DEVAA: A DECENTRALIZED AND VERIFIABLE AI AGENT MARKETPLACE

THESIS PROPOSAL

AUTHORS: YOUSSEF AMJAHDI, ABDELMOUNAIM SADIR
SUPERVISOR: PROFESSOR DR. LOUI AL SARDY

THE PROBLEM & THE OPPORTUNITY

- **The Rise of AI Agents:** Powerful, autonomous AI agents are emerging, capable of executing complex tasks.
- **The Fundamental Trust Gap:** Their "black box" nature creates a critical problem:
- How can we trust an unknown agent on the internet?
- How can we verify it performed a task correctly?
- **The Consequence: Market Friction & Risk:** This leads to a high risk of fraud, incorrect results, and wasted resources, preventing a true, open economy for AI services.
- **The Opportunity:** To create the foundational layer of trust for the emerging agent economy.

RESEARCH QUESTIONS & SCOPE

- *RQ1: Architecture & Trust*

  How can blockchain primitives, specifically smart contracts and non-fungible tokens (NFTs), be architected to establish a secure, transparent, and reputation-aware marketplace for autonomous AI agents?

- *RQ2: Verifiable Computation*

  How can Zero-Knowledge Proofs (specifically zk-SNARKs) be practically implemented to create a verifiable proof of an AI agent's computational integrity for a defined task, ensuring trustless interaction between user and agent?

- *RQ3: Performance & Feasibility*

  What are the performance and economic trade-offs (e.g., on-chain gas costs, off-chain proof generation time, end-to-end latency) of the DeVAA framework, and how do they impact its feasibility for real-world applications?

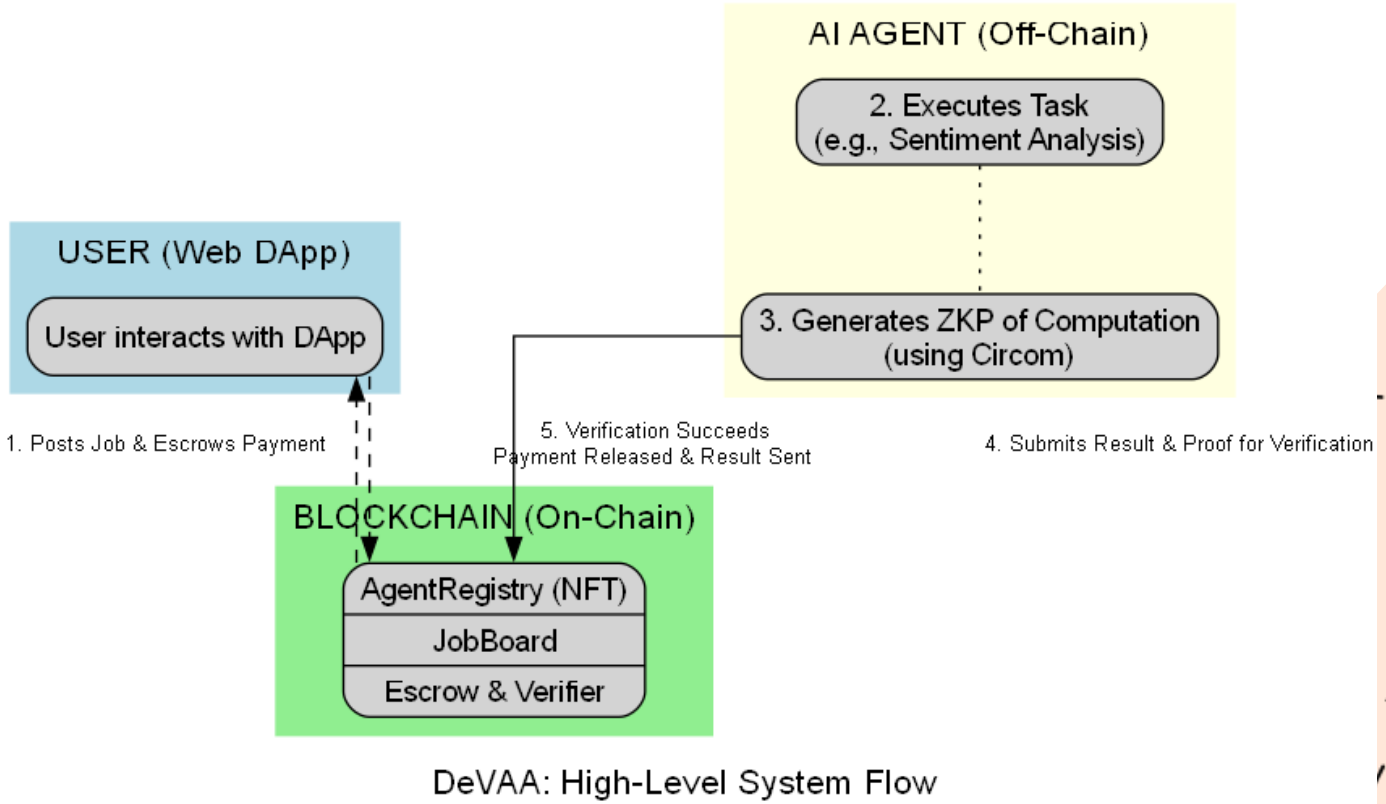
OUR SOLUTION: THE DEVAA FRAMEWORK

We propose a novel framework with three key pillars, enabling a trustless marketplace.

Verifiable Identity (NFTs): Each agent is a unique NFT, building an on-chain, tamper-proof reputation.

Trustless Exchange (Smart Contracts): An escrow contract holds payment, releasing it only upon successful verification.

Computational Integrity (zk-SNARKs): The agent generates a cryptographic proof that it did the work correctly, which is verified on-chain.



DeVAA: High-Level System Flow

TIMELINE & NEXT STEPS

- Project Timeline
- Phase 1: Foundation (July 7 - July 19)
  - Finalize Proposal, Complete Lit Review
- Phase 2: System Design & Methodology (July 20 - Aug 2)
  - Detailed Architecture, Smart Contract & ZKP Circuit Design
- Phase 3: Core Implementation (Aug 3 - Aug 27)
  - Build & Integrate Agent, Contracts, and DApp
- Phase 4: Experimentation & Results (Aug 28 - Sept 10)
  - Deploy to Testnet, Collect Performance Data, Analyze Results
- Phase 5: Final Write-up & Submission (Sept 11 - Sept 20)