Bitname: A Peer-to-Peer Name-Pegged Stablecoin

Cyphrs
cyphrs@gmx.com
www.bitname.info

Abstract. This is what I colorfully like to refer to as a "greenpaper": a *foreshadowing* of a stablecoin *that cannot exist today but which should emerge once a critical mass of users selects* a preferred decentralized naming blockchain. Existing stablecoins either expose holders to custodial risk and dollar debasement (centralized) or suffer reflexive death spirals (algorithmic). We propose a third structure whose stability is not a peg but a band: a floor set by genuine utility demand for name registration, and a ceiling set by a dollar-denominated mint valve through which new tokens can always be created at a known, escalating cost. Tokens are colored Namecoin backed by Bitcoin locked in timelock contracts for 500,000 blocks (approximately 10 years) and returned to the original minter at maturity. This collateral proves commitment and caps the minter's downside rather than granting redemption rights. A vesting schedule (1/5 immediately available, 4/5 unlocking over four cycles) suppresses selling pressure and pushes utility-seeking users toward secondary markets. Programmatic escalation of minting costs (5% per Year) denominates the ceiling in inflation-adjusted dollars. The proposition is explicitly conditional: if the chosen protocol wins the naming market, its registration token matures into a stable unit; if it does not, minters recover their Bitcoin. We state this bet honestly and build the machinery for the world in which it pays off.

1. Introduction

The stablecoin trilemma of achieving price stability, decentralization, and capital efficiency simultaneously remains unsolved. Centralized stablecoins (USDT, USDC) sacrifice decentralization and expose holders to custodial risk and dollar inflation. Algorithmic stablecoins (Terra) collapse when confidence wavers. Both merely preserve exposure to the melting ice cube that is the purchasing power of the US dollar.

We present a third path: stability derived from intrinsic utility. Just as commodity money historically derived stable value from non-monetary uses, a token pegged to decentralized naming rights can derive stability from constant demand for digital identity infrastructure.

Why a greenpaper. This document does not claim such stability exists today. No registration token can hold stable value before a critical threshold of users adopts its blockchain as the preferred global naming protocol; members of a community must believe demand for its names will grow indefinitely before the token anchoring those names can be trusted as money. The honest formulation of the offer is an expected value: P(this protocol wins) × (a utility-anchored, inflation-adjusted stable unit) + P(it does not) × (Bitcoin returned at maturity, tokens near

worthless). Everything that follows describes the machinery that converts a win into stability, and caps the cost of a loss.

2. The Name-Pegged Stablecoin Model

2.1 Stability as a Band, Not a Peg

Every previous stablecoin held its peg through redemption arbitrage. $BITNAME deliberately has no redemption right; instead, its price is bounded by two independent forces:

1. **The Utility Floor:** Constant demand for name registration and renewal creates natural price support. That millions today renew domains at roughly $20/year (and rising) is evidence of durable willingness to pay for digital identity. It is demand evidence rather than a peg mechanism in itself, which is why a ceiling is also required.
2. **The Mint Valve Ceiling:** New tokens can always be created at a known dollar-denominated cost. If tokens trade meaningfully above effective minting cost, arbitrageurs mint and sell, expanding supply and pressing price back down. This is the only dollar-referencing mechanism in the system, and it is what distinguishes $BITNAME from every prior utility token, including those, like ETH, with enormous utility demand but no dollar-linked supply valve and therefore no stability.
3. **No Artificial Peg:** Between floor and ceiling, price floats on supply and demand for a genuinely useful resource.
4. **Inflation Hedge:** The ceiling escalates programmatically, so the band itself tracks monetary debasement.

The ceiling is soft, since the timelock and vesting schedule slow the arbitrage, and the floor is thin until adoption matures. The band tightens as the naming market grows. That is the maturation path from speculative instrument to stablecoin.

2.2 Gold is to Bitcoin as Uranium will be to [Global Naming Protocol]

Earth's oceans hold 4.5 billion tons of uranium: abundance without cheapness, because extraction cost ($200-400/lb from seawater vs $20-60/lb mined) sets the price. Digital names are likewise effectively infinite, but committing one to a secure blockchain has a real and rising cost once blockspace becomes scarce.

The analogy carries a warning we accept openly: congestion-priced blockspace is historically volatile, not stable. Section 6.2 addresses how adaptive registration pricing can convert a volatile fee market into a smoothed cost curve. The key insight stands: stability comes not from scarcity of names but from the intersection of abundance, utility, and the cost of secure registration.

