "virtual battery" thesis in energy economics. As renewable energy grids face the challenge of intermittency—solar and wind produce power when nature dictates, not necessarily when demand peaks—grid operators require flexible loads to balance the system. Recent academic literature suggests that Bitcoin mining can function as a demand-response mechanism. By co-locating mining facilities with renewable generation sites, operators can monetize excess power during periods of low demand and curtail mining operations during peak load times to release energy back to the grid. In this model, Bitcoin does not merely compete for resources but potentially acts as a subsidy for renewable expansion, converting waste energy into financial security. The debate, therefore, remains bifurcated: while critics view the protocol's energy intensity as an ecological failure, proponents interpret it as a market-driven mechanism for energy efficiency and grid stabilization.

2.4. Intermediation: Exchanges, Wallets, and Regulation

While the technical architecture of Bitcoin was explicitly designed to disintermediate financial transactions, a paradox has emerged in its practical adoption: the development of a vast, centralized secondary layer known as the "off-chain" ecosystem. For the majority of users, the interaction with the blockchain is not direct but mediated through third-party service providers, primarily centralized exchanges. This creates a structural dichotomy between the trustless nature of the underlying protocol (Layer 1) and the trusted nature of the access points. As Böhme et al. (2015) observe, while the Bitcoin protocol itself has proven resilient to systemic failure, the intermediaries that facilitate the exchange between fiat currency and cryptocurrency have become the ecosystem's critical weak points. By holding the private keys on behalf of their customers, these institutions effectively reintroduce the very counterparty risk that Nakamoto sought to eliminate. The collapses of major platforms, ranging from the Mt. Gox insolvency in 2014 to the FTX fraud in 2022, demonstrate that when users entrust their assets to unregulated or poorly managed custodians, they face risks identical to those in the traditional shadow banking sector. Essentially, these failing intermediaries inadvertently recreated the fractional reserve dynamics described in Chapter 1, but without the regulatory safeguards or lender-of-last-resort protections typical of the fiat system. This reintroduction of trust necessitates a distinction in how assets are stored, defined by the operational security of digital wallets. The ecosystem distinguishes between "hot wallets," which are connected to the internet for liquidity and convenience, and "cold storage," where private keys remain offline on hardware devices or paper. This technical distinction underpins the ideological maxim "not your keys, not your coins." When a user leaves funds on a centralized exchange, they do not technically own Bitcoin; they own a claim against the exchange’s reserves. True ownership, as defined in Section 2.1, is only achieved when the user assumes full responsibility for the private key in a non-custodial environment. However, this self-sovereignty imposes a high barrier to entry in terms of technical literacy and security hygiene, leading the mass market to prefer the convenience of custodial intermediation despite the inherent risks.

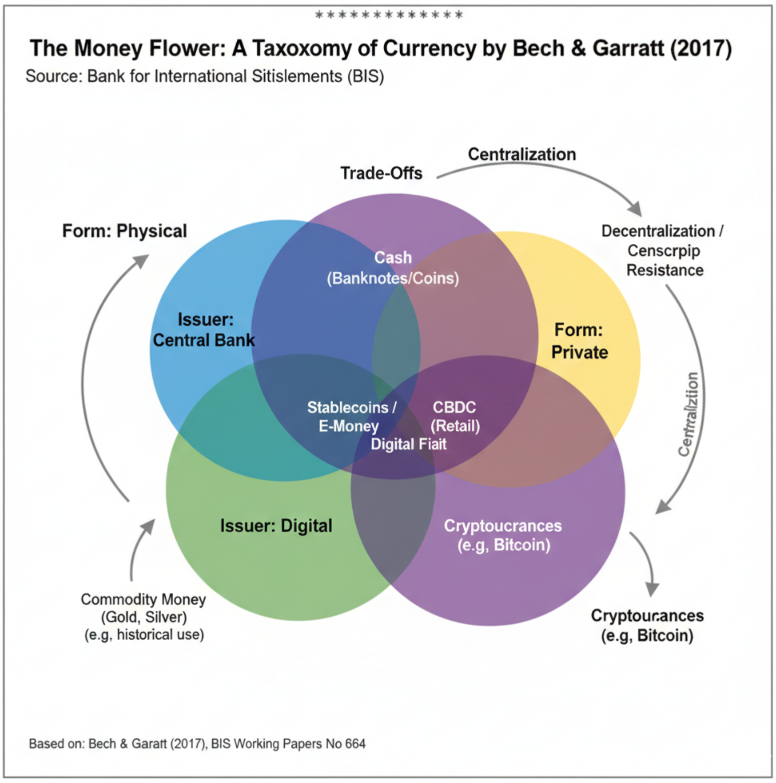
The centralization of entry points—the so-called "on-ramps" and "off-ramps"—has provided regulators with a mechanism to exert control over a theoretically ungovernable network. Since a decentralized protocol cannot be compelled to attend a court hearing or comply with sanctions, state authorities have focused their enforcement efforts on the intermediaries. This strategy relies on the integration of Know Your Customer (KYC) and Anti-Money Laundering (AML) protocols at the point where fiat currency converts to crypto. Foley et al. (2019), in their analysis of illegal activity on the blockchain, highlight that the pseudonymity of Bitcoin initially attracted a significant volume of illicit commerce, estimating that in the early years, a substantial portion of transaction volume was related to darknet marketplaces. However, Foley et al. (2019) also note that as regulation has tightened around these gateways, the "wild west" era of Bitcoin has increasingly given way to a surveillance-compliant environment. By mandating that exchanges verify user identities and report suspicious transactions, regulators have effectively de-anonymized a large segment of the network.

This regulatory encirclement forces the industry to navigate a complex trade-off between institutional legitimacy and its founding ethos of censorship resistance, bringing the analysis of Bitcoin’s internal functioning to a critical synthesis. As demonstrated throughout this chapter, Bitcoin functions as a complex sociotechnical system governed by the interplay of cryptography, game theory, and thermodynamics. Technically, the network achieves decentralized consensus through Proof-of-Work; economically, its algorithmic determinism creates a scarce but volatile "digital gold"; yet, physically, it demands a "costly signal" of energy consumption, and legally, it remains tethered to the traditional system through centralized intermediaries. Having understood the disruptive capability and the limitations of this private monetary technology, the thesis now turns to the inevitable institutional response. The state, challenged by the rise of non-sovereign money, is not remaining passive. Instead, it is preparing to counterattack by co-opting the underlying technology to reinforce, rather than dismantle, monetary sovereignty. This sets the stage for Chapter 3, which will analyze the rise of Central Bank Digital Currencies (CBDCs)—systems technologically similar to Bitcoin, but philosophically its polar opposite.

