DeQuant Agent: Secure, Verifiable, and Intelligent Quantitative Investing via TEE-based Autonomous Agent

Executive Overview

The world of investment is often bifurcated: exclusive, high-capital hedge funds on one end, and limited, low-yield retail options on the other. DeQuant is revolutionizing this landscape by providing a secure, AI-driven investment platform that offers immediate, verifiable trust through cutting-edge Trusted Execution Environments (TEEs) on the Phala Network.

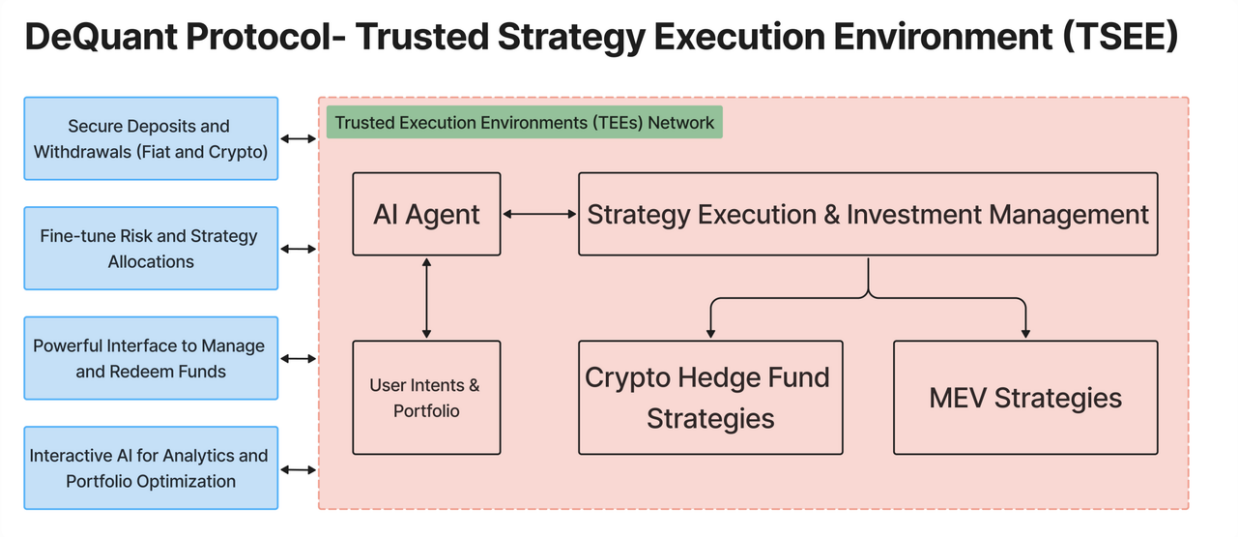
Our core product, accessible at **dequant.org**, introduces a novel user experience that seamlessly blends the intuitive nature of Graphical User Interfaces (GUIs) with the power of Conversational User Interfaces (CUIs). Investors interact with an AI-powered, autonomous agent via a chat interface on the left side of the screen. This interaction dynamically populates a strategy recommendation canvas on the right, offering personalized and transparent investment choices.

For quantitative funds, **dequant.org/quant-fund/claim** provides a dedicated platform. This interface aggregates investments from various users across a logged-in quant fund's strategies. Funds have the flexibility to claim returns at an individual strategy level or on an aggregated basis across all their deployed strategies.

The cornerstone of our platform is the autonomous agent, already developed and deployed on the Phala Network. The agent's operational integrity is ensured by its unmanipulatable database residing within a TEE. The RTMR3 hash of the Phala Confidential Virtual Machine (CVM) will be publicly available, making the agent's environment and its operations fully verifiable by anyone.

Further enhancing security and community trust, any code upgrades to the agent must be approved by the Dequant DAO. Additionally, strategies on the Dequant platform now feature a 'lock-in' field, which automatically governs withdrawals. These withdrawal schedules are unmanipulatable, providing a significant value add and peace of mind for investors.

