White Paper

Phase 1: Planning

Objective: Create a decentralized, automated, and transparent lottery.
Blockchain: Polygon.
Winner Selection Mechanism: Use of Chainlink VRF (Verifiable Random Function) to generate verifiable random numbers on-chain.
Participation Tokens: POL.
Legal and Compliance Aspects:

- Analyze local regulations for gambling and lotteries.
- Possible integration of KYC and AML if required by jurisdiction.

User Experience Design:

User Flow

- Wallet connection.
- Purchase of lottery tickets.
- Automated drawing with Chainlink VRF.
- Distribution of the prize to the winner.

User Dashboard

- Ticket status.
- Prize pool.
- Countdown to the next draw.

Phase 2: Technical Design

System Architecture:

Solidity Smart Contract:

- Ticket management.
- Winner drawing with Chainlink VRF.
- Automated prize distribution.

Frontend Next.js

- Wallet connection MetaMask, Phantom.
- Ticket purchase.
- Viewing winners.

Backend Next.js

- Data analysis for statistics.
- Tools and Technologies

Blockchain Polygon

- Smart Contracts: Solidity.
- Wallet Integration: MetaMask, Phantom
- Randomization: Chainlink VRF.
- Frontend: Next.js with Ethers.js.

Phase 3: Development

Create the Smart Contract with Chainlink VRF:

Main Functions

- buyTicket() → The user buys a ticket.
- requestRandomWinner() → Requests a random number from Chainlink.
- fulfillRandomness() → Selects the winner and distributes the prize.

Contract Testing

- Simulate ticket purchases.
- Verify Chainlink VRF integration on testnets.

Frontend Development:

Main Page

- Connect wallet.
- Display prize pool.

User Dashboard

- Purchase tickets.
- View winner history.
- Countdown to drawing.

Frontend and Smart Contract Integration:

Ethers.js Integration to call buyTicket() and requestRandomWinner() functions.

Phase 4: Testing and Audit

- Test on AmoyTestnet.
- Verify Chainlink VRF calls.
- Simulate ticket purchases and prize distribution.
- Security Audit with Slither.
- Check for vulnerabilities.

Phase 5: Deployment

- Deploy the Smart Contract on the Mainnet.
- Supported Blockchains: Polygon.
- Frontend Hosting on Vercel.

Phase 6: Launch and Marketing

- Promote on Crypto Communities.
- Announce on Twitter, Reddit, Telegram, Discord.
- Collaborate with Web3 influencers.

Phase 7: Maintenance and Enhancements

- Transaction Monitoring and Optimizations.
- Analyze gas costs and optimize.
- Implement New Features.
- Progressive jackpots, multiple winners.