VEYLOX

Self-Custody Multi-Chain Wallet

Complete project report · Mainnet release

Developer	Website
Vedhant Khajuria	veylox.vedhant.in

A technical and product overview covering purpose, features, architecture, user flows, security, deployment and limitations.

1. Executive summary

Veylox is a browser-based self-custody cryptocurrency wallet. It lets a person create or import a wallet, keep the recovery phrase encrypted on their own device, view blockchain balances, receive assets and sign outgoing transactions locally. The mainnet configuration supports Ethereum, BNB Smart Chain, Polygon, Bitcoin and Solana. Ethereum ERC-20 USDT is included as a verified default asset.

2. Product purpose

Veylox gives users a wallet interface without taking custody of their funds. Users control the recovery phrase and are responsible for protecting it. The server provides controlled access to public blockchain infrastructure and optional account services; it does not store private keys or provide a recovery backdoor.

3. Main capabilities

- Create or import a BIP-39 wallet.
- Encrypt wallet data locally with AES-256-GCM and PBKDF2-SHA256.
- Lock manually, after inactivity, or when the page is hidden.
- Derive and display addresses for five supported mainnet families.
- Read native and supported token balances directly from blockchains.
- Send native assets, ERC-20, SPL and Bitcoin funds after a fresh fee review.
- Receive using a public address and QR code.
- Track local transactions and blockchain confirmations.
- Use watch-only wallets without signing capability.
- Deploy on PHP/MySQL cPanel hosting without Node.js services.

4. Supported networks and assets

Network	Chain / Path	Native	Token support
Ethereum Mainnet	EVM 1	ETH	ERC-20, including USDT
BNB Smart Chain	EVM 56	BNB	EVM tokens
Polygon Mainnet	EVM 137	POL	EVM tokens
Bitcoin Mainnet	BIP-84	BTC	Native BTC
Solana Mainnet	Mainnet	SOL	Standard SPL tokens

Ethereum USDT uses contract 0xdAC17F958D2ee523a2206206994597C13D831ec7 and 6 decimals. The token protocol and network must match the sending wallet.

5. How users work with Veylox

Create or import: the user creates a wallet in an HTTPS browser or enters an existing recovery phrase. The phrase derives addresses locally and is encrypted before being saved in browser storage.

View balances: Veylox calls a restricted PHP proxy, verifies the selected chain and forwards public read requests to the configured RPC provider.

Receive: the user selects a network, copies the public address or QR code, and gives it to the sender. The sender must use the same network and token protocol.

Send: Veylox validates the recipient, balance, nonce or UTXOs, chain and fee. The user reviews the transaction and unlocks locally to sign. The signed transaction is broadcast and checked for confirmation.

Recover: recovery uses the offline phrase. Losing the phrase, password and encrypted browser data can make a wallet unrecoverable.

6. Technical structure

The repository separates the Apache public document root from private PHP code, configuration, database schema, browser modules and tests.

```
Veylox/
■■■ public/ document root, PHP endpoints and browser assets
■■■ app/ bootstrap, sessions, CSRF, PDO and HTTP helpers
■■■ config/ private configuration and safe example template
■■■ database/ MySQL schema
■■■ storage/ private server storage
■■■ tests/ wallet, signing and regression tests
■■■ tooling/ build, formatting, packaging and mainnet checks
```

EVM addresses use the Ethereum derivation path; Bitcoin uses BIP-84 mainnet derivation; Solana uses its standard derivation path. EVM signing uses ethers. Bitcoin and Solana use the bundled multichain implementation.

7. Security model

- Recovery phrases never belong in PHP configuration, MySQL or API request bodies.
- Vaults use AES-256-GCM, fresh salt and IV, PBKDF2-SHA256 with 600,000 iterations and authenticated wallet context.
- Signing requires a fresh review, password and verification of chain, address, nonce and balance.
- PHP uses HTTPS enforcement, secure sessions, CSRF, origin validation, prepared SQL, request limits and throttling.
- A compromised device, extension, server-delivered JavaScript or RPC endpoint can still compromise an unlocked wallet.

This is self-custody software, not a regulated custody service. Professional security audit, dependency review, monitoring and incident response are required before meaningful public funds.

8. cPanel deployment

Set the document root to /home/CPANEL_USERNAME/veylox/public. Keep app, config, database and storage above that directory. Import database/schema.sql, copy config.example.php to config.php, set the exact HTTPS origin and configure mainnet RPC endpoints. Verify private-file protection, RPC identity, small funded transfers and explorer confirmations. Clear the first-admin setup token after creating the administrator.

9. Fees and transaction behavior

Fees are paid in the native asset: ETH for Ethereum USDT, BNB for BNB-chain tokens, POL for Polygon tokens, SOL for Solana tokens and BTC for Bitcoin. The amount of USDT does not determine Ethereum gas. Veylox estimates and displays a maximum fee before signing; the actual fee may be lower. Broadcast failures remain uncertain rather than being retried automatically.

10. Current limitations

- Swap transactions are disabled because the former implementation targeted a testnet router.
- Market values are indicative and depend on the configured price provider.
- Public RPC endpoints can be rate limited; production use should use authenticated providers.
- Users must verify protocol and network before every deposit or withdrawal. Blockchain transfers cannot be reversed.
- The project has not received an independent security audit.

11. Developer

Vedhant Khajuria
Founder & Full-Stack Developer

Website: https://veylox.vedhant.in
LinkedIn: https://in.linkedin.com/in/vedhantkhajuriaofficial
GitHub: https://github.com/vedhant-khajuria
Email: vedhantkhajuriaofficial@gmail.com

12. Conclusion

Veylox combines browser-local key ownership with cPanel-compatible deployment. Its central design principle is that the user reviews and authorizes every movement of funds while the server provides controlled access to public blockchain infrastructure. The release is suitable for controlled testing after deployment verification, provider configuration and professional security review.