

NextGate Product Ecosystem — Architecture & Purchase Flows

Overview

NextGate's e-commerce layer handles two fundamentally different kinds of products: **physical products** (tangible goods that require shipping and delivery confirmation) and **digital products** (files that a buyer downloads). Both types share the same payment infrastructure, checkout session system, financial rails, and **inventory system** — but diverge completely at the fulfillment stage.

1. Product Types

Physical Products

A physical product has real-world stock. The platform tracks inventory, holds it during checkout, ships it through a seller, and releases escrow only after the buyer confirms physical receipt. The entire lifecycle can take days or weeks.

Digital Products

A digital product is a file (or collection of files) that the seller uploads to a private, access-controlled storage bucket. There is no shipping. There is no confirmation code. The moment payment clears, the buyer can download. Escrow releases immediately. The lifecycle is measured in seconds.

A single product can be either physical or digital — never both. The `productType` field on the product record is the authoritative signal that drives every downstream decision.

2. Inventory — Shared by Both Product Types



Key rule: Every product has a `stockQuantity`. Digital and physical products are treated identically by the inventory system. The only difference is what happens after payment.

Every product — physical or digital — requires a `stockQuantity` set by the seller at creation time. The seller decides what that number is:

```
10      → limited edition digital art, exclusive release
500     → cohort-based course intake
1,000,000 → effectively open – seller still sets a real number
```

There is no "unlimited" mode and no `trackInventory` toggle. All inventory mechanics apply to both product types without exception:

- `stockQuantity` check on add-to-cart
- Inventory hold at checkout session creation
- Hold released on session expiry or cancellation
- `stockQuantity` decremented on successful payment
- Low stock threshold warnings apply to both
- `isInStock()` and `canOrderQuantity()` run identically

This means zero special-casing in the codebase. Every product behaves the same through cart, checkout, and payment. The divergence only begins at fulfillment.

Why sellers set quantity for digital products

The business reasons vary:

```
Exclusivity / scarcity → "Only 500 copies ever sold" – creates urgency and perceived value
License seat control   → Software licensed for exactly N seats
Cohort control         → Course intake capped at N students for direct purchase
Business guardrail     → Seller wants a hard ceiling as a safety net
```

Even if a seller sets 1,000,000, the system enforces it as a real number. The seller always sees and manages a stock figure.

3. The Only Real Difference Between Physical and Digital

	Physical	Digital
stockQuantity	✓	✓
Inventory hold at checkout	✓	✓
Stock decrements on buy	✓	✓
Low stock warnings	✓	✓
Requires shipping	✓	x
Delivery confirmation code	✓	x
Escrow held until delivery	✓	x
Order → PENDING_SHIPMENT	✓	x
Escrow released immediately	x	✓
Order → COMPLETED	x	✓
DigitalDownloadAccess	x	✓

Everything above the dividing line is shared. Everything below is where the paths split.

4. How Sellers Prepare Digital Products

Before a digital product can be purchased, the seller must upload its files through a two-step process designed to handle large files without routing them through the API server.

```
Seller → Request presigned upload URL
  → Platform generates time-limited URL (MinIO private bucket)
  → Seller uploads file DIRECTLY to MinIO (API server bypassed)
  → Seller confirms upload to API
  → Platform records file metadata and links to product
```

A product can have multiple files. Each gets its own record. Buyers get access to all files on purchase.

Sellers configure per product:

```
stockQuantity      → required · how many units can ever be sold
lowStockThreshold  → when to trigger low stock warning
maxQuantityForDigital → max a single buyer can purchase in one order
                    (1 for personal-use content, higher for licenses/gifts)

Download rules:
  expiryDays       → days download links stay active after purchase (default: 7)
```

downloadCap → max downloads per buyer (default: unlimited)
clockStart → expiry from purchase time OR from first download

5. The Cart

The cart is a persistent bag of products. It does not distinguish between physical and digital items — both coexist freely. Stock availability is checked on add-to-cart for both types.

“ The physical/digital split only becomes relevant at fulfillment — not at cart, not at payment.

6. Checkout Session Types

Every purchase flows through a checkout session — a short-lived record holding purchase intent before payment. All four session types work for both physical and digital products.

Session Type	Description
REGULAR_DIRECTLY	Single-item purchase from the product page
REGULAR_CART	Multi-item purchase from a cart
GROUP_PURCHASE	Coordinated group buy at a discounted group price
INSTALLMENT	Down payment now, remainder paid over time

Sessions expire (typically 15–30 minutes). During this window, inventory is held for both physical and digital products — preventing overselling while the buyer completes payment.