3. Technical Requirements

The underlying naming protocol must possess:

Security Properties:

- Resistance to 51% attacks through high hashrate or robust consensus

- Censorship resistance at the protocol level
- No single points of failure or control

Economic Properties:

- Predictable, low-cost operations
- No dependence on volatile governance tokens
- Clear fee structure unaffected by speculation

Technical Properties:

- Support for cryptographic ownership proofs
- Ability to implement colored coins or equivalent
- Sufficient data storage for identity applications
- Reasonable expiration/renewal mechanisms

Decentralization Properties:

- No company or foundation with special privileges
- Open source and independently verifiable
- Geographic and jurisdictional distribution

4. Economic Dynamics

4.1 Price Discovery

Price emerges between the band's bounds from registration and renewal demand (the floor), the dollar-denominated mint cost (the ceiling), network effects (each user makes names more valuable), and, until a winner emerges, competition among naming protocols. Once the market selects a preferred protocol, external competition falls away and the band's internal mechanics govern.

4.2 Stability Mechanisms

- **Demand Floor:** People and organizations continuously need digital identity
- **Supply Valve:** Minting at known dollar cost caps sustained premiums
- **Utility Arbitrage:** Underpriced tokens get spent on registrations
- **Time Preference:** Names are registered to be used for years, not flipped. A name like alice.bit is held for identity, creating supply sinks that dampen volatility

Fungibility. Bitname tokens are fungible even though names are not. The token anchors to the cost of the marginal registration; premium names (alice.bit versus xj7k9q.bit) simply command premiums above that base in a separate market, exactly as premium .com domains trade above the standard registration fee without destabilizing it. Until spent on a name, tokens can function as money.

4.3 Inflation Protection

As fiat currencies inflate, the nominal cost of digital identity rises. A domain costing $20 today might cost $30 in a decade, not because names became more valuable but because dollars became less so. Everything is subject to inflation, even an entry in a database; the escalating mint valve tracks this reality, denominating the band in inflation-adjusted dollars for as long as the dollar remains the world's unit of account.

5. Advantages Over Existing Systems

5.1 Versus Centralized Stablecoins

Feature	**USDT/USDC**	**Name-Pegged**
Trust Required	Custodian, banks, auditors	Attestation only (bootstrap)
Censorship	Accounts routinely frozen	Permissionless
Inflation	Full dollar exposure	Band escalates automatically
Redemption	Issuer promise	None; band mechanics

5.2 Versus Algorithmic Stablecoins

Feature	**Terra/Algo**	**Name-Pegged**
Death Spiral Risk	Inevitable with confidence loss	Downside capped by returned Bitcoin
Complexity	Opaque algorithms	Transparent floor and ceiling
Real Backing	Circular (confidence only)	Locked Bitcoin + registration demand
Attack Surface	Many (algorithm gaming)	Minimal

Algorithmic stablecoins manufacture stability from nothing; Bitname's band emerges from utility demand below and a provable, dollar-priced supply valve above.

5.3 Costly Identity: The Coming Wave of Name Demand

Human demand for censorship-resistant identity grows as digital life migrates to decentralized systems: today's internet serves roughly 5 billion users through DNS, and many individuals and organizations will require multiple decentralized identifiers.

For AI agents the argument is sharper than mere uniqueness, since cryptographic keypairs already provide unique identifiers for free. What free keys cannot provide is **sybil resistance**. In a world of infinite costless agent identities, a name that provably cost $20 to register is a spam filter and a reputation anchor. Agents transacting with humans and with each other will pay for costliness itself: a burned-in stake that makes identities scarce enough to trust. As autonomous agents proliferate, paid names become the mechanism by which anyone distinguishes one persistent, accountable counterparty from a million disposable keys. With such demand plausibly arriving within a decade, names can credibly anchor a global money network independent of nation states.

6. Namecoin: The First Global Naming Protocol

6.1 Becoming Namecoin

In November 2010, users on the bitcointalk forum “BitDNS and Generalizing Bitcoin” explored blockchain-based domain registration. These discussions conceptualized domain objects, then called Bitnames, as indivisible units of value on a separate blockchain to avoid bloating Bitcoin. Though these indivisible objects were dropped for traditional fractional units, a key insight was missed: had attention been placed on preserving $BITNAME as a stable unit of account instead of an entirely new volatile cryptocurrency, Namecoin could have avoided being perceived as a threat by conservative community members primed to become Bitcoin maximalists. With less antagonism from ardent Bitcoin defenders, its chances would have been better. Nevertheless, from these discussions Namecoin became Bitcoin's first altcoin.

Namecoin extends Bitcoin's proven UTXO model with simple name operations. Through merge-mining it inherits approximately 60% of Bitcoin's hashrate at zero additional energy cost, providing security orders of magnitude beyond any independent naming blockchain. Operational since 2011, it demonstrates reliable, censorship-resistant naming with Bitcoin-level guarantees.

