Crypto: Scarcity and the Case for Abundance

A White Paper on Bitcoin, Good Money and Abundance Currency

Bart Van Coppenolle Executive Chairman, Good Money – Choice NV
Author of Good Money—How Complementary Value Currency can Save us from the Current Crisis (2012)

Abstract

This White Paper examines the existential fragility of Bitcoin's scarcity-based design and introduces **Good Money**, an abundance currency grounded in redeemable, real-world value. While Satoshi Nakamoto's 2008 paper solved the cryptographic problem of double-spending, it left unresolved the economic problem of scarcity. Bitcoin's fixed cap of 21 million coins, compounded by lost wallets and synthetic derivatives, has created unintended scarcity, volatility, and instability.

Good Money corrects these vulnerabilities by integrating Austrian principles of redeemability and full reserve with modern adaptability. Backed by value stocks selected according to intrinsic-value criteria, Good Money dynamically adjusts supply to demand, ensuring stability without inflationary abuse. Privacy, governance, and Personal Data Continuity secure trust across generations, while hazard-proof vaults and self-custodial wallets anchor ownership in human dignity. Together, these innovations transform digital currency from a fragile scarcity model into a resilient abundance system.

Keywords: Bitcoin; Scarcity vs. Abundance; Austrian Economics; Redeemability; Value Stocks; Intrinsic Value; Proof of Work; Proof of Stake; Privacy; Governance; Personal Data Continuity; Hazard-Proof Vaults; Self-Custodial Wallets; Abundance Currency; Locked Social Networks

1. Introduction: Beyond Cryptography, Toward Good Money

When **Satoshi Nakamoto** published **Bitcoin: A Peer-to-Peer Electronic Cash System** in **2008**, the paper was a breakthrough in cryptography and distributed computing. It solved the double-spending problem through proof-of-work and decentralized consensus, laying the foundation for a new era of digital money. Yet, for all its brilliance, the white paper was silent on one of the most fundamental questions of monetary science: scarcity and its economic consequences.

Bitcoin's fixed cap of 21 million coins was embedded in the protocol, but it was presented as a technical rule, not as an economic principle. The white paper did not explore how scarcity interacts with value, demand, or long-term sustainability. It did not address inflation, deflation, or the role of redeemability in securing trust. In short, it solved the cryptographic problem but left the economic problem untouched. This omission has become Bitcoin's existential threat. Scarcity, once hailed as the ultimate guarantor of trust, has revealed its fragility. Paper Bitcoin, synthetic derivatives, and competing cryptocurrencies dilute the scarcity narrative. Miner incentives weaken as issuance declines. Price volatility undermines Bitcoin's role as money. Scarcity alone cannot sustain trust in the long run.

My intention is therefore not to propose new cryptographic technologies or incremental tweaks to proof-of-work, proof-of stake or others. Instead, this White Paper speaks of what Satoshi did not: the economic foundations of money. It is a discussion of scarcity, abundance, and redeemability—concepts that lie outside cryptography but inside the heart of monetary science.

This paper argues that Bitcoin's scarcity model is insufficient and unstable. It proposes an alternative: Good Money, an abundance currency grounded in redeemable, real-world value. Where scarcity artificially limits supply and creates instability, abundance dynamically adjusts to demand, anchoring trust in productive assets. By integrating Austrian principles of redeemability and full reserve with modern mechanisms of adaptability, Good Money seeks to end the vulnerabilities inherent in scarcity-based money.

2. The Scarcity Debate in Crypto

2.1. Bitcoin Maximalists

Scarcity advocates argue that Bitcoin's fixed cap is the most trustworthy monetary policy ever devised. They liken it to digital gold, a system immune to inflationary abuse. For them, immutability is non-negotiable: scarcity equals trust. This camp sees the 21 million limit not as a technical choice but as a cultural cornerstone.

2.2. Critics of Fixed Scarcity

Adaptive critics challenge this view. **Eli Ben-Sasson**, co-founder of Zcash, has argued that perpetual issuance—around 4% annually—would better sustain miner incentives and prevent a collapse in network security. Vitalik Buterin, creator of Ethereum, has embraced adaptability through mechanisms like EIP-1559, which balances issuance with burning. For these thinkers, sustainability outweighs ideological scarcity.

2.3. Derivative Skeptics and Defenders

A third group focuses on derivatives and synthetic exposure. Analysts such as **Robert Kendall** warn that "paper Bitcoin" dilutes scarcity by creating claims on coins that don't exist on-chain. Others, like **Harriet Browning** of Twinstake and **Luke Nolan** of CoinShares, counter that futures and ETFs don't mint new coins; scarcity remains intact. They compare Bitcoin to gold, where paper markets coexist with physical scarcity without undermining it.

2.4. Academic Economists

Finally, academic research has added nuance. A 2024 study by **Yukun Liu and Aleh Tsyvinski** published in ScienceDirect found that scarcity does matter, but it is not the sole driver of excess returns. Network effects and utility also play critical roles, suggesting that scarcity alone cannot explain crypto's value dynamics.