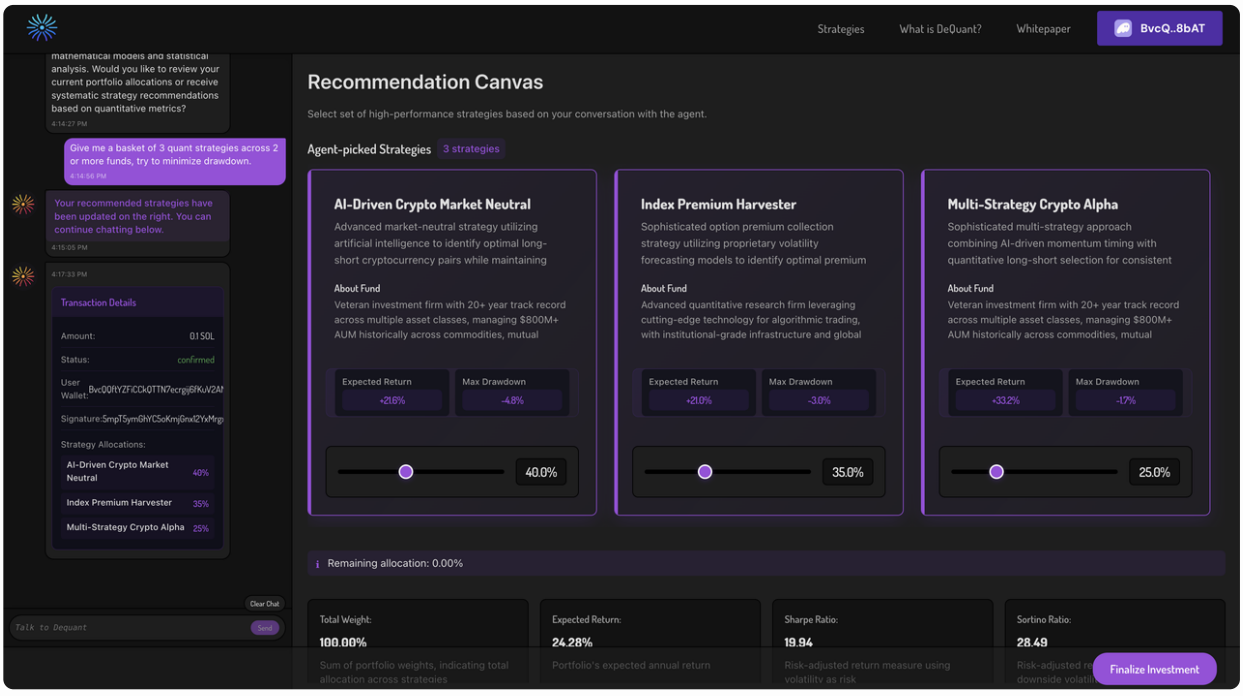
DeQuant is democratizing access to sophisticated, secure, and high-yield investing. It offers investors a single point of access to a diverse range of quantitative strategies from multiple funds, all backed by verifiable technology and community-driven governance, making portfolio diversification simpler and more powerful.



Section 1: The Dequant Platform - A New Paradigm in Quantitative Investing

DeQuant's innovation is built upon a unified platform designed for both investors and quantitative funds, leveraging a powerful autonomous agent and verifiable TEE technology.

