

VERITAS

YIELD-BEARING PREDICTION MARKETS

Technical Litepaper
Production-Ready Architecture

February 2026

Executive Summary

VERITAS is a **yield-bearing prediction market platform** that solves two fundamental problems: (1) idle capital earning 0% returns, and (2) prohibitive barriers to market creation. While Polymarket offers 0% returns and requires permissioned market creation, VERITAS delivers return to minority LPs and enables **\$50 permissionless market creation** through Veritas Ignition, our self-funding bonding curve mechanism.

Core Innovations

- **Veritas Ignition:** \$50 market launcher with bonding curve and virtual liquidity that requires ZERO protocol subsidies
- RWA Gravity Redistribution: Pure zero-sum redistribution of Treasury yield from majority to minority based on market urgency
- Bounded VALS - Velocity-Adjusted Liquidity Slippage (Protection: Maximum 50% slippage cap with adaptive circuit breakers for news events to solve toxic flow
- Inverse-Weighted LP Fees: Minority LPs earn more than proportional share
- Wash-Trading Immunity: Gravity fees accrue only on net directional flow
- Commitment Incentives solving “liquidity leaving near the event closing”

1. Liquidity Infrastructure

1.1 Hybrid AMM + Order Book Architecture

VERITAS implements a **dual liquidity model** combining instant AMM execution with yield-bearing passive orders:

- VALS-Protected AMM: Instant execution for market orders with built-in toxicity protection
- Yield-Bearing Limit Orders: Passive orders earn RWA yield while waiting to fill
- Intelligent Routing: System automatically selects cheapest execution path
- Aggregated Depth: Combined AMM + order book provides superior liquidity

1.2 Dutch Auction Bootstrapping (Sealed-Bid)

New markets launch via **sealed-bid Dutch auction** to establish fair initial pricing and prevent front-running:

Phase 1: Commit Period (12 hours)

- Participants submit encrypted bids (amount + price)
- Bids are cryptographically sealed and hidden from other participants
- Prevents front-running and gaming of auction mechanism

Phase 2: Reveal Period (12 hours)

- All participants reveal their bids
- Clearing price determined as median of all bids
- Orders at or better than clearing price execute immediately

Phase 3: Market Open

- AMM initializes with discovered price as midpoint
- Liquidity from auction participants forms initial depth
- Traditional trading begins with VALS protection active

Benefit: Immediate market depth at launch, fair price discovery, prevents MEV extraction

1.3 Yield-Bearing Limit Orders

Industry First: VERITAS is the only prediction market where passive limit orders earn yield while waiting to execute.

Mechanism

- LP deposits \$100k limit order at 60¢ (current market: 55¢)
- Capital immediately deployed to RWA Treasury bills
- LP earns 5% APY while order waits in book
- When market reaches 60¢, order executes + LP keeps accrued yield
- If cancelled, LP receives principal + all accrued yield

Example: Order sits for 30 days before executing → LP earns \$ in RWA yield (equivalent to 4% APY in feb 2026) + benefits if market moves in their favor

1.4 Intelligent Order Routing

For each trade, the system calculates:

- AMM execution cost (including VALS penalty if applicable)
- Order book execution cost (taking best available limit orders)
- Gas costs for each route
- Automatically selects cheaper path

Result: Best price execution guaranteed, combining benefits of AMM instant liquidity with order book price improvement

2. Anti-Toxic Flow Engine (VALS)

2.1 Bounded VALS Formula with Safety Caps

VALS (Velocity-Adjusted Liquidity Slippage) protects LPs from toxic order flow through **bounded exponential slippage**:

$$P(\text{execution}) = P(cp) \times \min(e^{[\lambda \times (\Delta x / L) \times \tanh(\sigma)]}, 1.5 \times P(cp))$$

Safety Mechanisms:

Component	Purpose
$\tanh(\sigma)$	Bounds toxic velocity to [-1, 1], preventing infinite price explosion

1.5x Cap	Hard ceiling at 50% maximum slippage (reasonable for prediction markets)
Result	Max slippage = 50% (vs unbounded: ∞)

2.2 Adaptive Circuit Breakers: News Detection

Rather than applying blanket penalties, VALS implements **intelligent event classification**:

