Verification can be checked on GitHub

Gnumer Whitepaper: A Next-Generation ZK-Powered Lottery Protocol on Solana

For decades, the gambling industry has been a walled garden, rigged and ruled by mega-corporations and shadow elites. But the tide is turning. Through the convergence of Decentralization and Zero-Knowledge Proofs, we are arming the community to dismantle the monopoly of the 'House'.

With 1+ SOL, you become an owner of a decentralized empire. With 5+ SOL, you can secure a yield-bearing legacy that could redefine your retirement.

The House no longer wins; the Community is the House.

1. Executive Summary

Gnumer is a decentralized, on-chain lottery protocol built on the Solana blockchain, engineered to redefine digital gaming through transparency and cryptographic integrity. By integrating **Switchboard VRF** (Verifiable Random Function) for unbiased randomness and **Zero-Knowledge Proofs (ZKP)** for private yet verifiable betting, Gnumer ensures a "Provably Fair" environment. Operating under a regulatory-compliant framework (license pending), Gnumer automates execution via smart contracts, merging the excitement of gaming with the robustness of decentralized finance (DeFi).

2. Market Opportunity & Outlook

The global crypto-gambling sector is experiencing exponential growth, with 2025 revenues surpassing **$81.4 billion**. Leading platforms have demonstrated remarkable capital efficiency, with some achieving $100 million in TVL within 60 days. Gnumer aims to capture this momentum by offering a trustless alternative to centralized "black-box" platforms, returning value to the community through a sustainable dividend model.

3. Tokenomics & Governance

Token Name: GNUM

Total Supply: about 62,000,000 GNUM

3.1 Distribution & Lock-up

Total Initial Mint: 32,000,000 GNUM

Mint from SOL: 10,000 GNUM/SOL (with a cap of 3000 SOL+ a minus OpEx budget)

Early Contributors: 750,000 GNUM (Distributed to initial 5,000 USDT contributors).

Internal Testing: 1250,000 GNUM (Team-allocated for testing).

Ecosystem Reserve: 30,000,000 GNUM (Locked for 730 days, which will then undergo a 10% monthly linear vesting).

3.2 Fundraising & Capital Allocation

Gnumer adopts a "Lean Startup" model. All funds raised will be collected in a multi-sig wallet. Fundraising and minting will automatically cease once the balance reaches **3,000 SOL**. To ensure transparency, the team draws only a minimal Opex to prioritize protocol

development over capital accumulation.

Use of Funds (3,000 SOL Soft Cap):

- **Initial Prize Pool (Liquidity):** 1000 SOL
- **Regulatory Compliance & Licensing:** 600 SOL
- **Security Audits (Smart Contract):** 400 SOL
- **Market Making & Price Stability:** 700+ SOL
- **OpEx Budget: Around** 300SOL

3.3 Holder Value Proposition (Staking & Dividends)

Gnumer incentivizes long-term conviction. Starting from the second month post-launch, all wallets holding >50,000 GNUM (equivalent to 5 SOL at issuance) without selling in the past 35 days qualify for a 2% revenue share from every lottery ticket sold. Addresses with an initial buy of 5+ SOL will be whitelisted. When participating in the current rev-share, rewards will be calculated as gnumer **+30%** of the position size.

4. Technical Architecture & Key Innovations

Gnumer utilizes a unique three-phase execution cycle to ensure privacy and scalability.

Phase 1: Encrypted Betting (Privacy-Preserving UX)

Users interact with the Solana contract to fetch a session-specific Temporary Public Key (PKr). Selections are encrypted client-side and submitted as ciphertext, preventing "front-running" or data leaks during the betting window.

Phase 2: Decentralized Randomness & Reveal

Upon session closure, a decentralized Crank (Trigger) locks the state. The protocol invokes Switchboard VRF to generate a verifiable random

seed. Simultaneously, the Decryption Private Key (SKr) is published to the Round PDA, ensuring full post-game transparency.

Phase 3: The Gatekeeper Game & ZK-Verification

To offload computation while maintaining security, Gnumer introduces the **Gatekeeper Role**:

Threshold: Gatekeepers obtain the SKr by threshold signatures.

Decryption: Staked Gatekeepers (Keepers) decrypt on-chain data using the released SKr.

ZK-Generation: Gatekeepers generate a **ZK-SNARK proof** certifying:

1.Data integrity relative to the on-chain ciphertext.

2.Accurate decryption and winner identification.

3.Correct Merkle Root generation containing all winning hashes.

4.Precise prize pool distribution according to protocol math.

Settlement: The Solana contract verifies the ZK-proof. Once validated, the **Merkle Root** becomes the immutable claim credential, and the Prize Pool PDA automates the payout.

5. Roadmap & Contingency

Phase 1 (Funding): Expected completion within 6 weeks. (Contingency: If funding is not met within another 8 weeks, all SOL will be proportionally refunded to contributors minus operational costs).

Phase 2 (Compliance): Licensing applications will commence within 7 days of successful funding.

Phase 3 (Mainnet): Full protocol launch and operational rollout within 2 months post-funding.