3. Austrian School Perspective

3.1. The Giants of the Austrian School

The Austrian School provides a powerful lens for interpreting the crypto scarcity debate. **Carl Menger (1871)** established that value is fundamentally subjective, arising from individual preferences rather than objective measures. **Ludwig von Mises (1912, *The Theory of Money and Credit*)** extended this to money, showing that its value depends on its purchasing power derived from historical use. **Murray Rothbard (1962, *Man, Economy, and State*)** emphasized full reserve principles, arguing that money must be backed to avoid instability. **Friedrich Hayek (1974, Nobel Prize in Economics)** highlighted the importance of price signals and the redeemability of money in its underlying assets, noting that trust in money must be anchored in objective mechanisms rather than left to subjective belief.

3.2. Methodology of the Austrian School

The Austrian School is distinctive in its methodology. Rather than relying on quantitative numerical models or mathematical equilibria, it builds on **axiomatic-deductive reasoning**. The foundation is **praxeology**, the science of human action, developed by Mises. Its axiom is simple yet profound: humans act purposefully. From this axiom, Austrian economists derive laws of value, exchange, and money. This approach contrasts sharply with mainstream economics, which often relies on statistical aggregates and mathematical equilibrium models.

3.3. Interpretation of the Austrian School in Bitcoin's Scarcity Debate

From the Austrian perspective, scarcity is independent of subjective value. This does not contradict the **Law of Diminishing Marginal Utility**, first formulated by **Hermann Heinrich Gossen (1854)** and later refined by Menger (1871). The law states that the subjective value of each additional unit of a good decrease as supply increases. Scarcity can therefore drive price upward without altering the subjective nature of value.

People who fail to appreciate the difference between value and price are easily influenced—sometimes genuinely, sometimes manipulatively—by price signals. Since their contribution to price equilibrium passes through their subjective perception of value, this does not contradict the Austrian axiom of subjective value.

Other authors have described the emotional dynamics of markets. **John Maynard Keynes (1936)** coined the phrase "**animal spirits**" to capture the panic of bear markets and the greed of bull markets, impulses rooted in the reptilian brain of the speculator.

In our interpretation, **(2012-2024**, ***The Good Money Trilogy*****)** value is a right-brain subjective moral projection, while price is a left-brain linguistic-numerical projection. This distinction clarifies why markets swing between emotional extremes while still obeying the Austrian axiom of subjective value.

3.4. Integrating the Law of Demand and Supply

The **Law of Supply and Demand**, first clearly formulated by **Adam Smith (1776, *The Wealth of Nations*)**, describes how price signals communicate scarcity or abundance. Scarcity can indeed drive objective market price at any given time by artificially limiting supply, often temporarily and thus creating volatile price signals. In the case of Bitcoin and its fixed supply cap, scarcity also creates long-term upward pressure on price, as long as the cap is not circumvented by "paper Bitcoin" and as long as no competition exists. Both conditions are no longer valid in today's market, which partially explains the downward trend in Bitcoin's current price.

Beyond temporary scarcity, network effects and utility drive fundamental demand. Network effects increase the number of participants who can weigh on price formation by becoming aware of a good, subjectively valuing it through its utility, or projecting its future value for society. This is where speculation detaches from mere temporary scarcity and short-term volatility, and becomes a long-term value-added activity for society—as Mises correctly pointed out.

Price serves as an objective measure of a temporary equilibrium emerging from the exchange of value between market participants and available supply. The responsiveness

of supply and demand to price changes is captured by **price elasticity**. When derived for supply (with constant demand), it is supply's price elasticity; when derived for demand (with constant supply), it is demand's price elasticity. The inverse of these elasticities can be understood as buying power and selling power.

3.5. Applied to Money and Currency

Money and currency must be distinguished. **Georg Friedrich Knapp (1905, *The State Theory of Money*)** first emphasized this difference, later reinforced by Mises. Money is the abstract medium of exchange, store of value, and unit of account. Currency is its tangible or digital representation in transactions.

In summary, scarcity drives price by artificially limiting supply, while network effects and utility drive demand. Price is an objective measure of value at any given point in time, but value itself remains fundamentally subjective. For **real goods**, the law of supply and demand describes how price signals communicate scarcity or abundance in a free, open market.

Fiat money and Bitcoin, however, are not real goods. They are purely **monetary** and not backed by real goods. That is why economists distinguish between real economic growth and monetary inflation or deflation. Real growth must be corrected for monetary effects. By artificially creating scarcity in the money supply, the price of money increases, causing deflation. Oversupply has the opposite effect: the price of money decreases, goods and assets rise in price, and monetary inflation occurs. Both inflation and deflation are monetary instabilities that should be avoided in any good form of money.

Naked shorting is a prime example of oversupply distorting price signals by artificially suppressing price and causing panic. **George Soros's shorting of the British Pound (1992), the Indonesian Rupiah (1997), and the Russian Ruble (1998)** are examples of such non-real price signals causing huge damage to underlying economies. Initially, Bitcoin could not be shorted nakedly, since the ledger would not allow selling coins not owned. Today, however, with "paper Bitcoin," the secondary monetary base can be expanded, and naked shorting is possible, since it occurs off-chain.