6.2 Critical Analysis: Strengths, Limitations, and the Scaling Unknown

Security: Merge-mined security dwarfs independent alternatives, which must bootstrap hash power or die. Layer two solutions require running both Bitcoin and layer two nodes to verify supply, an adoption barrier for users who only care about names.

Scalability Constraint: With roughly one billion potential Bitname tokens under current parameters, theoretical market cap reaches only $21 billion, which is modest for a global stablecoin. And since $NMC is burned in registrations, reaching $20 per token would consume much of the supply. A few million users would reveal these limits.

The Fee-Market Problem and the Adaptive-Cost Solution: A deeper issue: if millions adopt Namecoin, transaction fees alone to commit a name on-chain could exceed $20, and congestion-priced blockspace is among the most volatile prices in finance, a poor anchor if left raw. Namecoin developers have discussed two soft forks that together address both constraints. First, burned registration $NMC could be reintroduced through mining rewards. Second, registration cost could become algorithmic, set relative to the number of active registrations. This would convert a spiky fee market into a smoothed, demand-responsive cost curve and, since registrations only grow, adjust downward in $NMC terms in ways that benefit existing token holders.

We acknowledge candidly that a full scaling solution for billions of users does not yet exist; some hand-waving remains. The dream is that by the time this becomes the binding problem, the transition will already be underway: holders will no longer need the dollar to define stable value, and $NMC itself, anchored by global naming demand, will suffice as the preferred unit of account. At that point the band's dollar denomination becomes a historical artifact.

Comparative Assessment: These limitations are real, but alternatives face worse: new chains face security bootstrapping in a crowded field; smart contract platforms add complexity hostile to monetary stability; centralized registries defeat the purpose. Namecoin offers the most pragmatic balance, with identified upgrade paths where alternatives face architectural dead ends.

This greenpaper's mechanism, however, is portable: it applies to whichever protocol the market ultimately selects.

6.3 Understanding Colored Coins

Colored coins mark specific cryptocurrency units to represent value beyond their native denomination. In Bitname, standard $NMC is “colored” via metadata attached to specific UTXOs, marking them as Bitname tokens. Each colored UTXO cryptographically commits to the specific Bitcoin timelock UTXO backing it and records the BTC/USD rate at issuance. This one-to-one mapping is verifiable by any client, making unbacked issuance detectable by inspection. Users hold colored $NMC in standard wallets recognizing the protocol; the underlying chain provides security while the metadata provides the monetary properties. As $NMC appreciates toward the token's band through naming demand, the distinction between colored and uncolored $NMC diminishes until $NMC itself supplies the backing.

7. The Bitname System: Technical Architecture and Monetary Considerations

7.1 Timelock-Backed Token Creation

Step 1: Bitcoin Deposit. A user deposits Bitcoin plus a small additional amount (covering 0.02 $NMC for the Namecoin protocol costs and transaction fees) into a timelock contract locked for 500,000 blocks (approximately 10 years). The Bitcoin becomes provably unspendable for the duration and returns to the depositor at maturity. This is not a redemption reserve: it is commitment collateral that rewards conviction and caps the minter's downside.

Step 2: Foundation Token Issuance. The deposit triggers issuance of colored $NMC to the user's corresponding Namecoin address. This is seamless because Namecoin shares Bitcoin's codebase, giving perfect address mapping between chains. Only one-fifth of minted tokens is immediately available; the remaining four-fifths unlock one fifth per 50,000-block cycle.

Step 3: Cryptographic Linking. Each colored token commits to its backing timelock UTXO. Anyone can audit total supply against locked Bitcoin on-chain, a level of transparency impossible in custodial systems.

7.2 The Bitname Foundation: Attestor, not Custodian

Purely decentralized systems often fail to coordinate initial adoption. The Foundation is temporary scaffolding for that phase, but its trust surface is narrow. Because every token UTXO is cryptographically bound one-to-one to a locked Bitcoin UTXO, the Foundation cannot issue unbacked tokens without immediate public detection. Its trusted role reduces to attesting a single number: the BTC/USD exchange rate at each minting. It holds no user funds and no names.

Vesting for Price Stability: Graduated release prevents minters from dumping tokens below the band. Critically, it also creates buying pressure: obtaining one immediately spendable $20 token by minting requires locking roughly $100 in Bitcoin for a decade. Most users seeking a name will find secondary-market purchase more rational than minting, establishing demand for circulating tokens while ensuring minters contribute substantial locked backing.

Auxiliary Services: During bootstrap, when blockspace demand is low and 0.02 $NMC costs pennies, service providers add perceived value to the token through registration handling, resolution, and hosting, bridging the gap until on-chain demand itself justifies the band.