True News Events

Detection: Sudden volume spike ($>5\times$ baseline) + multiple market movements + verified news source (C2PA)

Response: Market pauses for 2-5 seconds to allow honest price discovery, then resumes with normal VALS protection

Toxic Arbitrage

Detection: High velocity without corresponding news + cross-market arbitrage signature

Response: Full exponential slippage penalty applied immediately (up to 50% cap)

Priority Fee Bypass

Purpose: Allow large traders to execute size without excessive slippage by compensating LPs directly

Mechanism: Trader pays premium (0.5-2%) directly to LPs → VALS penalty reduced proportionally

Example: \$1M trade normally faces 40% VALS penalty → Trader pays 1.5% premium (\$15k) → VALS reduced to 15%

2.3 VALS Penalty Distribution (Whale-Capped)

100% of VALS penalties flow to minority LPs, with **anti-centralization safeguards**:

```
Individual_VALS_share = min((LP_position / Total_minority), 0.20)
```

Result: Maximum 20% of VALS penalties to any single LP, regardless of position size. Prevents whale domination and ensures fair distribution.

3. Financial Architecture

3.1 Three-Way Sustainable Fee Distribution

All trades incur a **1.5% total fee**, distributed as follows:

Recipient	Share	Basis
Protocol	0.5% (33%)	Total volume
Liquidity Providers	0.7% (47%)	Inverse-weighted
Gravity Boost Pool	0.3% (20%)	Net directional flow

3.2 RWA Gravity Redistribution Mechanism

Core Principle: The protocol does NOT multiply or amplify RWA yield. Instead, 100% of Treasury bill yield (5% APY) is redistributed from majority to minority using an exponential gravity mechanism, with commitment-based vesting.

Step 1: Total RWA Yield Available

```
Total_RWA_yield = TVL * 5% * (T_elapsed / 365)
```

Example: \$10M × 5% × (7/365) = \$9,589

Step 2: Gravity-Based Distribution

The gravity mechanism redistributes yield exponentially toward the minority as settlement approaches:

```
Gravity_factor = (T_total / max(T_remaining, 0.1)) ^ 1.5 * (W_maj / W_min) ^ 0.3
```

```
Minority_alloc = Total_yield * min(base_share + (1 - base_share) *  
tanh(0.15 * Gravity), 0.95)
```

Key Properties:

- `tanh()` function ensures minority can NEVER capture >95% of yield
- At 50/50 equilibrium, minority gets base share only (no boost)
- As skew + urgency increase, minority share approaches 95% cap
- Majority always receives minimum 5% (prevents starvation)

Step 3: Commitment-Based Vesting

Each LP's allocated yield is split into **TWO components**:

```
Linear_vesting = Allocated_yield × 0.5 × (T_LP_duration / T_total)  
Completion_bonus = Allocated_yield × 0.5 × (Stayed_till_settlement ? 1  
: 0)  
Claimable = Linear_vesting + Completion_bonus
```

Example: LP leaves on day 5 of 7-day market

Linear vested: $50\% \times (5/7) = 35.7\%$ Completion bonus: $50\% \times 0 = 0\%$ (left early)
Total claimable: 35.7% Slashed: 64.3% → redistributed to remaining LPs

Step 4: Slashed Yield Redistribution

When an LP withdraws early, unvested yield is redistributed:

```
Remaining_LP_bonus = (LP_position / Remaining_TVL_side) ×  
Total_slashed
```

Result: LPs who commit until settlement earn 3.5-4× more than early leavers, creating strong incentive alignment.

Gravity Evolution Over Time

Example: 7-day market, 80/20 skew, minority allocation percentage:

Day	T_remaining	Minority Share	Boost
0 (start)	7 days	22.5%	1.13×
3	4 days	42.1%	2.11×
5	2 days	65.8%	3.29×
7 (settlement)	0.1 days	95.0% (capped)	4.75×

4. Four-Component Hybrid Yield Mechanism

4.1 Complete Minority APY Formula

```
APY_minority = RWA_gravity + LP_fees_inverse + Gravity_boost +  
VALS_capture
```

4.2 Component 1: RWA Gravity Yield

Covered in Section 3.2 - Sustainable redistribution from Treasury bills

4.3 Component 2: Inverse-Weighted LP Base Fees

LP fees (0.7%) distributed using **inverse weighting** to reward minority risk-taking:

$$\text{Minority_LP_share} = \frac{W_{\text{minority_inverse}}}{W_{\text{minority_inverse}} + W_{\text{majority_inverse}}}$$