4. Good Money: Towards an Abundance Currency

This chapter works further on my first book in the Good Money Trilogy (**2012, Good Money—How Complementary Value Currency can Save us from the Current Crisis**).

4.1. The principles of Good Money

Good Money, initially implemented as the Choice Coin (C^2), is designed to end the vulnerabilities inherent in scarcity-based hard money. Where scarcity artificially limits supply and creates instability, Good Money introduces a mechanism of abundance—adjusting money supply dynamically to its demand, while grounding monetary value in real, productive assets.

At its core, Good Money is fully backed by a diversified basket of publicly traded value stocks, selected according to **Benjamin Graham's (1934) intrinsic-value principles**—the same approach that inspired Warren Buffett's long-term investment philosophy. This ensures that every unit of currency is tied to real companies, real earnings, and real human value creation. In this way, Good Money integrates **Rothbard's full reserve principle (1962)**, guaranteeing that money is not an abstract claim but a redeemable instrument.

Redeemability is enforced through AI-driven smart contracts, which embody **Hayek's criterion (1974)** that trust in money must be rendered objective. Trust that remains subjective—as in fiat systems or crypto scarcity models—is always liable to collapse, producing volatility. By contrast, redeemability anchors monetary value in underlying assets, hedging against the risk of trust collapse and ensuring stability.

The system's **automatic arbitrage engine** ensures that market price converges to intrinsic value. When the price of the currency rises above liquidation value, smart contracts mint new tokens, sell them, and use the proceeds to buy more value stocks, expanding reserves and restoring balance. When the price falls below liquidation value, smart contracts buy tokens back, selling stocks to fund token repurchases, reducing supply and restoring equilibrium. In this way, Good Money integrates **Menger's insight (1871)** that value is subjective, while providing an objective benchmark for price evolution in a free, abundant market.

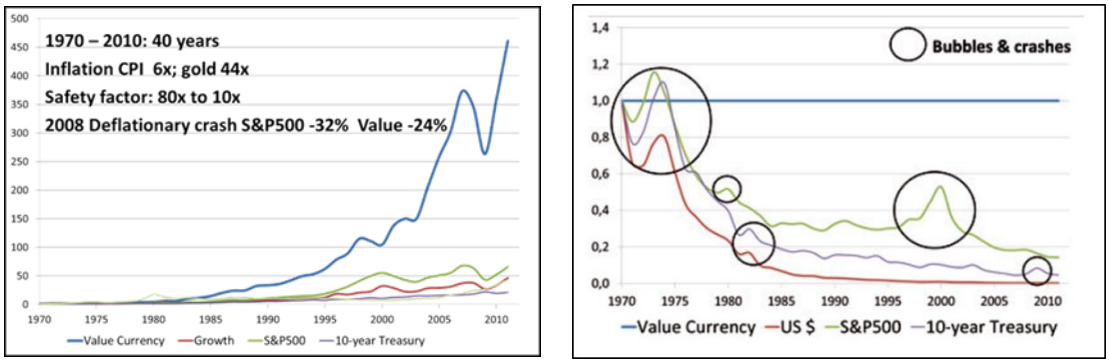
This design also addresses the critiques raised within the crypto community. **Ben-Sasson's concern** about miner incentives is resolved by ensuring supply adjusts dynamically, rather than relying on perpetual scarcity. **Buterin's principle of adaptability** is incorporated, but grounded in redeemable, real-world assets rather than abstract issuance. And the instability of Bitcoin's artificial scarcity is countered by creating an abundance currency that stabilizes price without inflationary abuse.

By combining Austrian principles with crypto-native critiques, Good Money becomes more than a monetary system—it truly is an abundance currency. It avoids the pitfalls of deflation and inflation, eliminates the distortions of oversupply such as naked shorting,

and ensures that monetary trust is not left to subjective belief but rendered objective through redeemability.

4.2. Historical Performance Compared to Bitcoin

The historical performance of Good Money rests on empirical foundations. Over a forty-year period from 1970 to 2010, **Steven De Klerck's** thesis **Value and The Rest (2012)** used a MATLAB-based model to validate the performance of value stocks against the U.S. dollar, the S&P 500, and bonds. His findings confirmed that value stocks consistently outperformed traditional monetary benchmarks, delivering resilience across inflationary and deflationary cycles, as shown in the figure below.



Empirical proof of protection against monetary instabilities by Good Money: left graph expresses Good Money in US$ fiat currency, the right graph does the inverse and expresses US$ and other fiat denominated assets in Good Money.

This evidence provides the foundation for Good Money's design: a currency backed by intrinsic value, capable of tracking real economic growth rather than speculative scarcity and other monetary instabilities.

Building on this foundation, the next fifteen years have been tested using **AI-based models**, which simulate the dynamic adjustment of supply to demand in a value-backed monetary system. These tests confirm that Good Money can maintain stability while appreciating in line with real economic value creation. By anchoring money in value stocks selected according to Benjamin Graham's principles, Good Money aligns with long-term profit and cashflow creation, while dynamically correcting for volatility. This ensures resilience against both inflationary fiat instability and deflationary hard caps.

