The Fizk Protocol
White Paper

Mina’s Native Algorithmic Stablecoin

GitHub

March 2025

Abstract

The Fizk Protocol introduces zkUSD, a trust-minimised collateral backed algorithmic stablecoin into the Mina ecosystem.

Mina's long term vision paints a picture of a truly decentralised future. By facilitating off-chain computation through the use of zero-knowledge(zk) proofs, Mina acts as a settlement layer significantly reducing the barrier of participation in network security. In mid 2024 this capability was extended to enable zkApps, a form of smart contract that governs the rules of an application through compiled zk circuits.[1] zkApps mark a paradigm shift within the Mina ecosystem providing new possibilities and a new way of thinking around web3 applications.

Despite Mina's groundbreaking architecture, its design has largely isolated the ecosystem from broader DeFi activity. Its native currency, MINA, has mainly been used for passive staking, with no meaningful way to use it beyond securing the network. Fizk unlocks this potential to serve as the bedrock for a new DeFi ecosystem on Mina.

With zkUSD, Mina transitions from a passive staking network to an active financial layer. This innovation sets the stage for a thriving DeFi ecosystem and as adoption grows, zkUSD will become the catalyst that transforms Mina into a vibrant and self-sustaining financial hub, all while preserving its core principles of low-cost network security and decentralisation.

Introduction - The Mina Landscape

The Mina Protocol embodies a vision of greater decentralisation by dramatically lowering barriers to participation. At its core lies a powerful concept: a lightweight blockchain where the entire network state can be verified instantly, even on a simple smartphone. Unlike traditional blockchains, which often require substantial resources and specialized infrastructure, Mina compresses its blockchain into a succinct cryptographic proof roughly the size of a few kilobytes.[2] With approximately 7 billion smartphones globally, Mina opens the door for widespread user participation, significantly enhancing network security, resilience, and the growth of network effects.

In contrast to traditional blockchains such as Ethereum and Solana, which rely on resource-intensive consensus mechanisms where every node must execute all transactions, Mina leverages zk-SNARKs technology, shifting transaction computation off-chain. Smart contracts on Mina are compiled into succinct zk circuits, and state transitions are executed locally by users who submit pre-authorised state updates on-chain. This unique approach makes Mina universally inclusive, allowing verification even from mobile devices. Furthermore, while complex smart contract interactions can be prohibitively expensive on traditional smart contract chains that use Gas, Mina's model means that each transaction costs the same flat fee as all the computation is off-chain.

However, Mina's unique architecture introduces several distinct technical challenges that developers must navigate when building zkApps. As all smart contract logic must compile down into zk circuits, developers face limitations such as constrained state sizes, limited transaction throughput, and restrictions on dynamic programming constructs (such as conditional branching or dynamic loops). Additionally, Mina's transaction model requires careful handling of state interactions to avoid concurrency issues, meaning developers must employ creative strategies and new design patterns. While these constraints initially complicate development, they also provide opportunities for innovation, enabling Mina to support complex, privacy-preserving, and scalable applications previously unattainable in traditional blockchain environments.

The Problem Space

The Need for a Native Stablecoin on Mina

Stablecoins are an indispensable component of any mature DeFi ecosystem, serving as the backbone for lending, borrowing, trading, and yield-generation activities. Stablecoins represent about a third of all daily crypto usage and provide crucial stability amidst the volatility inherent in cryptocurrencies, facilitating predictable transactions, risk management, and broader adoption among both individual users and institutional entities.[6]

Mina specifically requires a native stablecoin, distinct from existing stablecoins bridged from other blockchains, for several reasons:

1. **Alignment with Mina's Vision:** By developing and deploying its native stablecoin, Mina remains true to its unique ethos of decentralization, socialized verification, and off-chain computation. Relying solely on external bridged tokens like USDC or USDT would indirectly tether Mina's financial ecosystem to external networks, diluting Mina's core value proposition and ceding control of its economic sovereignty.
2. **Demonstrating Mina's Independence and Capability:** Launching a native stablecoin positions Mina prominently among leading blockchains, demonstrating its capacity to host sophisticated financial infrastructure independently. Rather than being dependent on other chains, Mina showcases its innovative technology stack, fostering greater developer interest, user adoption, and long-term ecosystem growth.
3. **Leveraging Mina's Unique Staking Model:** Mina's delegated staking mechanism uniquely positions it to create novel financial products, such as negative interest rate loans, a distinct competitive advantage in DeFi. Collateral deposits can be passively staked to earn protocol-level rewards, providing economic incentives unavailable in traditional stablecoin systems, and thereby enhancing capital efficiency.
4. **Optimising Mina's Liquidity and Ecosystem Growth:** A native stablecoin collateralized by MINA tokens directly enhances liquidity and incentivizes holders to actively participate in the ecosystem rather than merely holding assets passively.

Deploying a native stablecoin ensures Mina’s autonomy, enhances its competitive positioning, and amplifies the unique economic benefits offered by Mina’s validation model. Evident from its first year of existence, market sentiment and investor appetite was significant for MINA. The innovative nature of Mina’s zk architecture has required extensive development to reach our current inflection point. This has led to delays in the project that eroded investor confidence, causing MINA to underperform. As we begin to transition to this new phase with the introduction of zkUSD. Mina is poised to deliver on its promises, reigniting interest among investors, users, developers and the broader market as a whole.

zkUSD: Protocol Overview

The Fizk Protocol introduces zkUSD, a decentralised, algorithmic stablecoin fully collateralised by MINA. zkUSD maintains its peg to the US dollar through algorithmically enforced collateralisation, transparent governance, and a decentralised oracle network secured by off-chain zk proofs.

Protocol Mechanics

Collateralised Debt Positions (Vaults)

The core functionality of zkUSD centres around Collateralised Debt Positions (CDPs), referred to as vaults within the protocol. Vaults are managed on-chain through dedicated token accounts controlled by the zkUSD Engine contract, ensuring secure and isolated management of user funds.

Each vault maintains two essential balances:

- **Collateral Balance (MINA):** Represents MINA tokens deposited by the user.
- **Debt Balance (zkUSD):** Represents the amount of zkUSD minted against the collateral.

The collateralisation ratio defines the minimum amount of collateral required for a given amount of zkUSD minted. At launch, Fizk sets this collateralisation ratio conservatively at 150%, balancing safety with capital efficiency given Mina's current network performance constraints.

Collateralisation Ratio

The collateralisation ratio (CR) measures the proportion between collateral value and outstanding debt:

$$CR = \frac{\text{Collateral Value (USD)}}{\text{Debt (zkUSD)}} \times 100$$

To maintain solvency, vaults must keep $CR \geq 150\%$

Health Factor

The protocol tracks the financial safety of each vault through a Health Factor (HF), defined as:

$$HF = \frac{\text{Max Allowed Debt (USD)}}{\text{Debt (zkUSD)}} \times 100$$

A Health Factor over 100 is deemed safe and over-collateralised. A Health Factor under 100 is under-collateralised and eligible for liquidation.

Liquidations

Vaults whose Health Factor falls below 100 become eligible for liquidation by external participants, incentivised through economic rewards. Liquidators purchase the locked collateral inside a vault, paying the debt on the vault owners behalf. To reward the liquidator for their trouble, they receive an additional 10% (adjustable by governance) of the collateral from the vault.

Any remaining collateral after liquidation is returned to the original vault owner. Initially, Fizk Protocol allows only full liquidations due to Mina's throughput limitations, recognising the scarcity of bandwidth in the event of extreme market conditions. Governance retains authority to transition to partial liquidations as Mina's network performance improves.

Decentralised Oracle & zk-Proof Price Feed

Accurate price feeds underpin zkUSD's stability. Fizk employs a decentralised oracle mechanism leveraging off-chain zk proofs to securely deliver verified price data:

- **Oracle Submissions:** Trusted oracles, selected via governance, expose signed price data off-chain.
- **zk Aggregation:** Users interacting with vaults generate a zk proof aggregating oracle inputs, validating the price, and calculating a median MINA/USD price. This proof is then verified by the zkUSD Engine contract.
- **Price Validity:** Price proofs remain valid for approximately two Mina blocks (~6 minutes), balancing timeliness and practical latency. This can be adjusted by governance.

Risk Management & Reserve Fund

Fizk incorporates a risk management framework to safeguard protocol solvency through two main mechanisms:

- **Reserve Fund:** The protocol maintains a reserve fund capitalised by staking revenues generated from deposited collateral. The initial target size of this reserve is set to 10% of total outstanding debt, adjustable by governance.
- **Reserve Activation:** In catastrophic market downturns where liquidations outpace Mina's throughput, the reserve fund intervenes to purchase and liquidate insolvent vaults, eliminating accrued bad debt.

Should the reserve fund become depleted, the protocol employs a final safeguard. As a last resort, Fizk governance tokens will be minted and sold to acquire zkUSD from the market, buying and clearing bad debt. This mechanism directly aligns governance incentives with responsible risk management, as governance token holders bear potential dilution consequences.

Governance & Protocol Upgradability

The Fizk Protocol is designed for progressive decentralisation, with governance initially residing in a multisig structure controlled by the founding team. Gradually, governance responsibilities—including adjustments to collateralisation ratios, liquidation incentives, debt ceilings, oracle whitelists, and emergency protocol actions—will transition fully to a DAO driven by Fizk governance token holders.

Governance also oversees protocol upgradability through protocol contract verification key mutability, allowing ongoing innovation, security enhancements, and adoption of new economic strategies over time.