1.1 The Investor Platform (dequant.org): Intelligent and Interactive Investing



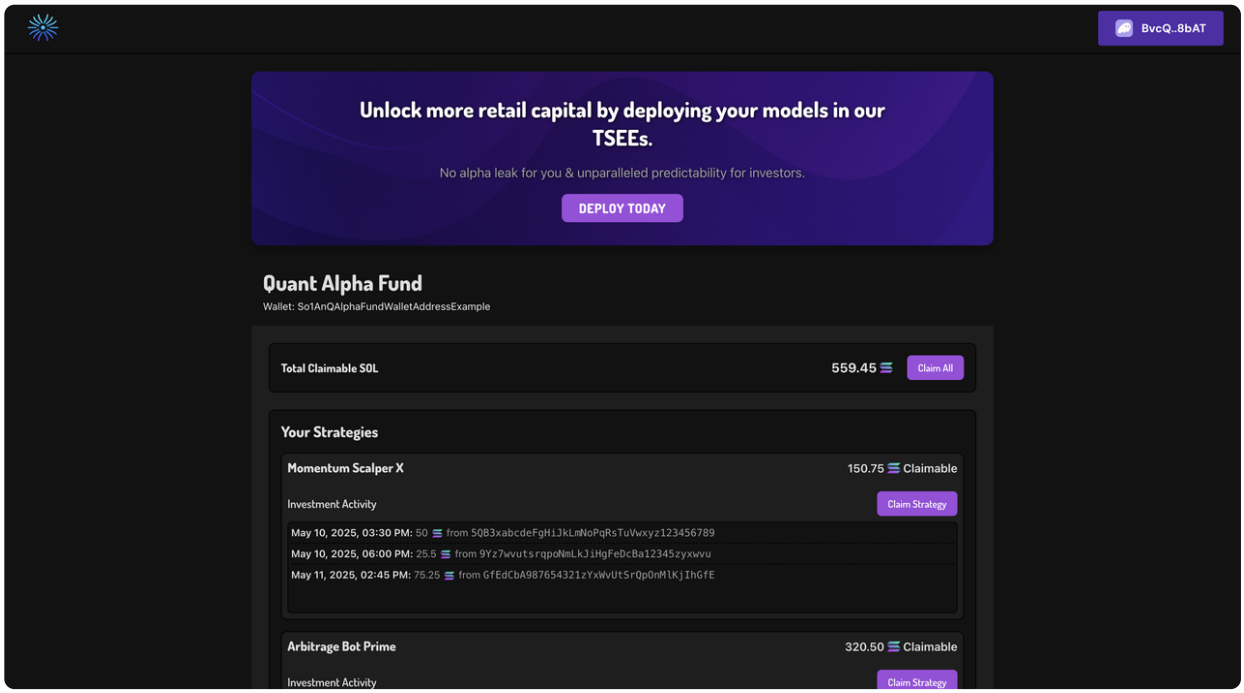
The primary investor-facing platform at dequant.org offers a unique and intuitive experience:

- **Agent-Driven Recommendations:** A sophisticated AI agent, accessible via a chat interface, guides investors. It understands their financial goals, risk appetite, and preferences. It is based on ElizaOS and has a massive RAG database with know-how on

quant research and on the specifics of the quant fund's past performance that forms the knowledge base for precise strategy recommendations.

- **Dynamic Strategy Canvas:** Based on the conversation with the agent, the right side of the screen populates with a curated selection of high-performance strategy recommendations. This visual canvas allows investors to easily compare and understand potential investments.
- **Seamless User Experience:** The blend of CUI (chat) and GUI (canvas) simplifies the complex world of quantitative investing, making it accessible even to those new to such strategies.
- **Multi-Fund Exposure:** Investors gain access to a curated selection of strategies from various vetted quantitative funds through a single, unified platform, simplifying diversification and discovery of unique investment opportunities.

1.2 The Quant Fund Platform (dequant.org/quant-fund/claim): Streamlined Management and Claims



For quantitative fund managers, Dequant provides a dedicated portal:

- **Aggregated Investment Overview:** Funds can view all user investments across their various strategies in a consolidated manner.
- **Flexible Claims Process:** The platform supports claiming returns at the individual strategy level or as an aggregated sum across all active strategies, providing operational flexibility.
- **Performance-based Capital Pipeline**: Platforms like Numerai require quants to stake their own NMR on models to earn yield, aligning incentives but limiting capital access.High-performing models can remain undercapitalized if their creators lack funds.

DeQuant solves this by using the agent's knowledge of each strategy's past performance and autonomously routing pooled capital to the best strategies. This ensures capital flows to merit, not wallets. DeQuant unlocks scalable, fair access for both quants and investors.

1.3 The Autonomous Agent: Deployed, Secure, and Verifiable

The intelligence behind Dequant is our autonomous agent, which is already live and operational:

- **Phala Network Deployment:** The agent is deployed on the Phala Network, leveraging its robust TEE capabilities.
- **Unmanipulatable TEE Database:** All critical operational data, including transaction records and strategy parameters, are stored in an unmanipulatable database within the TEE. This ensures data integrity and prevents tampering.
- **Verifiable Environment:** The RTMR3 hash of the Phala CVM where the agent operates will be made public. This allows anyone to verify the integrity and authenticity of the agent's execution environment.
- **Dequant DAO Governance:** To maintain transparency and security, all future code upgrades and significant changes to the agent's logic must be proposed to and approved by the Dequant DAO.