Bitcoin's historical trajectory, shown in the following figure, illustrates the vulnerabilities of scarcity-based design.

Initially, Bitcoin's price rose dramatically as early adopters recognized its societal potential as an alternative electronic money. Network effects amplified awareness, and scarcity—no competition, no paper Bitcoin, neither fiat pegged stablecoins —allowed price inflation.

Bitcoin's price expressed in US$ over its lifespan until today.

Yet Bitcoin lacked redeemable backing assets. As competition emerged and stablecoin and "paper Bitcoin" diluted scarcity, the downward trend could not be compensated. Today, Bitcoin's price volatility reflects this structural weakness.

4.3. Tesla's Frequency Lens on Intrinsic Value in AI-based models

Intrinsic value can be defined as the level to which markets organically converge in the long run. For stocks, this convergence is measurable in multiples of yearly profit or cashflow, the tangible outputs of real economic activity. In the shorter run, intrinsic value may be reflected in assets, revenue growth, traction, societal contribution, or market potential—signals that point toward sustainable value creation even before profits fully materialize.

Through the lens of frequency, intrinsic value represents the low-frequency component of markets: the slow-moving, grounded curve that reflects fundamentals. In contrast, the high-frequency component captures volatility—the rapid oscillations of buying and selling, driven by sentiment, news, or speculation. Technical Analysis (TA), rooted in **Charles Dow**'s insights from **1896**, excels at navigating these high-frequency swings, while Fundamental Analysis (FA), pioneered by Benjamin Graham in 1934, anchors to the low-frequency trajectory of intrinsic value. Nikola Tesla's inspiration on frequency reminds us that systems can be decomposed into stable waves and chaotic oscillations. Systems theory applies seamlessly to financial markets.

Applied to cryptocurrencies such as Bitcoin and Telegram coin, this frequency lens reveals their structural weakness. Initially, both were recognized for their societal potential—Bitcoin as an alternative form of money, Telegram coin as a privacy-enhancing medium.

Network effects amplified awareness, while scarcity inflated price. Yet without backing assets or redeemable value, the downward trend could not be compensated once competition and dilution emerged. Scarcity alone proved insufficient to sustain trust or stabilize price.

The conclusion is clear: long-term value creation aspirations are better captured in stocks than in unbacked money itself. Stocks embody real economic activity, measurable in profits and cashflows, and thus provide a foundation for intrinsic value. Money, by contrast, must remain stable to serve its purpose as a medium of exchange and store of value. When money is designed around scarcity without redeemable backing, it risks volatility and eventual decline. By integrating the frequency lens with the principles of Dow, Graham, and Tesla, we see that true stability lies not in scarcity but in anchoring money to real, productive value.

4.4. Liquidity and Flow of Value

Money only becomes currency when it flows. The very word “currency” derives from “current”—a stream, a movement. Scarcity without circulation is sterile; abundance without flow is meaningless. For a monetary system to serve society, it must generate liquidity, ensuring that value moves continuously between participants rather than stagnating in dormant wallets.

Good Money integrates liquidity-generating mechanisms that transform static value into dynamic currency. The **Good Food Initiative** exemplifies this principle: by collateralizing farmer–consumer guarantees, it creates a flow of value rooted in real production and consumption. Farmers receive stable demand, consumers secure reliable supply, and the currency itself becomes a conduit of trust. Similarly, **Traforex** extends liquidity into trade finance, enabling workers and businesses to exchange value seamlessly across borders.

4.5. Integration of Seed & Venture capital

To sustain a continuous supply of value itself, Good Money also embraces private equity such as venture capital, and seed capital activities, pre-IPO. Here, value is voluntarily locked in return for a dilutive premium—an additional **5% return**. Unlike traditional venture capital, where high returns compensate for concentrated individual risk, Good Money distributes risk across the community and the return flows back to the entire community in the form of increased value backing the currency. The premium therefore dilutes the monetary base and reduces per-token return slightly, ensures that no single participant bears the full burden of venture risk and increases the yearly return on the coin itself. This collective absorption of risk stabilizes the system, while the 5% premium rewards those

who commit their capital for the long run without exposing them to the extreme volatility or leverage typical of private equity.

In this way, voluntary lock-in creates a disciplined flow of value: capital is invested, returns are generated, and liquidity is replenished. Unlike speculative scarcity, which freezes coins in inaccessible wallets, Good Money's liquidity mechanisms ensure that value is continuously unlocked, circulated, and reinvested. Liquidity becomes the lifeblood of an abundance economy, transforming money into a true current of trust, labor, creativity and productivity.

4.6. The Human Factor

While liquidity mechanisms and venture integration ensure that Good Money remains dynamic and resilient, no system can rely solely on algorithms or automated contracts. Human judgment, conscience, and governance remain indispensable.

