ADCX
LAB

Full Disclaimer – ADC CryptoGuard

1. Purpose

ADC CryptoGuard is an informational tool for validating cryptocurrency wallet activity and potential risk indicators. It does not provide financial advice or guarantee the accuracy or completeness of any analysis.

2. Data Handling & Privacy

- **No sensitive user data is stored at any time.**
- **Wallet addresses are processed in memory only for the duration of validation and discarded immediately after generating results.**
- **The only persisted metric is a non-sensitive usage counter.**
- **All data transmitted between the user and ADC CryptoGuard is encrypted via HTTPS/TLS.**

3. Data Sources & Limitations

- **Risk analysis is based on publicly available blockchain data retrieved via third-party APIs (e.g., Etherscan, TronGrid, BlockCypher, Helius).**
- **Accuracy and availability are dependent on these external sources and may be affected by their uptime, data quality, and rate limits.**
- **Validation results may not reflect the complete transaction history or hidden wallet activities.**

4. Security Practices

- **API credentials are securely stored in environment variables on our hosting platform (Render) and are never hard-coded in the application.**
- **Rate limiting and request validation are implemented to mitigate abuse and automated bot attacks.**
- **Error handling mechanisms ensure graceful fallback if API services are unavailable.**

5. Compliance

- **Reports are generated in ISO 20022-compliant format to ensure structured, auditable, and institution-ready output.**

- **Users are responsible for ensuring compliance with local laws and regulations when using ADC CryptoGuard.**

6. Liability

- **Users are solely responsible for any actions taken based on the information provided.**
- **ADC CryptoGuard and ADCX Lab shall not be held liable for any losses, damages, or decisions made based on validator results.**

7. Supported Networks

BTC, ETH, BSC, XRP, TRON, SOL, BASE, Hedera.

DATA FLOW