1.4 Strategy Lock-in & Unmanipulatable Withdrawals

A key feature enhancing investor protection and strategy stability:

- **Automated Withdrawal Governance:** Each strategy listed on the Dequant platform includes a 'lock-in' field. This field defines the terms and schedule for investor withdrawals.
- **Unmanipulatable Schedules:** Once set, these withdrawal schedules are enforced by the TEE and cannot be altered, providing investors with predictable and fair access to their funds according to the agreed terms. This eliminates ambiguity and potential for manipulation, a significant improvement over traditional investment vehicles.

Section 2: Trust, Transparency, and Security by Design

DeQuant's architecture is fundamentally built on providing unparalleled trust, transparency, and security to its users.

2.1 Verifiable Trust through Phala Network TEEs

Trusted Execution Environments (TEEs) are secure areas within a main processor, isolated from the main operating system and other applications. They provide confidentiality and integrity for code and data. Phala Network's Confidential Virtual Machines (CVMs) are an

advanced implementation of TEEs, specifically designed for blockchain and decentralized applications. They create a hardware-enforced isolated environment where computations can occur with strong assurances of privacy and tamper-resistance.

Our deployment on the Phala Network leverages these CVMs. This ensures:

- **Confidential Execution:** The Dequant agent's logic and, critically, the investor's interaction data and provisional portfolio decisions, run within this encrypted CVM. This means they are protected from unauthorized observation or interference, not only from external attackers but also from the node operators or even the underlying cloud infrastructure providers.
- **Integrity Assurance:** The TEE guarantees that the code being executed is exactly the code that was deployed and approved, and that its outputs are genuine. The public RTMR3 hash serves as a cryptographic proof of this.

2.2 Unmanipulatable Operations

- **Immutable Database:** The agent's database within the TEE ensures that records of investments, performance, and distributions cannot be tampered with.
- **Enforced Withdrawal Schedules:** The 'lock-in' feature and its associated withdrawal schedules are programmatically enforced by the TEE, making them unalterable and reliably executed.

2.3 Community-Driven Security via Dequant DAO

The Dequant DAO plays a crucial role in the long-term security and evolution of the platform:

- **Decentralized Governance:** Agent upgrades, changes to core platform parameters, and other significant decisions are subject to DAO voting.
- **Enhanced Security:** This distributed approval process prevents unilateral changes and ensures that modifications are vetted by the community, aligning the platform's development with user interests.

Section 3: Current Status and Future Enhancements

DeQuant has moved beyond conceptualization and early development phases into a live, operational state.

3.1 Current Deployment:

- **Live Investor Platform (dequant.org):** The AI agent and strategy recommendation canvas are operational, allowing users to explore and understand quantitative strategies.

- **Live Quant Fund Platform (dequant.org/quant-fund/claim):** The portal for quant funds to manage and claim aggregated investments is active.
- **Autonomous Agent on Phala Network:** The core agent is deployed and functioning within the Phala Network's TEE, with its database secured and environment verifiable.
- **Dequant DAO Framework:** The foundational elements for DAO governance are in place to oversee future agent upgrades.

3.2 Future Enhancements:
While the core platform is robust and operational, future development will focus on:

- **Expanding Strategy Offerings:** Continuously onboarding new, high-quality quantitative strategies from reputable funds and developers.
- **Deepening AI Capabilities:** Enhancing the AI agent's analytical power, personalization features, and market insights.
- **Broadening Asset Class Support:** Exploring the integration of additional asset classes beyond the initial focus.
- **Community Growth and DAO Empowerment:** Fostering a vibrant community and progressively increasing the scope of DAO governance.
- **Mobile Accessibility:** Developing mobile-first interfaces for enhanced user convenience.

