Decentralized Uptime & Security Monitoring Platform

Project Overview

This platform is a decentralized Web3 SaaS designed to provide continuous uptime and security monitoring for websites. It leverages a network of globally distributed validators to create a trustless, community-driven monitoring ecosystem with built-in economic incentives.

How It Works

1. User Submission: Website owners submit their URLs via the platform dashboard for uptime and security monitoring.

2. Validator Participation: Anyone can download a Firefox extension(soon chrome extenstion too) to become a validator. Once active, validators receive randomly assigned websites to monitor.

3. Automated Monitoring: Validators run automated health checks including:

- Response time
- Latency
- SSL certificate status
- HTTP headers audit
- DDoS like conditions pattern detection

4. Decentralized Validation: Multiple validators perform checks on each website. Data is aggregated and cross-verified to ensure accuracy.

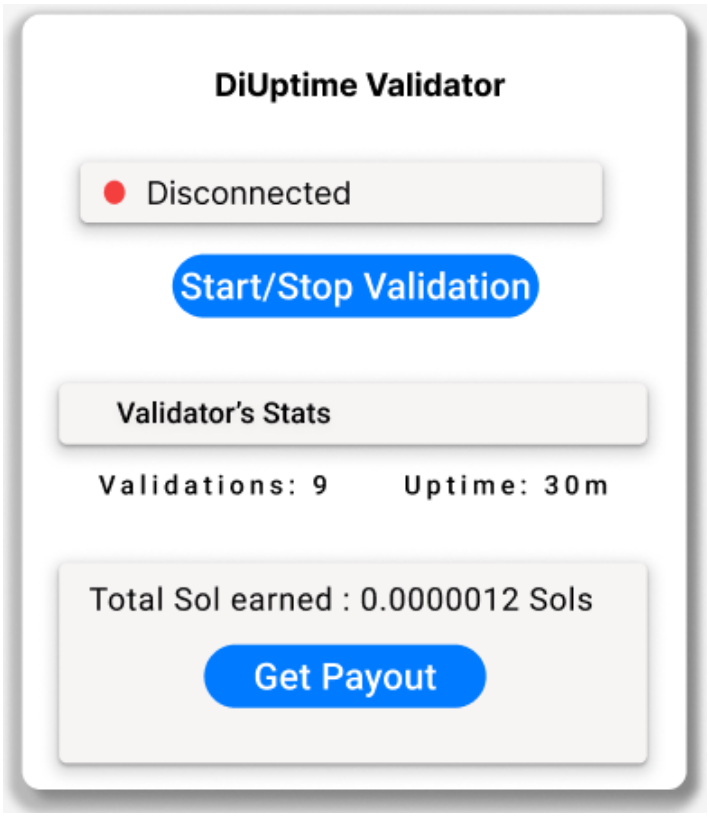
5. Solana-Based Rewards: Validators are rewarded in Solana (SOL) for each valid check. Rewards are handled via smart contracts using @solana/web3.js.

6. Payout Threshold: Validators can withdraw rewards after reaching a specified minimum balance.

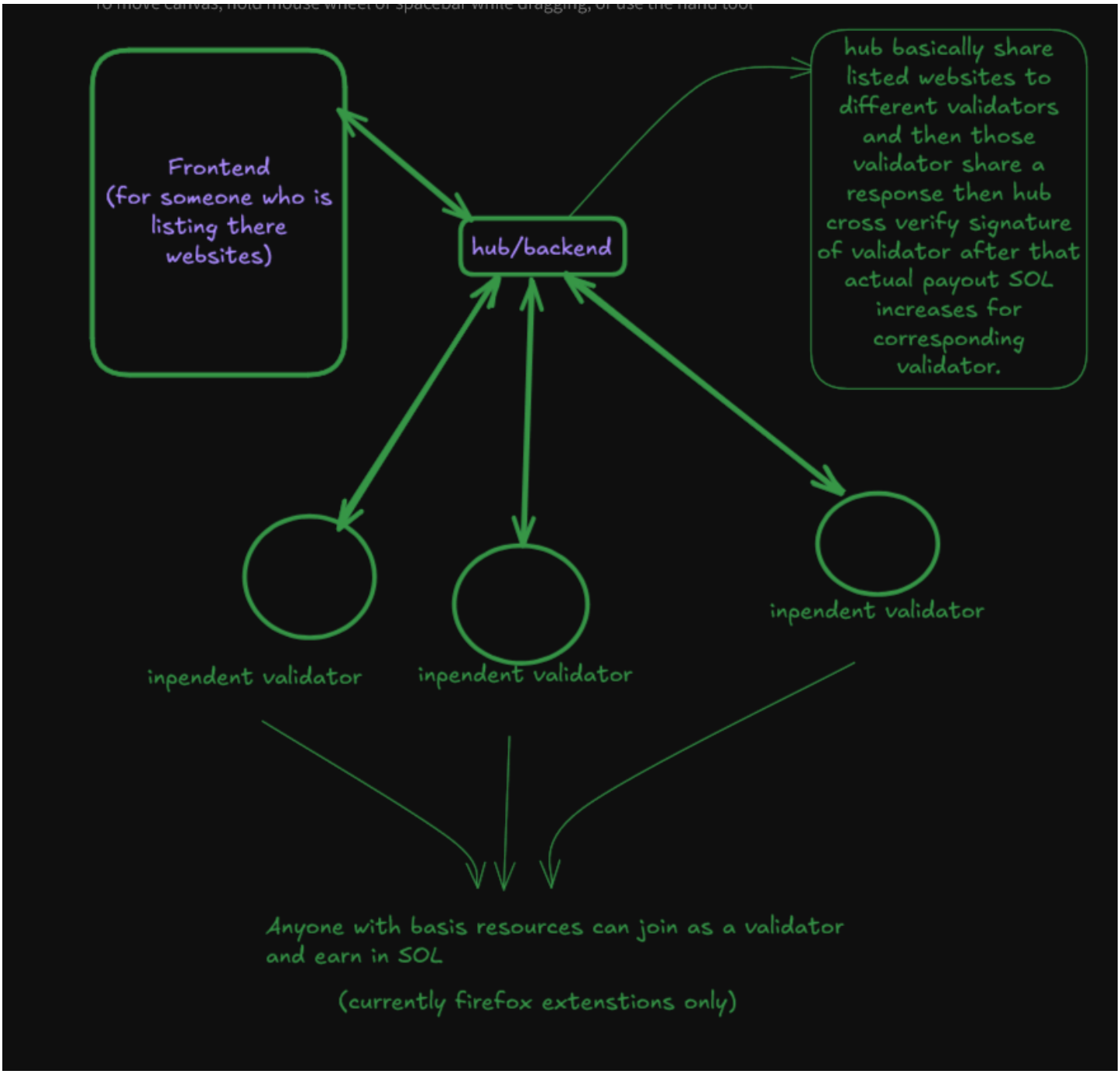
7. Public Logs : Monitoring results can be anchored on-chain or stored on IPFS/Arweave for transparency and auditability.