Chapter 3 – Case Study 1: Contrasting Systems and Perspectives on a Decentralized World

3.1. Structural Comparison: Central Banks vs. The Bitcoin Network

To understand the magnitude of the divergence between the traditional financial system and the Bitcoin network, it is necessary to move beyond surface-level similarities—both are digital, and both transfer value—and analyze their underlying institutional architectures. This comparison is best framed through the taxonomy provided by Bech & Garratt (2017) in their analysis for the Bank for International Settlements (BIS). They propose the "Money Flower," a Venn diagram that categorizes currency based on four key properties: the issuer (central bank vs. private), the form (digital vs. physical), accessibility (widely accessible vs. restricted), and the transfer mechanism (centralized vs. peer-to-peer).



The Money Flower taxonomy illustrating the structural divergence between central bank currencies and decentralized networks. Adapted from Bech & Garratt (2017).

As illustrated in Figure 3.1, Bitcoin and the Central Banking system represent polar opposites within this taxonomy. This visual contrast serves as the foundation for analyzing their divergent governance and monetary policies in the following sections.

Applying this lens reveals that the Bitcoin network and the Central Banking system represent polar opposites in terms of governance, monetary policy, and access.

Governance: Trust vs. Verification

The most profound distinction lies in the mechanism of governance and the locus of trust. The modern fiat system is fundamentally a "Trust-Based" hierarchical model. As discussed in Chapter 1.1, the value and stability of a sovereign currency depend entirely on the credibility of the issuing authority—the Central Bank. Governance is discretionary: decisions regarding interest rates, quantitative easing, or reserve requirements are made by a committee of appointed officials (e.g., the FOMC in the US or the ECB Governing Council) based on their subjective assessment of macroeconomic data. This centralization allows for rapid decision-making during crises but introduces "human risk," including potential political pressure, policy errors, or moral hazard.

Conversely, Bitcoin operates on a "Verification-Based" network model. As established in Chapter 2.1, governance is automated by the protocol's consensus rules. There is no central committee to lobby; the "monetary policy" is codified in the open-source software and enforced by a dispersed network of nodes. Trust is shifted from an institution to cryptographic proof. While the fiat system relies on the legal authority of the state to settle disputes and enforce value, the Bitcoin network relies on the objectivity of mathematics and the game-theoretic equilibrium of Proof-of-Work. In this system, "code is law," meaning the rules are applied impartially to all participants without exception.

Monetary Policy: Elasticity vs. Inelasticity

This governance structure dictates the nature of the monetary supply and highlights the central economic trade-off between the two systems. Central Banks prioritize "elasticity." Their primary mandate is to manage the money supply dynamically to target inflation (typically around 2%) and stabilize the economy during shocks. This flexibility allows them to act as the "Lender of Last Resort," injecting liquidity into the banking sector to prevent systemic collapse during liquidity crunches, as seen in the 2008 financial crisis.

In stark contrast, Bitcoin's policy is defined by "absolute inelasticity." The supply schedule is fixed, predetermined, and transparent, capped at 21 million units regardless of economic conditions. Ammous (2018) argues that this rigidity classifies Bitcoin as "Sound Money"—money that is difficult to produce and immune to arbitrary debasement—comparing it to a digital form of the Gold Standard.

Ammous (2018) further posits that this scarcity encourages a lower "time preference" among holders, incentivizing long-term savings over immediate consumption. However, this feature is a double-edged sword: while it protects holders from currency debasement (inflation), it deprives the system of any lever to mitigate liquidity crises or stabilize purchasing power in the short term. This structural rigidity renders Bitcoin an effective store of value (digital gold) but a potentially poor unit of account during periods of economic stress.

Access and Settlement: Permissioned vs. Permissionless

The third structural divide concerns accessibility and the finality of transactions. The traditional banking system is "Permissioned." Access is a privilege, not a right; it is gatekept by commercial banks that must enforce Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations. While these regulations are essential for preventing illicit finance, they create a system where financial exclusion is a structural byproduct, barring those who lack documentation or reside in sanctioned jurisdictions from global commerce.

Bitcoin, conversely, is "Permissionless." The protocol is blind to the identity of the user; it only verifies the validity of the cryptographic signature. This neutrality ensures that the network functions as a public utility, open to anyone with an internet connection, regardless of nationality or creditworthiness.

Finally, the settlement models diverge significantly. In the fiat banking system, transaction finality is often probabilistic and delayed. A credit card payment or bank transfer acts as a promise of payment that is settled in batches (often T+2 days) and remains reversible through chargebacks or fraud claims. In Bitcoin, settlement is deterministic. Once a transaction is buried under sufficient Proof-of-Work (block confirmations), it becomes computationally immutable. This eliminates the counterparty risk inherent in the credit-based legacy system, but it also removes the possibility of recourse in the event of error or theft.

3.2. The Institutional Response: The Counter-Model of CBDCs

The structural divergence analyzed in the previous section highlights a fundamental threat to the status quo: the rise of a parallel monetary system that operates outside the purview of the state. Central banks, acknowledging that the digitization of value is irreversible, have moved from a stance of observation to one of active technological co-optation. This response materializes in the development of Central Bank Digital Currencies (CBDCs). A CBDC represents a digital form of a country's sovereign currency that is a direct liability of the central bank. Unlike the decentralized architecture of Bitcoin, a CBDC is not a new asset class but a new format for the existing monetary unit. This distinction is ontological: while Bitcoin is a bearer asset with no counterparty, a CBDC serves as a digital representation of state debt, designed to combine the efficiency of cryptographic payment rails with the centralized governance of the fiat model.