3.3 Phase 2: Trusted Strategy Execution Environments (TSEEs) for Direct Execution
A significant evolution planned for Dequant is the introduction of Trusted Strategy Execution Environments (TSEEs) directly for quant fund strategy execution. This phase builds upon the secure capital aggregation of Phase 1 but takes trust and IP protection to a new level:

- **Direct TEE Execution:** Quant funds will be able to deploy their proprietary trading algorithms directly within a dedicated TSEE on the Dequant platform. Capital allocated by investors via the AI agent will flow through the established secure pipeline and be directly utilized by the strategy running in its own isolated TEE.
- **Automated Operations, No Manual Claiming:** This model eliminates the need for manual claiming of funds by the quant fund. Profit calculation, fee distribution, and reinvestment/payout logic can be automated within the TSEE, streamlining operations significantly.
- **Intellectual Property Protection:** The fund's strategy code and real-time trading activities are encrypted and isolated within the TSEE. This provides a powerful safeguard against IP theft or reverse engineering, a major concern for quantitative funds.
- **Preventing Undercutting and Front-Running:** A critical value proposition of TSEEs is the prevention of unfair practices. By executing within a private, verifiable TEE, funds are protected from scenarios where exchanges or other intermediaries might observe

their trading patterns and either front-run their trades or replicate their strategies to offer them at lower fees, thereby undercutting the original fund. Dequant's TSEE layer aims to create a truly fair and secure execution venue.

- **Secure Data Pipelines:** The TSEE will be equipped with secure and efficient data pipelines, allowing strategies to access necessary market data and execute trades without exposing sensitive information or logic outside the protected environment.

Section 4: Technology Architecture

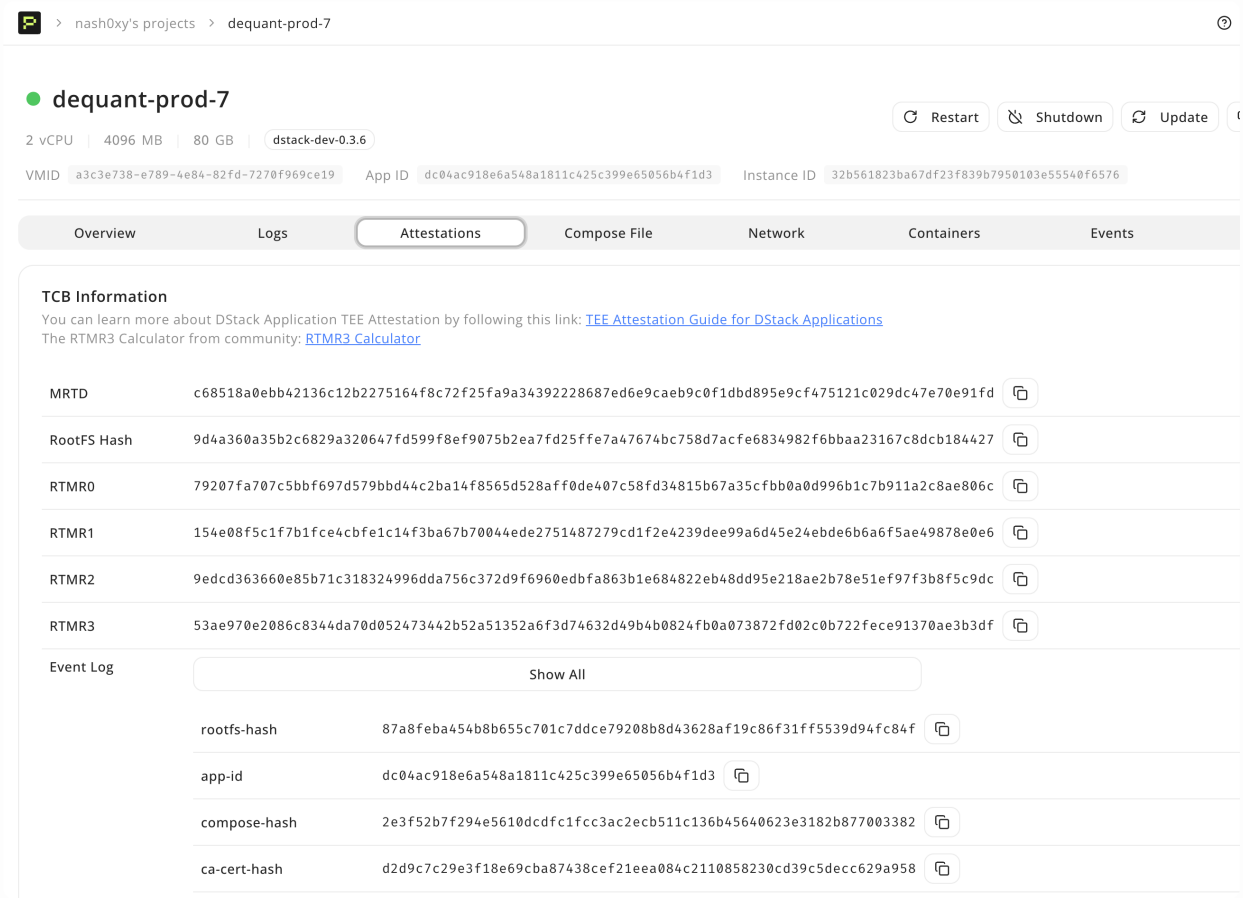
The DeQuant platform leverages a state-of-the-art technology stack centered around security, verifiability, and performance.