Where:

$$W_{\text{minority_inverse}} = 1 / (\text{Minority_TVL} / \text{Total_TVL})$$

$$W_{\text{majority_inverse}} = 1 / (\text{Majority_TVL} / \text{Total_TVL})$$

Comparison at Different Skews:

Skew	Linear	Inverse
50/50	50%	50%
70/30	30%	70%
80/20	20%	80%
90/10	10%	90%

4.4 Component 3: Wash-Trading Resistant Gravity Boost

Gravity pool (0.3%) accumulates only from **net directional flow**:

$$\text{Gravity_accumulation} = |\text{Net_buy} - \text{Net_sell}| \times 0.3\%$$

Comparison:

Trading Pattern	Without net	With net
Honest: \$10M net buy	\$30k	\$30k
Wash: \$5M buy + \$5M sell	\$30k (exploit)	\$0 (immune)

4.5 Component 4: VALS Capture (Whale-Capped)

Covered in Section 2.3 - 100% to minority, 20% cap per LP (4.2% APY avg)

4.6 Complete Economic Example: 7-Day Market

Market Parameters: \$10M TVL (80/20 skew), \$1M daily volume, 5% base APY

Component	Weekly Earnings	Yield	APY
RWA Gravity	\$5,951	0.30%	15.5%
LP Base Fees	\$27,087	1.35%	70.4%
Gravity Boost	\$12,600	0.63%	32.8%
VALS Capture	\$1,600	0.08%	4.2%
TOTAL	\$47,238	2.36%	122.9%
Polymarket	\$0	0%	0%

5. Settlement & Oracle Framework

5.1 TWAP Settlement (Anti-Manipulation)

Markets settle based on **Time-Weighted Average Price (TWAP)** to prevent flash manipulation:

```
Settlement_price = TWAP(oracle_price, last_1_hour)  
TWAP = Σ(price_i × duration_i) / Total_duration
```

Example:

Market: 'Bitcoin > \$100k by Friday 5pm EST' Oracle spot prices in final hour: 4:00pm: \$99,500 (20 min) 4:20pm: \$100,300 (15 min) 4:35pm: \$99,900 (10 min) 4:45pm: \$101,000 (15 min) $TWAP = (99,500 \times 20 + 100,300 \times 15 + 99,900 \times 10 + 101,000 \times 15) / 60$
= \$100,042 **Market settles: YES (Bitcoin > \$100k)**

Benefit: Attacker cannot manipulate settlement by briefly spiking price. Requires sustained movement to affect TWAP.

5.2 Multi-Oracle Consensus Layer

VERITAS uses a three-tier oracle hierarchy for maximum security:

Tier 1: Primary Price Feeds

- Pyth Network: Low-latency price data from exchanges
- Chainlink: Decentralized oracle network
- Minimum 3/5 oracle consensus required for settlement

Tier 2: Media Authenticity (for event markets)

- C2PA (Coalition for Content Provenance and Authenticity)
- Verifies image/video authenticity via cryptographic signatures
- Prevents deepfake manipulation

Tier 3: Human Verification (UMA)

- Economic security layer for disputed settlements
- Covered in detail in Section 5.3

5.3 Dispute Resolution via UMA

UMA's optimistic oracle provides **economic finality** for settlements:

Step 1: Proposed Settlement

- Primary oracles propose settlement result
- 24-hour challenge period begins
- If no challenge → settlement finalizes

Step 2: Challenge Mechanism

- Anyone can dispute by staking 1% of market TVL
- If dispute correct → disputer earns proposer's bond
- If dispute incorrect → proposer earns disputer's bond

Step 3: UMA Token Holder Vote

- Disputed settlements escalated to UMA voters
- 48-hour voting period
- Majority decision is final and enforced

Economic Security: For a \$10M market, attacking oracle requires successfully manipulating 3+ independent oracles AND winning UMA vote. Cost to attack: >\$1M. Benefit if successful: \$10M. But UMA voters economically incentivized to rule correctly (their tokens lose value if protocol fails). Makes attack economically irrational in most cases.