Strategic Motivations: The Defense of Monetary Sovereignty

The impetus for CBDC development is primarily defensive. As outlined by Panetta (2021) regarding the Digital Euro project, the proliferation of private cryptocurrencies and stablecoins (such as the proposed Libra/Diem or USDT) threatens the "monetary anchor" role of public money. If the digital economy were to migrate entirely to private ledgers, central banks would lose their ability to implement monetary policy and act as lenders of last resort. In this context, the CBDC is the state's counter-move to preserve monetary sovereignty. By providing a risk-free public digital asset, central banks aim to prevent the "privatization of money," ensuring that the state retains control over the unit of account and the finality of settlement.

To understand the operational scope, it is necessary to distinguish between Wholesale CBDCs, restricted to financial institutions for interbank settlement, and Retail CBDCs, accessible to the general public. While the wholesale model improves back-end efficiency, the retail model is the direct competitor to Bitcoin. It offers citizens a digital wallet directly linked to the central bank, effectively disintermediating commercial banks and theoretically removing the risk of bank runs, as the central bank cannot default on its own currency.

Technological Architecture: Centralization 2.0

From a technical perspective, CBDCs often utilize Distributed Ledger Technology (DLT), but they implement it within a "permissioned" environment. Unlike

Bitcoin’s permissionless blockchain, where validation is open to any participant with computational power (Proof-of-Work), a CBDC network is maintained by authorized nodes—typically the central bank and select regulated entities. This architecture resolves the "scalability trilemma" faced by decentralized blockchains: by sacrificing decentralization, CBDCs achieve high transaction throughput and energy efficiency.

However, this efficiency comes with a significant structural trade-off. In the Bitcoin network, security is derived from the distribution of the ledger; in a CBDC system, security depends entirely on the integrity of the central authority. The ledger is not immutable in the absolute sense; it is administratively mutable. The central bank retains the "God view" of the network, possessing the technical capability to reverse transactions, freeze assets, or correct errors. Thus, while CBDCs adopt the form of blockchain technology, they reject its function of censorship resistance, using the ledger to enhance, rather than eliminate, central oversight.

Functional Innovation: Programmable Money

The most radical innovation introduced by CBDCs is the concept of "programmable money." Unlike physical cash or Bitcoin, which are neutral mediums of exchange, a CBDC can be embedded with smart contracts that dictate how, when, and where the currency can be spent. Prasad (2021) argues that this programmability fundamentally alters the nature of money, transforming it from a passive store of value into an active tool of policy and reshaping the international banking order. In a theoretical application, a central bank facing a recession could issue "stimulus tokens" that expire if not spent within a certain timeframe, forcing an increase in the velocity of money (an application of Gesell's theory of demurrage). Alternatively, monetary policy could become surgically precise: interest rates could be applied directly to retail wallets, bypassing the slow transmission mechanism of commercial banks. While this offers unprecedented control over economic variables, it introduces a new dimension of risk regarding the fungibility of money, as one unit of currency might carry different conditions than another.

The Policy Trilemma and Systemic Trade-offs

Ultimately, the confrontation between Bitcoin and CBDCs can be framed through the lens of the economic trilemma, which posits the difficulty of simultaneously achieving price stability, free movement of capital, and independent monetary policy (Mundell-Fleming model). Bitcoin resolves this tension by optimizing for the free movement of capital and an independent, algorithmic policy, explicitly sacrificing price stability in the process. Conversely, CBDCs prioritize price stability and centralized policy control, but they inherently compromise the free movement of capital through programmable restrictions and, crucially, user privacy.

This analysis reveals that there is no perfect system, only trade-offs. The Bitcoin model prioritizes sovereignty and resilience at the cost of efficiency and stability. The CBDC model prioritizes control and efficiency at the cost of privacy and censorship resistance. The institutional response, therefore, is not merely a technical upgrade but a reassertion of the hierarchical model, using the very tools of the crypto-revolution to reinforce the centralization of the financial order.

3.3. Prospective Analysis: Benefits and Risks of Total Decentralization

Having established the structural divergence between the Bitcoin network and the emerging CBDC counter-model, it is necessary to conduct a prospective analysis of the "Bankless" paradigm. If the global economy were to shift significantly toward the decentralized model described in Chapter 2, it would entail a radical reconfiguration of financial risk and social utility. This scenario presents a stark dichotomy of benefits and systemic risks.

The Bull Case: Inclusion and Resilience

The primary economic argument for a decentralized standard rests on financial inclusion and systemic resilience. As discussed in Chapter 1, the legacy banking system is characterized by high entry barriers. Billions of adults worldwide remain "unbanked" or "underbanked" because they lack the necessary identity documentation or because serving them is not profitable for commercial banks. Antonopoulos (2014) argues that Bitcoin solves this by "banking the unbanked" through technology rather than policy. In a decentralized model, the removal of identity requirements creates a system of "open access." Anyone with a smartphone and an internet connection can participate in the global economy, effectively democratizing access to capital and payment rails without requiring the permission of a gatekeeper.

Furthermore, the decentralized model offers a structural solution to the "Single Point of Failure" problem. In the traditional hierarchical model, the insolvency of a major intermediary (e.g., Lehman Brothers in 2008) can trigger a systemic cascade requiring state intervention. The Bitcoin network, by contrast, is antifragile; it has no center to collapse. The ledger is replicated across thousands of independent nodes, ensuring that the system remains operational even if large segments of the network are compromised. This redundancy offers a theoretical hedge against the kind of institutional failures that define modern financial crises, providing a mechanism for wealth preservation that is uncorrelated with the solvency of the banking sector.

The Bear Case: Systemic Risks and the Absence of a Safety Net

However, the removal of intermediaries introduces severe economic risks, primarily the loss of the "Lender of Last Resort" function. In the current fiat system, central banks act as the ultimate backstop, providing liquidity during crises to prevent deflationary spirals and stabilize employment. A decentralized, inelastic currency like Bitcoin has no such mechanism. As Allen et al. (2020) argue in their analysis of central bank digital currencies and crypto-assets, a fully decentralized system lacks the policy tools necessary to smooth out business cycles. In the event of a liquidity crunch (such as the COVID-19 market shock), a Bitcoin-based economy would have no central authority to inject capital. Without this elasticity, economic shocks could result in prolonged periods of deflation and depression, as the protocol cannot adjust to stabilize the real economy.