Good Money therefore embeds a **governance** layer that balances technological automation with human oversight. A dedicated value and seed/venture team — composed of experienced professionals rather than bots — ensures that investment decisions, arbitrage processes, and capital commitments are guided by prudence rather than blind automation. This prevents the trust problem often associated with oracles and high-frequency trading bots, where mechanical signals can be manipulated or detached from real economic truth and thus value.

Governance is structured around rigorous checks and balances. Inspired by the classical idea of the "philosopher king," final veto rights are vested in a human authority who can be ostracized if trust is broken. Decision-making is prepared collectively, encrypted communications safeguard integrity, and signatures of trust are required before execution. In this way, conscience and human subjective human value attribution and judgement is not outsourced to AI; it remains firmly anchored in human responsibility.

By integrating the human factor, Good Money ensures that abundance is not only a technical construct but also a moral one. This prepares the ground for the next dimension — the hardware safeguards of self-custodial wallets — where individual ownership and security complete the circle of trust.

4.7. John Locke, values and virtues embedded of consciousness

The design of Good Money ought not to rest solely on cryptography or economics. It is anchored in a deeper philosophical and human foundation: the separation of inner conscience — and thus subjective value attribution — from external power — and thus regulation — articulated by **John Locke** (**1689, A Letter Concerning Toleration**) as the

principle of distinguishing the business of civil government from that of religion, later popularized as the *separation of church and state*, and confirmed centuries later by neuroscience.

Locke's principle was simple yet profound: the inner world of conscience — private belief, thought, and values — must remain free from intrusion, while the outer world of power — law, regulation, and public order — must be structured to manage risks without violating human dignity. This duality mirrors the architecture of the human brain itself. Right-brain consciousness projects empathy and positive emotion, treating humans as subjects; left-brain consciousness manages fear and external threats, treating risks as objects. Evolution's success lies in keeping these two hemispheres distinct, bridged only by a narrow corpus callosum — a reminder to *mind the gap* — as described in my second book in the Good Money Trilogy (**2024, The Secret of Success – Evolution of Brain, Mind and Spirit**).

Applied to money and networks, this separation becomes a law of good design. In **Locked Social Networks**, the inner world is protected: private data, communication, and conscience are locked in wallets in hazard-proof vaults, encrypted and shielded from surveillance or exploitation. The outer world is compliant: public communication operates under law, structured by constitutional safeguards and regulatory frameworks. Users are empowered as subjects, not commodified as objects in e.g. social media: *locked networks* instead of *media*, since not all people want to be journalists, all the time.

In Good Money, the same principle governs ownership. Self-custodial wallets embody Locke's separation: private keys remain in the inner world of the individual, shielded from external confiscation or dilution. Redeemability anchors trust in real assets, while governance ensures risks are managed in the external world. By embedding Locke's values into both currency and networks, Good Money restores the balance between freedom and responsibility — empathy and risk control — as virtues embedded in human consciousness.

4.8. Privacy

Privacy is the cornerstone of digital trust: without it, abundance collapses into instability and redeemability loses meaning. If abundance ensures stability and redeemability anchors value, privacy secures human dignity. Without it, neither networks nor money can serve humans as subjects rather than objects.

Locked Social Networks embody this principle by structurally separating the inner world from the outer world. The inner world — private data, conscience, cryptographic keys — is protected in hazard-proof vaults, encrypted and shielded against intrusion. The outer world

— public communication — is fully compliant with law and regulation, ensuring that risk is managed without violating human dignity.

This ethos was present at the very origins of crypto. Early pioneers such as **Len Sassaman and Hal Finney** focused first on privacy technologies — anonymous remailers, PGP encryption — before money itself. Bitcoin inherited this legacy, but its scarcity narrative overshadowed it in practice. Telegram's coin followed a similar trajectory: initially promising privacy in messaging and transactions, but ultimately too unstable to function as currency. Good Money restores balance by placing privacy at the foundation, redeemability as the anchor, and abundance as the principle.

In Good Money, privacy is not an accessory but a structural law of design. It ensures that the inner world of conscience and value remains inviolable, while the outer world of communication and exchange remains lawful.

4.9. Personal Data Continuity

The story of Bitcoin cannot be told without acknowledging its silences. Satoshi Nakamoto, the pseudonymous creator, vanished from public communication in 2010, leaving behind an untouched hoard of roughly 1.1 million BTC. His disappearance became the first great mystery of crypto. Yet he was not alone. Several early pioneers—**Len Sassaman, Hal Finney, Adam Tepper, Mircea Popescu, Gerald Cotten, John McAfee, Nikolai Mushegian, and Dave Kleiman**—died young or under suspicious circumstances. Some deaths were confirmed, others disputed, and in each case vast amounts of crypto wealth were frozen, inaccessible to markets. Studies estimate that nearly 18% of Bitcoin is no longer active, locked in wallets whose keys are lost forever. This unintended scarcity magnifies volatility and undermines trust, creating a monetary system that depends precariously on individual key management without continuity safeguards.