5.4 Economic Security Mechanisms

Attack Vector	Cost to Execute	Mitigation
Single Oracle Manipulation	Low (\$10k-100k)	3/5 consensus required, attack fails
All Oracles Agree on Wrong Data	High (\$500k+)	UMA dispute (1% stake + reward)
Flash Price Manipulation	Medium (\$100k-1M)	TWAP settlement (1-hour average)
UMA Vote Manipulation	Extreme (>\$100M)	Economic irrationality (kills protocol value)

6. Security & Resilience Framework

6.1 Smart Contract Security

Multi-Signature Requirements

- Critical functions (pause, upgrade, parameter changes) require 3/5 multisig
- Timelock delays: 48 hours for parameter changes, 7 days for upgrades
- Emergency pause requires only 2/5 signatures for rapid response

Formal Verification Targets

- Core AMM logic: Full formal verification via Certora/Halmos
- VALS formula: Mathematical proof of bounded slippage
- Fee distribution: Verification of conservation laws

Bug Bounty Program

- Critical vulnerabilities: \$ top range
- High severity: \$ mid range
- Ongoing program managed via Immunefi

6.2 Economic Attack Vectors & Mitigations

Attack	Mechanism	Mitigation
Flash Loan Attack	Borrow \$100M, manipulate market, repay	Time locks + VALS + TWAP settlement
Sybil Attack	Split position across wallets to game VALS cap	Vesting schedules apply per-position
Oracle Manipulation	Bribe/hack price feeds	Multi-oracle consensus + UMA economic security
Wash Trading	Trade with self to generate fees	Net flow only for gravity fees

6.3 Circuit Breakers & Emergency Procedures

Automated Circuit Breakers

- Trigger: >20% price movement in <1 minute
- Action: 2-5 second trading pause for price discovery
- Resume: Gradual with size limits for 60 seconds

Manual Pause Authority

- 2/5 multisig can pause all trading immediately
- Used for: Contract bugs, oracle failures, extreme market conditions
- Unpause requires: 3/5 multisig + 24-hour timelock

Emergency Withdrawal Procedures

- If paused >72 hours: Emergency withdrawal mode activates
- LPs can withdraw proportional share of TVL
- Markets settle at last known valid price

6.4 Insurance Fund & Safety Module

Allocation: 10% of protocol earnings → Safety Module (dynamic during crises)

Coverage Scenarios

- Oracle failure leading to incorrect settlement: Up to 20% of market TVL
- Smart contract exploit: Up to 100% of affected funds
- Extreme volatility/liquidity crisis: 15% emergency buffer

Accumulation Rate can be accelerated during high revenue periods

7. Market Creation & Curation

7.1 Protocol-created Markets

The Core markets are published by the protocol. There can be community requests for specific markets, or “copy market” to copy an existing prediction market on another platform, to launch on Veritas.

7.2 Permissionless creation

Veritas Ignition: Self-Funding Bonding Curve Launcher

"The Pump.fun of Prediction Markets — But Self-Funding & Truth-Oriented"

Veritas Ignition enables **permissionless market creation for \$50** using a bonding curve mechanism that requires **ZERO protocol subsidies**. Unlike traditional bonding curves that dump on latecomers, Ignition uses escrowed trading fees to create anti-hype economics at graduation.

7.2.1 The Cold Start Problem

Traditional prediction markets face a fundamental barrier:

- **Polymarket:** Requires manual approval (bottleneck)
- **Augur:** Fixed \$30 bond led to spam and low quality
- **Standard AMM:** Needs \$10,000+ upfront liquidity (unaffordable)

Result: Only well-funded entities can create markets, preventing long-tail innovation.

