# **Bikera Revamp Proposal**

## **Architecture Overhaul & Security Enhancement**

**Recommendation**: Do not deploy to production. Immediate remediation required across security, testing, and reliability.

### 🎯 **Revamp Objectives**

* **URGENT Security Fixes**: Address 63 critical vulnerabilities identified in audit
* **Independent Canister Architecture**: Separate canisters for different functions, one main canister for keeping track of information called main
* **Dual-Token Economics**: iMERA (Solana) + XP (ICP) token system
* **Move-to-Earn System**: GPS-based movement tracking with anti-gaming measures
* **Modern Stack**: React/JSX frontend with Motoko canisters
* **High Security**: Enterprise-grade encryption and authentication
* **Scalability**: 10,000+ users with optimized consensus mechanism
* **Privacy**: GDPR compliance with burnable tokens for data erasure

## 🏗️ **New Architecture Overview**

### **Technology Stack Migration**

1. Current: Rust Canisters + React Native + Mixed Backend
2. New:     Motoko Canisters + React/JSX Web App + Unified Backend

### **Core Components**

#### **1. Frontend Layer (React/JSX)**

* **Framework**: React 18+ with TypeScript
* **State Management**: Zustand + React Query
* **UI Library**: Tailwind CSS + Headless UI
* **Authentication**: Internet Identity + Wallet Connect
* **Real-time**: WebSocket connections for live updates

#### **2. Backend Layer (ICP Canisters)**

🏛️ **Main Canister**

* **Purpose**: Central information tracking and coordination
* **Functions**: System statistics, user tracking, coordination between canisters
* **Storage**: Global system state, user counts, mining statistics

**Independent Canisters (Each with specific functions)**

* **Consensus Canister**: Winner selection algorithm and anti-gaming enforcement
* **iMERA Token Canister**: ICRC-2 compliant token for Solana bridging
* **XP Token Canister**: Non-transferable experience points (1km = 1 XP)
* **User Canister**: Identity and profile management with Internet Identity
* **Rewards Canister**: iMERA distribution and claiming mechanism
* **Validator Canister**: Movement data validation and distance tracking

#### **3. External Integrations**

* **Solana**: iMERA token distribution and staking
* **CloudFlare Workers**: Data processing and rate limiting
* **Database**: User data and session management

## 🚨 **CRITICAL SECURITY ISSUES TO FIX**

### **Major Vulnerabilities Found**

* **Re-entrancy Attacks**: Token theft vulnerability
* **SQL Injection**: Database manipulation risks
* **Input Validation**: Missing validation on user inputs
* **Race Conditions**: Consensus mechanism vulnerabilities
* **Weak Authentication**: Poor session management
* **Memory Leaks**: Canister performance issues
* **Authorization Issues**: Unauthorized access to functions

## 💰 **Dual-Token Economics System**

### 🎯 **iMERA Token (Primary Reward Token)**

* **Blockchain**: Solana
* **Total Supply**: 100 million tokens
* **Distribution Period**: 2 years
* **Mining Schedule**: 500 iMERA distributed every 5 minutes
* **Mining Capacity**: 10,000 users maximum

#### **Staking Requirements**

* **Start Stake**: 1,000 iMERA (adjustable by governance)
* **Hard Floor**: 50 iMERA (cannot be reduced below this amount)
* **Validator Requirement**: 1 million iMERA for Raspberry Pi node operation
* **Dynamic Scaling**: 1M tokens = 0.9 iMERA reward, 10M tokens = 9 iMERA reward

#### **Reward Distribution**

* **Winners per Round**: 1 per 1,000 active users (max 10 winners)
* **Minimum Reward**: 50 iMERA per winner
* **Foundation Share**: 10% of all rewards (100 iMERA per round) // should be 50 iMERA with 500 iMERA block rewards every 5 min. (unless lowering to 10min rounds will reduce container cost drastically)
* **Lock Owner Rewards**: 20-30% of block rewards (future expansion)

### ⭐ **XP Token (Experience Points)**

* **Blockchain**: ICP (with future Solana bridge)
* **Purpose**: Non-transferable reputation system
* **Exchange Rate**: 1 kilometer = 1 XP
* **Minting Schedule**: Every 2 days
* **Minimum Activity**: 100m displacement per 5-minute interval
* **GDPR Compliance**: Burnable tokens for data erasure

#### **Key Features**

* **Non-transferable**: Locked to user accounts
* **Universal Access**: Available to all users regardless of iMERA holdings
* **Cross-chain Bridge**: Future ICP ↔ Solana bridging capability
* **Privacy-First**: No GPS coordinates stored, only distance data

### 🛡️ **Anti-Gaming Measures**

* **No consecutive wins** for same user
* **Maximum 25 wins per day** per user
* **Duplicate Solana addresses filtered** (random selection)
* **Minimum displacement requirements**: 100m per 5-minute interval
* **Speed validation**: Total distance calculated not more than 50km/h
* **Solana address verification**: Minimum stake requirement validation