Finally, a critical long-term structural risk concerns the network's "security budget." As the block subsidy—the primary incentive for miners—diminishes every four years and eventually vanishes once the 21 million cap is reached, the network's thermodynamic security will depend entirely on transaction fees. If transaction volume does not generate sufficient revenue to incentivize miners, the cost to attack the network could drop precipitously. This creates an existential economic uncertainty: whether a deflationary, fixed-supply system can maintain sufficient security in perpetuity without a state sponsor to subsidize its defense.

Additionally, the "sovereignty" of the user comes with the cost of total irreversibility and operational risk. The traditional financial system provides layers of consumer protection: fraud can be reversed, and lost passwords can be reset. In the "Bankless" model, the user bears 100% of the risk. Theft, error, or the loss of private keys results in the permanent destruction of wealth with no possibility of recourse. Finally, there is the persistent issue of volatility. As analyzed in Chapter 2.2, Bitcoin’s fixed supply schedule forces all demand shocks to be absorbed by price changes. Critics argue that an economy cannot function effectively if its unit of account fluctuates wildly in purchasing power, suggesting that while Bitcoin may serve as a pristine collateral asset, its rigidity makes it structurally unsuitable for the daily credit operations that drive modern commerce.

However, this critique largely focuses on the base layer of the protocol, ignoring the development of layered scaling solutions. Just as the traditional financial system relies on a tiered architecture—where high-velocity payments occur on commercial bank ledgers while final settlement occurs on the central bank's balance sheet—the Bitcoin ecosystem is adopting a similar "Layer 2" approach. Protocols such as the Lightning Network allow for instant, near-zero cost transactions off-chain, using the main blockchain solely for final settlement. This technological evolution theoretically resolves the scalability paradox, enabling Bitcoin to function simultaneously as a pristine collateral asset (store of value) and a high-velocity medium of exchange.

3.4. Critical and Ethical Considerations of the Bankless Model

Beyond the structural and economic dimensions, the confrontation between the Bitcoin network and the emerging CBDC model extends into the realm of political philosophy and ethics. The technical architecture of a monetary system is never neutral; it inevitably encodes specific values regarding the balance between state authority and individual liberty. As the digitization of money nears completion, the choice of infrastructure—decentralized or centralized—will determine the degree of financial privacy and autonomy available to the individual in the 21st century.

The Panopticon vs. Pseudonymity

The most contentious ethical divide concerns the future of privacy. The transition to a CBDC-based system risks creating what Zuboff (2019) describes as "Surveillance Capitalism," but applied to the sovereign monetary state. In her analysis of the digital economy, Zuboff (2019) warns that the extraction of behavioral data has become the primary logic of accumulation. A retail CBDC could theoretically grant the central bank a "God's eye view" of all economic activity, eliminating the anonymity historically provided by physical cash. In this potential "financial panopticon," every transaction is visible, traceable, and permanently linked to a digital identity. While this capability is powerful for fiscal enforcement and macroeconomic analysis, it represents an unprecedented expansion of state power over the private lives of citizens, effectively merging financial surveillance with governance.

In direct contrast, David Chaum, a pioneer of cryptographic privacy, has long argued that privacy is a prerequisite for a functional democracy. Chaum posits that without the ability to transact without observation, the balance of power shifts dangerously toward the observer, chilling civil discourse and political opposition. Bitcoin implements this philosophy through "pseudonymity." While the blockchain ledger is public and transparent, identities are encrypted behind cryptographic addresses. This design preserves a sphere of financial privacy akin to "digital cash," safeguarding the user from the granular surveillance inherent in account-based systems.

Censorship Resistance vs. Illicit Finance

However, this privacy is the specific target of regulatory scrutiny, framing the ethical debate around censorship resistance. The "Bankless" model asserts that the right to transact is a fundamental human freedom that should not be subject to state permission or pre-emptive restraint. This feature is critical for activists living under authoritarian regimes, where the banking system is frequently weaponized to freeze the assets of political dissidents. In this context, Bitcoin serves as a tool of civil liberties, ensuring that financial survival is not contingent on political alignment.

Furthermore, the concept of censorship resistance extends beyond the individual to the geopolitical stage. In an era where the global financial infrastructure (e.g., SWIFT) is increasingly weaponized for foreign policy objectives, Bitcoin offers a neutral alternative. As a supranational asset with no central issuer, it provides a theoretical solution to the "Triffin Dilemma," serving as a global reserve currency that does not privilege the monetary policy of a single hegemon. Consequently, the "Bankless" model may appeal not only to individuals seeking privacy but also to sovereign states seeking immunity from extraterritorial sanctions and strategic autonomy in a multipolar world.

Conversely, regulatory authorities view this censorship resistance as a systemic vulnerability. Leaders such as Christine Lagarde, President of the European Central Bank, have frequently argued that without the ability to identify users and pierce the veil of anonymity, decentralized networks become havens for money laundering, terrorism financing, and tax evasion. From this perspective, the "right to transact" is subordinate to the state's obligation to maintain security and the rule of law. The ethical trade-off is therefore stark: a CBDC system optimizes for collective security and legal compliance at the expense of individual privacy, while the Bitcoin network optimizes for individual sovereignty at the risk of enabling illicit actors.