7. Shipping Logic

All items digital? → Skip shipping entirely. Cost = 0.
Inventory hold still applies.

Any item physical? → Shipping address + method required. Inventory held.

Mixed cart (physical + digital, same shop)?

→ Engine splits into TWO sessions automatically:

Session 1: physical items → shipping lifecycle

Session 2: digital items → download lifecycle

8. Payment Infrastructure (Shared by All Types)

Payment works identically regardless of product type:

```
Buyer wallet → debited
Escrow       → credited (money held, not yet with seller)
Ledger entry → recorded (double-entry, full audit trail)
Tx history   → updated for buyer
```

For installment purchases, only the down payment moves at session time. Each subsequent payment creates its own ledger entry.

“ **Escrow is the control point.** Physical → held until buyer confirms delivery.
Digital → released immediately at order creation.

9. Post-Payment Fulfillment — The Core Split

Physical path

```
Payment completes
→ stockQuantity decremented
→ Inventory hold released
→ Order created [PENDING_SHIPMENT]
→ Seller notified
→ Seller ships → marks order SHIPPED
→ 6-digit confirmation code generated → sent to buyer
→ Buyer enters code in app
```

- Escrow releases to seller
- Order [COMPLETED]

“ Escrow is held the entire shipping period. The code is the handshake — seller cannot claim money without buyer confirming receipt.

Digital path

Payment completes

- stockQuantity decremented
- Inventory hold released
- Order created [COMPLETED immediately]
- Escrow released to seller immediately
- DigitalDownloadAccess records created (one per file)
- Buyer notified with download link
- Buyer downloads within expiry window

“ No shipping. No confirmation code. Delivery = access records created.

10. Group Purchase — Physical vs Digital

Both product types support group purchase. The financial hold (escrow per participant) and inventory hold are identical in both cases during the waiting period. What differs is post-completion fulfillment.

Physical group purchase

Each participant pays → Escrow held + Inventory held per participant

Group fills → COMPLETED

- Physical orders created for all participants [PENDING_SHIPMENT]
- stockQuantity decremented for all participants

- Each participant goes through shipping lifecycle individually
- Each escrow releases on individual delivery confirmation

Group expires without filling:

- All escrows refunded
- All inventory holds released

Digital group purchase

Each participant pays → Escrow held + Inventory held per participant

Group fills → COMPLETED

- Orders created for all participants [COMPLETED immediately]
- stockQuantity decremented for all participants
- All escrows released immediately
- DigitalDownloadAccess records created for every participant
- All buyers can download immediately

Group expires without filling:

- All escrows refunded
- All inventory holds released (identical to physical)

“ The seller's participant cap on the group instance is separate from `stockQuantity`. Both are enforced — a buyer cannot join if either the group is full or the product stock is exhausted.

11. Installment Purchase — Physical vs Digital

Both product types support installment. The payment schedule, ledger entries, agreement lifecycle, early payoff, and flexible payment features are identical. What differs is fulfillment timing.

Fulfillment timing options

IMMEDIATE — order and access created after the down payment. Buyer gets the product now, pays over time.

- Physical: seller ships after down payment, takes risk on future payments.
- Digital: buyer downloads immediately. If buyer defaults, downloaded files cannot be revoked. Seller has no recourse.

AFTER_PAYMENT — order and access created only after the final payment clears.

- Physical: layaway — seller holds stock, ships at the end.
- Digital: safest model — access never opens until fully paid. On default, access records simply never created.

“ **Platform recommendation:** AFTER_PAYMENT is the default for digital installment products. Sellers must explicitly opt into IMMEDIATE with acknowledgment that pre-delivery means no recourse on default.

On default — digital IMMEDIATE

Buyer stops paying → Agreement DEFAULTED

- No new access records created for future files
- Already-downloaded files cannot be revoked ← known limitation, seller accepts this

On default — digital AFTER_PAYMENT

Buyer stops paying → Agreement DEFAULTED

- Access records never created
- No content ever delivered ← clean outcome

12. The Download System

On every successful digital purchase (any session type, any fulfillment trigger):

Platform creates `DigitalDownloadAccess` record per file:

- buyer ID + order ID + file ID
- downloadCount (starts at 0)
- maxDownloads (null = unlimited, or seller-set cap)
- accessExpiresAt (now + expiry window)
- firstDownloadAt (set on first use)

On every download request:

Buyer hits authenticated endpoint

- Check 1: Does buyer own an active access record for this file?
- Check 2: Has expiry window passed?
- Check 3: Has download cap been reached?

