Security and privacy

When it comes to security in WEB3, it's up to both the developers and the end users to keep a secure relation. Blockchain technology is based on principles of cryptography, decentralization and consensus, which ensure trust in transactions.

Data in the HTTP/API requests

Use HTTPS instead of HTTP

HTTPS uses the SSL/TLS protocol to encrypt communications so that attackers can't steal data. It ensures that any data transferred remains unknown to read for unwanted participants.

Uses encryption to keep data secure.

Data in the WSS channels

Blockchain apps use the WebSocket protocol make realtime communication. Unlike HTTP, you don't need to continuously make requests to access the data. Instead of, WebSockets maintain a connection for you ensure information flow even faster.

Nodes are a critical component of a blockchain's infrastructure, and without them, a blockchain's data would not be accessible.

WebSocket doesn't come with CORS inbuilt. It means that any website can connect to any other website's websocket connection and communicate without any restriction.

The Origin HTTP header is set by the browser to the origin of the HTML page containing the JavaScript that is opening the WebSocket connection. A server MAY check that header and deny. But since you say other browsers are working (which?), this is unlikely

The WebSocket protocol runs on TCP, just like HTTP. To enable SSL connections, obtain any required SSL certificates.

Think about timing and even if you have multiple addresses, balance checks can give a good base for statistics on which addresses belong to the same wallet/browser?

Several methods have been proposed to improve the privacy of blockchains (mixers, zero knowledge, etc.). At the moment, the solutions relying on zero-knowledge proof of knowledge are the ones providing the strongest privacy features using Zcash z-address to send private transaction.

What the user can do to improve their privacy?

Just like the code, the user can be also a victim of malicious activities.

Use hardware wallets

Hardware wallets are designed store cryptocurrency keys offline while being unhackable, Altough it provides almost 100% security for your crypto, the user is stil vulnerable for social engineering attacks.

Use Two-Factor Authentication

Using Multi-factor authentication is a recommended thing, even outside of the crypto world. It ensures that the user has to provide two or more verification factors to gain access.