7.2.2 Phase 1: Market Creation (\$50)

Anyone can create a market by:

- **Pay \$50 USDC** → Goes directly to protocol (non-refundable)
- **Specify:** Question, resolution deadline, oracle source
- **Receive:** Instant bonding curve with virtual liquidity

Virtual liquidity initialization:

```
x * y = k = 100,000,000  
x_0 = 10,000 virtual YES shares  
y_0 = 10,000 virtual NO shares  
Starting price = $0.50 (50/50 odds)
```

Key properties:

- **No upfront liquidity:** Creator only pays \$50, no capital lock
- **Instant tradability:** Users can trade immediately against curve
- **Always solvent:** Constant-product ensures market never breaks

7.2.3 Phase 2: Bonding Curve Trading (Max 30 Days)

During the bonding phase, the market operates differently from Core:

Aspect	Bonding Phase	Post-Graduation
Trading Fee	3.0%	1.5% (normal)
Fee Destination	50% escrow / 33% protocol / 17% safety module	Standard split
RWA Yield	100% → Protocol	→ LPs (gravity)
Liquidity Withdrawals	LOCKED 100%	14-day linear vesting
VALS Protection	None	Full bounded VALS

Critical Design: Complete Liquidity Lock

All deposits are 100% locked until graduation or refund. This solves multiple problems:

- **No vesting complexity:** Simple binary (locked vs unlocked)
- **Prevents gaming:** Can't deposit \$9,999 yourself + wait for \$1 victim
- **Ensures commitment:** Participants prove genuine interest by locking capital
- **Simpler UX:** Users understand "locked until \$10k" better than "7-day linear vesting"

Example of prevented attack:

- Attacker deposits \$9,500 on day 0
- Waits for innocent users to add \$500
- Market graduates at \$10,000
- **Attack fails:** Attacker's \$9,500 remains locked for 14 more days post-graduation
- By day 14, market has rebalanced (anti-hype mechanism worked)
- Attacker can't dump on latecomers

7.2.4 The Anti-Hype Mechanism: Escrowed Fee Injection

This is how Veritas beats Pump.fun on token mechanics **without any protocol subsidy**:

The Problem: Hype-Driven Markets

Typical bonding curve outcome:

- Early hype pushes market to 99% YES
- Market graduates with 99/1 skew
- NO side has only \$100 liquidity
- Contrarian bets have no exit liquidity
- Market is effectively one-sided

The Solution: Fee Escrow → Minority

During bonding, 50% of all trading fees are **escrowed** (not distributed):

$$\text{Escrowed fees} = \text{Trading volume} \times 3.0\% \times 0.5$$

At graduation, 100% of escrowed fees → minority side.

Example: \$100k Trading Volume to Reach \$10k TVL

Bonding phase:

- Total volume: \$100,000 (realistic for reaching \$10k TVL)
- Trading fees: $\$100k \times 3\% = \$3,000$ - Escrowed (50%): \$1,500 - Protocol (33%): \$1,000 - Safety Module (17%): \$500
- Final state: 99% YES (\$9,900) / 1% NO (\$100)

At graduation:

- Escrowed \$1,500 injected into NO side
- New NO TVL: $\$100 + \$1,500 = \$1,600$
- New ratio: 86.1% YES / 13.9% NO

Result:

- Minority increased 16x
- Market has real two-sided liquidity • Contrarian positions have exit depth
- **100% funded by traders (zero protocol subsidy)**

7.2.5 Graduation Criteria

Markets graduate from Ignition to Core when ALL criteria are met:

Criterion	Threshold	Prevents
Total Value Locked	\$10,000	Tiny markets wasting Core resources
Unique Participants	30 addresses	Single whale gaming the threshold
Time Since Creation	< 30 days	Stale/forgotten markets lingering

Upon graduation:

- **Bonding curve freezes:** No more virtual trades
- **Escrowed fees → minority:** Anti-hype injection executes
- **Migration to Core:** All positions become real AMM liquidity
- **14-day vesting starts:** Linear unlock prevents immediate dump
- **Full Core features activate:** VALS, gravity, hybrid liquidity, RWA yield

7.2.6 Post-Graduation Liquidity Lock

To prevent graduated markets from immediately dying, all Ignition positions enter **14-day linear vesting**:

```
Withdrawable = Position_Size × min(Days_since_graduation / 14, 1.0)
```

Days Since Graduation	Withdrawable	Still Earning APY?
0 (graduation day)	0%	Yes (100% locked, earning)
7	50%	Yes (locked portion earning)
14	100%	Yes (if choose to stay)

Why this works:

- **Earning throughout:** Locked positions earn full Veritas Core APY
- **Natural incentive:** By day 14, LPs have experienced earning on their capital
- **Prevents coordinated dump:** Can't all exit simultaneously on graduation day
- **Graduated markets have time to find equilibrium** before early LPs can fully exit