To solve the fragility revealed by lost coins and vanished pioneers, another technology must be added: **Personal Data Continuity**. Unlike stocks, which remain active as long as companies operate, cryptocurrencies face unique risks when individuals lose access to their private keys or pass away unexpectedly. Continuity ensures that monetary assets survive beyond the lifespan of their holders. Hazard-proof vaults, shielded against both digital intrusion and physical disruption, can preserve private data and keys across generations. Legal escrow procedures can do the rest. This hybrid of cryptographic and legal technology secures not only the coins but the trust that underpins them. It integrates privacy, redeemability, and continuity into one system, ensuring that the inner world of conscience and value remains protected while the outer world of transactions remains lawful, just as John Locke wanted it almost half a millennium ago.

4.10. Self-custodial hazard free hardware wallets

The hardware dimension is therefore equally critical. Cold wallets, disconnected from the internet, cannot be hacked. Even electromagnetic pulses (EMPs), once feared as ultimate disruptors, are powerless against well-shielded vaults. Good Money integrates a hybrid model of hardware and software, balancing centralized safeguards with distributed resilience. Governance blends democracy with philosopher-king oversight, guided by common sense economics rather than ideology.

Self-custodial wallets are therefore indispensable. Only when individuals hold their coins directly, with private keys under their sole control, can ownership be considered complete. Indirect substitutes—financial derivatives, custodial accounts, or coins whose validity can be switched off by third parties under certain criteria—undermine the very principle of monetary sovereignty. In such arrangements, rights to coins are partial at best, and control can be revoked externally. Good Money rejects this fragility by ensuring that custody remains with the individual, backed by redeemable assets rather than abstract claims. In this way, self-custody becomes not only a technical safeguard but a moral commitment to genuine ownership and trust. Unlike "paper Bitcoin," which dilutes scarcity by creating off-chain claims without true personal control, self-custody in Good Money preserves integrity and ensures that every coin represents real, redeemable value.

5. Cryptographic Technology

5.1. History of Cryptography

Cryptography has always been driven by one enduring purpose: protecting information from adversaries. Yet the methods by which this protection has been achieved have evolved dramatically across eras, shaped by mathematics, technology, and the scale of threats.

Ancient and Classical Foundations (~1900 BCE – 500 CE)

Early cryptography served **military and diplomatic** secrecy. Substitution **ciphers**, such as the **Caesar** cipher, shifted letters by fixed amounts, while transposition ciphers like the Spartan scytale rearranged letters on a rod. Security depended entirely on the secrecy of the method, a fragile foundation once the technique became known.

Medieval and Renaissance Advances (500 – 1800)

As political intrigue deepened, cryptanalysis emerged. Arab scholars such as **Al-Kindi** pioneered frequency analysis in the 9th century, breaking simple substitution ciphers by exploiting predictable **letter frequencies**. In response, polyalphabetic ciphers like the

Vigenère cipher introduced complexity by varying substitutions with a keyword. Hybrid systems, known as nomenclators, combined cipher alphabets with codebooks, becoming standard in diplomatic correspondence.

The Mechanical Era (1800 – 1940s)

Industrialization and global conflict elevated cryptography to a matter of national survival. Mechanical cipher devices culminated in **rotor machines** such as the German **Enigma**, whose constantly shifting substitutions challenged adversaries. Cryptanalysis itself became industrialized: Poland's **Biuro Szyfrów** and Britain's Bletchley Park, with **Alan Turing**'s team, built electromechanical machines to break Enigma, shortening World War II and laying foundations for modern computing. **Claude Shannon**'s proof of the one-time pad's perfect secrecy (**1949**) marked a theoretical milestone, though its impracticality limited use to high-stakes diplomacy and intelligence.

The Dawn of Computer Cryptography (1940s – 1970s)

With electronic computing, cryptography expanded beyond military secrecy to civilian applications. Shannon's information theory formalized confusion and diffusion as design principles. The **Data Encryption Standard** (DES), adopted in 1977, became the first widely used symmetric-key standard. Yet the unsolved problem of secure key distribution remained: how could two parties share a secret key over an insecure channel without meeting in person?

The Public-Key Revolution (1976 – 1990s)

This problem was solved by **Diffie–Hellman** key exchange (**1976**), enabling two parties to establish a shared secret over a public channel. **RSA** (**1977**) introduced true asymmetric cryptography, pairing public keys for encryption with private keys for decryption. This breakthrough enabled digital signatures and became the backbone of secure web traffic, email encryption, and digital certificates. Alongside, hash functions matured to verify integrity and support authentication.

Modern Standardization (1990s – 2010s)

As the internet scaled globally, cryptography needed speed, efficiency, and public vetting. **AES** replaced **DES** in **2001** after an open competition, becoming the dominant symmetric cipher. **Elliptic Curve Cryptography (ECC)** offered equivalent security with smaller keys, ideal for mobile devices. Hash families **SHA-2** and **SHA-3** replaced weakened predecessors, while **TLS** became the universal protocol securing web traffic. Cryptography shifted from a specialist tool to invisible infrastructure embedded in everyday consumer technology.