Programmability vs. Neutrality

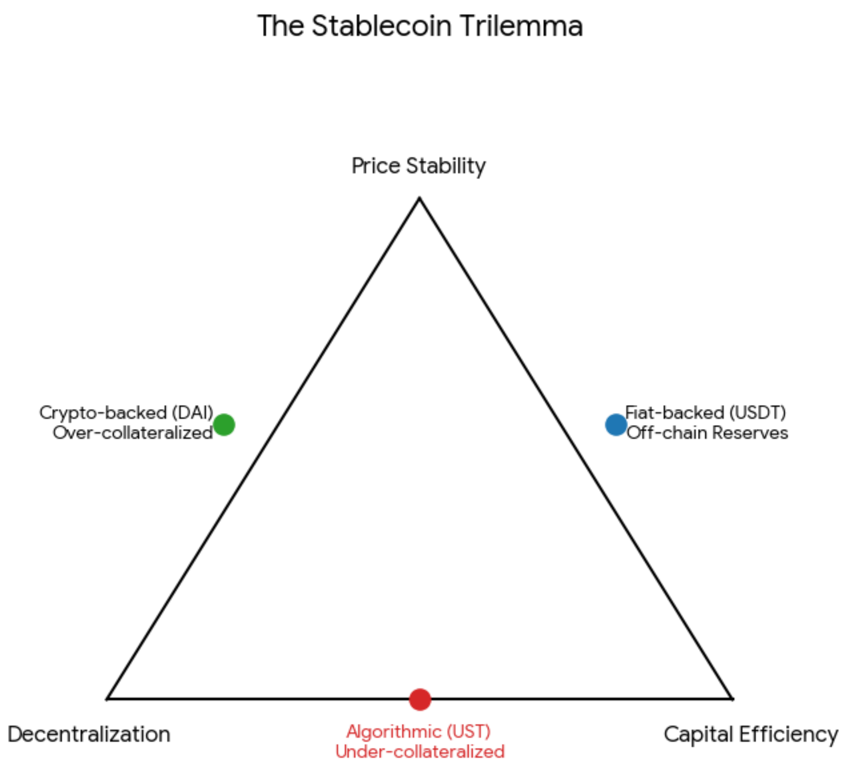
The final ethical consideration regards the nature of the currency itself: programmability versus neutrality. As analyzed in Section 3.2, CBDCs introduce the potential for "programmable money"—currency embedded with smart contracts that can enforce policy rules. This capability raises profound ethical questions about social engineering. If a central bank can program money to expire (to stimulate spending) or to be restricted from certain purchases (e.g., carbon-intensive goods), money ceases to be a neutral medium of exchange and becomes a tool of behavioral control. This could lead to a scenario where financial autonomy is conditional, subject to the changing objectives of the issuer.

Bitcoin, conversely, functions as a neutral bearer asset. It is "dumb" money; the protocol verifies only the validity of the digital signature, not the morality of the transaction or the identity of the sender. This neutrality ensures that money remains a tool of property rights rather than political coercion, treating all users equally regardless of their social credit or legal standing. The choice between these models forces society to decide whether money should be a public utility that is blind to its users, or a policy instrument that actively shapes their behavior.

Chapter 4 – Case Study 2: Stablecoins: Stability and Risks

4.1. Stablecoins: Definition, Classification, and the Role of USDT

The transition of the digital asset market has revealed a fundamental paradox: while Bitcoin established a decentralized store of value, its structural inelasticity and algorithmic determinism—analyzed in Chapter 2 as the rigid protocol governing its fixed supply—render it an inefficient medium of exchange for daily commerce. To bridge the gap between the efficiency of blockchain-based settlement and the price stability required for traditional economic activity, a new class of digital assets emerged known as stablecoins, which act as the connective tissue between the volatile crypto-economy and the traditional fiat financial system. The engineering of stability within this decentralized environment is governed by the "Stablecoin Trilemma," a framework suggesting it is nearly impossible for a digital currency to simultaneously achieve decentralization, capital efficiency, and peg stability. Graphical representation of the "Stablecoin Trilemma". The trade-offs between stability, decentralization and capital efficiency are highlighted for the main market models (USDT, DAI, UST).



Graphical representation of the "Stablecoin Trilemma". The trade-offs between stability, decentralization and capital efficiency are highlighted for the main market models (USDT, DAI, UST).

Every project must prioritize specific pillars, a trade-off best observed through the taxonomy of collateralization models categorized by Bullmann et al. (2019) for the European Central Bank. Fiat-collateralized models, or the "off-chain" approach, rely on reserves of traditional assets held in custody by financial institutions. These systems, exemplified by Tether (USDT), optimize for capital efficiency and peg stability but sacrifice decentralization by reintroducing the counterparty risk of centralized intermediaries who act as stewards of the deposits. This reintroduction of intermediaries recalls the discussion in Chapter 2.4 and 3.2 regarding how centralized access points bring the risks of the traditional system back into the cryptographic realm. Conversely, crypto-collateralized models utilize over-collateralized loans where users lock up digital assets to mint a stablecoin, prioritizing decentralization and transparency but suffering from low capital efficiency to buffer against market volatility. Finally, algorithmic systems attempt to maintain a peg through arbitrage incentives and the automated expansion or contraction of supply, though these have historically proven prone to "death spirals" during periods of extreme market contraction.

While marketed as a cryptographic innovation, the structural reality of the market leader, Tether, more closely resembles a traditional Money Market Mutual Fund. Gorton & Zhang (2021) draw an explicit historical parallel between stablecoins and the "Wildcat Banking" era, where private banks issued their own notes backed by opaque or illiquid reserves. In this shadow banking framework, the issuer acts as a private entity that accepts fiat currency and invests those proceeds into a portfolio of short-term debt instruments, such as US Treasury Bills and commercial paper. The issuer then creates digital claims that are nominally redeemable at par, creating a significant maturity mismatch where the issuer holds potentially illiquid assets while providing users with the promise of on-demand liquidity. This architecture inadvertently recreates the fractional reserve dynamics described in Chapter 1, where the total volume of digital claims is a multiple of the actual liquid reserves.