Protocol Contract Architecture

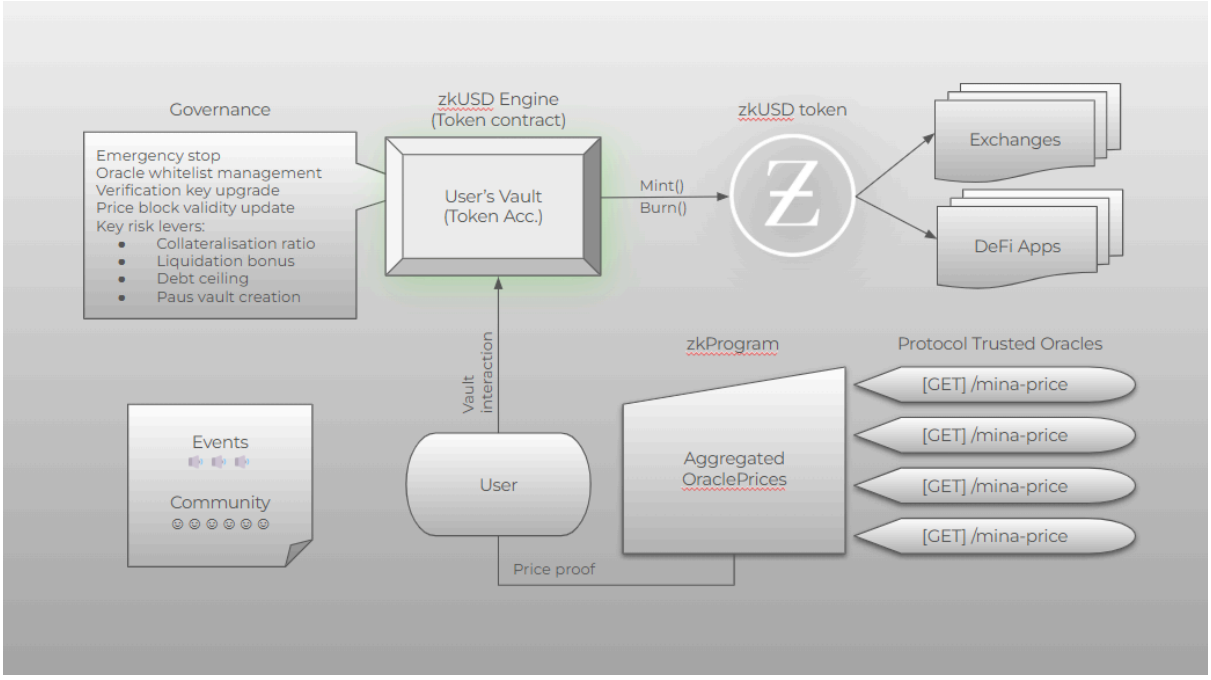

Figure 0.1: Fizk contract architecture

Fizk is structured around a primary smart contract called the zkUSD Engine. The engine serves as the central hub managing all core protocol functionality. It oversees vault management, collateral handling, debt issuance, liquidations, and key administrative functionality, such as governance and oracle management.

When a user creates a new vault, the zkUSD Engine deploys an individual Mina blockchain account to represent and securely track each vault. These vaults are implemented as specialised token accounts, derived from the zkUSD Engine's unique token ID. This architecture ensures that each user's vault is independently and securely tracked on-chain, while centralised logic within the zkUSD Engine controls interactions. By using individual token accounts for each vault, the protocol can handle concurrent user interactions despite Mina's constraints around concurrent state updates. Importantly, the zkUSD Engine contract is also the administrative contract for the zkUSD token itself. It directly manages the minting and burning of zkUSD tokens, altering token supply dynamically with user interactions and overall system debt. This integrated approach significantly optimises transaction efficiency on Mina's Layer 1, enabling all protocol actions to remain within the account update limit.

Decentralised Accessibility

Mina’s approach to off-chain computation introduces unique considerations around decentralised accessibility. Unlike traditional blockchains, Mina requires users to generate zk proofs off-chain, validating their transactions against the exact verification keys originally deployed to the network. Consequently, the smart contract code must remain permanently accessible in a decentralised manner. If such critical components become unavailable, due to reliance on a centralised server or single-point storage, the system may become unusable.

To mitigate these risks, the Fizk Protocol will proactively leverage decentralised storage solutions, such as IPFS. By distributing key protocol resources, such as smart contract code, zk proof circuits, oracle endpoints, and essential governance data across IPFS, the protocol achieves high resilience and availability. This decentralised architecture eliminates single points of failure, ensuring users can reliably generate transaction proofs, access up-to-date price data, and engage in protocol governance without interruption or centralised dependencies.

By embedding decentralised accessibility into its fundamental design, the Fizk Protocol guarantees fault-tolerant interactions for all users.

How Fizk Solves Mina's Development Challenges

O1js zkApps

Challenge

Developing smart contracts with Mina's zkApp framework via o1js introduces unique programming challenges compared to traditional smart contract platforms. A primary constraint faced by developers is that all contract code must be expressed in terms that can be compiled into a zk circuit. This requirement means typical control-flow constructs common in other programming environments—such as conditional branching based on dynamic variables (`if/else` statements) or traditional looping structures (`for, while` loops)—cannot be directly implemented unless fully bounded or unrolled at compile-time.

This limitation significantly influences development, requiring developers to rethink traditional logic flows and instead rely heavily on deterministic, provable computations. Dynamic execution paths must be redesigned into explicitly constrained circuits.

Solution

Fizk addresses these constraints through deliberate and careful design. Fizk application logic explicitly structures computations as deterministic operations, avoiding traditional branching and dynamic loops. Financial calculations and protocol interactions—such as collateralisation, debt management, and oracle price aggregation—are meticulously defined within Mina's constraints, using bounded logic and provable arithmetic patterns. An example of this can be found in how Fizk calculates aggregate median prices from protocol oracles. Fizk is limited to a bound number of oracle submissions and must calculate the median price for every possible outcome as it traverses the submissions.[4]

State Size Constraints

Challenge

Mina imposes strict limitations on the amount of state a zkApp can use. Currently this is limited to eight separate Field elements, Mina's fundamental data type.[5] This design choice further facilitates Mina's off-chain model, by intending most state to be managed on off-chain Merkle trees with roots stored on-chain.

Solution

Fizk employs data-packing techniques to store multiple protocol parameters within a single state field. Fields contain 255 bits, providing sufficient space to efficiently combine multiple smaller parameters. Fizk encapsulates these packed parameters into structured data types, enabling manipulation within contract code. Fizk packs critical protocol parameters such as the emergency flag, collateralisation ratio, and oracle price validity intervals into single fields, significantly optimising on-chain state.

For more extensive future state requirements, such as zk program verification keys for Fizk's governing layer, Fizk will store state within off-chain Merkle trees hosted securely on IPFS, or use upcoming mutable state solutions such as Project Untitled.[6]

This approach allows virtually unlimited state to be securely managed off-chain while ensuring full provability and verification on-chain.

Atomic Transactions and Account Updates

Challenge

Transactions on Mina consist of "account updates," which represent changes to the state of either externally owned accounts (EOAs) or zkApp accounts (smart contract accounts). Unlike other blockchains that directly execute contract logic on-chain, Mina requires users to perform computations off-chain, generating zk proofs to confirm the validity of state transitions. These proofs are then submitted to the network in the form of account updates. Each account update encapsulates three key components: the new intended state, the preconditions defining the state conditions required for the update to be accepted, and authorization provided either via cryptographic proof or signature.[4] Due to the computational overhead involved in verifying these updates, Mina currently imposes a strict limit of approximately seven account updates per atomic transaction.[5]

Solution

To overcome Mina’s account update limits, Fizk has designed its protocol architecture around the zkUSD Engine contract. By consolidating as much protocol logic as possible into this central contract, Fizk significantly reduces the number of account updates required per transaction. Specifically, the zkUSD Engine acts simultaneously as the token administrator for the zkUSD stablecoin and as a token owner itself for protocol-wide vault state management. This dual-role architecture ensures that minting, burning, collateral management, and vault interactions occur within unified transactions, carefully structured to satisfy all necessary preconditions within the constrained account update limit. The result is a highly efficient, carefully designed system capable of managing complex interactions within Mina's unique constraints.

Concurrent State Interactions

Challenge

As each transaction specifies preconditions that must precisely match the current on-chain state, concurrent updates to the same state item cannot occur within a single block. If two or more transactions attempt to modify the same state simultaneously, only the first transaction processed by the block producer will succeed, rendering subsequent conflicting transactions invalid. This sequential state update requirement imposes significant design challenges for multi-user applications.

Solution

Fizk resolves concurrency constraints by leveraging individual Mina token accounts dedicated to each user vault, which are owned and managed exclusively by the zkUSD Engine contract. Each vault state is encapsulated within carefully defined Vault Structs, explicitly controlling all state transitions and preconditions at the account level. By routing all interactions through the Engine contract’s central logic—and by explicitly managing permissions via the contract’s `approveBase()` function—Fizk securely restricts users from making unauthorised state updates. This design ensures state integrity and effectively circumvents Mina’s concurrent transaction limitations, enabling reliable, concurrent multi-user interactions within the Fizk Protocol.

Progressive Decentralisation

The Fizk Protocol embraces a model of progressive decentralisation, beginning with centralised yet transparent governance, as it moves towards a fully decentralised and community-driven structure. Transitioning to decentralisation is not straightforward and requires addressing carefully several critical technical and operational considerations. Fizk is committed to navigating these challenges thoughtfully, ensuring robust decentralisation that aligns with Mina's vision.

Verification Key Upgradeability

Mina's zkApps rely on verification keys deployed directly on accounts, controlling upgradability. After protocol hardforks that modify the proving system, Mina resets verification key permissions to "signature," temporarily centralising control and introducing trust assumptions. This means the smart contract's original deployer gains sole authority to upgrade the contract code through a signature. Fizk recognises this as a critical decentralisation challenge.

To mitigate this centralisation risk, Fizk is actively monitoring and preparing to leverage ongoing efforts from o(1) Labs, who are developing native multisig functionality that can be utilised for deploying zkApps. Once available, Fizk intends to implement multisig-controlled deployment, distributing upgrade authority among multiple governing parties to ensure transparency and community alignment.

Decentralised Management of Staking Rewards

In Mina's staking model, node-generated staking rewards typically reside under the direct control of the node operator, requiring manual distribution. By deploying a zkApp directly to Fizk's validator account, the protocol can utilise off-chain zk proofs to enforce rules governing the distribution of staking rewards. Under this approach, only participants who provide valid zk proofs will be able to claim their proportional share of rewards, automating and decentralising this critical financial operation.

Designing the Fizk DAO

A significant component of Fizk's decentralisation roadmap is developing a DAO tailored to Mina’s zk-based environment. Currently, no standard DAO framework exists within Mina’s ecosystem, meaning Fizk will need to pioneer the implementation of an off-chain DAO structure that seamlessly interacts with on-chain governance.

Fizk plans to use an off-chain voting system secured by recursive zk proofs and Merkle trees. Changes to protocol parameters or upgrades to verification keys will first be proposed off-chain. Token balances and public keys will be snapshotted off-chain, enabling token holders to vote privately. If a vote achieves quorum, a zk proof validating the vote will be submitted to the protocol’s governance layer. Once verified against the proof’s verification key, the approved parameter change or upgrade will be enacted on-chain.