7.2.7 Failed Market Cleanup

If a market fails to reach \$10k TVL + 30 participants within 30 days:

- **All participants refunded:** 100% of deposited capital returned proportionally
- **Creator fee non-refundable:** \$50 creation cost stays with protocol
- **RWA yield → protocol:** Earnings during bonding phase go to protocol
- **Trading fees → protocol:** Since no graduation, all fees kept by protocol

Example:

Market accumulated \$500 TVL over 15 days, then died:

- Participants: Get \$500 back
- Creator: Loses \$50 (spam cost)
- Protocol receives: - \$50 creation fee - $\$500 \times 5\% \times (15/365) = \1.03 (RWA yield) - ~\$15 trading fees (est. \$500 volume × 3%) - Total: \$66.03 revenue from failed market

With 100 people per day failing to graduate (at D+30), this represents an average of 2M370K\$ annualized revenues from failed markets only, the main markets not even touched.

Result: Failed markets are PROFITABLE for the protocol, with zero user capital loss.

7.2.8 Complete Lifecycle Example

Market: "Will it rain in Paris tomorrow?"

Day 0: Creation

Creator actions:

- Pays \$50 USDC → Protocol
- Specifies: Question, deadline (tomorrow 12pm CET), oracle (weather.com)
- Receives: Bonding curve market (k=100M, price=\$0.50)

Market state:

- TVL: \$0
- Participants: 0
- Days remaining: 30

Days 0-18: Bonding Phase

Trading activity:

- 65 unique participants trade
- \$8,200 TVL accumulated (82% toward threshold)
- Skew: 75% YES (\$6,150) / 25% NO (\$2,050)
- Trading volume: \$80,000

- Fees collected: $\$80k \times 3\% = \$2,400$ - Escrowed: $\$1,200$ - Protocol: $\$800$ - Safety Module: $\$400$
- RWA yield: $\$4,100 \text{ avg} \times 5\% \times (18/365) = \$10.11 \rightarrow \text{Protocol}$
- All deposits: 100% LOCKED (can't withdraw)

Day 19: Graduation Triggered!

Market hits thresholds:

- TVL: $\$10,000$ (reached)
- Participants: 72 unique addresses (exceeded 30)
- Within 30 days: **Graduation process:**
- Bonding curve FREEZES
- Final state: 82% YES ($\$8,200$) / 18% NO ($\$1,800$)
- Escrowed fees: $\$1,200 \rightarrow$ injected into NO
- New NO TVL: $\$1,800 + \$1,200 = \$3,000$
- **New ratio: 73% YES / 27% NO**
- All 72 positions migrate to Core AMM• 14-day linear vesting starts (0% withdrawable today)

Days 19-33: Post-Graduation (Vesting Period)

Market operates on Veritas Core:

- Full VALS protection active
- Minority earning 122.9% APY
- Majority earning 11% APY
- High minority yield attracts new contrarian bets
- Market naturally balances to 68% YES / 32% NO over 7 days

Liquidity unlock schedule:

- Day 19 (graduation): 0% withdrawable
- Day 26 (graduation + 7): 50% withdrawable
- Day 33 (graduation + 14): 100% withdrawable

Trading activity:

- \$120k volume over 14 days
- Protocol fees: $\$120k \times 1.5\% \times 0.33 = \594
- Original LPs earned ~2.8% on their capital in 14 days
- Most choose to stay (high APY + already profitable)

Day 20: Market Resolves

Weather.com TWAP settlement:

- It did NOT rain in Paris
- Market resolves: NO
- NO holders (32% of pool) get paid out
- Early contrarians who bet NO earned:
 - Capital appreciation ($18\% \rightarrow 32\%$ pool share)
 - RWA gravity yield
 - LP base fees

Result: Market successfully graduated, rebalanced, resolved fairly, and generated profit for both LPs and protocol. Zero subsidies required.