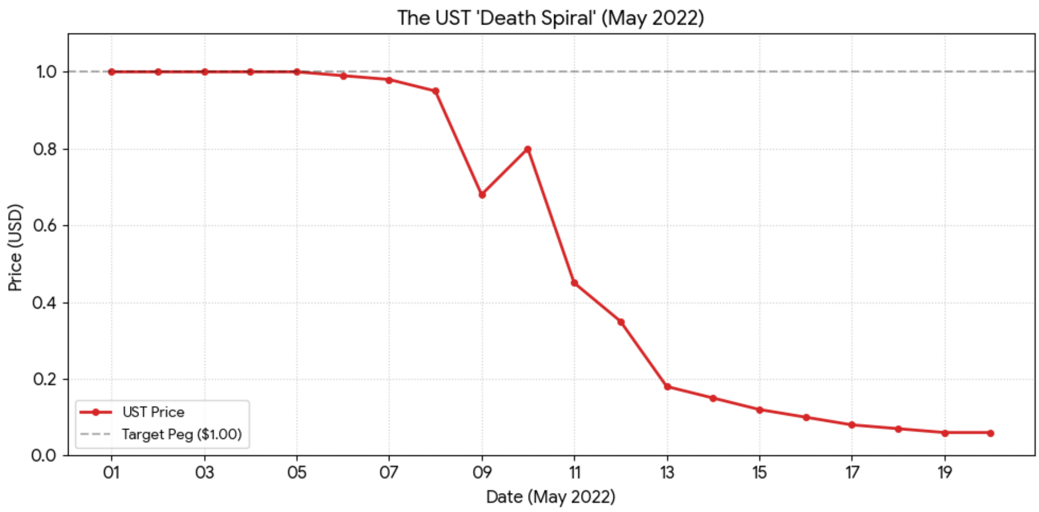
Furthermore, the quality and transparency of these reserves have sparked intense debate. Under mounting regulatory pressure and public scrutiny, Tether has transitioned the composition of its backing, significantly reducing its reliance on commercial paper in favor of more secure US Treasury Bills. This transition highlights the central role of "trust" and "counterparty risk," as the market remains sensitive to the distinction between various debt qualities. However, the debate is compounded by the issuer's use of periodic "attestations" rather than comprehensive, traditional financial audits. In accounting terms, an attestation merely provides a static snapshot of the reserves at a specific, predetermined moment in time. It does not evaluate the internal risk controls, the provenance of the funds, or the continuous financial health of the issuer over a fiscal period—all of which are standard requirements of a full banking audit. This gap in granular verification leaves room for market skepticism, reinforcing the dependency on the issuer's integrity rather than verifiable proof.

Consequently, the primary vulnerability of this model is "Run Risk," a phenomenon where the system's stability depends entirely on the collective trust placed in the managing institution. Because stablecoins lack the regulatory safeguards of the traditional banking sector—such as federally mandated deposit insurance or access to a central bank as a lender of last resort—their stability is fragile. This mirrors the systemic vulnerabilities of the fiat model discussed in Section 1.1, specifically the necessity of trust that central authorities will not debase the currency or fail as stewards of deposits. If users begin to doubt the solvency of the issuer or the liquidity of its reserves, a mass withdrawal can occur, forcing the issuer to liquidate assets at a discount and leading to a de-pegging event. Such a failure would not be isolated; given that stablecoins serve as a primary source of liquidity, a collapse could trigger a systemic contagion, paralyzing the digital economy and potentially spilling over into the traditional financial markets that hold the issuer's collateralized debt. This highlights the paradox of adoption: while stablecoins aim for the collective security and legal compliance characteristic of systems like CBDCs (Section 3.2), they remain exposed to the very counterparty risks they were designed to mitigate.

4.2. Crypto Instability: Analysis of the Terra–Luna (UST) Collapse

The collapse of the Terra network in May 2022 represents a definitive financial autopsy of algorithmic stability and serves as a catastrophic example of the risks inherent in "code without collateral." Unlike the fiat-collateralized models analyzed in the previous section, the TerraUSD (UST) stablecoin was not backed by traditional off-chain assets like Treasury Bills, but instead relied on a "Seigniorage Shares" model. This dual-token system used the native cryptocurrency, LUNA, as a volatility absorber for the UST peg, functioning as an automated market maker where one unit of UST could always be exchanged for $1 worth of LUNA. Under this mechanism, if UST traded below its $1 peg, arbitrageurs were incentivized to buy the undervalued UST and burn it to mint $1 worth of LUNA, theoretically contracting the UST supply and restoring the peg through market incentives.

However, this stabilization mechanism rested on the precarious assumption of perpetual baseline demand for both tokens, a logic that proved fallible during the sudden loss of trust in May 2022. Crucially, this baseline demand was not organic; it was artificially manufactured through the Anchor Protocol, a decentralized lending platform within the Terra ecosystem. Anchor offered a staggering, seemingly risk-free annual percentage yield (APY) of nearly 20% on UST deposits. From a macroeconomic perspective, this yield functioned as an aggressive, subsidized customer acquisition strategy rather than a sustainable interest rate derived from productive economic activity. The creators utilized reserve capital to pay these outsized returns, effectively creating a structural deficit. As long as the 20% yield was paid, demand for UST remained artificially high, masking the fragility of the algorithmic peg. However, as the system's reserve capital began to deplete—threatening the sustainability of the payout—this manufactured demand instantly evaporated. Investors realized the yield was a subsidy rather than an economic reality, and the rush to exit the Anchor Protocol became the primary catalyst for the ensuing bank run. As Uhlig (2022) highlights, such algorithmic pegs are inherently fragile and vulnerable to a self-reinforcing "Death Spiral," which was triggered when a wave of large-scale UST sell-offs sparked a bank run on the Terra ecosystem.



TerraUSD (UST) price performance in May 2022. The graph illustrates the failure of the algorithmic mechanism and the resulting "death spiral" that led to the total loss of the peg.

As confidence evaporated, the automated minting mechanism began to hyper-inflate the LUNA supply as investors rushed to redeem their failing UST. This massive issuance put extreme downward pressure on LUNA's price, requiring even more tokens to be minted for every unit of UST redeemed, a misalignment in token economics that Briola et al. (2023) identify as the primary driver of the network's total erasure and the loss of nearly $50 billion in market capitalization.

The collapse of this "decentralized" protocol did not remain contained within the blockchain; instead, it proved that decentralized risks can effectively destroy centralized institutions. The event triggered a profound "crypto winter," revealing deep interconnections within the digital asset ecosystem where major centralized lenders and hedge funds, such as Three Arrows Capital, Celsius Network, and Voyager Digital, held significant exposure to Terra through high-yield lending protocols like Anchor. The sudden evaporation of value led to a massive credit crunch and liquidity crisis, forcing these intermediaries into liquidation and triggering a chain reaction of insolvency. This failure demonstrated that the reintroduction of trust-based intermediation—the very centralized secondary layer discussed in Chapter 2.4—had inadvertently recreated the systemic moral hazard and fragility that characterized the 2008 financial crisis, starkly exposing the structural reliance on trust identified in traditional financial architecture.