A Path Forward

Although achieving true decentralisation introduces technical and operational complexities, Fizk is committed to leading the Mina ecosystem in pioneering effective decentralisation strategies. Fizk will continue innovating, designing, and openly sharing solutions with the broader community as it carefully transitions towards full decentralisation, enhancing transparency and trust for all participants.

Protocol Economics

Revenue

Mina employs a Proof-of-Stake (PoS) consensus mechanism, where validators secure the network by staking MINA tokens. Validators are randomly selected to produce blocks and, in exchange, earn block rewards funded by inflationary issuance of new Mina tokens and transaction fees.[8]

Participation in staking is accessible to all Mina holders through delegation, requiring no lock-up period or penalties for changing or withdrawing delegation. Rewards are distributed based on the proportion of a user's stake relative to the total stake delegated to the validator node. The initial annual inflation rate of Mina was set at 12% for the first two years after launch, with subsequent reductions of 1% every six months until stabilising at 7% by late 2025.[9] With approximately 99% of total Mina currently staked, users can realistically expect annual returns around 8%, depending on the specific validator's commission rates.[10]

An important detail is the latency associated with staking rewards. Due to Mina's consensus design, there is typically a 2-4 week delay between delegating stake and starting to earn rewards.[11] Moreover, staking reward calculations and distributions are managed off-chain by the validators, requiring delegators to place trust in the validators' accuracy and fairness.

The Fizk Protocol will generate consistent revenue by operating its own validator node, delegating the collateral deposited into its engine contract as stake.

The revenue will be allocated into three distinct streams:

- **33%** will be returned to users through negative interest rates on their loans, offering a competitive and unique incentive to liquidity providers.
- **33%** will be allocated directly to the protocol treasury, funding ongoing development, future innovations, and operational sustainability.
- **34%** will be dedicated to a reserve fund, ensuring long-term financial security and protocol stability.

Negative Interest Rate Debt Issuance

By depositing Mina into the Fizk Protocol, users temporarily forgo direct staking rewards. To compensate for this opportunity cost and incentivise liquidity provision, the Fizk Protocol introduces negative interest rate loans—effectively paying users for borrowing against their deposited collateral. In practice, this can be achieved by deploying a zkApp directly to the validator account, securing the account permissions, and enabling users to claim accrued staking rewards independently and securely. This approach not only incentivises liquidity providers but also enhances decentralisation by removing trust requirements typically associated with reward distribution.

The implementation of negative interest rates provides several key benefits:

- **Attractiveness of Liquidity:** Offering negative interest rates positions the Fizk Protocol as an exceptionally competitive platform in DeFi, creating a compelling economic incentive for users to provide liquidity. Users effectively earn returns simply by borrowing, increasing the attractiveness and retention of liquidity within the protocol.
- **Increased Capital Efficiency:** Users benefit doubly by accessing debt through zkUSD issuance at favourable negative interest rates. They can deploy this newly minted liquidity for additional investment opportunities within the broader Mina ecosystem or externally via token bridges, maximising their capital utility.
- **Competitive advantage:** Negative interest loans differentiate the Fizk Protocol from traditional DeFi platforms, leveraging Mina's unique staking model and capitalising on its distinct proof-of-stake incentives.

Protocol Treasury

The Fizk Protocol Treasury will serve as a dedicated fund supporting the ongoing growth and development of the Fizk ecosystem. As the funds flow from staking revenue directly linked to the TVL of the protocol, the treasury will have a predictable and reliable funding source.

Specifically, the Protocol Treasury will directly support the continuous development of the protocol, including development initiatives, grants and community driven innovations. Additionally the treasury will also be responsible for operational sustainability, and governance incentives. Ensuring that all regulatory and legal requirements are met and that the protocol relies on active and engaged governance participation.

Fizk Reserve Fund

To support the stability and increase the security of zkUSD, the Fizk Protocol will build and maintain a dedicated Reserve Fund. From its inception, a portion of the protocol's staking revenues will be allocated to this fund until it reaches a predefined percentage of the total outstanding debt in the system. This target percentage will be determined transparently through protocol governance, allowing stakeholders to collectively manage risk exposure.

The purpose of the Reserve Fund is to act as a safeguard against severe market volatility. In the event of a rapid and substantial price drop that causes vaults to become insolvent, the Reserve Fund will step in and liquidate the bad debt that has accrued to mitigate systemic risk. This proactive measure provides significant assurance to users and investors, ensuring confidence and resilience even under extreme market conditions.

The Reserve Fund will be managed transparently through a zkApp, with clear visibility and accountability to protocol stakeholders. Once the reserve reaches its governance-defined target level, surplus funds can be reallocated through governance consensus, either directly distributed back to protocol participants as incentives, by employing excess reserve revenue as a buy-back mechanism for the governance token. By using surplus reserve funds to purchase governance tokens from the market and to burn, the protocol aligns incentives strongly among governance participants, as reducing token supply can support strong token price action which encourages prudent governance and risk management decisions.

Tokenomics

The Fizk Protocol is currently in the early stages of development. At this point, the full details of the protocol's tokenomics remain intentionally speculative, as designing effective token incentives and governance requires careful, deliberate planning and must evolve together with the protocol itself. However, it is important to communicate motivations and guiding principles as the protocol moves forward.

Purpose and Utility of the Fizk Token

The primary role envisioned for the Fizk Token is a vehicle for governance. The exact governance structure—such as delegated voting, representative councils, or direct democracy—will be determined through community engagement and rigorous research. The end goal is to maximise decentralisation without overly compromising on operational efficiency. Beyond governance, the Fizk Token serves two main functions.

Lender of the Last Resort

In the unlikely scenario of a black swan event causing systemic risk, where outstanding debt exceeds the reserve fund. The Fizk Protocol would mint new tokens and sell them to acquire zkUSD and eliminate bad debt. While this mechanism acts as a final line of defence to preserve protocol stability, it also deliberately aligns incentives as token holders face dilution if risks are not effectively managed, incentivising careful risk oversight.

Token Buy Backs

When the reserve fund surpasses its predefined safety threshold, excess funds can be redirected towards buying Fizk Tokens on the open market and burning them. This mechanism rewards successful governance and prudent risk management by gradually reducing token supply, increasing token value and aligning token holder incentives.

By clearly linking token value to effective governance and risk management outcomes, we ensure a balanced incentive structure that encourages optimal decision-making and avoids excessively high-risk strategies (leading to dilution via token issuance) or overly conservative strategies (limiting revenue generation and protocol growth).

Token Distribution Principles

Decentralisation lies at the heart of the Fizk Protocol's mission. Achieving this vision requires thoughtful, strategic token distribution, rewarding genuine community contributions and active protocol engagement. Rather than incentivising short-term participation or airdrop-farming behaviours, the protocol seeks meaningful, long-term alignment between the protocol and its stakeholders. Potential avenues to reward valuable community engagement include:

Liquidity Mining

Early liquidity incentives can effectively bootstrap the protocol by quickly attracting initial TVL. Although liquidity mining alone is unsustainable as a long-term growth strategy, the early network effects gained through incentivised liquidity can significantly accelerate ecosystem development.

Developer and Community Contributions:

Token distribution will explicitly reward early and meaningful contributions such as technical development, early testing, ecosystem-building, and proactive protocol governance involvement. These targeted incentives aim to attract and retain committed community members who add tangible and lasting value to the protocol.

Voting and Governance

Governance participation is resource-intensive, requiring careful deliberation and nuanced understanding of complex issues. We recognise this challenge and therefore plan meaningful incentives specifically designed to attract thoughtful, committed governance participation with the goal to prioritise quality decision-making over superficial engagement metrics.

A preliminary token distribution model might be structured as follows:

- **20%** — Team (subject to a 1-year lock-up followed by vesting)

- **20%** — Strategic Partners (subject to a 1-year lock-up followed by vesting)
- **10%** — Protocol Treasury (funding ongoing operations, development, and research)
- **50%** — Community Incentives (liquidity rewards, developer grants, governance participation)

This structure aligns long-term incentives and clear stakeholder accountability, with involved parties committing to extended lock-up periods and gradual vesting, reinforcing their dedication to sustained growth and development.

Last, any token generation event must be carefully assessed to comply fully with applicable regulatory environments. Legal compliance is essential for the legitimacy of the Fizk Protocol, so that it can thrive within a transparent and secure regulatory framework.

Financial Risk Modelling

The success of any algorithmic stablecoin depends on its ability to effectively identify, analyse, and mitigate numerous potential risks. Key categories of risk the Fizk Protocol must manage include:

- **Market Risks**
    - Collateral volatility
    - Insufficient liquidity
    - Deleveraging risks
- **Technical and Smart Contract Risks**
    - Bugs, exploits, or vulnerabilities
- **Economic Model Risks**
    - Poorly designed incentives
    - Extreme economic scenarios
- **Reputational Risks**
    - Public confidence
    - Risk of bank runs and contagion effects
- **Regulatory Risks**
    - Changing regulatory landscapes

While this list is not exhaustive, these risks represent the most significant threats the protocol needs to actively manage. For an algorithmic stablecoin like zkUSD, maintaining economic stability is especially crucial. If at any point the total value locked in the protocol falls below the total outstanding debt, zkUSD risks losing its peg. Such an event would severely undermine user confidence, introducing significant deleveraging risks and ultimately causing systemic insolvency.[13]

Due to Mina's relatively slow throughput it's essential that we understand precisely how this impacts protocol stability during volatile market conditions. In periods of severe market volatility, large numbers of vaults can simultaneously become undercollateralised, requiring rapid liquidation to maintain the protocol's core economic invariant: ensuring total collateral value always exceeds total outstanding debt. Given Mina's limited transaction processing capacity, there's a risk that the protocol may not liquidate positions quickly enough, potentially leading to insolvency.

To proactively address this challenge, we have developed a comprehensive financial risk model. This model enables us to simulate various extreme market scenarios, evaluate how the protocol responds under stress, and determine the effectiveness of liquidation and risk management mechanisms. By understanding these dynamics clearly, we can confidently refine the Fizk Protocol's design parameters—such as vault limits, collateral ratios, and the size of the reserve fund—ensuring zkUSD remains stable and reliable even under adverse market conditions.

Key Assumptions and Scenario Parameters

Block Time and Transaction Throughput

The model assumes:

- A block time of approximately **3 minutes**.
- A realistic protocol throughput of around 18 zkApp transactions per block.

