₿ WHITEPAPER V2.0 · BITCOIN-ANCHORED

Proof of Merch Mining™

A capped-drop protocol that ties physical goods to the Bitcoin timechain.

Author of record: Terrence L. Thomas
Publisher: 21 Million Publishing House
Contact: `satoshinegromoto@21millionpublishing.com`
Nostr: `npub1nk7ycp3nz6ky892qptuq70tjh55w27342qmqu7szgr26qjgueguqpj6yjs`
First published: 2026-09-04 (v1.0) · v2.0 today
Bitcoin anchor: .ots proof file

> **Not financial advice.** This document establishes creative first-use provenance of a branded retail mechanic and its accompanying open reference implementation; it is not a securities instrument and confers no investment rights. The satoshis (sats) gifted with each mined block are consumer-goods promotional value denominated in USD, fully reserved, and delivered as spendable Bitcoin — not an investment offer, custody arrangement, or yield product.

1. Abstract

Proof of Merch Mining™ (POMM) is a retail mechanic that reframes the purchase of a physical good as *mining a block*. Each product design is issued as a **capped chain of numbered "blocks."** When a buyer claims one, they mine the next block in that chain: supply decrements publicly, the block is hash-linked to the previous one in an append-only ledger, that ledger's fingerprint is committed to the Bitcoin blockchain via OpenTimestamps, and the buyer receives (a) the physical made-to-order item, (b) a

reserved allocation of satoshis (sats), and (c) a cryptographic receipt that ties their purchase to the timechain.

POMM is not a token. It is not a smart contract. It is not a security. It is a **culturally-native scarcity + provenance protocol for physical goods** that borrows Bitcoin's language, math, and time-anchoring, and grounds each unit in a shippable object plus real charity dollars (10% of net to St. Jude, forever).

2. The coined terms

TERM	MEANING
Proof of Merch Mining™ (POMM)	The overall mechanic — a play on Bitcoin's "Proof of Work."
Merch Mining™	The act: claiming a capped-run piece = mining a block.
Mine your block	The buyer-facing call-to-action for a purchase.
The Merch Chain	The full set of sequential capped design "blocks" issued by one publisher.
Block (a design run)	One design = one hash-linked chain with a fixed maximum supply.
Halving batch	A pricing tier that raises unit price as the chain approaches its cap, echoing Bitcoin's block-reward halvings.
The tip	The most recently mined block of a chain (its current head).
The Genesis Block	Block #1 of each chain, always priced at the lowest batch.

All above terms are used as branded, coined, and reserved marks of 21 Million Publishing House. First use in commerce: the storefront at `twentyone-book-store.pages.dev` and this document.

3. Design intent

Bitcoin taught a generation the emotional power of *provably scarce*. Streetwear taught the same generation the emotional power of *drops*. POMM is the intersection: **every t-shirt is a numbered block, mined once, forever recorded, tied to the Bitcoin timechain by math not by marketing.** A buyer isn't merely buying a shirt — they are minting the next block in a chain of exactly 2,100 that will never be reprinted. When it's mined out, it's closed forever. That is what a real drop *should* mean.

POMM specifically rejects three things:

1. **Restocks.** A capped chain restocked is a lie about scarcity.
2. **Fake blockchain claims.** POMM is a hash-chained audit log timestamped to Bitcoin. It is not a blockchain, not a token, not a distributed network. Saying so is dishonest and we don't.
3. **Purely digital "mint" hype.** Every mined block ships a real physical item. No skeuomorphism.

4. Architecture (reference implementation)

4.1 PER-CHAIN BLOCK RECORD

```
{
  "chain_id":   "merch:bitcoinaire:tee",
  "block_no":   47,
  "ts":         1788556870.611,
  "price_cents": 2900,
  "batch":      "Genesis",
  "buyer":      "buyer@example.com",
  "prev_hash":  "72a4437...",
  "hash":       "ac9e0c7...",
  "state":      "paid-confirmed",
  "pod_order":  "175055863"
}
```

4.2 HASH FUNCTION

```
sha256( json.dumps({
    "chain": chain_id,
    "n":     block_no,
    "ts":    round(ts, 3),
    "price": price_cents,
    "buyer": buyer,
    "prev":  prev_hash
}, sort_keys=True) )
```

Deterministic and canonical. Any change to any past record causes the recomputed hash to diverge, breaking the chain from that point forward. The verifier walks from genesis to the buyer's block and re-derives every hash to prove the chain is intact.

4.3 GENESIS AND TIP

The first block uses `prev_hash = "0" * 64`, matching Bitcoin's genesis convention. The most recently mined block's hash becomes the chain's **tip**.

4.4 LEDGER PUBLICATION

1. Snapshot every chain to `/ledger/chains/merch_<slug>_tee.json` — public, immutable, cacheable.
2. Compose a manifest with metadata for all chains and their tip hashes.
3. Compute the merkle root of all chain tips (Bitcoin-style pairwise SHA-256) — one 32-byte fingerprint of the entire POMM ledger.
4. Write `/ledger/manifest.json` containing the merkle root.

4.5 BITCOIN ANCHOR VIA OPENTIMESTAMPS

The manifest is stamped by `ots stamp manifest.json`, which submits its SHA-256 to public OpenTimestamps calendars. Within a few hours those calendars fold your merkle root into a Bitcoin transaction and the `.ots` file self-upgrades to include the Bitcoin block header proof. Anyone can then run `ots verify manifest.json` and independently

confirm the merkle root was committed to a specific Bitcoin block at a specific height — **no trust in the publisher required.**

4.6 INDEPENDENT VERIFIER

The reference implementation ships `verify_block.py`: a ~90-line Python script a buyer can download and run to (a) fetch the public per-chain JSON, (b) recompute every hash from genesis to their block, (c) confirm the chain is unbroken, and (d) verify the ledger's Bitcoin anchor.