4.3. Comparison and Reflections on Monetary Stability (vs. Fiat Currency)

The emergence of stablecoins has forced a critical re-evaluation of the "Hierarchy of Money," a conceptual framework that distinguishes between a monetary unit and the various private promises to pay that unit. While the Bitcoin movement sought to create an independent, non-sovereign currency, stablecoins have effectively taken the opposite path by "piggybacking" on the credibility of the central bank's unit of account. In the digital asset ecosystem, these instruments function as a bridge between the fiat monetary model and decentralized ledgers, yet they remain structurally distinct from the base money they reference. Crucially, these private instruments served as the technological "test bed" for programmable money, demonstrating efficiencies in settlement that traditional systems lacked. This success, however, introduced the risk of "monetary displacement," where private issuers could undermine the sovereign's direct link to the economy. As discussed in Chapter 3, this threat to monetary sovereignty acted as a primary catalyst, forcing Central Banks to accelerate their own CBDC projects to ensure that the public unit of account remains the dominant anchor in a digitalized financial system.

In times of acute financial stress, the market tends to flee from these private liabilities toward the ultimate security of public liabilities—such as physical cash or sovereign debt—a dynamic that underscores the fact that stablecoins are not money itself, but rather digital claims on it. Eichengreen (2019) argues that while these tokens may offer operational improvements in payment speed, they are unlikely to solve the fundamental stability problems of fiat currency without the institutional backstops, such as deposit insurance and a lender of last resort, provided by the State.

The structural challenge of maintaining a stablecoin can be further analyzed through a variation of the "Impossible Trinity" in international macroeconomics, which posits the difficulty of simultaneously achieving a fixed exchange rate, free capital flow, and independent monetary policy. By attempting to fix their exchange rate to the US Dollar while allowing for the free, cross-border movement of capital, stablecoin issuers are forced to abandon an independent monetary policy, effectively importing the interest rate environment of the US Federal Reserve. This leads to a profound "Paradox of Adoption": whereas Bitcoin was designed as a tool for financial disintermediation (Section 1.3), stablecoins have primarily served to "dollarize" the internet. By extending the reach of the US dollar into digital realms where the traditional banking system cannot reach, these private networks are reinforcing the role of the state's unit of account rather than reducing it.

This increasing integration between crypto-assets and traditional finance has prompted a global regulatory shift toward the principle of "Same Activity, Same Risk, Same Regulation,". This is most clearly exemplified by the European Union's MiCA (Markets in Crypto-Assets) framework. Crucially, MiCA introduces stringent requirements for Asset-Referenced Tokens (ARTs) and E-Money Tokens (EMTs), mandating that issuers maintain robust liquidity reserves and high-quality liquid assets. By imposing these prudential standards, MiCA effectively treats stablecoin issuers with the same rigor as traditional banking institutions, acknowledging that while the delivery mechanism is novel, the underlying financial risks remain identical.

The Bank for International Settlements (BIS) has consistently warned that as these private monetary technologies grow, the potential for contagion from volatile crypto-markets into the traditional financial system increases, necessitating strict prudential standards for issuers. Ultimately, the transition from a trust-based institutional model to a purely privatized monetary system appears constrained by a fundamental requirement for stability; stablecoin integrity remains a derivative of state-managed credibility. This suggests that while the technological format of money may be revolutionized through distributed ledgers, its foundational reliance on the sovereign state remains the ultimate source of its public trust and systemic survival.

Chapter 4.4 Discussion

The analysis of the stablecoin ecosystem reveals a profound macroeconomic reality: monetary stability is not merely a technological feature that can be coded into existence, but an institutional by product. The attempt to marry the borderless efficiency of decentralized ledgers with the price stability of the fiat system has not eliminated traditional financial risks; rather, it has simply repackaged them.

Fiat-collateralized models, spearheaded by USDT, have successfully provided the digital economy with a highly functional unit of account. However, they achieve this by operating as unregulated shadow banks. By relying entirely on traditional financial assets like Treasury Bills, they import the exact counterparty and run risks that cryptographic money was originally designed to escape. Ultimately, these models do not subvert the fiat system; they digitize it. By extending the reach of the Federal Reserve's monetary policy into the blockchain, fiat-backed stablecoins ironically reinforce the global hegemony of the US Dollar rather than dismantling it.

Conversely, the catastrophic collapse of the Terra-Luna network demonstrated the fatal flaws of algorithmic stablecoins. The UST experiment proved that stability cannot be purely engineered through arbitrage incentives and code without robust, tangible collateral. In attempting to defy the economic gravity of supply and demand, the algorithmic model succumbed to a classic bank run, proving that "code without collateral" is fundamentally unsustainable during periods of acute market contraction.

The stablecoin trilemma thus forces a market compromise, serving as the final piece of the digital currency puzzle. While Bitcoin (analyzed in Chapter 2) attempts to invent an entirely new, decentralized money, and CBDCs (Chapter 3) represent the State's attempt to upgrade sovereign money, stablecoins represent a fragile middle ground—an attempt to digitize current money.

Conclusions

The evolution of digital money over the past decade represents one of the most significant architectural shifts in the history of finance. As analyzed throughout this thesis, the catalyst for this disruption was fundamentally macroeconomic.

Chapter 1 demonstrated that the advent of cryptographic currencies was a direct, ideological response to the systemic vulnerabilities of the traditional fiat monetary system—specifically, its reliance on centralized trust, the inherent fragility of fractional reserve dynamics, and the inflationary tendencies born from discretionary monetary policy.

Bitcoin, examined in Chapter 2, emerged as the first viable alternative, engineering a trustless, decentralized architecture through the Proof-of-Work consensus mechanism and the UTXO model. However, the thesis highlights a critical trade-off: Bitcoin's algorithmic determinism and perfectly inelastic supply create extreme price volatility. While this rigid monetary policy makes it a formidable, censorship-resistant "digital gold" and a hedge against fiat debasement, it fundamentally disqualifies it from serving as a stable unit of account or a functional medium of daily exchange.

The disruption caused by Bitcoin forced an inevitable institutional counter-offensive. As explored in Chapter 3, Central Bank Digital Currencies (CBDCs) represent the State's strategic maneuver to co-opt distributed ledger technology to preserve monetary sovereignty. By digitizing base money, central banks optimize settlement efficiency but categorically reject decentralization. In doing so, they replace the censorship resistance of the blockchain with a hierarchical "Financial Panopticon," expanding the state's capacity for financial surveillance and behavioral control.

