ContractWatch – MVP Business Requirements Document

Document Version: 0.1
Author: ChatGPT (draft for Rameez Jhaveri & team)
Date: 5 July 2025

---

1. Executive Summary

ContractWatch is a SaaS monitoring platform that provides real-time visibility, alerts, and historical insight into every smart-contract deployment made by one or more wallet addresses across EVM-compatible chains. The MVP focuses on developers and small protocol teams who currently lack a centralized, automated way to track and audit their own (and their teammates') contract creations on testnets and mainnets.

---

2. Goals & Objectives

Goal	Objective	KPI (MVP)
Visibility	Display a chronological ledger of all contract deployments for a wallet across at least three networks	≥ 95 % of deployments appear in dashboard within 60 seconds
Alerting	Notify users instantly when a monitored wallet deploys a new contract	< 30 sec median alert latency
Auditability	Allow export of deployment history for compliance / code review	CSV / JSON export enabled
Ease of Adoption	Onboard a developer in < 2 minutes (wallet address + email)	Time-to-first-alert < 2 min

---

3. Problem Statement

Developers have no consolidated, chain-agnostic method to: 1. *Know immediately* when a contract has been deployed by themselves or a teammate. 2. *Trace* which implementation/proxy/admin contracts belong together. 3. *Prove* provenance during audits or post-mortems. Manual Etherscan checks are error-prone, single-chain, and have no push notifications.

---

4. Scope (MVP)

In-Scope

- **Chains:** Ethereum Mainnet, Sepolia testnet, Polygon PoS, and Arbitrum One.
- **Wallet Types:** Externally Owned Accounts (EOAs) only.
- **Detection Logic:** `CREATE` and `CREATE2` tx receipts; basic proxy-pattern fingerprinting (OZ transparent + UUPS).
- **UI:** Single-page web dashboard (React + Tailwind) with list & detail views.
- **Alerts:** Email + Discord Webhook (simple JSON payload).
- **Data Export:** CSV download of deployment list.

Out-of-Scope (Future)

- Non-EVM chains (Solana, Aptos, etc.).
- Deep implementation diffing or storage-layout checks.
- On-chain transaction simulation.
- Role-based access control beyond single-team owner.

---

5. Target Users & Personas

Persona	Needs	Pain Today
Indie Dev	Quick feedback loop; history of testnet experiments	Loses track of which address is the “real” contract
Small Protocol Team	Shared visibility; security alerts; audit trail	Unknown teammate deploys without review
Security Engineer	Detect rogue or compromised key events	Must build custom scripts / monitors

---

6. Functional Requirements (MVP)

1. **Wallet Registration**
   a. User submits one or more EVM addresses.
   b. System backfills last 5 000 blocks per network.
2. **Live Monitoring Service**
   a. Stream blocks via WebSocket / polling.
   b. Identify contract creations (`to == null` or opcode trace).
   c. Match against watched wallets.
3. **Dashboard**
   a. Table view: timestamp, network, contract address, gas used, tx hash.
   b. Detail drawer: constructor bytecode hash, proxy flag, verified source link.
4. **Alerts**
   a. Rules: new deployment event triggers email & webhook.
   b. Retry logic (3 attempts, exponential back-off).

5. **Export**
   a. CSV download of filtered deployment list.
6. **Authentication**
   Email/password + Magic-link (no wallet login needed for MVP).

---

7. Non-Functional Requirements

- **Performance:** < 1 min full-page load for 1 000 deployments.
- **Scalability:** Up to 10 000 tracked wallets and 1 M historic deployments.
- **Reliability:** 99 % uptime for alerting service.
- **Security:** Read-only chain data; store user email & hashed pwd only; follow OWASP Top 10.
- **Compliance:** GDPR (data deletion on request).

---

8. Assumptions

- Public RPC endpoints provide sufficient throughput for MVP volume.
- Users are comfortable pasting wallet addresses manually.
- No immediate need for multisig or hardware-wallet auth flow.

---

9. Success Metrics

Metric	Target
First 3 months active users	200 developers
Avg. alerts per wallet accuracy (false-negatives)	≤ 1 %
Dashboard DAU/MAU ratio	≥ 0.25
Conversion to paid (post-MVP)	10 % of active users

---

10. Risks & Mitigations

Risk	Impact	Mitigation
RPC rate limits	Missed deploy events	Use multiple providers; caching; rate-limit backoff
High email spam rates	Alert deliverability	DKIM/SPF setup; opt-in confirmation
Mis-classification of proxy vs impl	User confusion	Label with confidence score; allow manual override

---

11. Timeline (Indicative)

Phase	Duration	Milestone
Discovery & Design	2 weeks	Wireframes approved
Backend Core (scanning + alerts)	4 weeks	Chain scanner live on testnet
Frontend Dashboard	3 weeks	MVP UI in staging
Beta & Feedback	2 weeks	20 pilot users onboarded
Public MVP Launch	Week 11	Free tier live

---

12. Glossary

- **EOA:** Externally Owned Account (wallet address controlled by a private key).
- **Proxy (Transparent/OZ):** A delegating contract forwarding calls to an implementation.
- **CREATE2:** Opcode allowing deterministic contract addresses.
- **Deployment Ledger:** The historical list of contract creation events.

End of Document