Path to Obsolescence: As name utility matures into a sufficient stabilizer, the Foundation's functions retire. The 500,000-block horizon provides the runway, with market forces rather than governance driving full decentralization.

7.3 Programmatic Inflation Adjustment

Every 50,000 blocks (approximately 11.5 months, henceforth a "Year"), minting cost increases 5%, a rate most economists accept as approximating long-run real asset inflation. In Year 1, users lock $100 of Bitcoin for 500,000 blocks to receive one token immediately (and four more per the vesting schedule). Year 2 requires $105; Year 3, $110.25; Year 4, $115.76; and so on.

To be precise about what this does: escalation raises the *ceiling* of the band. It does not itself push market price upward; only demand does that. What it guarantees is that whenever demand presses tokens toward the ceiling, that ceiling sits at an inflation-adjusted dollar figure, so the band as a whole tracks debasement without oracles, governance votes, or portfolio management by holders.

Emergency Response: Should US dollar inflation exceed 5% annually for two consecutive quarters, the Foundation may impose temporary surplus minting fees to moderate the demand surges accompanying monetary crises.

7.4 Economic Evolution Timeline

Phase 1: Bitcoin-Collateralized Launch (Years 1–3). Tokens derive credibility from locked Bitcoin. Service providers register names, converting tokens to the trivial $NMC amounts required on-chain; the spread funds bootstrap services.

Phase 2: Market Development (Years 3–7). Adoption across communication and identity platforms raises $NMC demand. Rising $NMC prices make minting dearer, favoring existing tokens and tightening the band.

Phase 3: Value Convergence (Years 7–10). $NMC approaches parity with token value; the underlying uncolored $NMC increasingly provides the backing, and dependence on locked Bitcoin fades.

Phase 4: Full Independence (Year 10+). Timelocks expire and depositors reclaim Bitcoin; tokens remain backed by $NMC value itself. If adoption has reached escape velocity, the unit of account itself may begin migrating from dollars to $NMC.

7.5 Risk-Reward Structure

Early participants face asymmetric payoffs: if the protocol wins, holders gain a stable, inflation-adjusted unit with upside; if it fails, minters recover their Bitcoin after 500,000 blocks. That is opportunity cost, not total loss.

The correct analogy is a self-issued certificate of deposit: the minter locks principal for a fixed decade-long term, receives no coupons, is guaranteed return of principal by the timelock itself rather than any issuer, and collects as "interest" five tokens whose value is a call option on the naming thesis. For the target demographic of low-time-preference Bitcoin holders who would

not have sold within the decade regardless, the opportunity cost approaches zero, and the tokens are nearly free optionality. The vesting schedule staggers that optionality across five Years. No counterparty owes anything; the structure's honesty is its appeal.

8. Conclusion

This greenpaper describes not a stablecoin but the conditions under which one crystallizes. The proposition is a stated bet: if a decentralized naming protocol reaches critical mass, its registration token, bounded below by genuine, ever-renewing demand for digital identity and bounded above by a dollar-denominated, inflation-escalating mint valve, matures into a stable unit that no custodian can freeze and no algorithm can death-spiral. Bitcoin timelocks (500,000 blocks) collateralize the bet and cap the minter's downside; one-to-one cryptographic linking reduces the Foundation to an attestor of exchange rates; vesting suppresses sell pressure while routing utility demand to secondary markets; and costly identity gives both humans and AI agents, drowning in free, disposable keys, a reason to pay for names that function as sybil-resistant reputation anchors.

What distinguishes this from every prior utility token is the band: utility demand alone has never produced stability, but utility demand beneath a known dollar-priced supply valve can. The unknowns are stated plainly. Scaling beyond millions of users requires soft forks already sketched by Namecoin developers, and the terminal dream is that by the time raw blockspace pricing binds, $NMC itself will have become the unit of account, retiring the dollar denomination as the scaffolding it always was. Early adopters risk a decade of liquidity, not their principal. If the naming thesis fails, Bitcoin returns home. If it succeeds, the fundamental human need for identity will have produced what custodians and algorithms never could: money whose stability is a property of what it does, not of who promises it.

References

[1] Grand View Research. (2023). “Decentralized Identity Market Size And Share Report, 2030.” grandviewresearch.com

[2] Nostr.how. “What are Nostr Relays?” nostr.how/en/relays

[3] Namecoin Project. “Namecoin – Decentralized secure names.” namecoin.org

[4] Bitcoin merge-mining technical documentation and Namecoin security analysis from Namecoin Core development documentation.

[5] Terra Luna collapse case study and algorithmic stablecoin analysis from various cryptocurrency industry sources and post-mortems (2022–2023).

[6] BitcoinTalk Forum. “BitDNS and Generalizing Bitcoin.” bitcointalk.org/?topic=1790.0