This assumption takes into account Mina’s targeted block time and current practical throughput constraints. While Mina currently supports approximately 24 zkApp transactions per block, the conservative figure of 18 transactions considers competition for block space, transaction prioritisation, and the fees users may be willing to pay to ensure inclusion.

Protocol Risk Parameters

The model assumes a set of protocol-specific risk parameters that are adjustable and fundamentally impact the risk profile of the system. These are key levels in the protocols governance toolbox that can be altered to manage system risk.

The model assumes:

- A collateralisation ratio of 150%
- A target reserve fund of 10% of outstanding debt

Vault Count

The model tests multiple adoption scenarios to get an understanding of how the protocol withstands various levels of network participation

- **Low-scale scenario:** Assumes 5,000 vaults. Although 5,000 vaults represent a relatively high initial scale for Mina, this scenario demonstrates the protocol's baseline resilience even at substantial early adoption.
- **Medium-scale scenario:** Assumes 20,00 vaults, capturing moderate adoption.
- **High-scale scenario:** Assumes 50,000 vaults, reflecting significant protocol adoption and robust DeFi activity.

Risk Profile (Vault Health Factors)

The model categorises users into three risk profiles, each reflecting different risk tolerances, using health factors follows:

- **Low-risk scenario:** Mean health factor of 220
- **Medium-risk scenario:** Mean health factor of 180
- **High-risk scenario:** Mean health factor of 150

At the outset of each simulation, vault health factors are distributed normally, emulating realistic market behaviour. Comparable data on similar protocols, mainly debt positions on Dai typically range from 2.5 - 5x which would place us firmly in the low-risk scenario range.[11]

Market Conditions

To rigorously stress-test protocol resilience, simulations incorporate worst-case historical benchmarks of price drops with accompanying more severe "black swan" events. The model maps out protocol resilience against one, three, five and seven day price drops:

Historical Mina benchmarks:

- Worst 1-day drop: 30% (September 2021)
- Worst 3-day drop: 40% (September 2021)
- Worst 5-day drop: 45% (September 2021)
- Worst 7-day drop: 50% (September 2021)

Extreme ("Black Swan") scenarios:

- 50% price drop in 1 day
- 60% price drop in 3 days
- 70% price drop in 5 days
- 80% price drop in 7 days

Scenarios

The model's testing runs simulations against each combination, covering all 72 distinct scenarios. Each simulation begins by segmenting the scenario's total duration into discrete steps matching Mina’s 3-minute block intervals. The simulated price decline is evenly distributed across these steps, and vault collateralisation levels are continuously recalculated over time. As the price declines, vaults that drop below the liquidation threshold become eligible for liquidation. The protocol then processes these liquidations at the expected throughput of 18 transactions per block.

In the event that liquidations outpace the network’s transaction throughput, some vaults may become insolvent, the model borrows five transactions from the 18 exclusively to address these. The Reserve Fund is activated at this stage, automatically purchasing the bad debt, liquidating collateral at current market prices, and recycling the recovered zkUSD back into the Reserve Fund.

Once the price shock concludes, the simulation enters a recovery phase and continues processing queued liquidations and insolvencies until all outstanding debt has been cleared and the protocol returns to a fully stable state.

While this financial risk model provides valuable insight into how the protocol might perform during periods of severe market volatility, it is important to acknowledge its limitations. The model offers a simplified view and does not capture every aspect of real-world dynamics. For example, it does not account for ongoing user actions during a crisis, such as continued re-collateralisation of vaults, active management strategies, or new zkUSD minting activity that could influence outcomes positively or negatively. Therefore, while the model provides critical insights into protocol resilience and risk exposure, it should serve as a guide rather than an exhaustive prediction of real-world protocol performance.

Analysis

To provide a birdseye view of each simulation and visualise how the Fizk protocol performs under each scenario the model creates Protocol Health and Liquidation heatmaps, grouped by the scale scenario modelled. For each simulation we capture two snapshots.

- **End of price drop phase:** Immediately following the simulated market volatility, this snapshot shows the protocol’s health, highlighting the protocol’s state.
- **End of Recovery Phase Snapshot:** Taken after the protocol fully processes any outstanding liquidation queues and recovers from the shock, this snapshot illustrates the final protocol health, confirming the effectiveness of liquidation mechanisms and the Reserve Fund's performance in restoring stability.

Low scale - 5,000 vaults

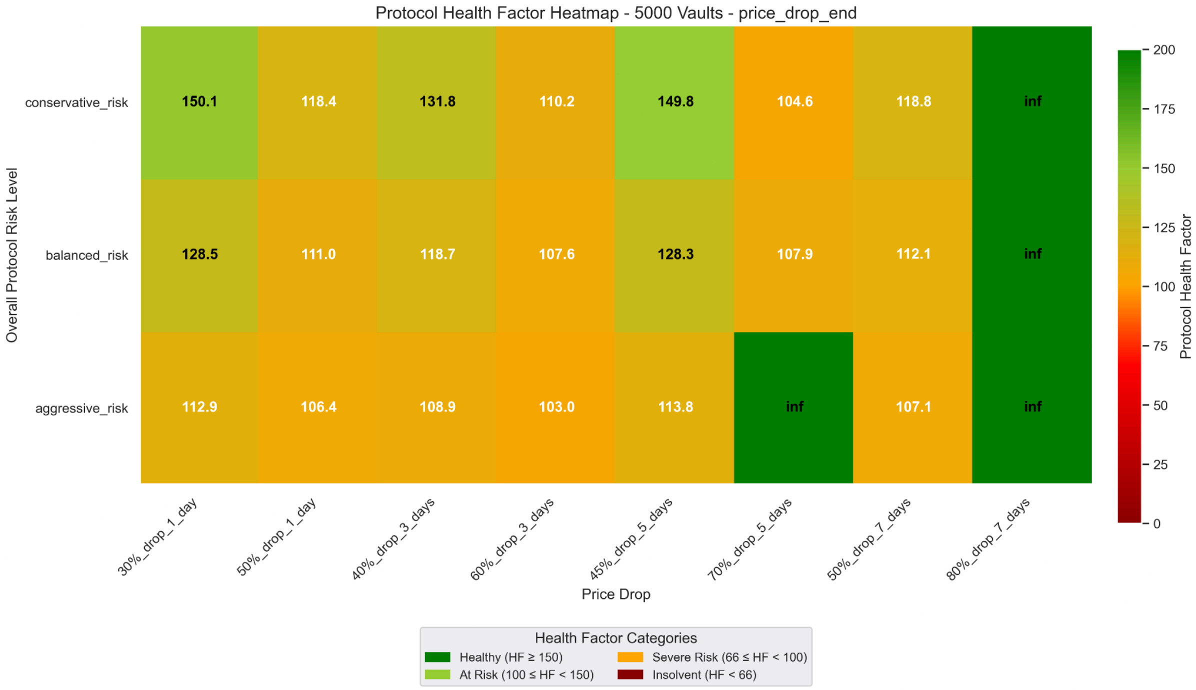

Figure 1.1: Heatmap of protocol health factors for the low scale scenarios and the end of the simulated price drop

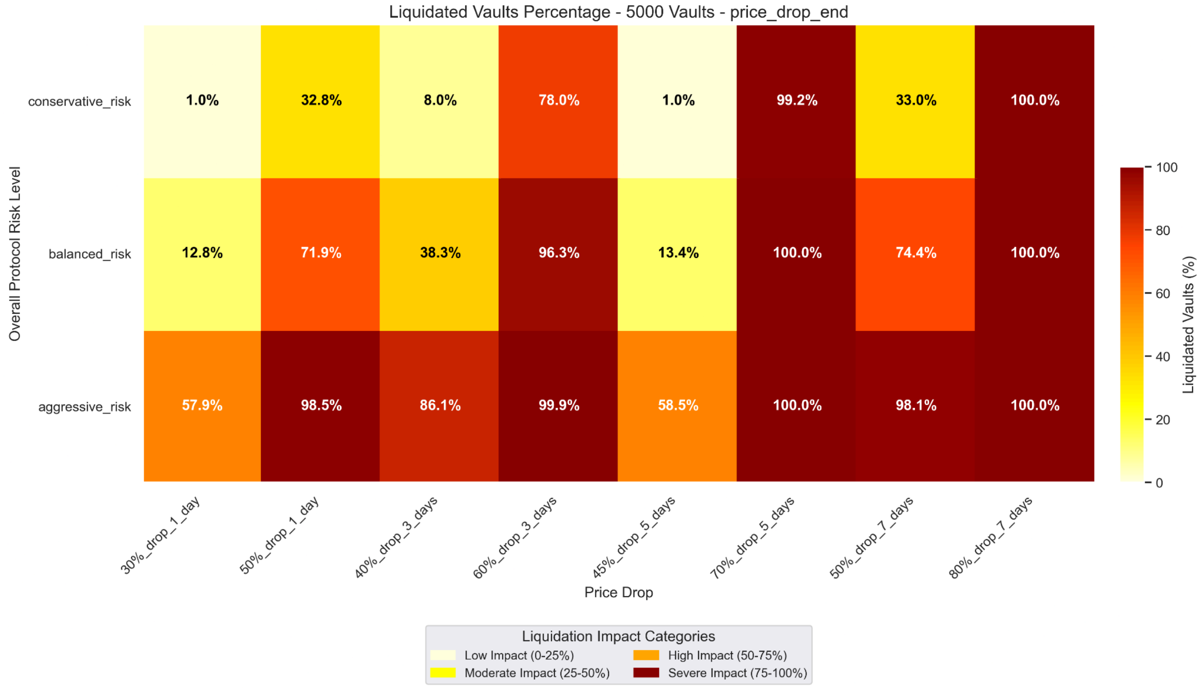

Figure 1.2: Heatmap of percentage of vaults liquidated for the low scale scenarios at the end of the simulated price drop

At the relatively modest scale of 5,000 vaults, the Fizk Protocol demonstrates strong resilience across nearly all simulated scenarios without requiring a recovery phase. Even in aggressive scenarios with severe market volatility, the protocol maintains solvency without significant risk to its core invariant. For example, in the most extreme short-term scenario—a 50% price drop within a single day—the protocol successfully manages liquidations despite approximately 98.5% of vaults requiring liquidation.