4.1 Phala Network Confidential Virtual Machine (CVM):

- **Core Trust Anchor:** The Phala CVM serves as the foundational trust anchor for the Dequant platform. The autonomous AI agent, responsible for investor interaction, strategy matching, and initial capital allocation logic, executes its critical functions entirely within a Phala CVM. This TEE provides hardware-level isolation, ensuring that the agent's operations are confidential and its integrity is maintained.
- **Enhanced Verifiability with RTMR3 Hash:** The Remote Attestation (RTMR) process, specifically the RTMR3 hash (or similar attestation measurement), provides a cryptographic fingerprint of the exact software (agent code, libraries, configuration) running within the CVM. By making this hash public, Dequant allows any third party to independently verify that the agent running is indeed the authorized and audited version, free from tampering or unauthorized modifications. This transparency is crucial for building investor confidence.

4.2 Unmanipulatable TEE Database:

- **Secure and Persistent Storage within TEE:** Critical data, such as investor commitments, strategy allocations, performance metrics, transaction logs, and withdrawal schedule parameters, are stored in a database that itself resides within or is strictly controlled by the TEE. This means that data at rest is encrypted and access to it is governed by the secure logic running within the TEE.
- **Integrity and Tamper-Resistance:** By being intrinsically linked to the TEE, the database inherits its security properties. This makes it highly resistant to unauthorized modifications, deletions, or insertions. Any attempt to tamper with the historical record or current state would be detectable or prevented by the TEE's integrity checks, ensuring a reliable audit trail and trustworthy data.



Verifiable TEE-based DeQuant Agent, deployed on Phala Network

4.3 Autonomous Agent:

- Developed with advanced AI and machine learning algorithms for strategy analysis, recommendation, and portfolio optimization.
- Interacts with the TEE database and executes strategy logic as defined.

4.4 Dequant DAO Smart Contracts:

- Govern the process for proposing, vetting, and approving code upgrades to the autonomous agent.
- Ensures decentralized control over critical platform components.