5. Economic construction

5.1 HALVING BATCHES (PER CHAIN)

BATCH	BLOCK RANGE	PRICE	NOTE
Genesis	1 – 21	$29	Honors Bitcoin's 21M cap
Batch 2	22 – 630	$34	+$5
Batch 3	631 – 1,260	$39	+$5
Final	1,261 – 2,100	$44	Last blocks

The 21-block Genesis is intentional. The step sequence 21 → 630 → 1,260 → 2,100 is a "reverse halving" where scarcity compounds late and rewards the earliest buyers.

5.2 RESERVED SATS (USD-DENOMINATED)

Each mined block reserves a fixed USD amount (default 10% of retail) converted to sats at time of sale using live BTC spot (Coinbase primary, CoinGecko fallback, Kraken backup). This gives the mechanic a **BTC-volatility-insensitive margin**: publisher margin is stable across BTC $40k → $290k because the sats gift is a USD budget, not a fixed sat count. Early buyers still receive more sats per dollar because they buy when BTC is cheaper.

5.3 CHARITABLE BLOCK

10% of net proceeds route to St. Jude Children's Research Hospital. Permanent term of every chain. Full reserve is booked at time of sale.

5.4 COST FLOOR: MAKE-TO-ORDER

Every mined block is fulfilled via print-on-demand (Printful) with no warehouse. This guarantees the cap is honored and keeps working capital at zero.

BATCH	RETAIL	PRINT + SHIP	SATS	ST. JUDE	NET
Genesis	$29	~$17.31	$2.90	$2.90	~$5.89
Batch 2	$34	~$17.31	$3.40	$3.40	~$9.89
Batch 3	$39	~$17.31	$3.90	$3.90	~$13.89
Final	$44	~$17.31	$4.40	$4.40	~$17.89

6. Full-cycle buyer flow

1. Buyer visits a product page.
2. Sees the current batch, next block number, live count of blocks mined vs. cap.
3. Selects a size, clicks **Mine Block #N**.
4. Redirects to a hosted Stripe checkout.
5. On payment success, returns to `/order-confirmed.html`.
6. The confirmation function: verifies payment → determines next block number → places Printful order → computes hash → persists block → returns receipt.
7. Buyer sees their block number, hash, Printful order id, and a link to the full ledger.
8. Nightly publication snapshots the updated ledger and stamps it to Bitcoin via OTS.
9. At any time thereafter, anyone can independently verify the block, the chain integrity, and the Bitcoin anchor.

7. Trust model

WHAT IT IS

- Append-only, tamper-evident audit log.
- SHA-256 hash chain — every block links to the previous.
- Merkle-rooted daily and Bitcoin-anchored via OpenTimestamps.
- Fully public JSON — anyone can download, audit, verify.
- A physical goods commitment: every block ships a real numbered item.
- A charitable commitment: 10% of net to St. Jude, permanently.

WHAT IT ISN'T

- Not a blockchain (single centralized ledger, not distributed).
- Not proof-of-work (the mint is centralized; Bitcoin timestamping is the accountability layer).
- Not a token — you own a numbered physical shirt, not a transferable coin.
- Not a security.

> *The honest metaphor: POMM is Git commits countersigned by the Bitcoin timechain.*

8. What can and cannot be spoofed

- **Cannot be spoofed:** the fact that a specific block hash existed at or before the Bitcoin block containing our merkle root. This is math.
- **Cannot be spoofed silently:** any retroactive edit to a past block. Every subsequent hash breaks and any verifier detects it in <100 ms.
- **Can be spoofed:** the identity of the buyer, if the publisher lies at time of mine. Mitigated by email verification, optional Nostr `npub` binding, and optional Bitcoin address signature at buy time.

- **Can be spoofed:** the physical shipping. Mitigated by the Printful `pod_order` id, publicly linked from the confirmation.

9. Product-line policies

- **No restocks, ever.** A capped chain, once mined out, is closed forever.
- **No hidden batches.** Full schedule fixed at chain creation, shown on every product page.
- **10% charitable block, permanent.** St. Jude, fully reserved at time of sale.
- **USD-denominated sats.** Converted at spot at mine time.
- **Public ledger, always.** All chains fully public in JSON with Bitcoin-anchored fingerprint.
- **Independent verifier.** The `verify_block.py` script ships with the store.

10. Prior art and coinage

The author is unaware of a prior public use of **"Proof of Merch Mining"** or **"Merch Mining"** to describe a retail scarcity mechanic that binds physical goods to Bitcoin-anchored hash-chained ledgers of numbered units. Related but distinct precedents: NFTs, Ordinals/Inscriptions, streetwear drops, ticketing hash-chains, kingdom drops.

POMM is the specific fusion of: **capped physical drops + hash-chained ledger + Bitcoin timestamp anchor + USD-denominated sats gift + charitable block.** The author claims the coinage of the terms in §2 and the specific full-stack mechanic composed of the above elements.

11. This document's Bitcoin anchor

This whitepaper file is timestamped with OpenTimestamps immediately upon publication. The corresponding `.ots` file is published alongside it. Anyone can run `ots verify PROOF-OF-MERCH-MINING-whitepaper.md` and independently confirm the SHA-256 of this

exact file existed at or before the Bitcoin block that contains the OTS calendar's aggregation transaction. That is the author's public, cryptographic proof of coinage date.

Download markdown | Bitcoin proof (.ots) | Print-ready PDF | Live ledger

12. License

Terrence L. Thomas
Founder, 21 Million Publishing House
Author, The Boy Who Cried Bitcoin
`satoshinegromoto@21millionpublishing.com`