7.2.9 Why This Beats Pump.fun on permissionless launches

Feature	Pump.fun	Veritas Ignition
Launch Cost	~\$2	\$50
Quality Filter	None (99% scams)	\$10k + 30 participants
Graduation Outcome	Dump on Raydium	Anti-hype fee injection
Failed Launch	Money lost	100% refunded
Protocol Subsidy	N/A	\$0 (self-funding)
Protocol Revenue from Spam	None	\$60+ per failed market
Purpose	Hype & speculation	Truth discovery & hedging

8. Implementation Roadmap

8.1 Phase 1: Testnet MVP

- Core AMM with bounded VALS protection
- Basic RWA integration (simulated Treasury bills)
- Single oracle (Pyth testnet)
- 5-10 test markets for community feedback
- Bug bounty program launch

8.2 Phase 2: Mainnet Launch

- Full hybrid liquidity (AMM + Order Book)
- Live RWA integration (real Treasury bills)
- Multi-oracle consensus (Pyth + Chainlink + UMA)
- Dutch auction bootstrapping
- 20-50 curated markets
- Smart contract audits

8.3 Phase 3: Advanced Features

- Conditional markets (if-then relationships)
- Advanced order types (stop-loss, trailing orders)
- Mobile app (iOS + Android)

8.4 Long-term Vision

- AI-powered market curation and quality control
- Decentralized oracle network (VERITAS-specific)
- Traditional finance integration (broker-dealer partnerships)
- Global compliance framework (CFTC, EU MiCA, etc.)
- 1000+ markets across all categories

9. Risk Disclosures

9.1 Smart Contract Risks

- Bugs in core contracts could lead to fund loss
- Upgrade vulnerabilities if governance compromised
- Composability risks with external RWA protocols
- Mitigation: Multiple audits, formal verification, bug bounties, gradual rollout

9.2 Oracle Failure Scenarios

- All oracles simultaneously report incorrect data
- Oracle network outage preventing settlement
- Delayed settlement causing market uncertainty
- Mitigation: Multi-oracle redundancy, UMA dispute layer, TWAP settlement

9.3 Market Risks

- Extreme volatility causing circuit breaker activations
- Liquidity crises in extreme market conditions
- Market manipulation attempts by well-funded actors
- Mitigation: VALS protection, wash-trading immunity, Safety Module reserves

9.4 Regulatory Considerations

Prediction markets occupy a complex legal landscape. Key considerations:

- U.S.: Prediction markets on certain topics may be regulated as commodity futures (CFTC jurisdiction)
- EU: MiCA regulations may apply to certain market types
- Asia: Regulatory status varies significantly by jurisdiction
- Platform implements geo-blocking for restricted jurisdictions
- Users responsible for compliance with local laws

Disclaimer: VERITAS is not available to U.S. persons or residents of restricted jurisdictions. This document does not constitute legal or investment advice. Consult qualified professionals before participating.

10. Conclusion & Competitive Analysis

Competitive Positioning

Feature	Polymarket	Kalshi	VERITAS
Minority incentivization	No	No	Yes
Wash Trading Protection	None	None	Net flow only
VALS Protection	None	None	Bounded (max 50%)
Circuit Breakers	None	Manual only	Adaptive + manual
Settlement	Single oracle	Centralized (Kalshi)	Multi-oracle + UMA
Yield-Bearing Orders	No	No	Yes (industry first)

VERITAS introduces a **dual innovation** that fundamentally changes prediction markets:

1. Yield-Bearing Markets: Minority positions earn through RWA gravity redistribution, inverse-weighted LP fees, wash-resistant gravity boost, and VALS capture — versus Polymarket's 0%.

2. Veritas Ignition: Permissionless market creation for \$50 with **zero protocol subsidies**. Failed markets generate revenue, successful markets self-fund anti-hype rebalancing through escrowed trading fees.

Where Polymarket requires permissioned creation and offers no yield, and where Pump.fun enables launches but creates dump-on-Raydium dynamics, VERITAS offers **\$50 accessible creation with automatic quality filtering** (economic graduation) and **self-funding anti-hype mechanics** that prevent early buyer dumps.

With production-grade security (formal verification, multi-oracle consensus, UMA economic layer), sustainable economics (failed markets fund the protocol at ~\$60/each), post-graduation liquidity locks (14-day vesting), and advanced liquidity infrastructure (hybrid AMM + order book, Dutch auctions, yield-bearing orders), VERITAS is positioned to become the **dominant prediction market platform** for both retail users seeking yield and institutions requiring robust infrastructure.



VERITAS *The Future of Yield-Bearing Prediction Markets*