The Current Era (2010s – Now)

Cryptography today faces new challenges: **mass surveillance**, **decentralized trust** systems, and the looming threat of **quantum computing**. End-to-end encryption, blockchain, homomorphic encryption, zero-knowledge proofs, and post-quantum cryptography define this frontier. Each represents not only technical innovation but also a response to evolving adversaries. A deeper exploration of these threads follows in the next subchapter.

5.2. Current Cryptographic Technology

The current era of cryptography is defined by its dual role: invisible infrastructure securing billions of daily interactions, and frontier science preparing for existential mathematical threats. Five major threads illustrate how cryptography today balances practical deployment with future resilience.

End-to-End Encryption (E2EE)

Since **Edward Snowden**'s **2013** revelations on mass surveillance, **E2EE** has become mainstream in consumer messaging. The Signal Protocol, adopted by Signal, WhatsApp, and others, combines the Double Ratchet Algorithm with **X3DH** key exchange to ensure forward secrecy and post-compromise security. Each message uses fresh keys, so even if one is compromised, past and future communications remain protected. This marks a structural shift: service providers themselves cannot access user content, reinforcing privacy as a design principle rather than an optional feature.

Blockchain and Cryptocurrencies

Bitcoin's **2008** white paper applied cryptographic hashing and digital signatures to create decentralized, trustless ledgers. **SHA-256** secures Bitcoin's block chain, while elliptic-curve signatures (**ECDSA**) authorize transactions. **Merkle trees** summarize blocks efficiently, and consensus mechanisms such as **Proof-of-Work and Proof-of-Stake** secure networks against tampering. Beyond currency, these primitives enable **smart contracts**, **decentralized identity**, and supply-chain verification, extending cryptography's role from secrecy to trust in open, adversarial systems.

Homomorphic Encryption

Craig Gentry's **2009** breakthrough in fully homomorphic encryption (**FHE**) opened the possibility of computing directly on encrypted data. Schemes such as **BGV**, **BFV**, and **CKKS** now allow privacy-preserving analytics and machine learning, though performance

remains a barrier to widespread use. Current deployments focus on high-value domains such as medical data and secure cloud computing, where confidentiality is paramount.

Zero-Knowledge Proofs (ZKPs)

Originally theoretical in the **1980s**, ZKPs have matured into practical tools for privacy and scalability. **zk-SNARKs** and **zk-STARKs** allow one party to prove a statement without revealing underlying data. Applications range from privacy coins like **Zcash** to blockchain rollups that batch transactions with a single proof, and emerging identity systems where eligibility can be proven without disclosing documents. These methods extend cryptography's scope from secrecy to selective disclosure.

Post-Quantum Cryptography (PQC)

Quantum computing threatens to break RSA and ECC via Shor's algorithm, prompting a global migration to quantum-resistant algorithms. In **2024**, **NIST** finalized its first **PQC standards**: **ML-KEM** (encryption, based on lattice problems), **ML-DSA** (signatures), and **SPHINCS+** (hash-based signatures as a backup). Hybrid deployments combining classical and post-quantum algorithms are now common, ensuring continuity during transition. This represents the largest cryptographic infrastructure overhaul since the advent of public-key cryptography in the 1970s.

In summary, current cryptographic technology is no longer confined to secrecy between known parties. It now secures decentralized networks, enables privacy-preserving computation, and prepares for a quantum future. The throughline is clear: cryptography evolves not only to protect information, but to sustain trust in systems where adversaries, scale, and mathematics themselves continually shift.

5.3. Bitcoin's Cryptographic Technology

The foundations of crypto money are technological, and each breakthrough carries both brilliance and limitation. Bitcoin's design drew on decades of cryptographic innovation, combining asymmetric keys, consensus mechanisms, and immutable ledgers into a functioning digital currency. Yet these same components reveal structural fragilities that Good Money seeks to address.

Asymmetric Keys

Whitfield Diffie and Martin Hellman's 1976 breakthrough in **public-key cryptography** enabled secure communication without prior exchange of secrets. In Bitcoin, private keys authorize transactions and public keys verify them, ensuring ownership and integrity. This remains the bedrock of all cryptocurrencies.

Computational Difficulty, not impossibility

Alan Turing's codebreaking work at Bletchley Park **(1939 – 1940)**, during World War II, demonstrated that **brute force attacks** can eventually overcome highly complex systems through sustained computational effort. **Claude Shannon**'s 1949 proof of the one-time pad established that perfect secrecy is possible when keys are truly random, used only once, and kept secret — a standard Bitcoin does not achieve, since it relies instead on computational hardness. While Bitcoin relies on computational hardness to secure its network, advances in hardware — from supercomputers to quantum machines — remind us that no algorithm is invulnerable indefinitely.

Consensus Mechanisms

Satoshi Nakamoto's 2008 design solved the **double-spending problem** through **majority agreement**, but it introduced the risk of 51% attacks: if one actor controls most of the network's computing power, trust collapses. **Proof of Work**, adapted from **Cynthia Dwork and Moni Naor's 1993** proposal, secures Bitcoin through energy-intensive computation. **Proof of Stake**, introduced in **2012** by **Sunny King and Scott Nadal**, ties consensus to ownership rather than computation. Both approaches reduce reliance on central authority but remain vulnerable to concentration of power.