Medium scale - 20,000 vaults

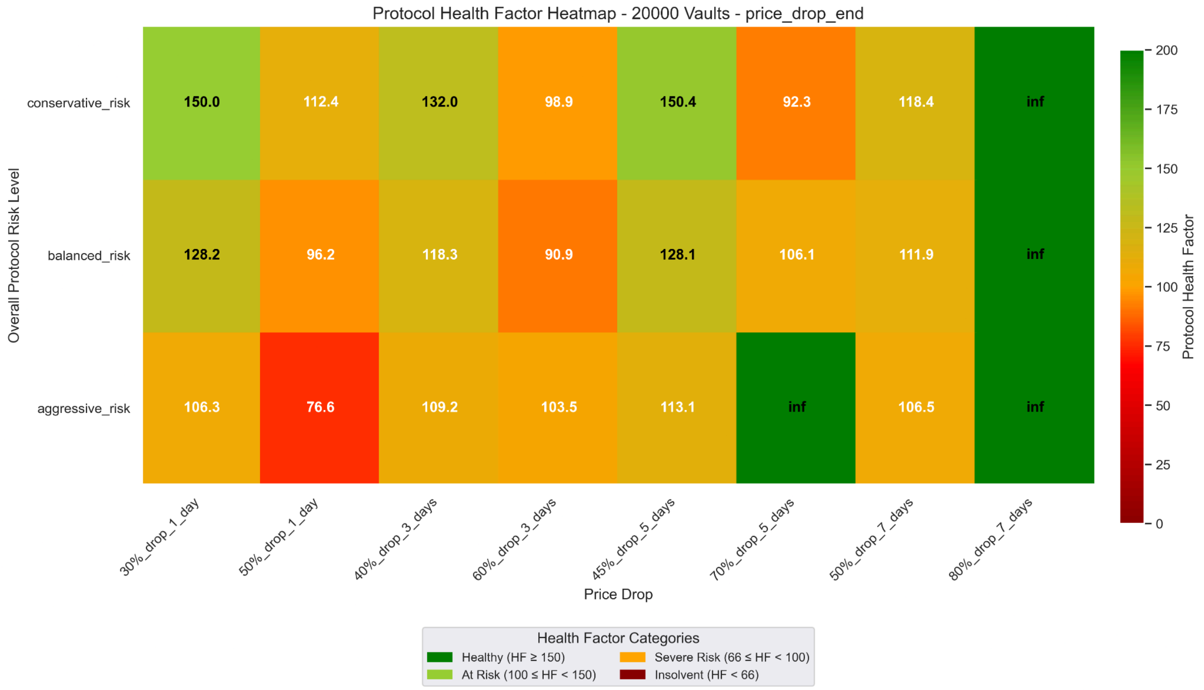

Figure 2.1: Heatmap of protocol health factors for the medium scale scenarios and the end of the simulated price drop

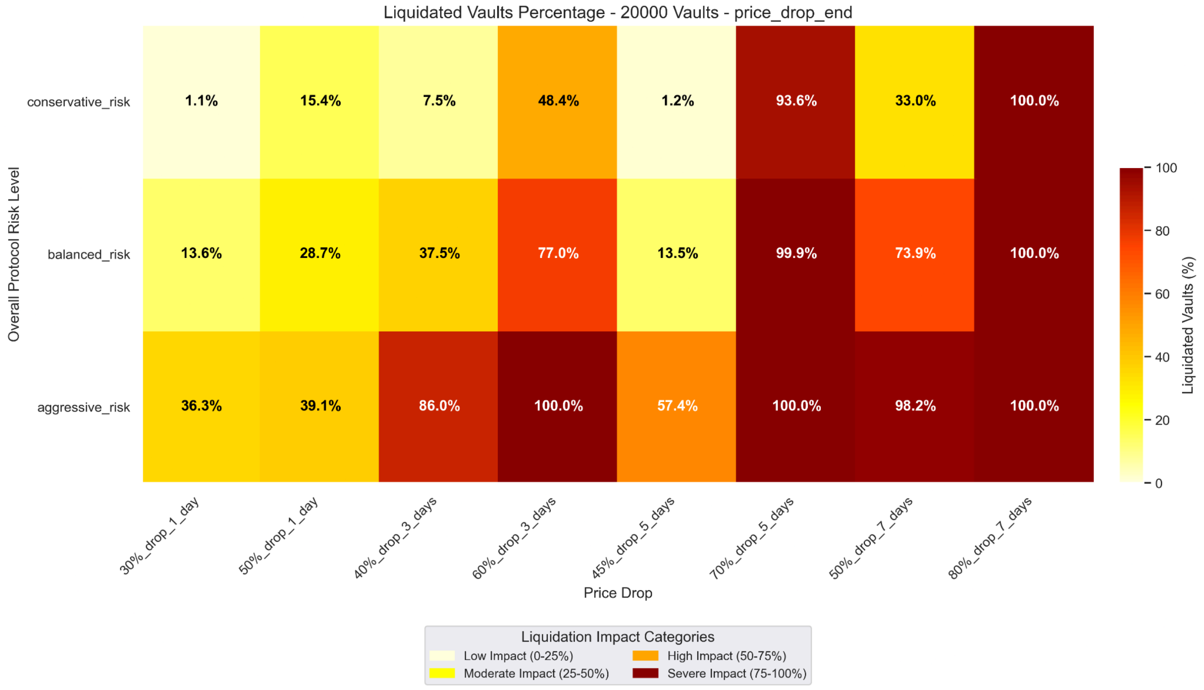

Figure 2.2: Heatmap of percentage of vaults liquidated for the medium scale scenarios at the end of the simulated price drop

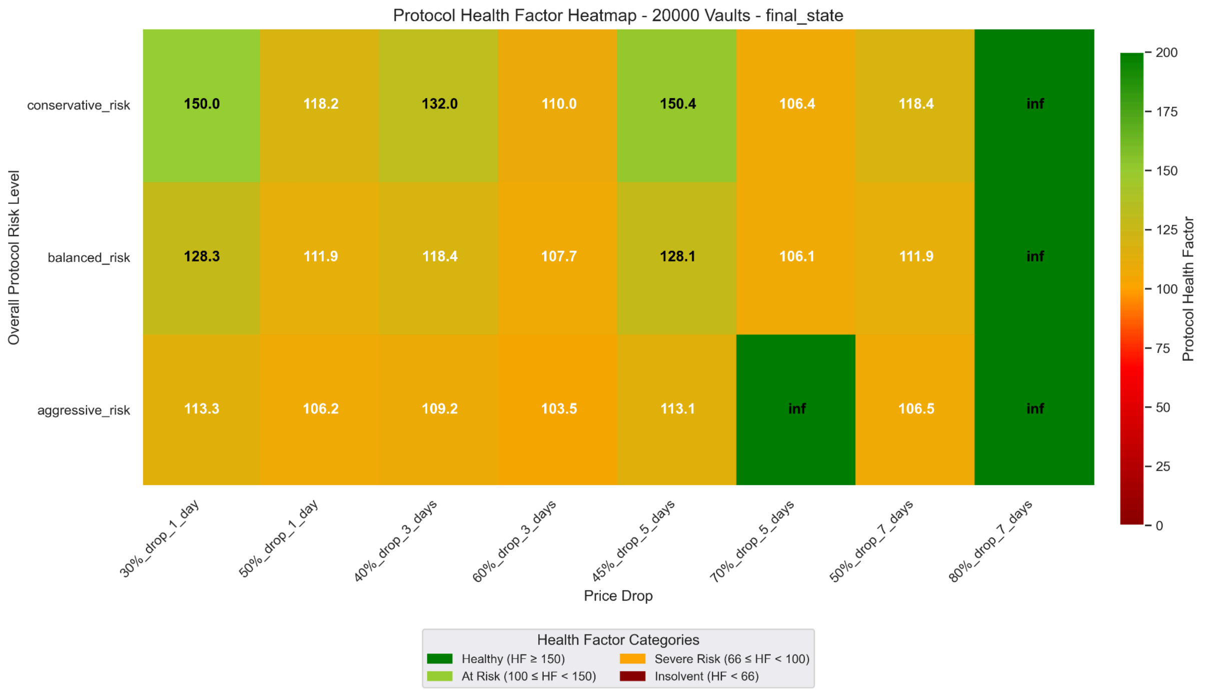

Figure: 2.3: Heatmap of protocol health factors for the medium scale scenarios at the end of the simulations recovery period

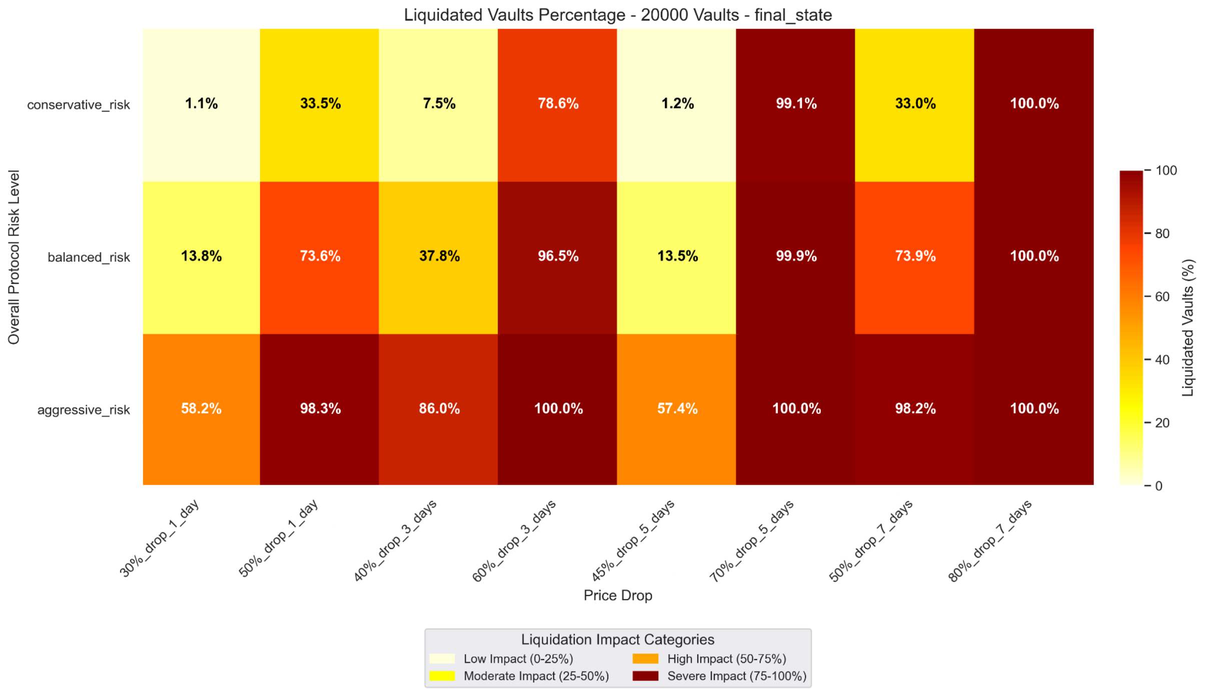

Figure 2.4: Heatmap of percentage of vaults liquidated for the medium scale scenarios at the end of the simulated recovery period

At a medium scale of 20,000 vaults, the Fizk Protocol continues to demonstrate resilience, but starts to show vulnerability under the most extreme conditions. The critical scenario—a 50% price drop in a single day with an aggressive risk profile—results in significant stress, reducing the protocol's health factor to approximately 76.6, indicating severe insolvency risk. At this point, vaults became insolvent, triggering engagement of the Reserve Fund.