Finally, Chapter 4 illustrated the market's pragmatic attempt to bridge this divide through stablecoins. While fiat-collateralized models like USDT successfully digitized the stability of the US Dollar, they simultaneously reintroduced the classic vulnerabilities of "Shadow Banking," including maturity mismatches and run risk. Conversely, the catastrophic collapse of the Terra-Luna network proved that algorithmic stability is a mathematical illusion when deprived of tangible collateral. The stablecoin experiment ultimately proved that monetary stability is not purely a technological feature, but an institutional byproduct that requires centralized backing.

The Digital Monetary Trilemma

Drawing from this comprehensive analysis, it becomes evident that the future of digital currency is governed by a "Digital Monetary Trilemma." The empirical evidence of the last fifteen years suggests that it is structurally impossible for a digital asset to simultaneously achieve perfect *Decentralization*, absolute *Price Stability*, and *Regulatory Sovereignty*. Every model analyzed in this work represents a deliberate optimization of one variable at the severe expense of another. Perhaps the most revealing outcome of this trilemma is the stark divergence between the theoretical ethos of the cryptocurrency movement and its practical implementation. A critical paradox of the current digital asset landscape is the mechanism of retail adoption. Despite the foundational "Cypherpunk" vision of complete disintermediation and financial self-sovereignty, the vast majority of market participants do not interact with the blockchain directly. Instead, mass adoption has been facilitated by heavily centralized exchanges (such as Binance and Crypto.com) and integrated neo-banking platforms (such as Revolut and Trade Republic).

By opting for the frictionless user experience of these custodial platforms, retail investors willingly surrender their cryptographic independence, routinely ignoring the foundational maxim: "not your keys, not your coins." Consequently, this mode of adoption does not facilitate true decentralization; it merely recreates a secondary layer of financial intermediation. Users have effectively substituted traditional commercial banks with new, corporate custodians, reintroducing the exact counterparty risks the blockchain was invented to eliminate.

Furthermore, the illusion of pseudonymity and independence has been systematically neutralized by the State. Because these centralized gateways must operate under strict Know Your Customer (KYC) and Anti-Money Laundering (AML) regulatory frameworks, every conversion between fiat and crypto is perfectly traceable by state authorities. The original promise of censorship resistance is entirely bypassed at the point of access. Additionally, these new intermediaries engage in aggressive rent-seeking behavior, imposing substantial fees on crypto purchases, conversions, and network withdrawals. The financial system has not been disintermediated; it has merely shifted its gatekeepers, forcing retail users to pay traditional transaction costs to corporate entities in exchange for convenience.

Therefore, the ultimate conclusion of this thesis is a projection of assimilation rather than revolution. Bitcoin will not replace the US Dollar or the fiat system as the global unit of account; its economic rigidity and the market's preference for centralized convenience make that outcome impossible. The future of money is definitively hybrid. CBDCs and highly regulated, compliant stablecoins (governed by frameworks like the EU's MiCA) will dominate daily commerce, effectively upgrading the speed and efficiency of the traditional banking perimeter without disrupting its hierarchical power structure.

However, the failure of the utopian, bankless global economy does not negate the profound impact of the cryptographic revolution. Bitcoin has successfully carved out a permanent, undeniable niche. It will persist alongside the regulated fiat system as an asymmetric, non-sovereign reserve asset—a highly volatile but unacceptable safe haven for capital. Ultimately, money is no longer solely a legal and political construct mandated by the State; it has permanently evolved into a competitive, cryptographically enforced technology.

Works Cited

Adrian & Mancini-Griffoli. (2021). Analysis of Deep-Seated Inefficiencies in Legacy Financial Systems.

Allen et al. (2020). Analysis of Central Bank Digital Currencies and Crypto-Assets.

Ammous. (2018). Argument Classifying Bitcoin as Sound Money.

Antonopoulos. (2014). Banking the Unbanked through Technology.

Baur et al. (2018). Investigation into Bitcoin's Correlation with Traditional Financial Assets.

Bech & Garratt. (2017). The Money Flower: A Taxonomy of Currency. Bank for International Settlements.

Böhme et al. (2015). Observation on the Resilience of the Bitcoin Protocol.

Briola et al. (2023). Identification of Token Economic Misalignment in the Terra Network.

Bullmann et al. (2019). Taxonomy of Stablecoin Collateralization Models. European Central Bank.

Chaum, D. (n.d.). Philosophical Arguments on Cryptographic Privacy as a Prerequisite for a Functional Democracy.

CoinShares. (2019). Studies Suggesting Economic Incentives Align Bitcoin Mining with Renewable Energy.

Dai, W. (1998). The B-Money Proposal and Blueprint for Decentralized Monetary Systems.

De Vries. (2018). The Digiconomist Index Quantifying Energy Consumption.

De Vries. (2019). Electronic Waste and the Bitcoin Network.

Dwyer. (2015). The Economics of Bitcoin and Similar Private Digital Currencies.

Eichengreen. (2019). Arguments Regarding Stablecoins and Fiat Currency Stability.

European Central Bank. (2012). Early Institutional Reports Categorizing Bitcoin as a Virtual Currency Scheme.

Foley et al. (2019). Analysis of Illegal Activity on the Blockchain.

Gorton & Zhang. (2021). Historical Parallel between Stablecoins and the Wildcat Banking Era.

Guesmi et al. (2019). Observations on the Weakening Trust in the Existing Financial Structure.

Hughes, E. (1993). A Cypherpunk's Manifesto.

Luther. (2016). Bitcoin and the Future of Digital Payments.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing List.

Narayanan & Clark. (2017). Bitcoin's Academic Pedigree.

Narayanan et al. (2016). Explanation of the Unspent Transaction Output Model and Cryptography.

Panetta. (2021). Defensive Motivations behind the Digital Euro Project.

Prasad. (2021). Programmable Money as an Active Policy Tool.

Szabo, N. (1998). The Bit Gold Concept and Architecture.

The Times. (2009). Chancellor on Brink of Second Bailout for Banks.

Uhlig. (2022). The Inherent Fragility of Algorithmic Pegs and Death Spirals.

World Bank. (2023). Remittance Prices Worldwide.

Yermack. (2013). Is Bitcoin a Real Currency?

Zuboff. (2019). Surveillance Capitalism and the Extraction of Behavioral Data.

Acknowledgements