4.5 User and Quant Fund Interfaces:

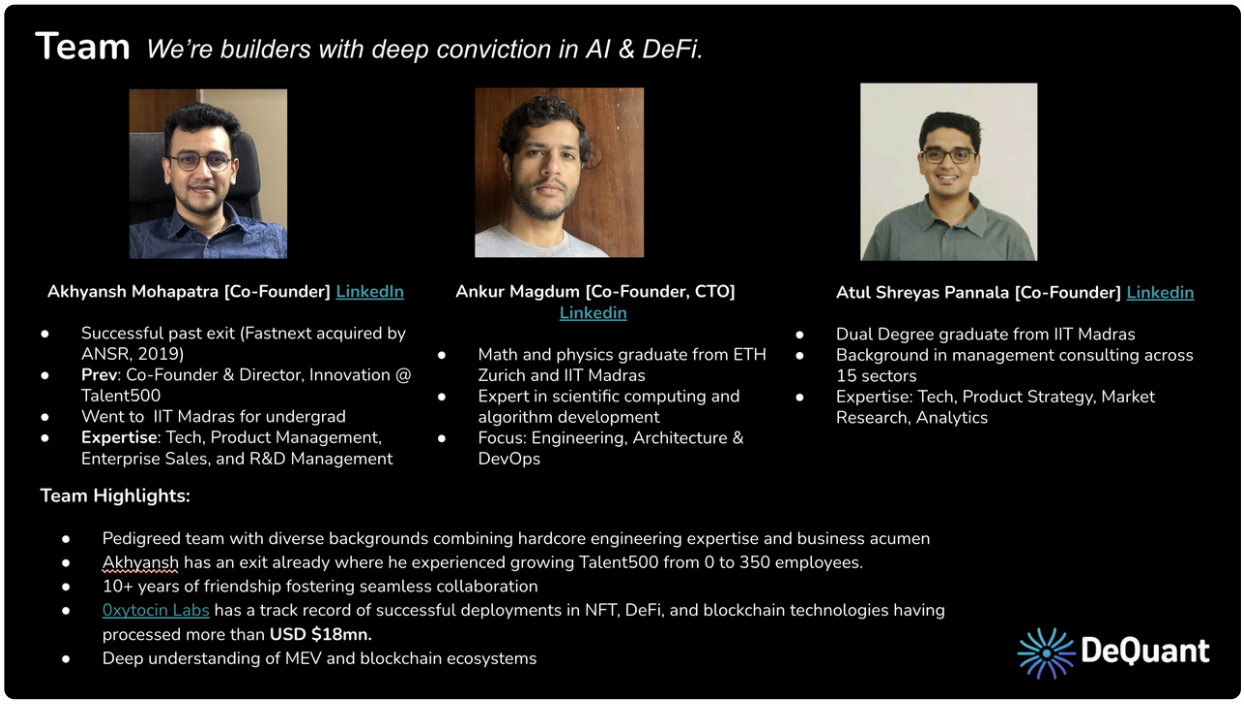
- Web platforms (dequant.org and dequant.org/quant-fund/claim) built with modern frameworks for a responsive and intuitive user experience.
- Secure API integrations for data flow between the front-end, the agent, and the TEE.

4.6 Future: Trusted Strategy Execution Environment (TSEE) Layer (Phase 2 Architecture)

The introduction of TSEEs for direct strategy execution will add another sophisticated layer to our architecture:

- **Dedicated Strategy Enclaves:** Each quant fund's strategy will operate within its own isolated TSEE instance. This ensures no cross-contamination or interference between different strategies.
- **Secure Data Feeds and Execution APIs:** The TSEE layer will incorporate hardened interfaces for secure ingestion of real-time market data and for routing trade execution orders to exchanges or liquidity venues. These interfaces will be designed to prevent data leakage and ensure that strategy logic remains confidential.
- **Attested Co-location of Code and Data:** The TSEE ensures that the fund's proprietary algorithms are executed directly alongside the data they need, all within a verifiable, confidential environment.
- **Automated Accounting and Distribution Modules:** Smart contracts or secure off-chain logic within the TSEE will handle the complex calculations for profit sharing, fee deductions, and distribution of returns to investors, further automating and securing the process.

Section 5: Team Expertise



Built at 0xytocin Labs, our founding team combines deep expertise in blockchain technology, quantitative trading, AI, and security architecture:

- **Ankur Magdum(LinkedIn):** Math and physics graduate from ETH Zurich and IIT Madras, expert in scientific computing and algorithm development.
- **Atul Shreyas Pannala(LinkedIn):** Engineering Design @ IIT Madras with extensive consulting experience across 15 sectors.