After the recovery period, the protocol manages to stabilise effectively, restoring the health factor to an acceptable level of around 106 by successfully processing liquidations and insolvencies for approximately 98.3% of all vaults.

Despite this scenario's severity, the protocol's ability to recover demonstrates the effectiveness of its liquidation and reserve mechanisms. It also highlights the importance of carefully managing the protocol's risk parameters to ensure stability as the protocol scales further.

High Scale - 50,000 vaults

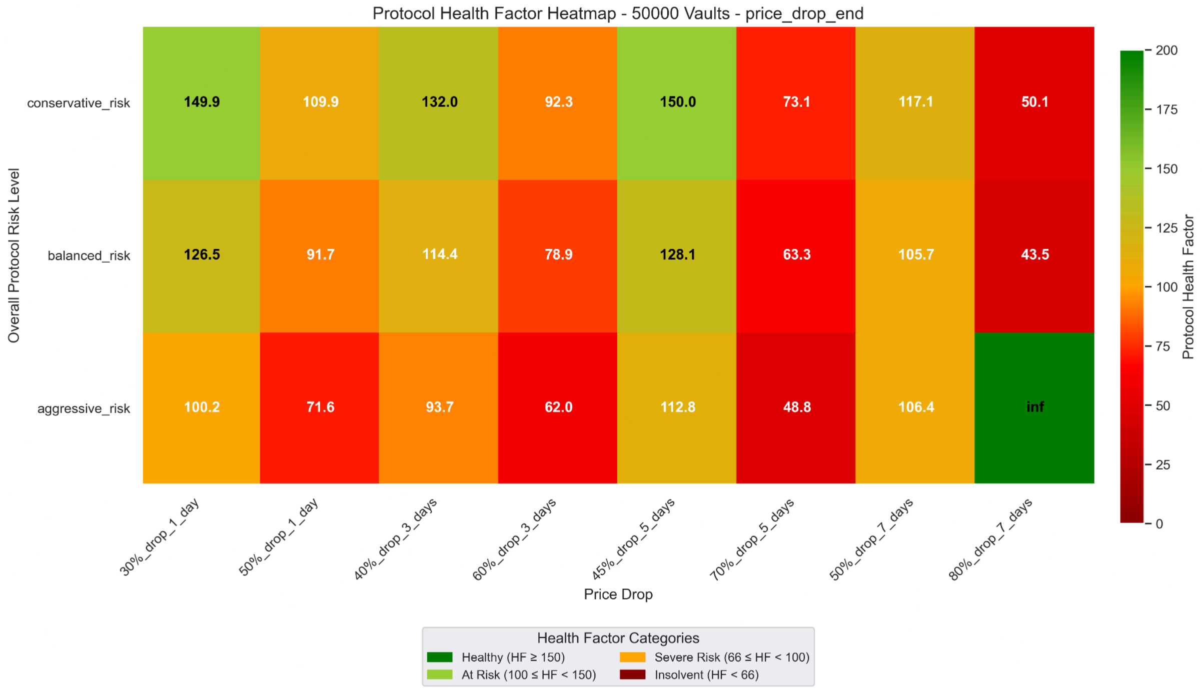

Figure 3.1: Heatmap of protocol health factors for the high scale scenarios and the end of the simulated price drop

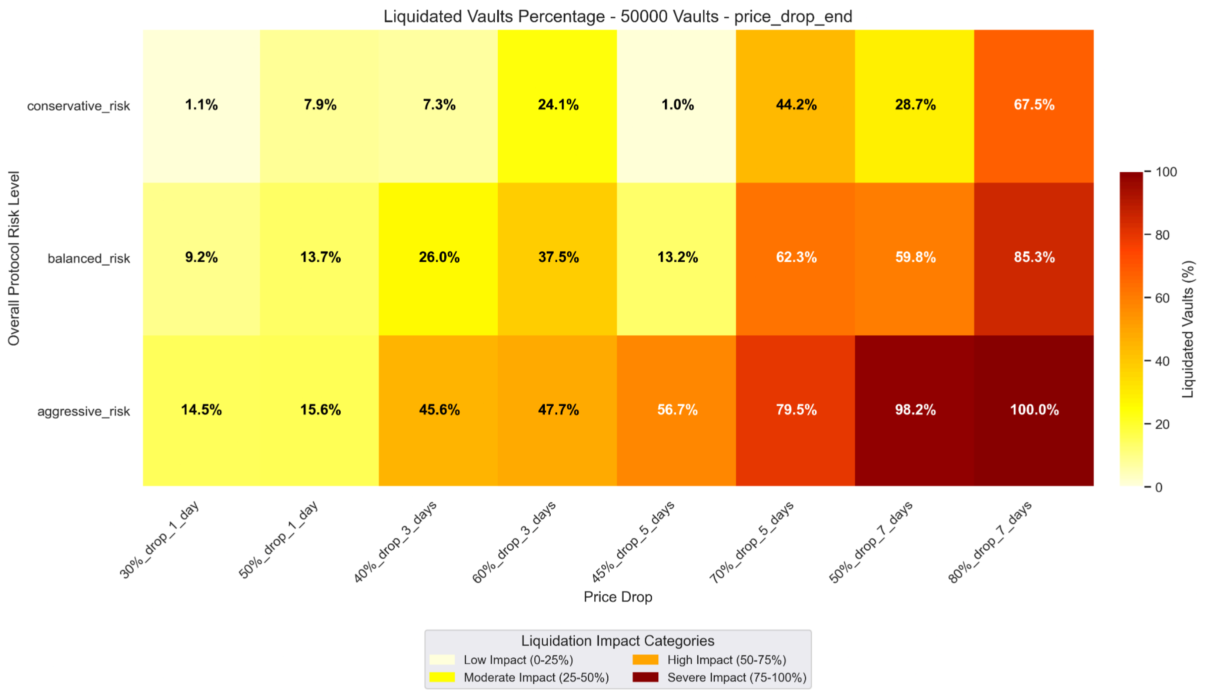

Figure 3.2: Heatmap of percentage of vaults liquidated for the high scale scenarios at the end of the simulated price drop

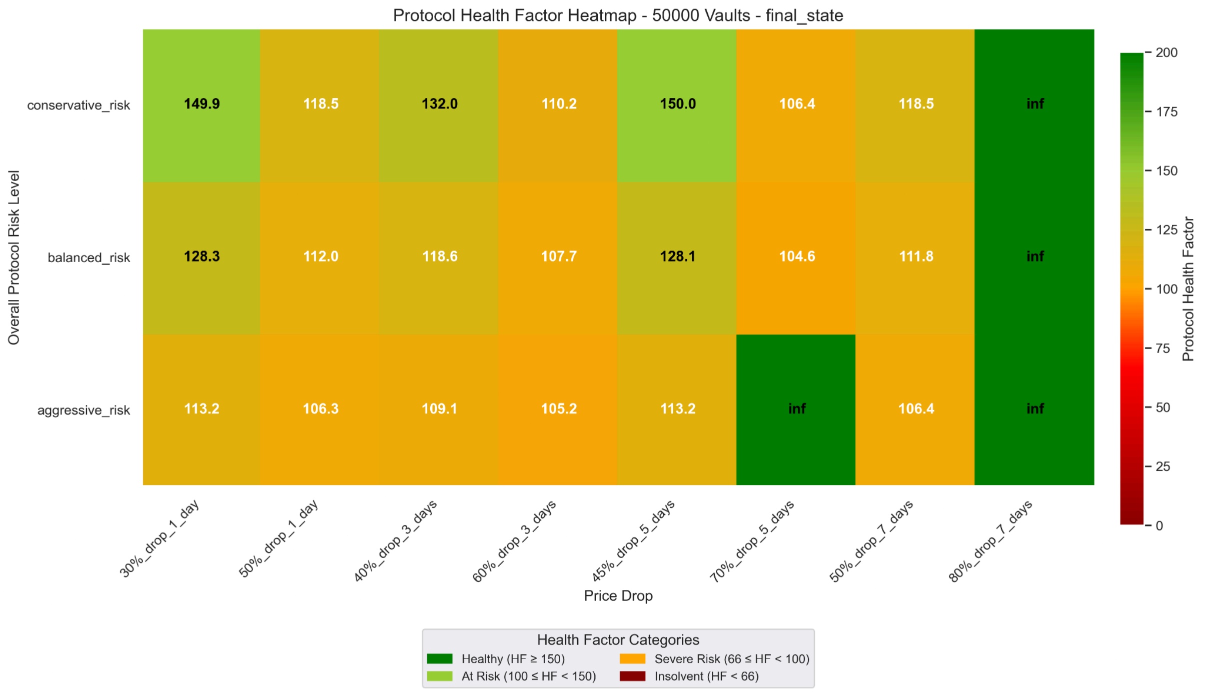

Figure 3.3: Heatmap of protocol health factors for the high scale scenarios and the end of the simulated recovery period