Dashboard overview :

Validator Extn:



Arch. overview :



Key Features

Decentralized Infrastructure: Eliminates single backend or censorship.

Security-First Monitoring: Goes beyond uptime to include real security signals.

Global Validator Network: Ensures geographically accurate performance data. as there can be multiple small validators which can word indepentendly from different regions.

dApp Integration(in future) : API/SDK for Web3 Projects.

- Custom Alerts: Set up triggers and receive notifications when downtime or security anomalies are detected.
- Decentralized Trigger Automation: Web3 or decentralized platforms can use our SDK/API to build automated responses. For example, if our system detects downtime on their infrastructure, they can perform some custom triggers.
    - **dApps depend on availability** — if their frontend goes down, users are locked out.

- They want to **show transparency** and build user trust.
- Some DAO insurance or uptime guarantees **require proof** of stability.
- They can use your monitoring service without building it themselves.

How are we marking as Down Server or DDoS

✅ **1. Multi-Metric Anomaly Detection :** Instead of relying on just request count (RPS), combine **several metrics**:

- 📈 **RPS Spike**: 3x or more over baseline
- ❌ **Error Rate Spike**: >30% 5xx status codes
- 🕒 **Latency Surge**: response times 2x or 3x over average
- 🌍 **Geo/IP Skew**: e.g., 90% traffic from 3 ASNs or IPs
- 🤖 **Low Entropy** in headers, user-agents, or TLS fingerprints

If **4 out of 5** of those happen at once → high confidence of DDoS.

🤝 **2. Validator Consensus Mechanism (Web3 Native):** Here's where your decentralization shines.

Let's say 7 validators are monitoring xyz.com:

- Each flags a DDoS only if it sees anomalies.
- If **5 out of 7** validators agree within a 2–5 minute window → you **mark it as DDoS**.

Note: these things can be improved in Future by more R&D.

Why Validator Logic Is Better than Traditional methods.

1. **Global Distribution = Real-World Accuracy**
   Validators are spread worldwide, simulating real users. This catches region-specific downtime that centralized systems often miss.
2. **No Central Point of Failure**
   Centralized monitoring services can be targeted or fail. Your decentralized network continues functioning even if parts go down.
3. **More Resistant to Manipulation**
   No one entity controls uptime reports. Validators independently verify, making it harder to fake reports or cover up outages.
4. **Scalable by Community**
   As more validators join, monitoring power increases—without you needing more servers or infrastructure.
5. **Earn-to-Participate Model**
   Validators are incentivized with Solana, which builds an engaged, self-sustaining community instead of a passive user base.
6. **Cost efficient -** As we dont have to burn centralised server resoources when there are less websites listed.

🚀 Future Prospects & Growth Plans

1. **Open Source Expansion**

- Open the full codebase (Hub, Validators)
- Add contribution guidelines & good first issue tags
- Launch on GitHub and Web 3 community.

2. **Smart Contract Migration**

- Move validator tracking, signature validation, and payouts on-chain
- Emit uptime data as on-chain events for transparency
- Add dispute resolution via DAO governance (e.g., in validator slashing)

3. **Advanced Threat Detection**

- Incorporate real-time DDoS pattern detection

4. **Multi-Chain Validator Support**

- Let validators sign on EVM, Solana, or L2s

5. **Mobile App for Site Owners**

- Push notification alerts (via wallet login)
- Graphs of uptime history and validator data

6. **SaaS Features for Devs**

- Custom webhook alerts
- White-label uptime dashboards
- Premium SLA reporting for DeFi/Web3 companies