All pass → Platform generates presigned GET URL (5-min TTL)

- Buyer browser downloads DIRECTLY from MinIO private bucket
- Access record downloadCount incremented
- API server is NOT in the file transfer path

“ The 5-minute TTL means a leaked URL is useless within minutes. The raw MinIO object key is never exposed to the buyer.

13. Scenario Walkthrough — All Combinations

Scenario A — Direct purchase, physical product

“ Buyer finds a T-shirt. Clicks "Buy Now". Quantity: 1.

REGULAR_DIRECTLY session created

- Stock check passes · Inventory held
- Shipping address + method required
- Buyer pays → Escrow funded
- stockQuantity decremented · hold released
- Order created [PENDING_SHIPMENT]
- Seller ships → marks SHIPPED
- 6-digit code sent to buyer
- Buyer confirms → Escrow released
- Order [COMPLETED]

Scenario B — Direct purchase, digital product

“ Buyer finds a PDF course. Clicks "Buy Now". Quantity: 1.

REGULAR_DIRECTLY session created

- Stock check passes · Inventory held
- No shipping fields collected
- Buyer pays → Escrow funded and immediately released
- stockQuantity decremented · hold released
- Order created [COMPLETED]
- 3 DigitalDownloadAccess records created (one per chapter PDF)
- Buyer receives download link · downloads within 7 days

Scenario C — Direct purchase, digital product, quantity 3

“ Buyer wants 3 software licenses to distribute to colleagues.

REGULAR_DIRECTLY session created (quantity: 3)

- Stock check: stockQuantity >= 3? passes · 3 units held
- No shipping fields collected
- Buyer pays (unitPrice × 3) → Escrow funded and immediately released
- stockQuantity decremented by 3 · hold released
- Order created [COMPLETED]
- 6 DigitalDownloadAccess records created (3 sets × 2 files per product)
- Each set is independent – buyer can share with colleagues

Scenario D — Cart, physical only, multiple shops

“ Phone case from Shop A + charger from Shop B.

REGULAR_CART session created

- Inventory held for both items
- Buyer pays once
- Order engine groups by shop:
 - Order 1: Shop A [PENDING_SHIPMENT]
 - Order 2: Shop B [PENDING_SHIPMENT]
- Each seller ships independently
- Each escrow releases on individual buyer confirmation

Scenario E — Cart, digital only

“ Video course + design template pack.

REGULAR_CART session created

- Stock check + inventory hold for both digital products
- No shipping.
- Buyer pays once
- Order 1: video course [COMPLETED] → 4 access records
- Order 2: template pack [COMPLETED] → 2 access records
- Buyer downloads all 6 files within 7 days

Scenario F — Cart, mixed physical + digital, same shop

“ Printed book (physical) + PDF supplement (digital), same shop.

Engine detects mixed cart → splits automatically:

- Session 1: printed book → shipping lifecycle · inventory held
- Session 2: PDF → download lifecycle · inventory held

Buyer sees one checkout flow, gets two orders in history:

- Order 1 (book): [PENDING_SHIPMENT] → shipping → confirmation → escrow releases
- Order 2 (PDF): [COMPLETED] → download access immediate

Scenario G — Group purchase, physical product

“ 5 buyers collectively buy a speaker.

Buyer 1 initiates → GROUP_PURCHASE session → pays → group instance created (timer starts)

Buyers 2–5 join → each pays → inventory held + escrow held per participant

Group fills → COMPLETED

- Physical orders created for all 5 [PENDING_SHIPMENT]
- stockQuantity decremented for all 5
- Each participant ships independently
- Each escrow releases on individual delivery confirmation

Timer expires before filling:

- All 5 escrows refunded · all inventory holds released

Scenario H — Group purchase, digital product

“ 30 buyers join a cohort-based online course. Seller stock: 30.

Buyers 1–30 join → each pays → inventory held + escrow held per participant

Group fills (30th seat) → COMPLETED

- Orders created for all 30 [COMPLETED immediately]
- stockQuantity decremented by 30 (now 0 – sold out)
- All 30 escrows released immediately
- DigitalDownloadAccess records created for every participant
- All 30 buyers can download immediately

Timer expires before filling:

- All escrows refunded · all inventory holds released

Scenario I — Installment, physical, IMMEDIATE fulfillment

Laptop, 6-month plan, 20% down, seller ships immediately.