## 🔐 **Security Enhancements**

### **1. Authentication System**

* **Internet Identity**: Primary authentication method
* **Session Management**: Secure token handling
* **Multi-Factor Auth**: Additional security layers

### **2. Data Protection**

* **Encryption**: All data encrypted at rest and in transit
* **Privacy**: No GPS coordinates stored, only distance data
* **GDPR Compliance**: User data can be completely erased
* **Secure Communication**: TLS 1.3 for all connections

### **3. Anti-Gaming Measures**

* **Speed Validation**: Realistic movement patterns only
* **Distance Requirements**: Minimum movement thresholds
* **Rate Limiting**: Maximum rewards per user
* **Duplicate Prevention**: Random selection for duplicate addresses

## 🏛️ **Canister Architecture**

### **Main Canister**

* **Purpose**: Central information tracking and coordination
* **Functions**: System statistics, user counts, mining data
* **Storage**: Global state, coordination between other canisters

### **Independent Canisters**

#### **1. Consensus Canister**

* **Winner Selection**: 1 winner per 1,000 users (max 10 winners)
* **Anti-Gaming**: No consecutive wins, max 25 wins/day
* **Security**: Re-entrancy guards, input validation

#### **2. iMERA Token Canister**

* **Token Supply**: 100 million iMERA total
* **Mining**: 500 iMERA every 5 minutes
* **Solana Bridge**: Burn ICP tokens, mint on Solana
* **Security**: Re-entrancy protection, bounds checking

#### **3. XP Token Canister**

* **XP Rate**: 1km = 1 XP
* **Minting**: Every 2 days
* **Privacy**: Burnable for GDPR compliance
* **Non-transferable**: Locked to user accounts

#### **4. User Canister**

* **Profiles**: User identity and profile management
* **Devices**: Device registration and tracking
* **Privacy**: User privacy settings and controls

#### **5. Validator Canister**

* **Movement Validation**: GPS data verification //if possible this needs to be done by the Front -end so that no GPS coordinates leave the device, or it should be Immediately pruned after verification. Privacy and GDPR or the coordinates need to be obfuscated but stil vector proofable. See security enhancements
* **Distance Tracking**: Movement distance calculation
* **Anti-Gaming**: Speed and pattern validation

#### **6. Rewards Canister**

* **Distribution**: iMERA reward distribution
* **Claiming**: Cross-chain reward claiming
* **Staking**: Solana staking verification

## 📱 **Frontend Architecture (React/JSX)**

### **1. Project Structure**

1. src/
2. ├── components/          # UI components
3. │   ├── auth/           # Login/signup components
4. │   ├── dashboard/      # Main dashboard
5. │   ├── map/           # Location tracking
6. │   └── wallet/        # Wallet integration
7. ├── hooks/             # Custom React hooks
8. ├── services/          # API services
9. ├── stores/           # State management
10. └── utils/            # Helper functions

### **2. Key Features**

* **Authentication**: Internet Identity + Solana wallet ( optional )
* **Location Tracking**: GPS movement tracking
* **Real-time Updates**: Live mining statistics
* **Wallet Integration**: Token management
* **Dashboard**: User statistics and rewards

## 🔄 **Migration Plan**

### **Phase 1: Security Fixes (Weeks 1)**

1. **Critical Security Patches**
   * Fix re-entrancy vulnerabilities
   * Add input validation
   * Implement proper authentication
   * Fix memory leaks
   * Add error handling
2. **Stop Production Deployment**
   * Freeze all changes
   * Enable monitoring
   * Deploy emergency fixes

### **Phase 2: Backend Development (Weeks 2-3)**

1. **Canister Development**
   * Migrate to Motoko canisters
   * Implement main canister for tracking
   * Create independent canisters for each function
   * Add security measures
2. **API Development**
   * Create REST APIs
   * Implement WebSocket connections
   * Add rate limiting

### **Phase 3: Frontend Development (Weeks 4-5)**

1. **React/JSX Application**
   * Build authentication system
   * Create dashboard interface
   * Implement location tracking
   * Add wallet integration
2. **User Interface**
   * Design responsive UI
   * Add real-time updates
   * Implement user statistics

### **Phase 4: Testing & Deployment (Weeks 6)**

1. **Testing**
   * Unit tests
   * Integration tests
   * Security testing
   * Performance testing
2. **Deployment**
   * Staging environment
   * Mainnet deployment
   * User migration

## 🔄 **Data Flow**

### **Simple Data Flow**

1. User Movement (GPS) → Backend Processing → ICP Consensus → Solana Distribution

### **Key Components**

1. **Frontend**: GPS tracking and user interface
2. **Backend**: Data processing and validation
3. **ICP Canisters**: Consensus and token management
4. **Solana**: Token distribution and staking

## 🎯 **Success Metrics**

### **Security Goals**

* Fix all critical vulnerabilities
* Implement proper authentication
* Add comprehensive input validation
* Ensure GDPR compliance

### **Performance Goals**

* Fast API response times
* Reliable consensus mechanism
* Smooth user experience
* Scalable architecture

### **User Experience Goals**

* Easy authentication
* Clear dashboard
* Real-time updates
* Mobile-friendly interface