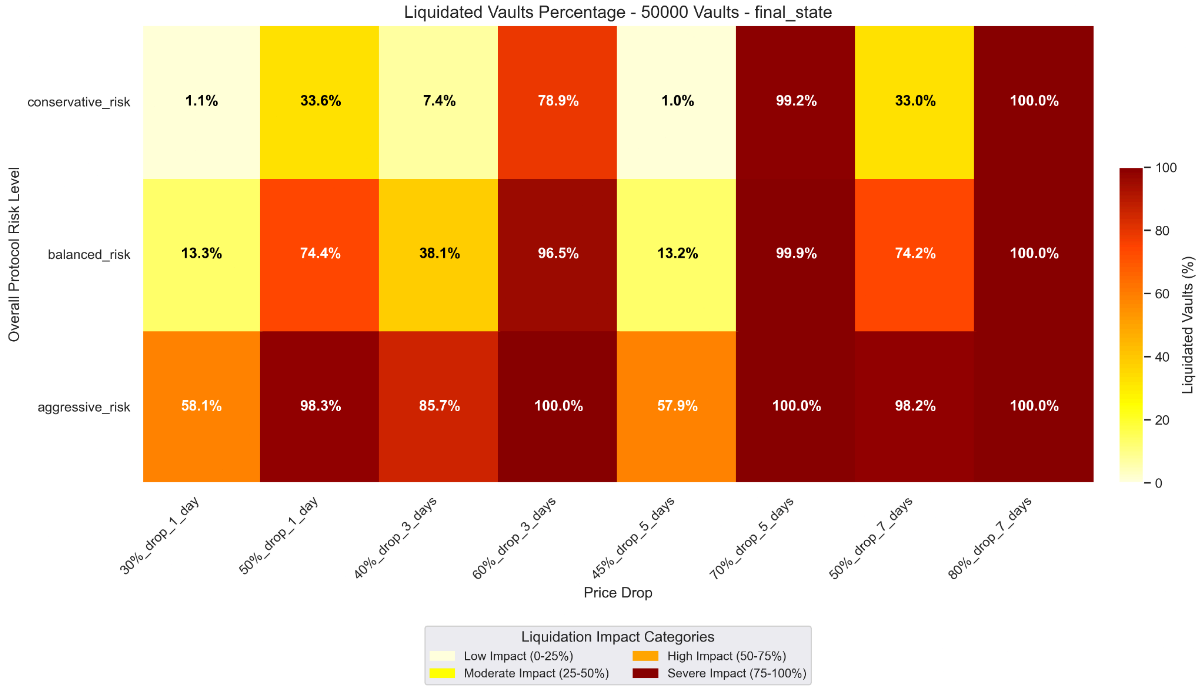

Figure 3.4: Heatmap of percentage of vaults liquidated for the high scale scenarios at the end of the simulated recovery period

At the highest scale tested—50,000 vaults—the Fizk Protocol shows significant strain under extreme market conditions. During severe price shocks, particularly the "black swan" scenarios, the protocol struggles to maintain solvency. For instance, examining the 70% price drop scenario over 5 days with an aggressive risk profile, the protocol health factor drops critically to 48.8, indicating substantial insolvency. At this stage, the reserve fund is actively engaged to restore the protocol to solvency.

At the precise moment the price drop concludes, approximately 80.9% of vaults have already been liquidated, with 19.1% (9,548 vaults) remaining insolvent. At this point, the collateralisation ratio has dropped significantly to approximately 74%. Despite the severity of this scenario, the Fizk Protocol successfully activates its reserve fund to systematically clear the outstanding bad debt.

If you are wondering why shows an inf protocol health factor at the end of the 80% drop in 7 days price drop phase it is because in the aggressive risk profile, enough vaults were sufficiently undercollateralized at the early stages of the price drop allowing the liquidations enough time to process over the duration of the price drop.

Ultimately, despite experiencing severe stress and a significant liquidation event, the protocol demonstrates its ability to fully recover even at this high scale. To ensure long-term protocol stability, governance must prioritise a balanced approach to risk management, adjusting parameters proactively to minimise the risk of insolvency under realistic market conditions.

Case Study

Balanced Risk Profile / Medium Scale (20,000 Vaults) / Historical Worst 1-Day Drop (30%)

To better illustrate how the Fizk Protocol responds under realistic market conditions, we examine a representative scenario in greater detail—a medium-scale scenario involving 20,000 vaults with a balanced risk profile undergoing Mina's worst historical one-day price drop of 30%.

Initial Vault Health Factor Distribution

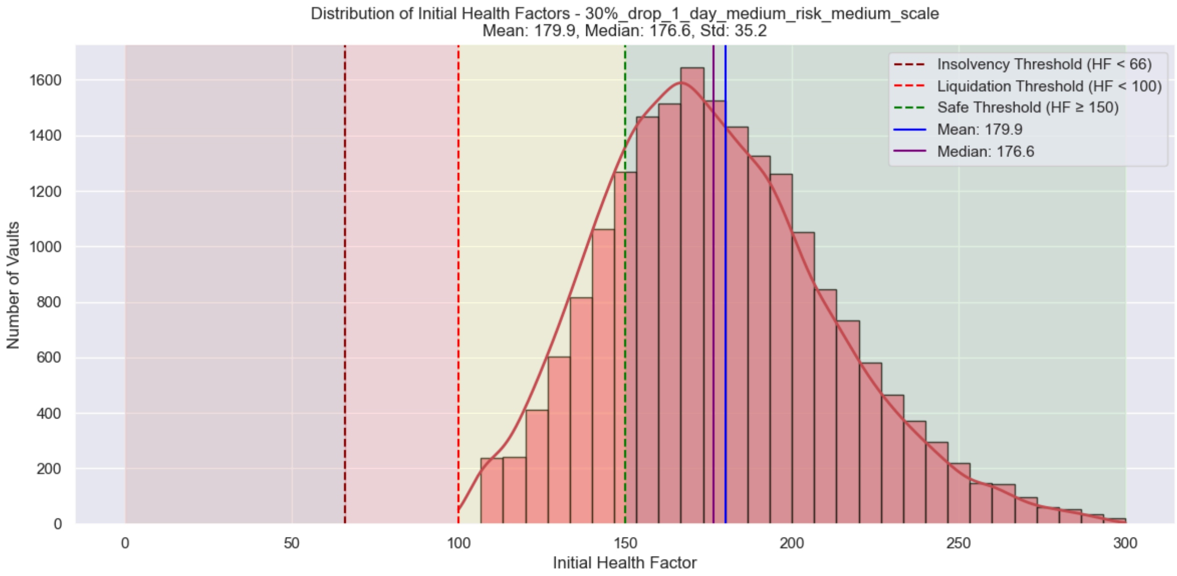

Figure 4.1: Vault Health Factor distribution for the simulation

The initial vault health factors follow a normal distribution, reflecting realistic user behaviour commonly observed in established DeFi protocols. With an average health factor of approximately 180 and a standard deviation of 35, most vaults begin comfortably above the liquidation threshold. The distribution indicates that the majority of vaults are initially safe, though there is a tail-end of vaults closer to or just above the liquidation threshold, representing higher-risk positions.

This distribution provides a realistic starting point, setting the stage for observing how effectively the protocol manages liquidations and maintains stability through a moderate yet impactful market downturn.

Simulation

At the beginning of this simulation scenario, the protocol starts in a strong and stable position, with a protocol-wide collateralisation ratio of approximately 260%, a health factor of 173, and a fully funded reserve fund of roughly $20.7 million. About 80% of the vaults are initially healthy, with the remaining 20% considered "at risk."

```
INITIAL STATE:
--------------------------------------------
Total Collateral: 539,790,255
MINA Current Price: $1.000
Protocol Health Factor: 173
Status: HEALTHY - Protocol stable
Total Collateral Value: $539,790,255.00
Total Debt: $207,461,737.05
Collateralization Ratio: 260.19%
Total Insolvent Collateral: 0 MINA
Total Insolvent Collateral Value: $0.00
Total Debt in Insolvent Vaults: $0.00
Initial Reserve Fund: $20,746,173.71
Reserve Fund: $20,746,173.71 (100.00%)
Reserve Fund Used: $0.00

Vault Distribution:
Healthy Vaults: 15976 (79.9%)
At Risk Vaults: 4024 (20.1%)
Liquidatable Vaults: 0 (0.0%)
Insolvent Vaults: 0 (0.0%)
Liquidated Vaults: 0 (0.0%)
Liquidation Queue Size: 0
---------------------------------------------
```