Ledger Immutability

The blockchain, formalized by Satoshi as a distributed timestamp server, ensures that once transactions are recorded they cannot be altered. This immutability is elegant, but without redeemable backing assets it leaves scarcity as the sole anchor of trust. Bitcoin's fixed cap of 21 million coins is a technical rule rather than a monetary policy, and derivatives such as "paper Bitcoin" or stablecoins dilute the scarcity narrative by creating off-chain claims.

Toward Abundance

Good Money builds on these same technologies while correcting their disadvantages. It retains asymmetric keys for secure ownership, consensus for distributed trust, and immutable ledgers for transparency. But it anchors value in redeemable assets, ensuring that trust does not rest solely on scarcity. Where **Bitcoin's hard cap risks deflationary instability**, **Good Money dynamically adjusts supply to demand, backed by value stocks**. Where derivatives dilute scarcity, redeemability restores integrity. In this way, Good Money transforms the technological foundations of crypto into a monetary system grounded in stability, resilience, and abundance.

5.4. Collaboration of Foundations

The question of whether to adopt existing technologies or to develop new ones is not merely technical and commercial; it is moral and philosophical. Cryptography, governance, and abundance currency are built on foundations that must be both resilient and trustworthy. Some components — such as ledgers, consensus mechanisms, and custody hardware — already exist in mature, battle-tested form. Others — such as the vault, continuity safeguards, and the integration of conscience with power — must be created anew, because they embody the unique values of Good Money and Locked Social Networks.

This is not a binary choice between "**buy and build**." It is a layered strategy. Commodity resilience and baseline infrastructure can be adopted from the best of what is already available, accelerating deployment and reducing risk. But the philosophical pillars — the vault, the continuity of personal data, and the separation of inner conscience from external power — must be built, because they define identity and trust.

In practice, this means working with existing chains, wallets, and protocols where they are strongest, while inviting cryptographers, professional hackers, and commercial partners to join in building the components that do not yet exist. The ledger may be licensed, but the vault must be authored. Hardware may be bought, but continuity must be engineered. Protocols may be borrowed, but integration must be designed.

The future of Good Money therefore rests on collaboration: adopting proven technologies where they serve, and building new ones where they are essential. This dual path ensures speed to market without sacrificing the integrity of our vision. It also opens the door for specialists — from cryptographic researchers to resilience engineers — to contribute their expertise. In this way, Good Money becomes not only a currency of abundance, but a collective project of abundance in knowledge, skill, and trust.

We invite cryptographers, engineers, and builders to join us in shaping this foundation.

Conclusion

Scarcity alone cannot sustain trust in money. Bitcoin's fixed cap, once celebrated as digital gold, has revealed its fragility: volatility, dilution through derivatives, and deflationary instability. Good Money offers a structural alternative. By anchoring currency in redeemable value stocks, dynamically adjusting supply, and embedding privacy, governance, and continuity safeguards, it restores stability and resilience to digital money. The abundance model does not reject cryptography; it builds upon it. Asymmetric keys, consensus mechanisms, and immutable ledgers remain essential foundations. Yet true

trust arises not from scarcity but from redeemability, continuity, and human conscience. Good Money integrates these dimensions into one coherent system, ensuring that money serves people as subjects, not objects. This vision is not only technological but philosophical. Inspired by John Locke's separation of conscience and power, and confirmed by modern neuroscience, Good Money embodies freedom and responsibility as virtues embedded in human consciousness. It invites collaboration from cryptographers, economists, engineers, and communities to build a currency of abundance — one that flows like a current of trust, labor, creativity, and productivity across generations.

References

- Satoshi Nakamoto (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

- Carl Menger (1871). *Principles of Economics*.

- Ludwig von Mises (1912). *The Theory of Money and Credit*.

- Murray Rothbard (1962). *Man, Economy, and State*.

- Friedrich Hayek (1974). *The Pretence of Knowledge*. Nobel Lecture.

- Benjamin Graham (1934). *Security Analysis*.

- Adam Smith (1776). *The Wealth of Nations*.

- Hermann Heinrich Gossen (1854). *The Laws of Human Relations and the Rules of Human Action Derived Therefrom*.

- Georg Friedrich Knapp (1905). *The State Theory of Money*.

- John Maynard Keynes (1936). *The General Theory of Employment, Interest and Money*.

- John Locke (1689). *A Letter Concerning Toleration*.

- Claude Shannon (1949). *Communication Theory of Secrecy Systems*.

- Cynthia Dwork & Moni Naor (1993). *Pricing via Processing or Combatting Junk Mail*.

- Sunny King & Scott Nadal (2012). *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*.

- Steven De Klerck (2012). *Value and the Rest. Thesis*.

- Bart Van Coppenolle (2012). *Good Money — How Complementary Value Currency can Save us from the Current Crisis*.

- Bart Van Coppenolle (2024). *The Secret of Success – Evolution of Brain, Mind and Spirit*.