INSTALLMENT session created

- Stock check · inventory held
- Down payment charged (20%)
- Agreement created (6 scheduled payments)
- Order created [PENDING_SHIPMENT] ← immediately after down payment
- stockQuantity decremented · hold released
- Seller ships
- Monthly payments auto-process via scheduled jobs

Scenario J — Installment, physical, AFTER_PAYMENT fulfillment

“ Same laptop, layaway model.

INSTALLMENT session created

- Stock check · inventory held
- Down payment charged
- Agreement created
- NO order created yet · inventory held until final payment
- Monthly payments auto-process
- Final payment clears → Agreement COMPLETED
- Order created [PENDING_SHIPMENT] ← only now
- stockQuantity decremented · hold released
- Shipping lifecycle begins

Scenario K — Installment, digital, AFTER_PAYMENT (recommended)

“ Video course library, 500,000 TZS, 3-month plan.

INSTALLMENT session created

- Stock check · inventory held
- Down payment charged (30%)
- Agreement created (3 scheduled payments)
- NO order, NO download access yet · inventory held
- Monthly payments auto-process
- Final payment clears → Agreement COMPLETED
- stockQuantity decremented · hold released
- Order created [COMPLETED]
- DigitalDownloadAccess records created ← only now
- Buyer downloads

If buyer defaults:

- Agreement DEFAULTED
- Inventory hold released · stockQuantity restored
- Access records never created · no content delivered

Scenario L — Installment, digital, IMMEDIATE fulfillment

“ Same course, seller opts into IMMEDIATE.

INSTALLMENT session created

- Stock check · inventory held
- Down payment charged (30%)
- Agreement created
- stockQuantity decremented · hold released
- Order created [COMPLETED] ← immediately
- DigitalDownloadAccess records created ← immediately
- Buyer downloads now

Monthly payments continue auto-processing.

If buyer defaults:

- Agreement DEFAULTED
- Already-downloaded files CANNOT be revoked ← seller accepted this risk

14. Escrow Behavior Summary

Scenario	Inventory Held	Escrow Released
Physical — direct	Yes, at session creation	On delivery confirmation
Digital — direct	Yes, at session creation	Immediately at order creation
Physical — group	Yes, per participant	Per delivery confirmation
Digital — group	Yes, per participant	Immediately when group completes
Group — expired / failed	Released to stock	Refunded to all participants
Physical — installment IMMEDIATE	Yes, until down pmt	Per installment via direct ledger
Physical — installment AFTER_PAYMENT	Yes, until final pmt	After final payment
Digital — installment IMMEDIATE	Yes, until down pmt	After down payment
Digital — installment AFTER_PAYMENT	Yes, until final pmt	After final payment

15. MinIO Bucket Architecture

nextgate-public (world-readable)

- Product images · shop logos · avatars · category images
- URLs are permanent · no expiry

nextgate-digital-content (private · no public access)

- Paid digital product files only
- Accessible only via presigned URLs (5-min TTL)
- Generated by API after access verification
- Raw object key never exposed to buyers

“ This separation ensures a seller can never accidentally expose a paid file by uploading to the wrong location.

16. Key Invariants

- Every money movement goes through the double-entry ledger.
No direct wallet balance adjustments exist.
- Escrow receives the full payment before any fulfillment action begins.
- Every product has a stockQuantity – physical and digital alike.
There is no "unlimited" mode. Sellers set a real number.
- Inventory is held for both physical and digital products during the checkout session window. Released on expiry, cancellation, or payment.
- Orders are never created before:
 - regular purchase → payment completes
 - group purchase → group fills
 - installment → fulfillment trigger (down pmt or final pmt)
- Download links never expose the raw MinIO object key.
Only opaque access identifiers resolve to presigned URLs via authenticated API.
- A checkout session produces orders exactly once.
Idempotency checks prevent duplicates under retry or failure.
- Session expiry is enforced before payment processing.
An expired session cannot be paid.
- For digital installment IMMEDIATE: already-downloaded files cannot be revoked on default. Sellers must explicitly accept this risk.
- For digital installment AFTER_PAYMENT: default means access records are never created and stockQuantity is restored. Clean outcome.

Revision #6

Created 2 May 2026 16:52:41 by Admin Qbit

Updated 2 May 2026 18:18:52 by Admin Qbit