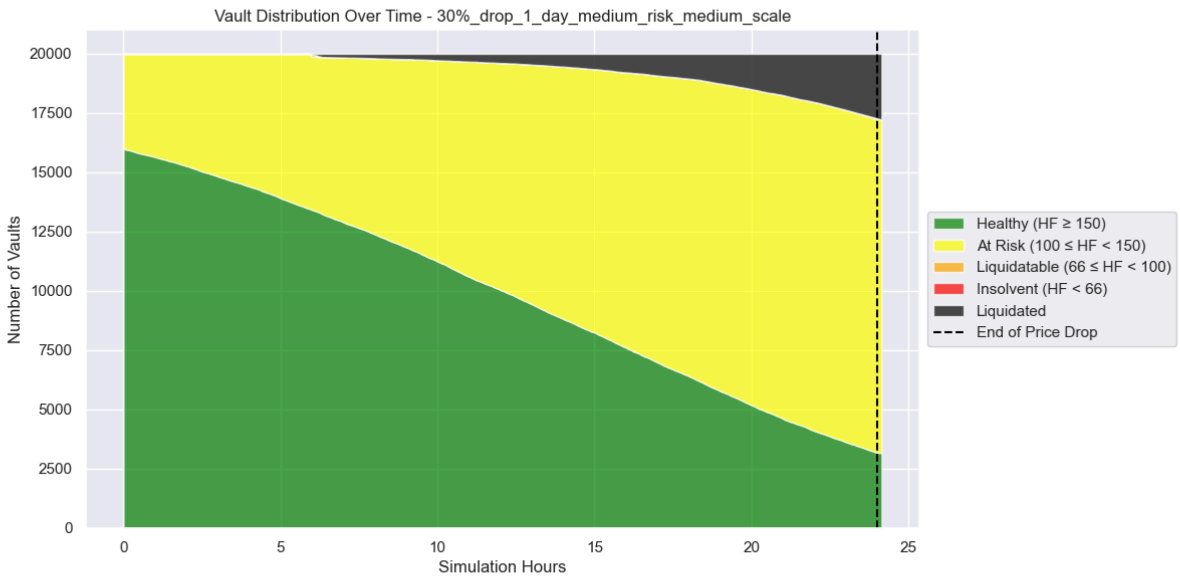

Figure 4.2: Vault Health Factor distribution over time

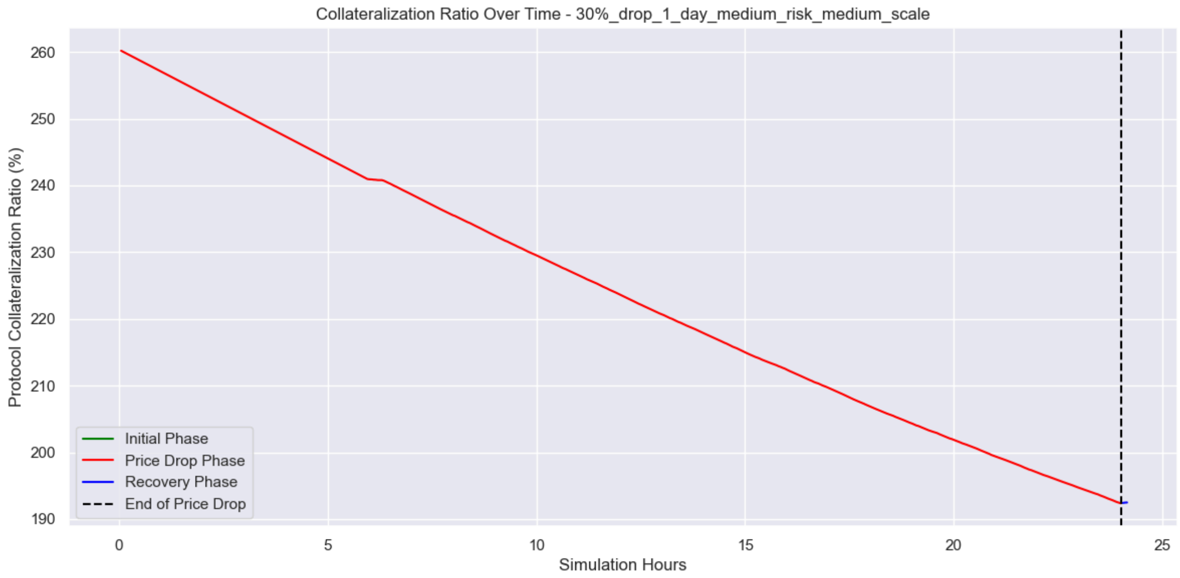

Figure 4.3: Protocol collateralisation ratio over time

The progression of the simulation shows how vault and protocol health evolves over the simulated 24-hour period of the 30% price drop. Initially, most vaults are healthy or at risk, but as the price declines, the share of healthy vaults gradually diminishes. Vaults begin transitioning into liquidatable states, with liquidation throughput easily able to handle the load.

By the end of the price drop, the protocol successfully manages liquidations, as seen by the increasing proportion of liquidated vaults.

Protocol stats and the end of the simulation:

```
FINAL STATE (Step 483):
----------------------------------------
PROTOCOL STATUS REPORT
----------------------------------------
Total Collateral: 466,447,128
MINA Current Price: $0.700
Protocol Health Factor: 128
Status: WARNING - Protocol at risk
Total Collateral Value: $326,512,989.60
Total Debt: $169,627,546.77
Collateralization Ratio: 192.49%
Total Insolvent Collateral: 0 MINA
Total Insolvent Collateral Value: $0.00
Total Debt in Insolvent Vaults: $0.00
Initial Reserve Fund: $20,746,173.71
Reserve Fund: $20,746,173.71 (100.00%)
Reserve Fund Used: $0.00
Vault Distribution:
Healthy Vaults: 3169 (15.8%)
 At Risk Vaults: 14069 (70.3%)
 Liquidatable Vaults: 0 (0.0%)
 Insolvent Vaults: 0 (0.0%)
 Liquidated Vaults: 2762 (13.8%)
 Liquidation Queue Size: 0
----------------------------------------
```

Risk Mitigation

Effectively managing risk is critical for ensuring zkUSD’s long-term stability, particularly given Mina’s current network throughput constraints. Protocol governance has several levers it can pull to actively balance risk and maintain solvency. Primarily, governance can adjust the collateralisation ratio, reducing the overall risk exposure of vault positions and mitigating the potential impact of volatile market conditions. Additionally, governance may temporarily pause the creation of new vaults if network limitations begin to affect the protocol's ability to efficiently manage liquidations.

While Mina currently faces throughput constraints, immediate improvements planned by O1js will enhance performance through reduced block times and increased zkApp transaction allowance, directly improving overall protocol resilience.

By aligning incentives of governance with the stability and sustainability of the protocol, we can ensure that risk is effectively and actively managed in the system.

Market Potential & Protocol Vision

Immediate Outlook

Mina's emerging DeFi landscape is approaching an important inflection point. Key infrastructure developments are nearing completion, positioning the ecosystem for rapid growth. Notably, the upcoming release of Protokit Starter Kit v2, a framework that enables the creation of specialised app-chains using sequencers settled on Mina's L1, is expected to significantly accelerate DeFi adoption. This infrastructure enhancement will immediately unlock applications such as DinoDex, a decentralised exchange awaiting Protokit's mainnet settlement capabilities to go live.

In parallel, the upcoming deployment of the Zeko zk-rollup L2 further strengthens Mina's scalability. With Lumina DEX, Zeko's first partner protocol, nearing the end of its audits and approaching mainnet deployment, these rollups promise substantially higher transaction throughput and shorter block times, providing a fertile ground for new DeFi activity.

Together, these developments will create significant organic demand for zkUSD. Users will seek stable liquidity pairs on decentralised exchanges to benefit from trading fee revenues, driving substantial early demand for zkUSD within the Mina ecosystem.

Future Vision

The growth trajectory of any algorithmic stablecoin is fundamentally constrained by the value and diversity of its collateral base. Initially, zkUSD will utilise MINA exclusively as collateral. However, as the Fizk Protocol matures, diversifying the collateral pool will become a critical strategic initiative. Expanding into multi-collateral support, including tokens bridged from other ecosystems, will unlock broader liquidity sources and extend zkUSD's economic utility across Web3.

Beyond crypto-native assets, Fizk Protocol envisions integrating Real World Assets (RWAs) as collateral through innovative custodial frameworks secured by zk proofs. Incorporating RWAs, such as tokenised securities or commodities, significantly expands the stablecoin's utility, connecting traditional finance with the Mina blockchain. This bridge between off-chain and on-chain assets will provide users with diversified exposure, reduce systemic risk, and strengthen zkUSD’s position as a versatile financial asset.

By positioning Fizk Protocol at the intersection of decentralised finance, scalable zk infrastructure, and traditional asset markets, zkUSD will become a foundational component of Mina's broader economic ecosystem—driving long-term adoption and creating sustainable value for both investors and users alike.

Legal Considerations

[SECTION UNDER DEVELOPMENT]

Conclusion

The Fizk Protocol represents a significant leap forward for the Mina ecosystem, addressing various application design limitations and unlocking Mina's potential in DeFi. By introducing zkUSD the protocol lays essential foundations for the start of a thriving DeFi activity. zkUSD not only amplifies the utility of the MINA token but also firmly positions Mina as an independent and attractive blockchain ecosystem capable of hosting sophisticated financial applications.

Comprehensive risk modelling demonstrates that, even in severe market scenarios, Fizk's architecture and governance mechanisms effectively protect protocol stability, particularly at realistic scales of early to mid-stage adoption. However, the simulations also highlight important growth considerations, emphasising the critical role of active governance and prudent risk management as the protocol expands.

Looking ahead, immediate ecosystem developments—such as the imminent deployment of Protokit App-chains and Zeko zk-rollups—promise significant early-stage demand and increased scalability, driving widespread adoption of zkUSD within the ecosystem. Furthermore, the potential to diversify collateral by bridging additional crypto-native assets and integrating RWAs presents substantial long-term growth opportunities, connecting Mina's innovative zk technology directly to broader financial markets.

Ultimately, the Fizk Protocol sets Mina on an exciting path: transforming a largely passive staking network into an active, interconnected DeFi landscape. By balancing ambitious innovation with rigorous risk management, Fizk and zkUSD can sustainably support Mina's growth into a mature, resilient, and economically vibrant blockchain ecosystem.

References

[1] Vitor Silva, "Mina Protocol's Upcoming Major Upgrade: Everything You Need to Know", Mina Blog, 2024. Available: https://minaprotocol.com/blog/mina-protocols-upcoming-major-upgrade-everything-you-need-to-know

[2] "Decentralized, Scalable and Secure Blockchain", Mina Protocol, 2025. Available: https://minaprotocol.com/about

[3] "Lifecycle of a Payment", Mina Documentation, 2025. Available: https://docs.minaprotocol.com/mina-protocol/lifecycle-of-a-payment

[4] zkUSD-Protocol, "Oracle Price Aggregation", GitHub Repository, accessed March 2025, https://github.com/zkUSD-Protocol/core/blob/develop/src/proofs/oracle-price-aggregation/prove.ts

[5] "How zkApps Work", Mina Documentation, 2025. Available: https://docs.minaprotocol.com/zkapps/writing-a-zkapp/introduction-to-zkapps/how-zkapps-work

[6] Project Untitled, "Whitepaper", GitHub Repository, accessed March 2025, https://github.com/o1-labs/project-untitled-whitepaper/blob/main/whitepaper.pdf

[7] o1js, "Transaction Validation", GitHub Repository, accessed March 2025, https://github.com/o1-labs/o1js/blob/6ebbc23710f6de023fea6d83dc93c5a914c571f2/src/lib/mina/transaction-validation.ts#L-87

[8] D. Matsuoka, R. Hackett and E. Lazzarin, "State of Crypto Report 2024", a16zcrypto, 2024. Available: https://a16zcrypto.com/posts/article/state-of-crypto-report-2024/

[9] Mina Foundation, "What is Ouroboros Samasika?", Mina Blog, 2021. Available: https://minaprotocol.com/blog/what-is-ouroboros-samasika

[10] Mina Foundation, "Mina Token Distribution and Supply", Mina Blog, 2023. Available: https://minaprotocol.com/blog/mina-token-distribution-and-supply

[11] Mina MINA Staking, Coinbase, 2025. Available: https://www.coinbase.com/en-nl/earn/staking/mina

[12] Mina Delegations Explained, Staketab Docs, 2023. Available: https://docs.staketab.com/academy/mina/mina-delegations-explained

[13] A. Klages-Mundt and A. Minca, “While stability lasts: A stochastic model of non-custodial stablecoins,” *arXiv preprint arXiv:2004.01304*, 2020. [Online]. Available: https://arxiv.org/abs/2004.01304