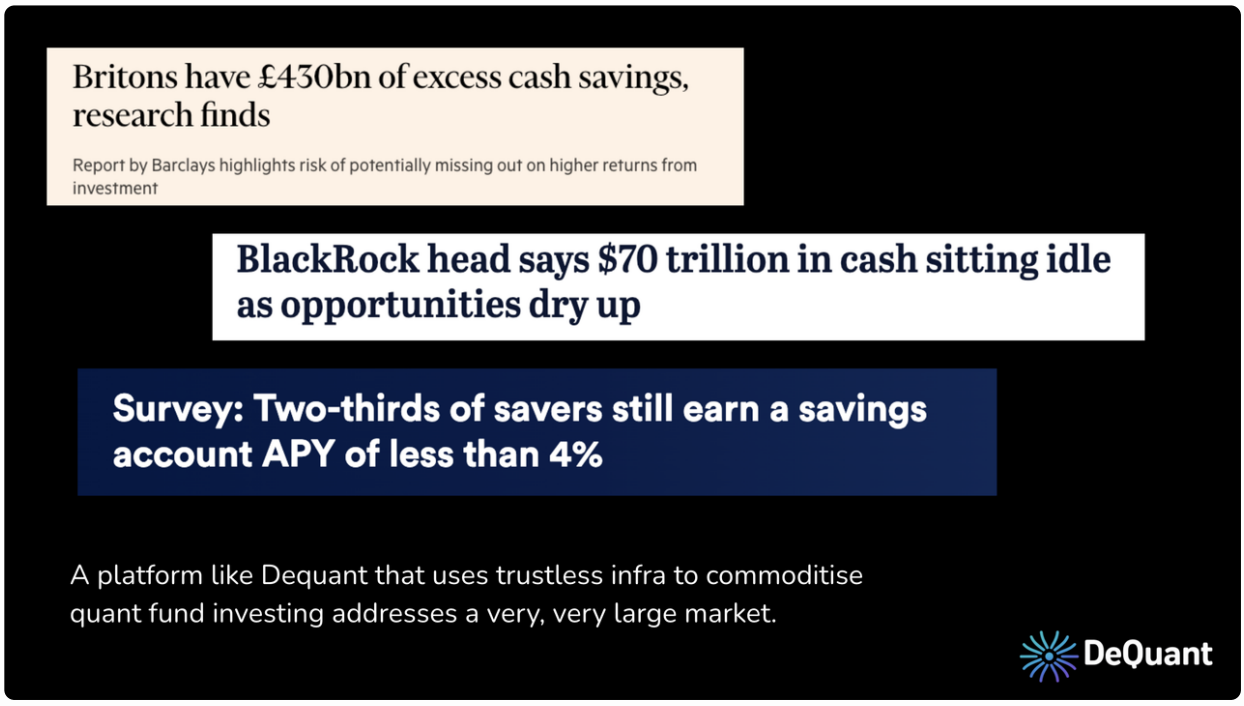
- **Akhyansh Mohapatra(LinkedIn):** Aerospace Engineering @ IIT Madras with a previous successful AI exit (Fastnext acquisition).

Our collective experience includes:

- Implementing bottom-of-block arbitrage using Intel TDX trusted execution environments.
- Developing and deploying proven atomic and CEX/DEX arbitrage strategies.
- Deep expertise in blockchain technology, TEEs, and secure system design.
- A track record of successful technology ventures and deployments.

Section 6: Market Opportunity & Revised Revenue Model

DeQuant addresses a significant gap in the investment market by making sophisticated quantitative strategies accessible and secure for a broader audience, while providing a streamlined platform for quant funds.



6.1 Market Opportunity:

With the right support, reach and quant fund partners, DeQuant could scale into 100s of billions in AUM by tapping into and managing the savings of millions of retail investors.

- **Retail Investors:** Tapping into the vast market of retail investors seeking higher yields and more sophisticated investment options than typically available.
- **Quantitative Funds:** Providing a platform for quant funds to reach a wider investor base, manage aggregated capital efficiently, and operate with enhanced trust.

6.2 Revenue Model:

DeQuant's revenue model is designed for sustainability and alignment with user success:

- **Platform Fees:** A transparent management fee on assets under management (AUM) processed through the platform.
- **Performance Fees:** A percentage of the profits generated by the strategies, ensuring Dequant's incentives are aligned with investor returns.
- **Future Value-Added Services:** Potential for future revenue streams through premium features, advanced analytics, or specialized strategy offerings.

By focusing on a live, verifiable, and secure platform, DeQuant is poised to capture a significant share of the evolving quantitative investment market.

At the point of drafting this whitepaper, we have struck key partnerships with hedge funds like Algoedge, that have a highly experienced quant team and have been running strategies atop millions of dollars for about a decade.

Contact: ak@0xytocin.com